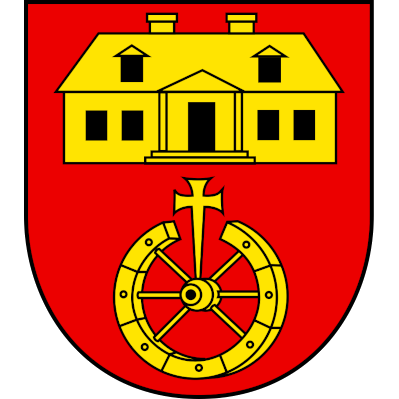
**Szczegółowy**

**Opis przedmiotu zamówienia**



Nozdrzec, 24 kwiecień 2025 r.

**Spis treści**

[Wprowadzenie 4](#_Toc196418609)

[Metodyka projektu 4](#_Toc196418610)

[Etapy wdrożenia 5](#_Toc196418611)

[Termin realizacji 6](#_Toc196418612)

[Zestawienie zakresu dostaw i usług dla części I 6](#_Toc196418613)

[**I.** **CZĘŚĆ I – OPROGRAMOWANIE (Platforma e-usług)** 7](#_Toc196418614)

[Zakres dot. integracji 7](#_Toc196418615)

[Zakres usługi instalacji i konfiguracji 7](#_Toc196418616)

[Wymagania gwarancyjne 8](#_Toc196418617)

[1.1. eBOM - elektroniczne Biuro Obsługi Mieszkańca – szt.1 lic. 8](#_Toc196418618)

[1.2. Aplikacja mobilna – szt.1 lic. 11](#_Toc196418619)

[1.2.1. Wymagania funkcjonalne 12](#_Toc196418620)

[1.2.2. Wymagania techniczne i wdrożeniowe 14](#_Toc196418621)

[1.3. Oprogramowanie dziedzinowe – szt.1 lic. 14](#_Toc196418622)

[1.4. System GIS – szt.1 lic. 16](#_Toc196418623)

[1.4.1 Wymagania ogólne 17](#_Toc196418624)

[1.4.2 Wymagania dotyczące GEOPORTALU 18](#_Toc196418625)

[1.4.3 Wymagania dotyczące modułów dziedzinowych 35](#_Toc196418626)

[1.4.4 Wymagania dotyczące digitalizacji danych 41](#_Toc196418627)

[1.4.5 Wymagania dotyczące e-usług 45](#_Toc196418628)

[1.5 E-edukacja – szt.1 lic. 52](#_Toc196418629)

[1.5.1 Dziennik elektroniczny 53](#_Toc196418630)

[1.5.2 Moduł finansowo-księgowy 72](#_Toc196418631)

[1.6 Obieg dokumentów – szt.35 lic. 83](#_Toc196418632)

[1.7 ePSZOK – szt.1 lic. 85](#_Toc196418633)

[1.8 eRada – szt.1 lic. 88](#_Toc196418634)

[1.9 Monitoring środowiska – szt. 1 zestaw 93](#_Toc196418635)

[1.10 System eWoda – szt. 1 97](#_Toc196418636)

[1.11 Strona WWW – szt.1 99](#_Toc196418637)

[1.12 Szkolenia TiK typ II – 160 godzin 100](#_Toc196418638)

[**I.** **CZEŚĆ II – SPRZĘT i INFRASTRUKTURA** 102](#_Toc196418639)

[Wymagania ogólne dla urządzeń i oprogramowania infrastruktury 103](#_Toc196418640)

[Wymagania gwarancyjne 104](#_Toc196418641)

[2.1 Licencja na system Backupu – szt. 1 lic. 104](#_Toc196418642)

[2.2 Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa – szt.1 lic. 125](#_Toc196418643)

[2.3 Serwer – szt.1 147](#_Toc196418644)

[2.4 Firewall – klaster – szt.2 149](#_Toc196418645)

[2.5 Centralny system logów – szt.1 157](#_Toc196418646)

[2.6 Zestaw komputerowy z oprogramowaniem – szt.15 160](#_Toc196418647)

[2.7 Laptop – szt.20 177](#_Toc196418648)

[2.8 Centralny UPS – szt.1 193](#_Toc196418649)

[2.9 Agregat – szt.1 197](#_Toc196418650)

[2.10 System do transmisji obrad Rady Gminy – sprzęt – 1 kpl. 199](#_Toc196418651)

[2.11 Szkolenia TiK typ I – 120 godzin 201](#_Toc196418652)

[2.12 Opracowanie procedur bezpieczeństwa informacji i przetwarzania danych 202](#_Toc196418653)

[2.13 Instalacja i konfiguracja (Platforma sprzętowa) – 250 RBH 204](#_Toc196418654)

[2.14 Wodomierze – szt. 296 218](#_Toc196418655)

[5.6 Wodomierze – szt. 296 218](#_Toc196418656)

[5.12 Przepływomierz – szt. 2 220](#_Toc196418657)

[5.12.1 Model – 6 DN 65 220](#_Toc196418658)

[5.12.2 Model – 6 DN 100 220](#_Toc196418659)

# Wprowadzenie

Niniejszy dokument stanowi Szczegółowy Opis Przedmiotu Zamówienia (SOPZ) w zakresie dostawy i wdrożenia oprogramowania i sprzętu służącego realizacji projektu pn. „Platforma e-usług publicznych w Gminie Nozdrzec”. Wszystkie parametry techniczne określone w niniejszym SOPZ określają minimalne wymagania stawiane oferowanym urządzeniom i oprogramowaniu. Wykonawca nie ma prawa żądać dodatkowego wynagrodzenia, jeśli dostarczone elementy systemów posiadały będą większą funkcjonalność niż wymagana niniejszym SOPZ.

Projekt pn. „Platforma e-usług publicznych w Gminie Nozdrzec” realizowany jest przez Gminę Nozdrzec. Głównym miejscem realizacji Projektu jest:

* **Urząd Gminy Nozdrzec, Nozdrzec 224 36-245 Nozdrzec.**

Projekt realizowany przez Gminę Nozdrzec ma na celu jest rozwój społeczeństwa informacyjnego w Gminie Nozdrzec poprzez dostarczenie mieszkańcom i podmiotom gospodarczym nowoczesnych i bezpiecznych e-usług administracji lokalnej.

## Metodyka projektu

W celu efektywnej realizacji projektu wdrożeniowego rozwiązania, projekt powinien być realizowany zgodnie z zaproponowaną przez wykonawcę i zaakceptowaną przez Zamawiającego metodyką projektową zgodą ze standardami branżowymi dostępnymi powszechnie, tj. PRINCE 2, IPMA lub innymi równoważnymi standardami, w tym metodyki zwinne AGILE takie jak SCRUM.

Wykonawca jest zobowiązany wraz z zaproponowaną metodyką dostarczyć jej szczegółowy opis zawierający minimalnie strukturę zadań, podział obowiązków, ról   
w projekcie, harmonogram, opisy podstawowych procesów projektowych. W razie zaproponowania równoważnej metodyki opartej o równoważne standardy Wykonawca musi wykazać ich równoważność w zakresie wskazanym w powyższym zapisie.

## Dokumentacja techniczna wymagana dla obu części, tj. I i II

Całość pracy w niniejszym opisie przedmiotu zamówienia musi znaleźć się w dokumentacji technicznej i powykonawczej. Dokumentacja powykonawcza w zakresie czynności IT odnosi się do zestawu dokumentów i raportów, które są przygotowywane po zakończeniu wdrożenia systemu informatycznego, projektu IT lub innego rodzaju prac technicznych. Jest ona kluczowa dla zapewnienia przejrzystości, utrzymania i dalszego rozwoju systemu.

Zamawiający będzie wymagał następujących opisów:

**1. Opis systemu i architektury**

* Szczegółowy opis infrastruktury IT, w tym serwerów, sieci, urządzeń, baz danych, aplikacji i ich wzajemnych powiązań.
* Architektura systemu z przedstawieniem wszystkich komponentów, ich wersji oraz ról.

**2. Instrukcje instalacji i konfiguracji**

* Kroki związane z instalacją i konfiguracją oprogramowania oraz sprzętu.
* Wersje używanych narzędzi, frameworków oraz systemów operacyjnych.

**3. Instrukcje użytkownika i administracyjne**

* Instrukcje obsługi systemu dla użytkowników końcowych.
* Dokumentacja dla administratorów dotycząca utrzymania systemu, wykonywania kopii zapasowych, monitorowania wydajności oraz zarządzania użytkownikami.

**4. Raporty z testów**

* Wyniki testów akceptacyjnych, testów wydajnościowych i innych rodzajów testów przeprowadzanych w trakcie wdrożenia.
* Zgłoszone błędy i sposoby ich naprawienia.

**5. Zmiany wprowadzone podczas realizacji**

* Opis modyfikacji w stosunku do pierwotnego planu, w tym zmiany w zakresie funkcjonalności, konfiguracji lub architektury systemu.

**6. Plany awaryjne i odzyskiwanie po awarii**

* Procedury dotyczące radzenia sobie z krytycznymi awariami i przywracania systemu do działania.
* Sposób wykonywania i przechowywania kopii zapasowych oraz procedury odzyskiwania danych.

**7. Zasady bezpieczeństwa**

* Polityki bezpieczeństwa, w tym konfiguracja zapór sieciowych, zabezpieczenia dostępu, monitorowanie logów oraz zarządzanie hasłami.

**8. Lista komponentów i licencje**

* Szczegółowy spis wszystkich komponentów sprzętowych i programowych użytych w projekcie, wraz z informacjami o licencjach i ich okresie ważności.

**9. Kontakt do wsparcia technicznego**

* Informacje kontaktowe do osób lub firm odpowiedzialnych za utrzymanie systemu lub jego poszczególnych części.

**Dokumentacja powykonawcza w IT jest niezbędna do dalszej eksploatacji i wsparcia systemu, umożliwiając nowym zespołom szybkie zapoznanie się z wdrożeniem oraz umożliwiając efektywne zarządzanie systemem w przyszłości**

## Etapy wdrożenia

Zamawiający oczekuje, że Wykonawca lub Wykonawcy przedstawią Szczegółowy Harmonogram realizacji projektu wg złożonych ofert opracowany zgodnie ze swoją metodyką wdrożeniową, wraz ze szczegółową strukturą zadań oraz produktów poszczególnych etapów projektu z uwzględnieniem spodziewanych przez Zamawiającego dat uruchomienia poszczególnych elementów systemu, jednak nie mniej niż w podziale na:

* prace przygotowawcze, analiza przedwdrożeniowa,
* dostawa sprzętu, licencji, instalacja oprogramowania na dostarczonej infrastrukturze,
* wdrożenie poszczególnych modułów systemów w kolejności pozwalającej na optymalne obciążenie pracą zespołu Zamawiającego i Wykonawcy, obejmujące podział na: prace konfiguracyjne, szkolenia personelu, uruchomienie modułu, oddanie modułu,
* migracje danych zgodnie z wymaganiami poszczególnych modułów uwzględniające termin oraz zakres migrowanych danych (np. przenoszenie całych kartotek pacjentów „na starcie” lub jedynie bilansów otwarcia w systemie FK w momencie uruchomienia modułu). Szczegółowy opis tego zakresu musi znaleźć się w analizie przedwdrożeniowej – zwłaszcza w zakresie terminów i danych wymaganych od Zamawiającego do przekazania Wykonawcy,
* terminy i zakresy integracji pomiędzy poszczególnymi systemami zarówno nowymi jak i obecnie używanymi. Zamawiający oczekuje, że Wykonawca określi przewidywane.

## Termin realizacji Przedmiotu umowy dla obu części.

**Nie dłuższy niż 6 miesięcy od podpisania Umowy**.

Szczegółowy harmonogram zostanie przygotowany przez Wykonawcę lub Wykonawców w zakresie, którym złożył ofertę i zaakceptowany przez Zamawiającego.

Wymagania ogólne dotyczącą integracji oraz Instalacji i konfiguracji Platformy e-usług oraz Instalacji i konfiguracji Platformy sprzętowej).

## Zestawienie zakresu dostaw i usług dla części I

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| LP | NAZWA | Min. Gwarancja  (m-ce) | Typ/ Rodzaj gwarancji | Ilość | JM |
|  | eBOM - elektroniczne Biuro Obsługi Mieszkańca | 36 | Wykonawcy/ producenta | 1 | lic. |
|  | Aplikacja mobilna | 36 | Wykonawcy/ producenta | 1 | lic. |
|  | Oprogramowanie dziedzinowe | 36 | Wykonawcy/ producenta | 1 | lic. |
|  | System GIS | 36 | Wykonawcy/ producenta | 1 | lic. |
|  | e-edukacja | 36 | Wykonawcy/ producenta | 1 | lic. |
|  | ePszok | 36 | Wykonawcy/ producenta | 1 | lic. |
|  | eRada | 36 | Wykonawcy/ producenta | 1 | lic. |
|  | Obieg  dokumentów | 36 | Wykonawcy/ producenta | 35 | Lic. |
|  | Monitoring środowiska | 36 | Wykonawcy/ producenta | 1 | zestaw |
|  | System eWoda | 24 | Wykonawcy/ producenta | 1 | Lic. |
|  | Strona WWW | 24 | Wykonawcy | 1 | szt. |
|  | Szkolenia TiK typ II | Nd. | Nd. | 160 | RBH |
|  | Dokumentacja techniczna | Nd. | Nd. | 20 | RBH |
|  | Integracja (Platforma e-usług publicznych) | Nd. | Nd. | 400 | RBH |
|  | Instalacja i konfiguracja - część nr 1 (Platforma e-usług publicznych) | Nd. | Nd. | 200 | RBH |

# **CZĘŚĆ I – OPROGRAMOWANIE (Platforma e-usług)**

## Zakres dot. integracji

Usługa obejmuje integrację wszystkich elementów oprogramowania w jeden spójny system, gdzie głównym kanałem dostępu do wszystkich funkcjonalności i e-usług będzie system eBOM. Zamawiający oczekuje pełnej i bezproblemowej integracji   
z istniejącymi systemami dziedzinowymi. Usługa obejmuje również połączenie poszczególnych systemów dziedzinowych z węzłami autentykacji, bramkami płatnościowymi, formularzami ePUAP w taki sposób, aby możliwe było realizowanie   
e-usług opisanych w projekcie na wskazanych poziomach dojrzałości.

## Zakres usługi instalacji i konfiguracji

Obejmuje wykonanie instalacji, konfiguracji oraz uruchomienia i przetestowania poprawności działania wszystkich modułów oprogramowania dziedzinowego objętych projektem:

* (eBOM - elektroniczne Biuro Obsługi Mieszkańca,
* aplikacja mobilna,
* Oprogramowanie dziedzinowe,
* System GIS,
* e-edukacja,
* ePszok,
* eRada,
* Obieg dokumentów,
* Monitoring środowiska,
* System eWoda,
* Strona WWW).
* Szkoleni TIK II,

W szczególności w ramach usługi zostaną wykonane następujące czynności:

1. instalacja dostarczonego oprogramowania na infrastrukturze gminy
2. wygenerowanie kont użytkowników, nadanie im odpowiednich uprawnień zgodnie z ustaleniami z gminą
3. o ile to konieczne, zaktualizowanie posiadanych modułów oprogramowania do najnowszych dostępnych wersji,
4. przeprowadzenie testów użytkownika na systemie roboczym i produkcyjnym celem weryfikacji prawidłowości działania,
5. sporządzenie dokumentacji powykonawczej z instalacji i konfiguracji
6. asysty stanowiskowe.

## Wymagania gwarancyjne

* oprogramowanie powinno posiadać min. 24-miesięczną gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba, że zapisy szczegółowe stanowią inaczej);
* gwarancja nie obejmuje kosztów bieżącego utrzymania (opieka serwisowa, upgrade systemów, wersji, prawa do aktualizacji) wdrożonego oprogramowania po okresie realizacji projektu.

## eBOM - elektroniczne Biuro Obsługi Mieszkańca – szt.1 lic.

Przedmiotem zamówienia jest zaprojektowanie, dostawa, instalacja, konfiguracja oraz optymalizacja Elektronicznego Biura Obsługi Mieszkańca (eBOM) dla Gminy.

System ma umożliwiać świadczenie e-usług na rzecz mieszkańców oraz integrację z innymi platformami administracyjnymi.

Przedmiotem zamówienia jest kompleksowe wdrożenie systemu eBOM, którego głównym celem jest ułatwienie dostępu do e-usług dla mieszkańców gminy oraz poprawa organizacji informacji JST. System będzie zgodny z obowiązującymi standardami prawnymi i technologicznymi oraz zapewni wysoką jakość usług   
w ramach cyfrowej administracji publicznej.

Z uwagi na to, że system Elektronicznego Zarządzania Dokumentami (EZD) oraz portal eBOM będą stanowił rdzeń integracyjny wszystkich systemów dziedzinowych oraz e-Usług wdrażanych w ramach projektu, funkcjonalność modułu integracyjnego musi być zrealizowana w oparciu o jego interfejsy komunikacyjne.

**1. Funkcjonalności systemu**

**1.1. Udostępnianie e-usług -** System eBOM będzie odpowiedzialny za prezentację  
 i obsługę e-usług świadczonych na rzecz mieszkańców gminy. E-usługi zostaną podzielone tematycznie i pogrupowane według odpowiednich wydziałów, a ich wyszukiwanie będzie możliwe za pomocą haseł tematycznych.

**1.2. Organizacja informacji -** Portal będzie gromadził w jednym miejscu informacje dotyczące różnych aspektów działalności JST, prezentowane w uporządkowanej formie. System umożliwi publikowanie danych otwartych w ogólnodostępnej części serwisu, z podziałem na grupy tematyczne oraz obsługą różnych formatów plików do pobrania.

**1.3. Publiczny serwis WWW -** Portal eBOM zostanie wdrożony jako publicznie dostępny serwis WWW, podzielony na dwie główne strefy:

* **Część ogólnodostępna** dla użytkowników anonimowych.
* **Część wymagająca uwierzytelnienia** dla użytkowników posiadających konto.

Publikowane treści będą formatowane na podstawie zdefiniowanych szablonów, co zapewni ich spójną prezentację w całym systemie.

**1.4. Zgodność prawna i techniczna -** System będzie zgodny z aktualnymi przepisami prawa dotyczącymi funkcjonowania samorządu terytorialnego, w tym Krajowymi Ramami Interoperacyjności. Dodatkowo:

* Obsługa najpopularniejszych przeglądarek internetowych oraz urządzeń mobilnych.
* Wysoka dostępność oraz zgodność ze standardami WCAG 2.1.
* Intuicyjna nawigacja umożliwiająca łatwe przechodzenie od informacji ogólnych do szczegółowych.

**1.5. Integracja z innymi systemami -** System będzie umożliwiał integrację z platformą ePUAP poprzez:

* Wykorzystanie kart usług platformy ePUAP;
* Publikowanie własnych dokumentów do pobrania (np. RTF, PDF).

**1.6. Architektura systemu -** System eBOM będzie oparty na architekturze zorientowanej na usługi (SOA) i udostępni API umożliwiające wymianę danych z innymi systemami.

1.7 Moduł musi posiadać ustandaryzowane interfejsy zewnętrzne, obejmujące udostępnianie usług integracyjnych (m.in. wymiany danych), systemom zewnętrznym poprzez:

* usługi Web Services (w oparciu o standardy SOAP 1.2, WSDL co najmniej 1.1);
* możliwość komunikacji z wykorzystaniem plików XML zlokalizowanych w strukturach plikowych jednostki,
* JMS, zgodność ze standardami XML 1.0 i XSD 1.1.
  1. Komunikacja z systemem EZD odbywać się ma za pośrednictwem serwisu komunikacyjnego.
  2. Moduł musi zapewniać integrację modułów dziedzinowych systemów informatycznych z systemem Elektronicznego Zarządzania Dokumentami. Musi być możliwość automatycznego przekazywania dokumentów tworzonych w tych modułach wraz z automatycznym dodawaniem ich do teczek spraw bezpośrednio w systemie EZD.
  3. Moduł musi zapewniać integrację systemu EZD z systemem finansowo-księgowym. Musi być możliwość przekazywania do systemu FK danych w zakresie niezbędnych do jego zaksięgowania wynikających z wpływających dokumentów finansowych na dziennik podawczy (np. faktury, umowy itp.).
  4. Moduł musi pozwalać na integrację z systemem kadrowym na poziomie obsługi wniosków urlopowych. W e-formularzu (wniosek urlopowy) systemu EZD muszą być wyświetlane dane o wykorzystanych dniach urlopowych dla użytkownika systemu EZD wnioskującego o urlop.
  5. Moduł musi zapewniać synchronizacje kartotek kontrahentów na poziomie modułów dziedzinowych i systemu EZD zapewniając dwukierunkową wymianę metadanych dokumentów przysyłanych z platformy ePUAP oraz systemu   
     e-Doręczeń.
  6. Moduł musi zapewniać automatyzację następujących procesów:
  7. Faktury przychodzące rejestrowane w systemie EZD muszą być kierowane bezpośrednio do modułu FK zapewniając jednokrotne wprowadzanie danych.
  8. Umowy rejestrowane w systemie EZD kierowane są bezpośrednio do modułu Rejestr Umów zapewniając jednokrotne wprowadzanie danych.
  9. Dokumenty elektroniczne dotyczące wszystkich typów deklaracji podatkowych (wypełnionych na ePUAP lub w systemie e-Doręczeń) muszą być przekazywane poprzez EZD do modułów podatkowych zapewniając pobierania metadanych z plików XML w systemie dziedzinowym.
  10. Dokumenty elektroniczne dotyczące deklaracji za gospodarowania odpadami komunalnymi (wypełnionych na ePUAP), muszą być przekazywane poprzez EZD do modułów podatkowych zapewniając czytywanie metadanych z plików XML w dedykowanym module dziedzinowym.
  11. Dokumenty elektroniczne dotyczące oświadczeń o sprzedaży napojów alkoholowych (wypełnionych na ePUAP) muszą być przekazywane poprzez EZD do modułu związanego z obsługą zezwoleń na sprzedaż napojów alkoholowych zapewniając pobierania metadanych z plików XML w systemie dziedzinowym.
  12. Decyzje elektroniczne pochodzące z modułów podatkowych muszą być przekazywane do systemu EZD (obsługa podpisu elektronicznego jest realizowana z poziomu EZD ), a następnie kierowane na skrytkę ePUAP podatnika lub na konto w systemie e-Doręczeń.
  13. Niezbędną wymianę danych z platformą ePłatności (PeP)
  14. Moduł musi umożliwić publikację dokumentów (rejestrów) na stronie podmiotowej BIP oraz musi umożliwić informowanie o statusie sprawy na stronie podmiotowej BIP.
  15. Moduł musi udostępniać metody komunikacyjne niezbędne do funkcjonowania portalu eBOM w zakresie udostępnienia odpowiednich danych zapewniając ich wizualizację po stronie www, możliwość dokonania zapłaty za pośrednictwem systemu płatności elektronicznych oraz dostarczania odpowiednich komunikatów do interesantów.
  16. Moduł musi posiadać mechanizm kontroli dostępu do usług pozwalający na dostęp do danej usługi ze względu na użytkownika oraz grupę (jednostkę organizacyjną) do której należy.
  17. Moduł musi umożliwiać administratorom zarządzanie udostępnianymi usługami i interfejsami (w tym harmonogramem komunikacji, lokalizacją plików, uprawnieniami do nich). Moduł będzie umożliwiał wdrażanie nowych interfejsów komunikacyjnych.

**2. Zakres usług**

Koszty związane z instalacją, konfiguracją i optymalizacją systemu zostały uwzględnione w następujących pozycjach specyfikacji usług:

* Integracja (Platforma e-usług publicznych);
* Instalacja i konfiguracja (Platforma e-usług publicznych).

W ramach realizacji zamówienia wykonawca będzie zobowiązany do zapewnienia wsparcia stanowiskowego w zakresie wdrożenia i obsługi systemu.

**3. Wymagania dodatkowe**

* System powinien być elastyczny i umożliwiać jego przyszłą rozbudowę.
* Oprogramowanie powinno być bezpieczne, chronione przed atakami cybernetycznymi oraz posiadać mechanizmy autoryzacji i kontroli dostępu.

## Aplikacja mobilna – szt.1 lic.

Przedmiotem zamówienia jest dostarczenie, wdrożenie i integracja aplikacji mobilnej dla Gminy, działającej na zasadach licencji OPEN na jednostkę/Gminę. Aplikacja będzie zintegrowana z posiadanym systemem dziedzinowym oraz stroną internetową Zamawiającego.

|  |  |  |  |
| --- | --- | --- | --- |
| LP | System dziedzinowy | Wersja | Krótki opis |
| 1 | Gospodarka  mat.-magaz. SU | 1.xx | system wspierający zarządzanie zasobami magazynowymi, ewidencję materiałów oraz kontrolę stanów magazynowych. |
| 2 | Ewidencja  zwrotów pod. akc. SU | 1.5x | narzędzie umożliwiające prowadzenie ewidencji zwrotów podatku akcyzowego, generowanie raportów oraz obsługę wniosków. |
| 3 | System Ewidencji Podatkowej SU | 3.x.x | kompleksowe oprogramowanie do zarządzania podatkami lokalnymi, ewidencji wpłat oraz monitorowania zaległości podatkowych. |
| 4 | Ewidencja środków trwałych – SU | 8.3.x | system wspomagający zarządzanie majątkiem trwałym, amortyzacją i inwentaryzacją. |
| 5 | System płacowy  - SU | 3.xx | narzędzie do obsługi wynagrodzeń pracowników, naliczania pensji oraz generowania dokumentacji kadrowo-płacowej. |
| 6 | System finansowo-księgowy SU | 4.xx | zintegrowane oprogramowanie do prowadzenia księgowości, zarządzania finansami oraz raportowania zgodnie z obowiązującymi standardami rachunkowości. |
| 7 | Podatek od śr. transport. SU | 1.xx | aplikacja wspierająca ewidencję, naliczanie i kontrolę zobowiązań podatkowych z tytułu posiadania środków transportowych. |
| 8 | System obsługi kasy  - SU | 1.xx | oprogramowanie do zarządzania operacjami kasowymi, obsługi wpłat i wypłat oraz prowadzenia ewidencji kasowej. |
| 9 | System kadrowy  - SU | 3.xx | moduł wspomagający zarządzanie zasobami ludzkimi, ewidencję pracowników oraz dokumentację kadrową. |
| 10 | System ew.i roz. opł.za.śm.SU | 2.xx | dedykowane narzędzie do ewidencji odbiorców, naliczania opłat za gospodarkę odpadami oraz prowadzenia rozliczeń. |
| 11 | System ew.i roz.  opłat SU | 4.xx | system wspierający obsługę różnorodnych opłat administracyjnych, ich naliczanie oraz monitorowanie zaległości. |
| 12 | eVat | 3.x.x | narzędzie do obsługi ewidencji VAT, generowania raportów oraz integracji z systemami księgowymi. |
| 13 | Ewidencja mienia komunalnego – SU | 6.00 | oprogramowanie umożliwiające prowadzenie rejestru mienia komunalnego, zarządzanie nieruchomościami oraz monitorowanie ich wartości. |
| 14 | Ewid.i roz.op. kom-woda, śc. SU | 6.x.x | system do obsługi rozliczeń związanych z dostawą wody i odprowadzaniem ścieków, generowania faktur oraz monitorowania należności. |
| 15 | e-Należności | 1.xx | moduł do ewidencji, monitorowania i egzekwowania należności administracyjnych oraz podatkowych. |

Zamawiający zastrzega sobie prawo do przeprowadzenia testów aplikacji przed jej ostatecznym odbiorem.

### 1.2.1. Wymagania funkcjonalne

1. Integracja - Aplikacja musi zostać zintegrowana z istniejącym systemem dziedzinowym oraz stroną internetową Zamawiającego.
2. Klucz API - Aplikacja musi zapewniać klucz API umożliwiający komunikację   
   z aplikacjami zewnętrznymi.
3. Platformy mobilne - Aplikacja powinna być dostępna w wersjach dla systemów android oraz iOS.
4. Podział na strefy - Aplikacja powinna posiadać:

* Strefę ogólnodostępną,
* Strefę dla zalogowanego użytkownika.

1. Bezpieczne logowanie - Aplikacja powinna umożliwić logowanie poprzez krajowy węzeł identyfikacji elektronicznej oraz profil zaufany (https://pz.gov.pl).
2. Dostęp do danych i płatności - Zalogowany użytkownik musi mieć możliwość dostępu do danych z systemów dziedzinowych oraz możliwość dokonywania opłat w ramach portalu eBOM.
3. Obsługa dokumentów - Aplikacja powinna umożliwić przeglądanie załączników w formacie PDF.
4. Powiadomienia:

* Aplikacja musi umożliwiać odbieranie powiadomień z systemów dziedzinowych zgodnie z ustawieniami modułów i kontem użytkownika.
* Powiadomienia będą spersonalizowane i wysyłane do konkretnych użytkowników.
* Zalogowany użytkownik powinien mieć możliwość zarządzania powiadomieniami (włączanie/wyłączanie oraz wybór metody dostarczania).

1. Obsługa zgłoszeń - Aplikacja powinna umożliwić automatyczne wysyłanie wiadomości e-mail do urzędu gminy z wyborem tematu oraz automatycznym kierowaniem do odpowiedniej osoby.
2. Dostępność - Aplikacja musi być dostępna do pobrania w popularnych sklepach z aplikacjami (Google Play, App Store).
3. Aplikacja mobilna powinna być dostępna w wersjach na popularne systemy operacyjne stosowane dla urządzeń mobilnych (Android, iOS)
4. Aplikacja powinna być podzielona na strefę ogólnodostępną oraz strefę użytkownika zalogowanego.
5. Konto użytkownika zalogowanego powinno być wspólne z kontem na platformie eBOM. Aplikacja zapewni bezpieczne logowanie przez autoryzację   
   z wykorzystaniem Krajowego Węzła Identyfikacji Elektronicznej.
6. Rejestracja konta użytkownika powinna być możliwa po stronie aplikacji mobilnej i konto to powinno być wspólne z kontem użytkownika na platformie eBOK. Konfiguracja parametrów konta jak i uwierzytelnienie może być dokonane przez użytkownika po dowolnej stronie (eBOM, aplikacja mobilna).
7. Zalogowany użytkownik posiada dostęp do danych z systemów dziedzinowych zgodnie z zakresem wymaganym dla portalu eBOM z możliwością dokonywania zapłat za pośrednictwem systemu płatności elektronicznych tożsamego z tą platformą (eBOM). Wizualizacja danych w swoim zakresie i sposobie prezentowania powinna być w miarę możliwości technicznych jednolita   
   z portalem eBOM.
8. Aplikacja musi umożliwić prezentację załączników (dokumentów z systemów dziedzinowych) z wykorzystaniem formatu PDF.
9. Ekran powitalny („Dane urzędu”) powinien wizualizować informacje pobierane z serwera a administrator powinien mieć możliwość aktualizowania   
   i konfigurowania tych danych.
10. Aplikacja powinna mieć obsługę „Aktualności” dynamicznie pobieranych z list aktualności zarządzanych przez administratora portalu eBOM. Zakres aktualności musi byś tożsamy z tą platformą.
11. Aplikacja powinna mieć obsługę „Miejsc” dynamicznie pobieranych z listy zarządzanej przez administratora portalu eBOM. Wizualizacja musi umożliwiać zamieszczanie w niej plików graficznych, prosty edytor treści, oraz określenie położenia na mapie – gogle maps. Lokalizacje powinny byś pogrupowane na typy a użytkownik może je potem wybierać wg. zadanego kryterium. Wizualizacja na mapie powinna umożliwić pokazanie na niej zarówno wszystkich lokalizacji jak i tylko lokalizacji wybranego typu (np. same obiekty sportowe lub zabytki).
12. Aplikacja powinna zawierać obsługę i wizualizację „Galerii” z podziałem na kategorie. Galeria jest dostępna dla użytkowników niezalogowanych.
13. Aplikacja powinna zawierać obsługę kalendarzy tożsama z systemem eBOM (zarówno w zakresie merytoryczny jak i zbliżonej formie wizualizacji).
14. Aplikacja mobilna musi otrzymywać powiadomienia z systemów dziedzinowych zgodnie z ustawieniami na koncie zalogowanego użytkownika portalu eBOM. Powiadomienia będą spersonalizowane i wysyłane do konkretnych użytkowników zarejestrowanych w systemie. Zalogowany użytkownik powinien mieć możliwość włączenia lub wyłączenia wybrany typ powiadomienia oraz określenie metody jego dostarczania.
15. Aplikacja powinna umożliwiać wyświetlenie listy otrzymanych komunikatów
16. Aplikacja umożliwi automatyczne wysłanie e-maili do gminy. System umożliwi wybranie tematu wiadomości i automatycznie skieruje ją do osoby odpowiedzialnej za dane zadanie.

Aplikacje mobilne powinny być udostępnione na powszechnie dostępnych serwisach do ich pobierania.

### 1.2.2. Wymagania techniczne i wdrożeniowe

1. Integracja z platformą e-usług publicznych, w tym obsługa jednolitego systemu logowania i uwierzytelniania.
2. Instalacja i konfiguracja - Pełne wdrożenie obejmujące konfigurację aplikacji i jej dostosowanie do potrzeb Zamawiającego.
3. Optymalizacja i asysta stanowiskowa - Wsparcie w zakresie optymalizacji działania aplikacji oraz szkolenie użytkowników.

3. Licencja Aplikacja będzie dostarczona na licencji OPEN, obejmującej całą jednostkę samorządową (Gminę).

4. Warunki realizacji zamówienia

1. Pełne wdrożenie zgodnie z harmonogramem ustalonym z Zamawiającym.
2. Zapewnienie odpowiedniego poziomu wsparcia technicznego i serwisowego.
3. Przekazanie pełnej dokumentacji technicznej oraz instrukcji użytkownika.

## Oprogramowanie dziedzinowe – szt.1 lic.

Przedmiotem zamówienia jest podniesienie wersji posiadanego systemu dziedzinowego do najnowszej wspieranej przez producenta wersji oraz jego dostosowanie do aktualnych potrzeb Gminy. Zamówienie obejmuje wszystkie składowe aplikacji dziedzinowych, czyli specjalizowanych programów przeznaczonych do obsługi wydzielonych obszarów aktywności jednostek administracji.

Zamawiający zastrzega sobie prawo do przeprowadzenia testów systemu przed jego ostatecznym odbiorem.

**1. Zakres aktualizacji i modernizacji**

1. Podniesienie wersji systemu dziedzinowego - Aktualizacja do najnowszej wersji wspieranej przez producenta.
2. Objęcie aktualizacją wszystkich aplikacji dziedzinowych wchodzących w skład systemu.
3. Przystosowanie systemów dziedzinowych do przekazywania danych do platformy EBOM w celu świadczenia e-usług publicznych.
4. Przystosowanie oprogramowania do obsługi płatności elektronicznych - integracja z dostępnymi systemami płatniczymi.
5. Zapewnienie logowania z wykorzystaniem kont domenowych, zgodnie   
   z polityką autoryzacji i bezpieczeństwa.
6. Wprowadzenie wersjonowania umożliwiającego śledzenie zmian   
   w oprogramowaniu i jego konfiguracji.
7. Logowanie zdarzeń bezpieczeństwa, w tym rejestrowanie dostępu i operacji krytycznych.
8. Szyfrowanie danych i komunikacji - zapewnienie bezpiecznego przesyłu   
   i przechowywania informacji.
9. Zapewnienie otwartych mechanizmów wymiany danych - interfejs API umożliwiający integrację z aplikacjami zewnętrznymi.

**2. Wymagania techniczne i wdrożeniowe**

1. Integracja z platformą e-usług publicznych, w tym obsługa jednolitego systemu logowania i uwierzytelniania.
2. Instalacja i konfiguracja - Pełne wdrożenie obejmujące konfigurację systemu oraz jego dostosowanie do wymagań Zamawiającego.
3. Optymalizacja i asysta stanowiskowa - Wsparcie w zakresie optymalizacji działania systemu oraz szkolenie użytkowników.

**3. Licencja**

Oprogramowanie będzie dostarczone na licencji OPEN, obejmującej całą jednostkę samorządową (Gminę).

**4. Warunki realizacji zamówienia**

1. Pełne wdrożenie zgodnie z harmonogramem ustalonym z Zamawiającym.
2. Zapewnienie odpowiedniego poziomu wsparcia technicznego i serwisowego.
3. Przekazanie pełnej dokumentacji technicznej oraz instrukcji użytkownika.

Zamawiający dysponuje następującym oprogramowaniem dziedzinowym:

|  |  |  |  |
| --- | --- | --- | --- |
| LP | System dziedzinowy | Wersja | Krótki opis |
| 1 | Gospodarka  mat.-magaz. SU | 1.xx | system wspierający zarządzanie zasobami magazynowymi, ewidencję materiałów oraz kontrolę stanów magazynowych. |
| 2 | Ewidencja  zwrotów pod.akc. SU | 1.5x | narzędzie umożliwiające prowadzenie ewidencji zwrotów podatku akcyzowego, generowanie raportów oraz obsługę wniosków. |
| 3 | System Ewidencji Podatkowej SU | 3.x.x | kompleksowe oprogramowanie do zarządzania podatkami lokalnymi, ewidencji wpłat oraz monitorowania zaległości podatkowych. |
| 4 | Ewidencja środków trwałych – SU | 8.3.x | system wspomagający zarządzanie majątkiem trwałym, amortyzacją i inwentaryzacją. |
| 5 | System płacowy – SU | 3.xx | narzędzie do obsługi wynagrodzeń pracowników, naliczania pensji oraz generowania dokumentacji kadrowo-płacowej. |
| 6 | System finansowo-księgowy SU | 4.xx | zintegrowane oprogramowanie do prowadzenia księgowości, zarządzania finansami oraz raportowania zgodnie z obowiązującymi standardami rachunkowości. |
| 7 | Podatek od śr. transport. SU | 1.xx | aplikacja wspierająca ewidencję, naliczanie i kontrolę zobowiązań podatkowych z tytułu posiadania środków transportowych. |
| 8 | System obsługi kasy  - SU | 1.xx | oprogramowanie do zarządzania operacjami kasowymi, obsługi wpłat i wypłat oraz prowadzenia ewidencji kasowej. |
| 9 | System kadrowy  - SU | 3.xx | moduł wspomagający zarządzanie zasobami ludzkimi, ewidencję pracowników oraz dokumentację kadrową. |
| 10 | System ew.i roz. opł.za.śm.SU | 2.xx | dedykowane narzędzie do ewidencji odbiorców, naliczania opłat za gospodarkę odpadami oraz prowadzenia rozliczeń. |
| 11 | System ew.i roz.  opłat SU | 4.xx | system wspierający obsługę różnorodnych opłat administracyjnych, ich naliczanie oraz monitorowanie zaległości. |
| 12 | eVat | 3.x.x | narzędzie do obsługi ewidencji VAT, generowania raportów oraz integracji z systemami księgowymi. |
| 13 | Ewidencja mienia komunalnego – SU | 6.00 | oprogramowanie umożliwiające prowadzenie rejestru mienia komunalnego, zarządzanie nieruchomościami oraz monitorowanie ich wartości. |
| 14 | Ewid.i roz.op. kom-woda, śc. SU | 6.x.x | system do obsługi rozliczeń związanych z dostawą wody i odprowadzaniem ścieków, generowania faktur oraz monitorowania należności. |
| 15 | e-Należności | 1.xx | moduł do ewidencji, monitorowania i egzekwowania należności administracyjnych oraz podatkowych. |

## System GIS – szt.1 lic.

Modernizacja obecnego Systemu Informacji Przestrzennej wraz z integracją z dziedzinowymi Systemami w zakresie obsługi E-usług.

1. Pozycja dotyczy podniesienia wersji posiadanego systemu GIS do najnowszej wspieranej przez producenta wersji.
2. Aktualizacja ma dotyczyć wszystkich pozycji wchodzących w skład Systemu GIS – specjalizowane programy przeznaczone do obsługi wydzielonych obszarów aktywności jednostek administracji.
3. Przystosowanie systemów GIS do przekazywania danych do platformy EBOM celem świadczenia e-usług publicznych.
4. Przystosowanie oprogramowania do świadczenia płatności elektronicznych.
5. Zapewnienie logowania z wykorzystaniem kont domowych.
6. Wprowadzenie wersjonowania.
7. Logowania zdarzeń bezpieczeństwa.
8. Szyfrowanie danych i komunikacji przesyłu danych.
9. Zapewnienie otwartych mechanizmów wymiany danych z aplikacjami zewnętrznymi - interfejs API.

Zakres:

1. publikacja planów zagospodarowania,
2. MPZP w postaci wektorowej,
3. zbiór APP + metadane,
4. wydawanie wypisów i wyrysów

Oprogramowanie - Systemu GIS wraz z E-usługami. System GIS (gdzie wszystkie wymagania funkcjonalne Systemu GIS będą realizowane przez aplikacje internetową za pośrednictwem przeglądarki internetowej) służy do gromadzenia, przechowywania, analizy i wizualizacji danych przestrzennych. Podstawowym elementem całego zadania będzie digitalizacja danych przestrzennych (z obszaru uchwał oraz rejestrów gminnych) oraz ich migracja do specjalistycznych systemów dziedzinowych Systemu GIS. Pozycja ma na celu usprawnienie pracy Urzędu, publikacji tych danych   
w wybranych obszarach oraz uruchomieniu E-usług publicznych dla mieszkańców   
i innych interesariuszy.

Całość kosztów związanych z instalacją, konfiguracją, optymalizacją oraz asystami stanowiskowymi została ujęta w pozycjach specyfikacji usług tj.

* Integracja (Platforma e-usług publicznych)
* Instalacja i konfiguracja (Platforma e-usług publicznych)

### 1.4.1 Wymagania ogólne

|  |  |
| --- | --- |
| Nr | Opis wymagania |
| 1.1. | Usługi i serwisy aplikacji muszą wymagać autoryzacji. |
| 1.2. | Dostęp do systemu powinien być bezpieczny i chroniony przed nieautoryzowanym dostępem, zapewniając stosowne mechanizmy uwierzytelniania (np. login i hasło, 2FA). |
| 1.3. | System musi posiadać historię logowań użytkowników co najmniej z rozbiciem na udane i nieudane próby logowania do systemu. |
| 1.4. | Po zdefiniowanym czasie bezczynności musi następować automatyczne wylogowanie użytkownika z Systemu. |
| 1.5. | System musi ostrzegać użytkownika przed kolejnym (drugim i kolejnym) zalogowaniem się tego samego użytkownika w tym samym czasie. |
| 1.6. | Po określonej liczbie nieudanych prób logowania system musi blokować konto użytkownika (administrator musi mieć możliwość odblokowania konta). |
| 1.7. | System musi przechowywać historię dotyczącą blokowania i odblokowywania kont użytkowników. |
| 1.8. | Wszystkie komponenty Systemu (aplikacje bazodanowe, aplikacje/moduły oraz Geoportal) muszą być zainstalowane na serwerach w infrastrukturze Zamawiającego |
| 1.9. | System musi posiadać architekturę trójwarstwową. |
| 1.10. | Interfejs Użytkownika Systemu musi być interfejsem webowym (dostępny z wykorzystaniem przeglądarek internetowych, zwanym także przeglądarkowym). Dostęp do Systemu musi być poprzez przeglądarki internetowe najczęściej wykorzystywane na rynku, to jest: Chrome, FireFox, Opera, Edge w co najmniej aktualnie wspieranych wersjach. |
| 1.11. | System nie może mieć ograniczeń co do liczby jednoczesnych dostępów. |
| 1.12. | Dostęp do poszczególnych funkcjonalności dla użytkowników musi być realizowany poprzez przeglądarkę WWW i definiowany na podstawie uprawnień przyznawanych przez administratora systemu. |
| 1.13. | Formularze w Systemie muszą być zrealizowane według zasad UX oraz wytycznych WCAG 2.1. W przypadku WCAG 2.1 System musi być zgodny co najmniej z rozporządzeniami i ustawami obowiązującymi w Polsce w tym zakresie. |
| 1.14. | System musi pracować w takiej architekturze sieciowo-serwerowej, która zapewni bezpieczeństwo danych Systemu oraz umożliwia bezpośredni dostęp aplikacji do bazy danych z pominięciem serwera. |
| 1.15. | Działania użytkownika w systemie muszą być mu przypisywane na podstawie unikalnego identyfikatora (domenowego lub loginu do aplikacji). |
| 1.16. | System posiada wbudowane funkcjonalności umożliwiające anonimizację danych. |
| 1.17. | System posiada wbudowane funkcjonalności umożliwiające pseudonimizację danych. |
| 1.18. | System musi posiadać wbudowany mechanizm logów (zdarzeń bezpieczeństwa). |

### 1.4.2 Wymagania dotyczące GEOPORTALU

|  |  |
| --- | --- |
| Nr | Opis wymagania |
| 2.1. | **GEOPORTAL** - zaawansowany portal mapowy przeznaczony do publikowania, udostępniania i przeglądania map online. Portal mapowy powinien umożliwiać użytkownikom dostęp do różnorodnych danych przestrzennych, takich jak mapy topograficzne, ortofotomapy, dane katastralne oraz inne warstwy tematyczne prezentujące rejestry urzędowe. Portal powinien działać w środowisku internetowym i być dostępny poprzez przeglądarkę internetową z wykorzystaniem bezpiecznego protokołu HTTPS, zapewniającego ochronę przesyłanych danych. Geoportal powinien wspierać analizę przestrzenną, nawigację oraz integrację z innymi systemami opisanymi w niniejszym dokumencie. |
| 2.2. | Zamawiający wymaga, aby portale mapowe były w pełni kompatybilne oraz poprawnie obsługiwane przez najnowsze wersje przeglądarek internetowych dostępne w dniu odbioru końcowego. Dodatkowo, system powinien wspierać również co najmniej jedną wersję poprzednią dla każdej z następujących przeglądarek: Google Chrome, Mozilla Firefox, Opera, Apple Safari oraz Microsoft Edge.  Wymagana kompatybilność obejmuje zarówno poprawne wyświetlanie i działanie interfejsu użytkownika, jak i pełną funkcjonalność wszystkich dostępnych narzędzi oraz modułów systemu. W przypadku zmian w specyfikacji przeglądarek, które mogą wpłynąć na działanie portalu mapowego, wykonawca zobowiązany jest do zapewnienia stosownych aktualizacji i dostosowania systemu, tak aby jego działanie pozostało niezakłócone.  Ponadto, system powinien być zoptymalizowany pod kątem wydajności, tak aby zapewnić płynne działanie na wszystkich wskazanych przeglądarkach, niezależnie od ich wersji, przy zachowaniu wysokiej responsywności i kompatybilności z nowoczesnymi standardami webowymi. |
| 2.3 | Mapy podkładowe w Geoportalu będą mogły być definiowane i wyświetlane według potrzeb użytkownika. System zapewni możliwość wyboru różnych źródeł danych, takich jak OpenStreetMap, ortofotomapy, a także dane z serwisu Geoportal.gov.pl oraz serwisów powiatowych i wojewódzkich. Użytkownik będzie mógł dostosować warstwy podkładowe do swoich wymagań, włączając i wyłączając poszczególne źródła, a także zmieniając ich kolejność wyświetlania. Dodatkowo przewidziana jest integracja z innymi serwisami kartograficznymi, umożliwiająca korzystanie z map topograficznych, planów miast oraz specjalistycznych warstw tematycznych, takich jak granice administracyjne, sieć dróg, hydrografia czy dane o pokryciu terenu. |
| 2.4 | Podstawową funkcją Geoportalu będzie wyświetlanie map szerokiemu gronu odbiorców, zapewniając dostęp do różnorodnych źródeł danych przestrzennych. System będzie obsługiwał standardowe usługi sieciowe, umożliwiające dynamiczne pobieranie, wizualizację oraz analizę danych geoprzestrzennych z wielu źródeł. Wspierane będą następujące standardy:   * **WMS 1.3.0 (Web Map Service)** – usługa umożliwiająca pobieranie i wyświetlanie rastrowych map tematycznych generowanych na żądanie użytkownika. Pozwala na wizualizację danych przestrzennych w określonych skalach i formatach, z możliwością stosowania legend oraz stylizacji warstw. * **WMTS 1.1.1 (Web Map Tile Service)** – usługa dostarczająca mapy w postaci predefiniowanych kafli, co zapewnia szybkie i efektywne wyświetlanie dużych zbiorów danych geoprzestrzennych. Sprawdza się w obsłudze podkładów mapowych oraz map o wysokiej rozdzielczości. * **WFS 2.0 (Web Feature Service)** – usługa umożliwiająca pobieranie, edycję i analizę obiektów wektorowych wraz z atrybutami. Dzięki niej użytkownicy mogą przeglądać, filtrować i pobierać dane przestrzenne w formacie GML, co pozwala na ich dalsze przetwarzanie w systemach GIS. * **CSW (Catalog Service for the Web)** – usługa katalogowa umożliwiająca wyszukiwanie i pobieranie metadanych dotyczących zbiorów danych geoprzestrzennych, usług mapowych oraz innych zasobów dostępnych w geoportalu.   Dzięki obsłudze tych standardów Geoportal zapewni interoperacyjność z innymi systemami GIS oraz umożliwi integrację z zewnętrznymi serwisami kartograficznymi. Użytkownicy będą mieli możliwość dostosowania wyświetlanych warstw do własnych potrzeb poprzez włączanie, wyłączanie i nakładanie różnych źródeł danych, co pozwoli na pełniejsze wykorzystanie dostępnych informacji geoprzestrzennych. |
| 2.5. | **Nawigowanie po mapie**  Portal Mapowy zapewnia użytkownikom intuicyjne narzędzia do nawigacji po mapie, umożliwiające wygodne przeglądanie i eksplorację danych przestrzennych. Do podstawowych funkcji nawigacyjnych należą:  **Przesuwanie mapy** – możliwość swobodnego przesuwania widoku mapy w dowolnym kierunku za pomocą myszy, gestów dotykowych lub przycisków symbolizujących poszczególne kierunki świata.  **Powiększanie i pomniejszanie mapy** – funkcja umożliwiająca zmianę skali mapy poprzez przyciski interfejsu, rolkę myszy, gesty zoomu na ekranach dotykowych lub wprowadzanie precyzyjnej wartości skali.  **Przejście do pełnego zakresu mapy** – szybkie dostosowanie widoku do maksymalnego dostępnego zasięgu danych, pozwalające na szybkie odnalezienie się w przestrzeni mapowej.  **Poprzedni i następny widok** – funkcje umożliwiające nawigację pomiędzy wcześniej oglądanymi zakresami mapy, co ułatwia analizę danych i porównywanie różnych obszarów.  **Pełny widok** – opcja wyświetlania mapy na całym ekranie, eliminująca zbędne elementy interfejsu i zapewniająca maksymalny obszar roboczy do pracy z danymi.  **Przybliżanie prostokątem** - funkcjonalność umożliwiająca przybliżenie mapy nad wybrany fragment terenu poprzez precyzyjne wskazanie na mapie fragmentu terenu do którego mapa powinna zostać przybliżona. |
| 2.6. | **Wyszukiwanie danych na mapie.**  Geoportal powinien oferować zaawansowane narzędzie wyszukiwarki, które umożliwia użytkownikom szybkie i precyzyjne odnalezienie obiektów na mapie na podstawie wprowadzonej frazy. Wyszukiwanie powinno obejmować szeroką gamę danych przestrzennych, a jego funkcjonalność może obejmować:   * **Wyszukiwanie działek** – umożliwiające odnalezienie konkretnych działek ewidencyjnych na podstawie numeru działki, jej granic lub innych atrybutów związanych z nieruchomościami, takich jak nazwa właściciela czy identyfikator ewidencyjny. * **Wyszukiwanie adresów** – funkcja pozwalająca na szybkie znalezienie lokalizacji na podstawie pełnego adresu lub jego części (np. numeru ulicy, nazwy ulicy, kodu pocztowego), z precyzyjnym wskazaniem miejsca na mapie. * **Wyszukiwanie ulic** – umożliwiające użytkownikom wyszukiwanie określonych ulic, zarówno na podstawie pełnej nazwy, jak i skróconej wersji, oraz pokazujące ich położenie na mapie. * **Wyszukiwanie obiektów z innych warstw** – funkcja, która pozwala na wyszukiwanie obiektów w różnych warstwach mapy zdefiniowanych przez administratora systemu, takich jak punkty użyteczności publicznej (np. szkoły, szpitale, sklepy), granice administracyjne, strefy ochrony środowiska, czy infrastruktura transportowa.   Wyszukiwarka powinna oferować również dodatkowe funkcje, takie jak:   * **Filtrowanie wyników** – użytkownik będzie mógł zawęzić wyniki wyszukiwania, wybierając określone kategorie lub typy obiektów, np. tylko działki, tylko budynki czy tylko obiekty publiczne. * **Wyszukiwanie za pomocą współrzędnych geograficznych** – umożliwiające użytkownikom podanie współrzędnych geograficznych (np. długości i szerokości geograficznej), by szybko przejść do określonego miejsca na mapie. * **Sugestie wyszukiwania** – system powinien oferować sugestie podczas wpisywania frazy, na przykład automatyczne uzupełnianie nazw ulic, miejscowości, czy numerów działek, co przyspiesza proces wyszukiwania i zmniejsza ryzyko błędów wprowadzenia danych. * **Podgląd wyników na mapie** – po wykonaniu wyszukiwania użytkownik powinien mieć możliwość natychmiastowego podglądu wyników bezpośrednio na mapie, z możliwością nawigowania do dokładnej lokalizacji wybranego obiektu.   Wszystkie te funkcje razem pozwolą użytkownikom na szybkie, wygodne i precyzyjne znajdowanie interesujących ich obiektów i informacji na mapie, a także na efektywniejsze poruszanie się po dostępnych danych geoprzestrzennych. |
| 2.7. | **Selekcja przestrzenna i atrybutowa**  Geoportal powinien oferować zaawansowaną funkcjonalność wyszukiwania obiektów z mapy, umożliwiając użytkownikom precyzyjne wyszukiwanie na podstawie wskazanych lokalizacji oraz atrybutów. Wśród dostępnych narzędzi wyszukiwania wyróżniają się:   1. **Wyszukiwanie obiektów poprzez zaznaczenie obiektów na mapie** – użytkownik ma możliwość wskazania na mapie obiektów za pomocą różnych narzędzi geograficznych:    * **Punkt** – umożliwia kliknięcie w dowolnym miejscu na mapie, aby wskazać konkretną lokalizację i wyszukać obiekty znajdujące się w tym punkcie. Może to dotyczyć np. wyszukiwania działek lub punktów użyteczności publicznej.    * **Linia** – użytkownik może narysować linię, na przykład drogę lub rzekę, w celu wyszukiwania obiektów, które są w jej pobliżu lub w jej obrębie, takich jak budynki przy drodze czy inne obiekty związane z infrastrukturą transportową.    * **Poligon** – za pomocą narzędzia wielokąta użytkownik może zaznaczyć określony obszar na mapie, aby wyszukać wszystkie obiekty znajdujące się wewnątrz tego obszaru, takie jak działki w określonej strefie lub obszary chronione. 2. **Wyszukiwanie obiektów poprzez zapytanie atrybutowe** – geoportal powinien umożliwiać bardziej zaawansowane wyszukiwanie na podstawie specyficznych atrybutów obiektów. Użytkownik będzie mógł zdefiniować zapytania w oparciu o wartości atrybutów, takich jak:    * Numer działki, powierzchnia, właściciel, typ budynku, typ drogi, kategoria terenu, czy inne cechy obiektów.    * Możliwość filtrowania wyników na podstawie określonych zakresów wartości atrybutów, np. wyszukiwanie działek o powierzchni większej niż określona wartość, budynków w określonej lokalizacji, czy obiektów znajdujących się w strefie ochrony środowiska.    * Wsparcie dla zapytań przestrzennych, które pozwalają na wyszukiwanie obiektów znajdujących się w określonym promieniu od wskazanej lokalizacji lub w obrębie narysowanej linii/poligonu. 3. **Podświetlanie wyników na mapie oraz wyświetlanie ich w tabeli atrybutów** – po wykonaniu wyszukiwania, geoportal powinien:    * **Podświetlić wyniki na mapie** – obiekty spełniające kryteria zapytania powinny zostać zaznaczone na mapie, np. poprzez zmianę koloru, obramowanie lub wyróżnienie, co pozwala użytkownikowi szybko zlokalizować interesujące obiekty.    * **Wyświetlić wyniki w tabeli atrybutów** – wszystkie obiekty spełniające zapytanie powinny być widoczne w tabeli, zawierającej kluczowe informacje o obiektach, takie jak identyfikator, nazwa, atrybuty przestrzenne (np. współrzędne), typ obiektu, itp. Tabela atrybutów powinna być interaktywna, umożliwiająca sortowanie, filtrowanie oraz edytowanie wyników.    * **Zgodność między mapą a tabelą** – wybierając obiekt na mapie, użytkownik powinien widzieć odpowiedni wiersz w tabeli atrybutów i odwrotnie, co umożliwia łatwe przejście między wizualizacją a danymi tekstowymi.   Dodatkowo, funkcjonalność ta powinna być wspierana przez odpowiednie narzędzia umożliwiające **eksport wyników wyszukiwania**, zarówno w postaci plików (np. CSV, Excel, GeoJSON), jak i generowanie raportów na podstawie wybranych obiektów. Wszystkie te funkcje razem pozwolą użytkownikom na efektywne i precyzyjne przetwarzanie danych przestrzennych, a także umożliwią ich łatwą analizę i prezentację. |
| 2.8. | **Filtrowanie mapowe**   * Funkcjonalność umożliwiająca zastosowanie filtra na mapie, dzięki któremu wyświetlone zostaną tylko te obiekty, które spełniają określone kryteria zapytania. Na przykład, użytkownik może nałożyć filtr, który wyświetli jedynie tereny objęte Miejscowym Planem Zagospodarowania Przestrzennego (MPZP) o przeznaczeniu MN – tereny zabudowy mieszkaniowej jednorodzinnej, a pozostałe obiekty zostaną ukryte na mapie. |
| 2.9. | **Zmiana odwzorowania kartograficznego / informacja o mapie**   * Geoportal powinien umożliwiać zmianę odwzorowania kartograficznego, np, w celu wyświetlenia danych WMS w innym układzie współrzędnych. * Wyświetlanie aktualnych współrzędnych kursora mapy, skali mapy, podziałki liniowej obrazującej skalę oraz informacji o układzie współrzędnych. |
| 2.10. | **Miniaturka** to funkcjonalność w geoportalu, która umożliwia użytkownikom szybki podgląd aktualnie wyświetlanego fragmentu mapy w kontekście całej mapy gminy lub większego obszaru. Miniaturka stanowi narzędzie wspierające nawigację, oferując dodatkowy widok, który ułatwia orientację w przestrzeni.  Dzięki miniaturce użytkownik ma możliwość:   * **Prezentacji aktualnie wyświetlanego fragmentu mapy** – miniatura pokazuje zaznaczony obszar, który jest obecnie widoczny na głównej mapie. Jest to zwizualizowane jako prostokąt lub kontur, który wskazuje dokładne położenie wybranego widoku na większej mapie. * **Tło mapy gminy** – miniaturka może zawierać w tle całą mapę gminy, powiatu, województwa lub innego szerszego obszaru, co pozwala użytkownikowi zobaczyć, gdzie znajduje się aktualnie przeglądany fragment w odniesieniu do większej jednostki administracyjnej. * **Zwiększenie kontekstu lokalizacji** – dzięki miniaturce użytkownicy mogą łatwo zorientować się w geograficznej lokalizacji, dostrzegając sąsiednie obszary, inne miasta, drogi czy granice administracyjne, co znacznie ułatwia nawigację. * **Zwiększenie wygody nawigacji** – użytkownicy mogą kliknąć na miniaturkę, by automatycznie przesunąć widok mapy do nowego obszaru, co pozwala na szybsze poruszanie się po mapie i łatwiejsze odnalezienie interesujących fragmentów.   Miniaturka powinna być na tyle czytelna i responsywna, aby łatwo można było zorientować się, jak dany obszar mapy odnosi się do całego regionu, zachowując odpowiednią proporcję i szczegółowość. Może to również obejmować możliwość **dynamicznego powiększania** miniaturki, by umożliwić lepszy podgląd w przypadku bardzo dużych obszarów. Dzięki tej funkcjonalności, użytkownik zawsze ma pełną kontrolę nad tym, jaki obszar jest aktualnie wyświetlany, co znacznie podnosi komfort pracy z mapą. |
| 2.11. | **Informacja o obiekcie** narzędzie powinno pozwalać użytkownikom na uzyskanie szczegółowych informacji na temat obiektów znajdujących się w danym punkcie na mapie. Po kliknięciu w konkretne miejsce na mapie, użytkownik powinien otrzymać precyzyjne dane o obiektach zlokalizowanych w tym miejscu, z wyświetleniem kluczowych atrybutów.  Jeśli w obszarze kliknięcia znajdują się obiekty z różnych warstw tematycznych, dane te powinny zostać odpowiednio **pogrupowane w zakładki tematyczne**, co umożliwia łatwiejszą nawigację i analizę danych. Przykładowe grupy mogą obejmować:   * **Warstwy administracyjne** (np. granice działek, gmin, powiatów), * **Infrastruktura** (np. drogi, sieć wodociągowa), * **Obiekty użyteczności publicznej** (np. szkoły, szpitale, urzędy), * **Obiekty geograficzne** (np. rzeki, jeziora, wzniesienia), * **Warstwy tematyczne** (np. strefy ochrony środowiska, MPZP, dane o zanieczyszczeniu powietrza).   Takie grupowanie danych w zakładki tematyczne pozwoli użytkownikom na szybkie zidentyfikowanie, jakie informacje są dostępne dla wybranego punktu, a także na lepszą organizację danych, zwłaszcza gdy obiekty mogą pochodzić z różnych źródeł lub różnych kategorii tematycznych.  Dodatkowo, w ramach narzędzia **informacja o obiekcie**, powinna zostać zapewniona możliwość obsługi **linków URL**, umożliwiająca użytkownikowi przejście do **konkretnej strony internetowej** po kliknięciu w odnośnik. Może to obejmować linki do zewnętrznych zasobów, takich jak:   * Strony urzędów i instytucji związanych z danym obiektem, * Strony z dodatkowymi informacjami o planach zagospodarowania przestrzennego, * Formularze kontaktowe, plany miejscowe, raporty środowiskowe lub inne dokumenty powiązane z obiektem.   Funkcja linków URL ułatwia dostęp do bardziej szczegółowych informacji, zasobów zewnętrznych lub oficjalnych dokumentów, co zwiększa użyteczność geoportalu. Dzięki tej opcji użytkownicy mogą szybko przejść do istotnych stron internetowych,  bez potrzeby wychodzenia z aplikacji. |
| 2.12 | **Tabela atrybutów** narzędzie powinno pozwalać użytkownikom na wyświetlenie w formie tabeli szczegółowych informacji na temat obiektów zawartych w wybranej warstwie mapy. Po włączeniu tej funkcji, użytkownik zobaczy tabelę, która zawiera listę wszystkich obiektów przypisanych do danej warstwy, wraz z ich atrybutami, takimi jak identyfikatory, nazwy, daty, wartości powierzchni, lokalizacje, typy obiektów czy inne istotne dane.  W szczególności, użytkownik powinien mieć możliwość:   1. Włączenia tabeli atrybutów – funkcja umożliwia włączenie okna tabeli, które może być wyświetlane obok mapy, w formie oddzielnego panelu lub okna. Tabela ta będzie zawierała wszystkie obiekty z danej warstwy, prezentując je w czytelny sposób. 2. Sortowania obiektów wg wybranego atrybutu – użytkownik będzie miał możliwość sortowania obiektów na liście według wybranego kryterium, np. według:    * Identyfikatora obiektu – np. numer działki, identyfikator budynku, numer ulicy,    * Nazwa obiektu – np. nazwa ulicy, obiektu publicznego, typu terenu,    * Wartości atrybutów liczbowych – np. powierzchnia działki, powierzchnia budynku, powierzchnia użytkowa,    * Daty – np. data wydania pozwolenia na budowę, data wykonania prac, data aktualizacji danych,    * Typu obiektu – np. rodzaj zabudowy, kategoria działki, klasyfikacja terenu. 3. Filtrowania wyników – tabela powinna umożliwiać filtrowanie wyników na podstawie określonych kryteriów. Użytkownik może np. zawęzić widok do obiektów spełniających określone warunki, takie jak określona powierzchnia działki, typ zabudowy czy przynależność do określonej strefy. 4. Interakcji z tabelą – użytkownicy powinni mieć możliwość kliknięcia na dowolny wiersz tabeli, co spowoduje wyświetlenie obiektu na mapie. W ten sposób łatwo będzie przejść do szczegółów wybranego obiektu bez konieczności ręcznego przeszukiwania mapy. 5. Eksportu danych – użytkownik powinien mieć możliwość eksportowania tabeli atrybutów do różnych formatów plików, takich jak CSV, Excel, PDF czy GeoJSON, co pozwala na dalszą obróbkę danych, tworzenie raportów lub integrację z innymi systemami GIS. 6. Dynamicznego odświeżania danych – tabela powinna być automatycznie odświeżana w przypadku zmiany warstwy na mapie lub dodania nowych danych do warstwy, zapewniając zawsze aktualne informacje o obiektach.   Dzięki tej funkcjonalności użytkownicy zyskają wygodne narzędzie do przeglądania i analizy danych przestrzennych, co pozwoli im na lepsze zrozumienie struktury i charakterystyki obiektów w danej warstwie, a także na szybkie znalezienie interesujących ich informacji. |
| 2.13. | **Mapy tematyczne** - geoportal powinien posiadać funkcjonalność umożliwiającą użytkownikowi dostęp do różnorodnych zestawów danych przestrzennych, które są prezentowane w formie dedykowanych map. Geoportal powinien obsługiwać wiele map tematycznych (profilów mapowych), które zostały zdefiniowane przez administratora systemu w zależności od potrzeb użytkowników oraz specyfiki prezentowanych danych.  Oto szczegóły rozbudowanej funkcjonalności dla map tematycznych:   1. **Obsługa wielu map tematycznych** – geoportal powinien umożliwiać przełączanie pomiędzy różnymi mapami tematycznymi, z których każda może prezentować inny zestaw danych, np. mapy zagospodarowania przestrzennego, mapy geologiczne, mapy dróg, mapy ochrony środowiska, mapy infrastruktury, czy mapy analityczne, takie jak dane dotyczące zanieczyszczenia powietrza lub statystyki demograficzne. Każda z map powinna mieć przypisany zestaw warstw oraz stylów wizualnych, który najlepiej pasuje do jej tematyki. 2. **Zmiana mapy tematycznej** w ramach sesji użytkownika – przełączanie pomiędzy mapami tematycznymi powinno być możliwe w obrębie jednej sesji użytkownika, bez konieczności przeładowania całej mapy. Dzięki temu użytkownik będzie mógł płynnie przechodzić z jednej mapy tematycznej do drugiej, zachowując spójność sesji i nie tracąc wprowadzonego ustawienia mapy, np. wybranej lokalizacji czy skali. Umożliwi to szybkie porównanie różnych warstw danych i dostosowanie widoku mapy w zależności od bieżącej potrzeby. 3. **Zachowanie skali i przybliżenia przy zmianie mapy tematycznej** – przy przełączaniu map tematycznych geoportal powinien zachować aktualną skalę oraz przybliżenie nad określonym obszarem. Dzięki temu użytkownik nie będzie musiał na nowo dostosowywać widoku mapy, a zmiana mapy będzie odbywać się w sposób płynny i intuicyjny. Niezależnie od tego, czy użytkownik przechodzi z mapy dotyczącej infrastruktury na mapę dotyczącą ochrony środowiska, mapy powinny automatycznie dostosować się do wcześniej wybranego obszaru i skali, co oszczędza czas i upraszcza obsługę systemu. 4. **Dostosowanie stylów wizualnych** **w ramach map tematycznych** – każda mapa tematyczna powinna być wyposażona w odpowiednio zaprojektowane style wizualne, które pozwalają na efektywne przedstawienie danych. Na przykład, mapy MPZP mogą być przedstawiane z różnymi kolorami dla różnych stref, podczas gdy mapy geologiczne mogą używać określonych schematów kolorystycznych do prezentacji różnych typów gruntów. Użytkownicy powinni mieć możliwość dostosowania wyglądu mapy do swoich preferencji, np. poprzez regulację intensywności kolorów lub przezroczystości warstw. 5. **Łatwość przełączania map tematycznych** – system powinien oferować intuicyjny interfejs umożliwiający szybkie przełączanie pomiędzy mapami tematycznymi. Może to obejmować rozwijane menu, panel boczny, zakładki, lub inny rodzaj nawigacji, który pozwala użytkownikowi na łatwy wybór żądanej mapy tematycznej bez potrzeby głębokiego zanurzenia w interfejsie.   Dzięki tym funkcjom użytkownicy będą mogli wygodnie korzystać z różnych map tematycznych w geoportalu, porównywać różne dane i uzyskiwać pełną kontrolę nad prezentacją mapy, co znacznie zwiększy funkcjonalność i użyteczność platformy. |
| 2.14. | **Lista warstw** narzędzie powinno umożliwiać użytkownikom zarządzanie i nawigowanie po dostępnych warstwach w geoportalu. Użytkownik będzie mógł włączać i wyłączać różne warstwy mapy, a także modyfikować kolejność w celu uzyskania optymalnego widoku mapy. Lista warstw powinna oferować następujące funkcje:   1. **Zestaw warstw do włączenia/wyłączenia** – lista powinna zawierać pełen zestaw dostępnych warstw, które użytkownik może łatwo włączać lub wyłączać. Każda warstwa będzie miała odpowiednią ikonę, która pozwala na jej szybką identyfikację, a także checkbox, umożliwiający jej aktywację lub dezaktywację. Warstwy te mogą obejmować mapy, dane przestrzenne, informacje tematyczne, a także różne źródła danych, takie jak WMS, WFS czy WMTS. 2. **Drzewo warstw z grupowaniem w foldery i podfoldery** – warstwy powinny być prezentowane w formie drzewa, które pozwala na ich łatwą organizację i przeglądanie. Warstwy powinny być pogrupowane w **foldery** oraz **podfoldery**, co pozwoli na hierarchiczne zarządzanie dużą liczbą warstw. Na przykład, warstwy dotyczące infrastruktury mogą być umieszczone w folderze „Infrastruktura”, a warstwy z danymi topograficznymi w folderze „Zagospodarowanie terenu”. 3. **Okno wyszukiwania warstw** – w ramach listy warstw powinna być dostępna funkcjonalność **wyszukiwania**, która umożliwi użytkownikowi szybkie znalezienie warstwy na liście na podstawie wpisanej frazy. Wyszukiwanie powinno dynamicznie zawężać listę warstw, pokazując tylko te, które odpowiadają zapytaniu. Na przykład, użytkownik może wpisać nazwę warstwy 4. **Zmiana kolejności warstw** – użytkownik powinien mieć możliwość zmiany **kolejności warstw** na liście w ramach jednej sesji. Może to być przydatne w sytuacji, gdy użytkownik chce zmienić widoczność warstw na mapie. Umożliwi to manipulację hierarchią wyświetlania obiektów, tak aby warstwa o wyższym priorytecie była wyświetlana na wierzchu, a warstwa o niższym priorytecie była na dole. 5. **Zmiana stopnia przeźroczystości warstw** – użytkownik powinien mieć możliwość dostosowania **przeźroczystości warstw**. Dzięki temu można lepiej dostosować widoczność obiektów na mapie i sprawić, że obiekty z różnych warstw będą widoczne jednocześnie, nie zasłaniając się nawzajem. Na przykład, użytkownik może zmniejszyć przezroczystość warstwy z mapą satelitarną, aby lepiej widzieć dane przestrzenne nakładające się na nią. 6. **Wyświetlanie informacji o warstwie** – użytkownik powinien mieć dostęp do szczegółowych informacji na temat danej warstwy. W ramach tego okna użytkownik będzie mógł uzyskać:    * **Opis warstwy**, wyjaśniający jej zawartość i przeznaczenie,    * **Adres usługi WMS**, WFS lub WMTS powiązanej z warstwą, co pozwala na integrację z innymi systemami GIS, 7. **Funkcjonalność przybliżenia do zasięgu warstwy** – użytkownik powinien mieć możliwość **przybliżenia mapy** do zakresu danej warstwy. Po aktywacji tej funkcji mapa automatycznie przejdzie do obszaru, który obejmuje wszystkie obiekty danej warstwy. Może to być szczególnie przydatne, gdy użytkownik chce dokładnie obejrzeć szczegóły obiektów zawartych w warstwie, takich jak granice działek, budynki czy inne elementy geograficzne.   Te funkcje pozwolą użytkownikowi na wygodne i elastyczne zarządzanie warstwami, umożliwiając lepsze dostosowanie widoku mapy do swoich potrzeb i uzyskanie pełnej kontroli nad prezentowanymi danymi. |
| 2.15. | **Legenda** to kluczowa funkcjonalność geoportalu, która powinna umożliwiać użytkownikowi zrozumienie zastosowanych symboli graficznych na mapie, ułatwiając interpretację danych przestrzennych i poprawiając ogólną użyteczność platformy. Legenda powinna być dostosowana do specyfiki wyświetlanych warstw, umożliwiając użytkownikowi szybki dostęp do informacji o symbolice mapy oraz pozwalając na dynamiczne zarządzanie warstwami. Funkcjonalność legendy powinna obejmować następujące cechy:   1. **Wyświetlenie okna legendy z objaśnieniami symboli** – **Legenda** powinna być prezentowana w formie okna, które zawiera szczegółowe objaśnienia symboli graficznych wykorzystywanych w aktualnie widocznych warstwach mapy. Okno to będzie przedstawiało kluczowe elementy wizualne, takie jak:    * Kolory i symbole reprezentujące różne typy obiektów (np. granice działek, rodzaje zabudowy, typy dróg),    * Linie, punkty i poligony używane do reprezentowania obiektów przestrzennych,    * Ikony i inne elementy graficzne wykorzystywane do oznaczenia obiektów lub kategorii danych (np. oznaczenia miejscowych planów zagospodarowania przestrzennego, obiektów użyteczności publicznej). 2. Dzięki tej funkcji użytkownicy będą mogli szybko dowiedzieć się, co oznaczają konkretne elementy na mapie. 3. **Dynamiczna legenda** – legenda powinna być **dynamiczna**, co oznacza, że jej zawartość będzie automatycznie dostosowywać się do aktualnie wyświetlanych warstw mapy. Jeżeli użytkownik włącza lub wyłącza warstwy, legenda powinna natychmiastowo aktualizować się, pokazując tylko te symbole, które są związane z widocznie warstwami. W ten sposób użytkownicy zobaczą tylko te objaśnienia, które są bezpośrednio związane z danymi, które aktualnie analizują. 4. **Możliwość włączania/wyłączania warstw z poziomu legendy** – funkcjonalność legendy powinna umożliwiać **włączanie i wyłączanie warstw** bezpośrednio z okna legendy. Dzięki temu użytkownicy mogą szybko zarządzać widocznością poszczególnych warstw, co pozwala na lepszą kontrolę nad tym, które dane są wyświetlane na mapie. Przełączanie warstw z poziomu legendy będzie intuicyjne, za pomocą checkboxów lub ikon przy każdej warstwie, co pozwala na łatwe włączenie lub wyłączenie warstwy i natychmiastowe zobaczenie efektów na mapie. 5. **Grupowanie warstw w legendzie** – w przypadku, gdy geoportal obsługuje dużą liczbę warstw, legenda powinna umożliwiać **grupowanie warstw w foldery** lub kategorie tematyczne. Na przykład, wszystkie warstwy związane z infrastrukturą (drogi, sieć wodociągowa, oświetlenie) mogą być grupowane razem, podczas gdy warstwy geograficzne (granice administracyjne, ukształtowanie terenu) będą miały swoją osobną grupę. Takie grupowanie pomoże użytkownikom szybciej odnaleźć odpowiednie warstwy i zrozumieć ich związki. 6. **Zoptymalizowany układ legendy** – okno legendy powinno być zaprojektowane w sposób umożliwiający łatwe przeglądanie, bez zasłaniania istotnych obszarów mapy. Może to obejmować możliwość **przesuwania okna legendy**, zmiany jego rozmiaru lub minimalizacji. Dodatkowo, legenda powinna mieć możliwość **automatycznego dostosowania rozmiaru** w zależności od liczby widocznych warstw, aby nie zajmowała zbyt dużo miejsca na ekranie, zachowując równocześnie pełną czytelność. 7. **Łatwość dostosowania** – użytkownicy powinni mieć możliwość łatwego **dostosowania legendy do swoich potrzeb**, np. poprzez zmianę układu warstw, sortowanie symboli, dostosowywanie stylów czy skalowania ikonek w legendzie. Tego typu funkcjonalność zwiększa wygodę korzystania z geoportalu, szczególnie w przypadku bardziej złożonych map z dużą liczbą warstw. |
| 2.16. | **Dodawanie warstw** geoportal powinien posiadać funkcjonalność,, która umożliwia użytkownikowi wzbogacenie mapy o własne dane przestrzenne. Dzięki tej opcji użytkownik może dodać różnorodne warstwy w popularnych formatach, co pozwala na jeszcze lepsze dostosowanie widoku mapy do swoich potrzeb i specyficznych wymagań. Geoportal powinien wspierać dodawanie warstw w następujących formatach:   1. **WMS (Web Map Service) / WFS (Web Feature Service)** – użytkownik powinien mieć możliwość dodawania warstw w formacie **WMS** lub **WFS**, co pozwala na integrację z zewnętrznymi źródłami mapowymi.    * **WMS** umożliwia dodanie mapy jako obrazu rastrowego, generowanego przez serwer na podstawie zapytania użytkownika, co może obejmować różnorodne mapy, takie jak mapy topograficzne, ortofotomapy czy mapy tematyczne.    * **WFS** pozwala na dodanie warstw wektorowych, takich jak punkty, linie i poligony, które można później wykorzystać do analizy przestrzennej lub dalszej obróbki danych.   Użytkownicy będą mogli wprowadzić adres URL usługi WMS/WFS oraz ewentualnie dostarczyć wymagane parametry, takie jak wersja usługi czy identyfikator warstwy, by dodać je do mapy. Funkcjonalność ta zapewni elastyczność, umożliwiając korzystanie z szerokiego zakresu usług GIS dostępnych w Internecie lub wewnętrznych zasobów organizacji.   1. **GeoJSON** – użytkownik powinien mieć możliwość dodawania własnych warstw w formacie **GeoJSON**, który jest popularnym formatem do przechowywania i wymiany danych geograficznych. GeoJSON jest szczególnie wygodny w przypadku pracy z danymi wektorowymi, takimi jak granice działek, linie dróg, punkty interesów (POI) czy inne obiekty przestrzenne. Dodawanie warstw w tym formacie umożliwia łatwą wizualizację i dalsze przetwarzanie danych, np. poprzez filtrowanie, analizowanie lub edytowanie obiektów. 2. **GPX (GPS Exchange Format)** – użytkownicy powinni mieć możliwość dodawania warstw w formacie **GPX**, który jest powszechnie stosowany w przypadku wymiany danych GPS. Format ten jest idealny do dodawania tras, punktów trasy lub szlaków turystycznych, a także do integracji danych z urządzeń GPS. Dzięki tej funkcjonalności, geoportal będzie w stanie wyświetlić dane GPS, umożliwiając na przykład przedstawienie tras przejazdów, pieszych wędrówek czy szlaków rowerowych na mapie. 3. **KML (Keyhole Markup Language)** – geoportal powinien także obsługiwać **format KML**, popularny w aplikacjach Google Earth, który umożliwia dodanie warstw zawierających różnorodne dane przestrzenne. W KML przechowywane są m.in. informacje o punktach, liniach, poligonach, a także o animacjach i innych elementach wizualnych. Użytkownicy będą mogli dodawać pliki KML, co umożliwi łatwe udostępnianie danych geograficznych oraz ich integrację z innymi aplikacjami. 4. **Możliwość dodawania danych z dysku użytkownika** – geoportal powinien umożliwiać użytkownikom dodawanie warstw również **z lokalnego dysku**. Powinno to obejmować wczytywanie plików w różnych formatach, takich jak GeoJSON, GPX, KML czy shapefile. Użytkownicy będą mogli łatwo przesłać plik z własnego komputera i wyświetlić go na mapie, co jest szczególnie przydatne, gdy dane są lokalnie przechowywane i nie są dostępne w zewnętrznych serwisach.   Dzięki powyższym funkcjom użytkownicy będą mieli pełną swobodę w dodawaniu, zarządzaniu i edytowaniu danych przestrzennych na mapie, co pozwoli na dostosowanie geoportalu do indywidualnych potrzeb i specyficznych wymagań projektów. |
| 2.17. | **Pomiary** funkcjonalność geoportalu, która powinna umożliwiać użytkownikowi dokładne wykonywanie pomiarów przestrzennych na mapie. Dzięki tym narzędziom, użytkownicy będą mogli łatwo obliczać długości, powierzchnie, a także usuwać pomiary. Funkcjonalność pomiarów powinna obejmować następujące elementy:   1. **Pomiar długości** – użytkownik powinien mieć możliwość **pomiaru długości** dowolnych odcinków na mapie. Funkcjonalność ta pozwala na dokładne obliczanie odległości pomiędzy dwoma punktami lub długości wybranej ścieżki, np. drogi, ścieżki turystycznej czy granicy działki. Pomiar powinien być intuicyjny, realizowany poprzez kliknięcie na mapie w punktach początkowym i końcowym, a wynik powinien być wyświetlany w jednostkach takich jak metry, kilometry. 2. **Pomiar powierzchni** – funkcjonalność **pomiaru powierzchni** powinna pozwalać użytkownikowi na obliczenie powierzchni zamkniętych obszarów na mapie. Użytkownik może wybrać obszar, np. działkę, park, obszar zabudowy, rysując wokół niego kontur (wielokąt) i uzyskując wynik powierzchni w jednostkach takich jak metry kwadratowe, czy hektary. 3. **Czyszczenie pomiarów** – użytkownik powinien mieć możliwość **usunięcia** wykonanych pomiarów z mapy. Funkcja czyszczenia pozwala na eliminację wcześniejszych pomiarów, co jest przydatne w sytuacjach, gdy użytkownik chce rozpocząć nowy pomiar lub gdy poprzedni wynik jest już nieaktualny. Możliwość czyszczenia pomiarów zapewnia porządek na mapie i umożliwia bardziej efektywne korzystanie z narzędzi pomiarowych. 4. **Przyciąganie do obiektów (precyzyjne pomiary)** – dla uzyskania **precyzyjnych pomiarów**, powinna być dostępna funkcjonalność umożliwiająca przyciąganie pomiarów do istniejących obiektów na mapie. Przy użyciu tej opcji użytkownik może wykonać dokładne pomiary, które będą automatycznie **przyciągane** do wybranych obiektów, takich jak granice działek, budynki, drogi czy inne obiekty przestrzenne z dostępnych warstw. Przyciąganie do obiektów umożliwia większą dokładność pomiaru, eliminując błędy związane z ręcznym umieszczaniem punktów pomiarowych. Na przykład, przy pomiarze długości granicy działki, system może automatycznie „przyciągnąć” punkty pomiarowe do dokładnych granic obiektu, zapewniając, że pomiar jest zgodny z rzeczywistymi granicami na mapie. |
| 2.18. | **Szkicowanie** to funkcjonalność geoportalu, która powinna umożliwiać użytkownikowi tworzenie i rysowanie obiektów na mapie w celu przedstawienia nowych danych przestrzennych. Dzięki tej opcji użytkownicy mogą dodawać własne elementy do mapy w różnych formatach, takich jak punkty, linie czy obszary, a także dostosować ich wygląd i wykorzystać dane z innych warstw. Funkcjonalność szkicowania powinna obejmować następujące elementy:   1. **Rysowanie obiektów punktowych, liniowych i powierzchniowych** – użytkownik powinien mieć możliwość rysowania **obiektów punktowych**, **liniowych** oraz **powierzchniowych** na mapie.    * **Obiekty punktowe** mogą być używane do zaznaczania konkretnych punktów na mapie, takich jak miejsca interesu (np. punkty dostępu do drogi, źródła wody, miejsca budowy).    * **Obiekty liniowe** umożliwiają rysowanie linii, np. dróg, granic działek, ścieżek rowerowych czy przebiegów instalacji podziemnych.    * **Obiekty powierzchniowe** pozwalają na rysowanie poligonów, które mogą reprezentować obszary, takie jak działki, tereny zielone, obszary zabudowy czy strefy ochrony środowiska. 2. **Definiowanie symbolizacji dla wrysowanych obiektów** – użytkownik powinien mieć możliwość **definiowania symbolizacji** (wyglądu) dla wrysowanych obiektów. Obejmuje to możliwość wyboru kolorów, typów linii, wypełnienia obszarów 3. **Kopiowanie obiektów z innych warstw i wykorzystanie ich jako elementy szkicu** – geoportal powinien umożliwiać użytkownikowi **kopiowanie obiektów** z innych warstw mapy, które będą mogły zostać wykorzystane jako elementy szkicu. Na przykład, użytkownik może skopiować **granice działek** z warstwy wektorowej, a następnie edytować je. Funkcja ta ułatwia korzystanie z już istniejących danych, pozwalając na ich wykorzystanie w nowych kontekstach, bez konieczności tworzenia nowych obiektów od podstaw. |
| 2.19. | **Drukowanie** to funkcjonalność geoportalu, która powinna umożliwiać użytkownikom generowanie i drukowanie map w różnych formatach, umożliwiając dalsze wykorzystanie fizyczne lub prezentację wyników na papierze. Funkcjonalność ta powinna obejmować następujące elementy:   * funkcjonalność drukowania mapy wg określonego szablonu drukowania (format A4, A4, A2, A1), * możliwość ustawienia orientacji arkusza wydruku: poziomo, pionowo oraz pod dowolnym kątem, * funkcjonalność przesuwania arkusza wydruku na mapie, arkusz powinien być zaznaczony np., w postaci prostokąta, aby obrazować jakiego obszaru dotyczy, * drukowanie powinno być możliwe dla wszystkich warstw dostępnych w geoportalu, włącznie z obiektami narysowanymi narzędziem szkicowania. |
| 2.20. | **Link do widoku mapy**   * Możliwość wygenerowania linku URL lub kodu QR do aktualnego widoku mapy, widok powinien zapamiętywać skale, przybliżenie nad wybrany fragment mapy oraz układ warstw. |
| 2.27. | **Logowanie**  Musi być możliwość logowania do Geoportalu. W zależności od posiadanych uprawnień użytkownicy mogą posiadać dostęp do danych wymagających autoryzacji. |
| 2.28. | **Edycja danych** w geoportalu powinna umożliwiać wybranym użytkownikom modyfikowanie zarówno danych przestrzennych, jak i opisowych, zapewniając pełną kontrolę nad danymi oraz ich aktualizację. Funkcjonalność edycji danych jest kluczowa, aby zapewnić dynamiczność i aktualność informacji dostępnych na geoportalu, a także wspierać procesy zarządzania danymi geograficznymi. Oto szczegółowy opis funkcji, które powinny być dostępne w ramach edycji danych:  **1. Edytowanie danych przestrzennych**   * **Edycja obiektów wektorowych**: Użytkownicy powinni mieć możliwość modyfikowania istniejących obiektów wektorowych na mapie (punktów, linii, poligonów). Funkcje edycji powinny obejmować:   + **Przemieszczanie obiektów** – możliwość zmiany lokalizacji obiektów na mapie poprzez przesunięcie punktów, linii lub całych poligonów,   + **Zmiana kształtu obiektów** – możliwość dodawania, usuwania lub modyfikowania wierzchołków (np. w poligonach czy liniach),   + **Tworzenie nowych obiektów** – możliwość rysowania nowych obiektów (punktów, linii, poligonów) na mapie.   **2. Edycja danych opisowych**   * **Modyfikacja atrybutów obiektów**: Użytkownicy powinni mieć możliwość edytowania atrybutów obiektów geograficznych, takich jak:   + **Dodawanie/edycja wartości atrybutów** – możliwość zmiany danych opisowych, np. adresów, numerów działek, typów budynków,   + **Tworzenie nowych atrybutów** – administratorzy powinni mieć możliwość dodawania nowych atrybutów do istniejących obiektów,   + **Usuwanie atrybutów** – możliwość usuwania zbędnych atrybutów z obiektów.   **3. Zarządzanie uprawnieniami do edycji**   * **Różne poziomy dostępu**: Edycja danych powinna być dostępna tylko dla uprawnionych użytkowników, którzy zostali przypisani do odpowiednich ról (np. administratorzy, redaktorzy). Użytkownicy powinni mieć różne poziomy dostępu do edycji danych:   + **Pełne uprawnienia** – umożliwiające pełną edycję danych przestrzennych i opisowych,   + **Ograniczone uprawnienia** – pozwalające na edycję tylko wybranych warstw lub obiektów,   + **Brak uprawnień** – użytkownicy bez możliwości edytowania danych. |
| 2.29. | **Serwer map** - w ramach wdrożenia powinien zostać dostarczony serwer map, który powinien obsługiwać różne standardy i technologie, umożliwiające skuteczne zarządzanie i udostępnianie danych przestrzennych. Jego zadaniem jest dostarczenie elastycznych rozwiązań do publikacji, udostępniania i analizy danych geograficznych, wspierając różne formaty i protokoły. Oto szczegółowy opis wymagań dla serwera map:   1. **WMS - Web Map Service** Serwer powinien obsługiwać standard **WMS (Web Map Service)**, który umożliwia dostarczanie map rastrowych (zdjęć, obrazów) w czasie rzeczywistym przez sieć. Dzięki WMS użytkownicy będą mogli za pomocą przeglądarek GIS lub innych aplikacji wyświetlać mapy bazujące na różnych źródłach danych. WMS zapewnia:    * Możliwość wyświetlania map z różnych warstw (np. ortofotomap, map topograficznych, map tematycznych),    * Obsługę zapytań o określony obszar, skale czy formaty graficzne (np. PNG, JPEG),    * Integrację z różnymi aplikacjami i systemami GIS. 2. **WFS - Web Feature Service** Serwer powinien również wspierać standard **WFS (Web Feature Service)**, który umożliwia dostęp do danych wektorowych w postaci obiektów geograficznych. WFS pozwala na:    * Udostępnianie danych wektorowych w formie punktów, linii i poligonów,    * Możliwość pobierania danych w czasie rzeczywistym w formacie XML (GML),    * Wykonywanie zapytań atrybutowych, co pozwala na interakcję z danymi, np. filtrowanie obiektów na podstawie ich właściwości. 3. **CSW – Catalog Service for the Web** Serwer powinien obsługiwać także standard **CSW (Catalog Service for the Web)**, który umożliwia katalogowanie i wyszukiwanie zasobów danych geograficznych. Dzięki CSW możliwe będzie:    * Publikowanie metadanych geograficznych (opisów danych, ich pochodzenia, jakości itp.),    * Udostępnianie zasobów przestrzennych przez wyszukiwarki katalogów, co ułatwi odnalezienie odpowiednich zasobów danych w sieci,    * Integracja z innymi systemami katalogów danych przestrzennych. 4. **Obsługiwane formaty danych** Serwer map powinien obsługiwać przynajmniej następujące formaty danych, zapewniając wszechstronność i kompatybilność z różnymi źródłami i aplikacjami:    * **PostGIS** – rozszerzenie bazy danych PostgreSQL, umożliwiające przechowywanie, analizowanie i zarządzanie danymi przestrzennymi. PostGIS obsługuje szeroki zakres operacji geograficznych, takich jak obliczanie odległości, analiza przestrzenna czy przekształcanie współrzędnych.    * **Shapefile** – jeden z najpopularniejszych formatów wektorowych wykorzystywany w systemach GIS, wspierający przechowywanie danych wektorowych, takich jak punkty, linie i poligony. Shapefile jest szeroko stosowany w wielu aplikacjach GIS.    * **Oracle Spatial** – rozszerzenie bazy danych Oracle, które zapewnia funkcje zarządzania danymi przestrzennymi. Umożliwia przechowywanie, przetwarzanie i analizowanie danych geograficznych w bazie danych, oferując zaawansowane narzędzia analityczne.    * **GeoTiff** – format rastrowy, który przechowuje dane przestrzenne z dodatkowymi informacjami o georeferencji. GeoTiff jest wykorzystywany do przechowywania obrazów satelitarnych, ortofotomap, map topograficznych i innych danych przestrzennych w postaci rastrów. 5. **Elastyczność i kompatybilność** Serwer map powinien być elastyczny i kompatybilny z różnymi aplikacjami GIS, umożliwiając integrację z popularnymi narzędziami GIS, oraz umożliwiać korzystanie z usług opartych na standardach OGC (Open Geospatial Consortium). Dzięki temu użytkownicy będą mogli w łatwy sposób udostępniać i analizować dane przestrzenne w różnych aplikacjach i systemach. 6. **Zabezpieczenia i dostępność** Serwer powinien również zapewniać odpowiednie mechanizmy zabezpieczające dostęp do danych, takie jak:    * **Autoryzacja i uwierzytelnianie użytkowników**, co pozwala na kontrolowanie, kto ma dostęp do danych i usług,    * **Monitoring i logowanie** dostępu do usług, co ułatwia zarządzanie bezpieczeństwem i identyfikację ewentualnych nieprawidłowości,    * **Wysoka dostępność i skalowalność** – serwer powinien być zaprojektowany tak, aby zapewniał dostępność usług 24/7, a także skalowanie w zależności od obciążenia.   Serwer map pełni kluczową rolę w udostępnianiu i zarządzaniu danymi geograficznymi, umożliwiając efektywną pracę z danymi przestrzennymi w systemach GIS. Wdrożenie takiego serwera zapewni elastyczność i wszechstronność w pracy z danymi, umożliwiając ich szeroką dystrybucję i analizę. |
| 2.30. | **Zarządzanie geoportalem** powinno być prostym i intuicyjnym procesem, dostosowanym do potrzeb administratorów, którzy zarządzają i utrzymują portal w trybie online. Panel administracyjny geoportalu powinien umożliwiać pełną kontrolę nad wszystkimi jego funkcjonalnościami i danymi, a także umożliwiać sprawne zarządzanie użytkownikami oraz zasobami, bez konieczności instalowania dodatkowych komponentów lub oprogramowania. Oto szczegółowy opis funkcji, które powinien zawierać system zarządzania geoportalem:  **1. Dostęp online**   * **Panel administracyjny** powinien być dostępny **z poziomu przeglądarki internetowej**, co pozwala administratorom na zarządzanie systemem z dowolnego miejsca, bez konieczności instalacji dodatkowych aplikacji lub narzędzi. * Panel powinien być **bezpieczny i chroniony** przed nieautoryzowanym dostępem, zapewniając stosowne mechanizmy uwierzytelniania (np. login i hasło, 2FA).   **2. Zarządzanie użytkownikami**   * **Tworzenie i zarządzanie kontami użytkowników**: Administrator powinien mieć możliwość dodawania, edytowania i usuwania kont użytkowników, nadawania im odpowiednich ról oraz uprawnień. * **Przydzielanie ról i uprawnień**: Administrator może przypisać różne poziomy dostępu, np. użytkownik, moderator, administrator, co pozwala kontrolować dostęp do poszczególnych funkcji geoportalu. * **Monitorowanie aktywności użytkowników**: Panel administracyjny powinien umożliwiać monitorowanie aktywności użytkowników w systemie (np. logi logowania).   **3. Zarządzanie danymi**   * **Dodawanie i edytowanie warstw mapowych**: Administratorzy powinni mieć możliwość dodawania nowych warstw mapowych do geoportalu, edytowania ich właściwości (np. zmiana symboliki, opisu, metadanych), a także usuwania warstw. * **Zarządzanie danymi przestrzennymi**: Powinna istnieć możliwość zarządzania danymi wektorowymi i rastrowymi oraz ustawiania praw dostępu do tych danych (np. widoczność publiczna, prywatna). * **Zarządzanie bazami danych**: Administratorzy powinni mieć dostęp do narzędzi umożliwiających zarządzanie bazami danych przestrzennych.   **4. Zarządzanie warstwami mapy**   * **Tworzenie i edytowanie grup warstw**: Panel administracyjny powinien umożliwiać organizowanie warstw w grupy i foldery, aby ułatwić ich zarządzanie i organizację. * **Ustawianie priorytetów wyświetlania warstw**: Administrator powinien mieć możliwość ustawiania kolejności wyświetlania warstw na mapie, co ma wpływ na to, które warstwy będą wyświetlane na wierzchu. * **Konfiguracja widoczności warstw**: Możliwość przypisania reguł widoczności dla warstw w zależności od kryteriów (np. zoom, region geograficzny).   **5. Zarządzanie mapami tematycznymi**   * **Tworzenie i edytowanie map tematycznych**: Administrator powinien mieć możliwość tworzenia i konfigurowania map tematycznych (np. mapy dla poszczególnych typów użytkowników, mapy projektów). Powinna istnieć możliwość przełączania się między różnymi mapami tematycznymi bez konieczności przeładowywania geoportalu. * **Dostosowanie mapy do potrzeb użytkowników**: Administrator powinien mieć możliwość ustawiania domyślnych map tematycznych i ich układów, które będą wyświetlane dla różnych grup użytkowników.   **6. Zarządzanie funkcjonalnościami geoportalu**   * **Zarządzanie narzędziami interaktywnymi**: Administrator powinien mieć możliwość zarządzania dostępnością i konfiguracją narzędzi interaktywnych, takich jak narzędzie pomiarowe, narzędzie do szkicowania, wyszukiwania obiektów na mapie itp. * **Konfigurowanie filtrów i wyszukiwania**: Możliwość tworzenia i edytowania filtrów do danych oraz konfigurowania narzędzi wyszukiwania w celu ułatwienia użytkownikom dostępu do danych przestrzennych.   Dzięki tym funkcjonalnościom, panel administracyjny geoportalu będzie narzędziem umożliwiającym efektywne zarządzanie całym środowiskiem geoportalu w sposób wygodny, bezpieczny i bez potrzeby instalacji dodatkowych komponentów. |

### 1.4.3 Wymagania dotyczące modułów dziedzinowych

|  |  |
| --- | --- |
| Nr | Opis wymagania |
| 3.1 | **Moduł – MPZP,  Studium oraz Plan Ogólny**  Moduł będący integralną częścią systemu GIS w zakresie zarządzania informacją przestrzenną, dotyczącą Miejscowych Planów Zagospodarowania Przestrzennego (MPZP),  Studium Uwarunkowań i Kierunków Zagospodarowania Przestrzennego (Studium) oraz Plan Ogólny. Moduł ten zapewnia kompleksową obsługę i analizę danych planistycznych oraz umożliwia użytkownikom szybki i intuicyjny dostęp do informacji przestrzennych.  **Główne funkcjonalności modułu:**   * **Dostęp przez przeglądarkę internetową** – moduł działa w trybie online bez konieczności instalacji dodatkowego oprogramowania po stronie użytkownika. * **Możliwość wyświetlania warstw MPZP, Studium** **oraz Plan Ogólny** na tle innych warstw tematycznych dostępnych w systemie, w tym ortofotomapy, map ewidencyjnych, warstw środowiskowych i infrastrukturalnych. * **Generowanie dokumentów** – automatyczne tworzenie wyrysu, wypisu oraz zaświadczenia z MPZP, Studium oraz Planu Ogólnego na podstawie cyfrowych wersji dokumentów. * **Prowadzenie rejestru wydanych dokumentów**, takich jak wyrysy, wypisy i zaświadczenia, zarówno w formie tabelarycznej, jak i mapowej, z możliwością edycji, usuwania i rejestrowania nowych dokumentów,   + wyszukiwanie pozycji w rejestrze wydanych dokumentów, z możliwością sortowania oraz filtrowania danych,   + automatyczne generowanie gotowych raportów dla określonego okresu, uchwały oraz obszaru gminy. * **Interaktywne narzędzia do analizy informacji planistycznych:**   + **Informacja o działce** – po wskazaniu działki na mapie użytkownik uzyska szczegółowe informacje o wszystkich obowiązujących MPZP, które nachodzą na daną działkę, wraz z ich przeznaczeniem i parametrami zabudowy.   + **Wyszukiwanie działek** – możliwość odnalezienia działki po numerze, adresie lub identyfikatorze oraz uzyskania szczegółowych informacji dotyczących jej statusu planistycznego.   + **Prowadzenie rejestru MPZP MPZP, Studium** **oraz Plan Ogólny** – aktualizacja, zarządzanie i przeglądanie obowiązujących oraz archiwalnych dokumentów planistycznych w jednym miejscu.   + **Udostępnianie widoku mapy** – możliwość wygenerowania linku URL oraz kodu QR do konkretnego widoku mapy, ułatwiającego szybkie udostępnienie danych planistycznych innym użytkownikom.   **Funkcje nawigacyjne i interfejs użytkownika:**   * **Łatwa nawigacja po mapie:**   + Przybliżanie i oddalanie za pomocą suwaka oraz rolki myszki.   + Przesuwanie mapy w dowolnym kierunku.   + Zmiana skali mapy na dowolną wartość wskazaną przez użytkownika.   + Centrowanie mapy na wybraną warstwę tematyczną lub wyszukany obiekt.   + Miniatura mapy umożliwiająca szybkie przesuwanie i zmianę zasięgu widocznego obszaru.   + Możliwość cofania i przywracania poprzedniego widoku mapy (minimum 10 poziomów historii). * **Personalizacja mapy:**   + Swobodne komponowanie treści mapy – dodawanie, usuwanie oraz układanie warstw tematycznych.   + Możliwość zapisywania własnych kompozycji mapowych, uwzględniających wybrane warstwy, lokalizację oraz skalę mapy.   + Obsługa wielu warstw rastrowych i wektorowych, w tym możliwość wczytywania i usuwania wielu warstw jednocześnie.   + Zmiana kolejności warstw na mapie oraz regulacja ich przezroczystości.   + Możliwość włączania i wyłączania etykiet obiektów na żądanie użytkownika.   + Obsługa różnych układów współrzędnych, umożliwiająca precyzyjną analizę danych.   **Obsługa wydruków i raportów:**   * **Zaawansowane narzędzie do wydruku map:**   + Możliwość wydrukowania wybranego obszaru mapy w różnych formatach (np. PDF, PNG, JPG).   + Opcja dołączenia legendy oraz dostosowania parametrów wydruku.   + Generowanie kompletnego dokumentu wyrysu/wypisu/zaświadczenia z MPZP i Studium z możliwością wyboru zakresu informacji, formatu oraz dodatkowych elementów (np. pieczęci elektronicznej, opisu planu).   Moduł MPZP oraz Studium znacząco usprawnia dostęp do informacji planistycznych oraz umożliwia szybkie i precyzyjne analizy przestrzenne, wspierając użytkowników w procesach decyzyjnych. |
| 3.2 | **Moduł - Oś czasu.** Moduł będący integralną częścią systemu GIS, dedykowany do zarządzania informacją przestrzenną w kontekście archiwalnych dokumentów planistycznych. Moduł powinien umożliwiać analizę zmian zagospodarowania przestrzennego w czasie oraz szybki dostęp do historycznych wersji MPZP i Studium. Moduł powinien zawierać następujące funkcjonalności:   * **Dostępność poprzez przeglądarkę internetową** – możliwość  korzystania  z modułu bez konieczności instalacji dodatkowego oprogramowania. * **Prowadzenie rejestru archiwalnych MPZP i Studium** – system umożliwia przechowywanie uchwał w formie tabelarycznej i mapowej, z możliwością edycji, usuwania oraz dodawania nowych dokumentów planistycznych. * **Odczytywanie informacji o MPZP i Studium według stanu na wybraną datę** – użytkownicy mogą przeglądać dane historyczne i analizować zmiany w zagospodarowaniu przestrzennym. * **Obsługa załączników** – moduł pozwala na dodawanie oraz przeglądanie załączników powiązanych z dokumentami planistycznymi, zapewniając pełną archiwizację materiałów. * **Zaawansowane wyszukiwanie i filtrowanie** – system umożliwia szybkie odnalezienie pozycji w rejestrze archiwalnych MPZP i Studium na podstawie różnych kryteriów, a także sortowanie wyników. * **Wyświetlanie stanu zagospodarowania przestrzennego na wybraną datę** – użytkownicy mogą wizualizować dane w formie tabelarycznej oraz mapowej, analizując ich zmienność w czasie. * **Generowanie dokumentów według stanu na wybraną datę** – moduł umożliwia automatyczne generowanie wypisów, wyrysów oraz zaświadczeń, uwzględniając stan zagospodarowania przestrzennego na konkretny moment w przeszłości. * **Elastyczny wybór daty** – użytkownicy mogą wybrać datę poprzez ręczne wpisanie, skorzystanie z kalendarza lub ustawienie punktu na interaktywnej osi czasu, co ułatwia analizę historycznych danych. * **Przetwarzanie archiwalnych MPZP do postaci cyfrowej** – w ramach wdrożenia system umożliwia konwersję posiadanych przez Zamawiającego dokumentów planistycznych do formatu cyfrowego, co pozwala na ich dalsze przetwarzanie i analizę.   Dzięki tym funkcjonalnościom moduł **Oś czasu** stanowi kluczowe narzędzie do monitorowania i analizy zmian w zagospodarowaniu przestrzennym, wspierając procesy planistyczne oraz ułatwiając dostęp do historycznych danych. |
| 3.3 | **Moduł - Procedura planistyczna**  Moduł będący częścią systemu GIS, dedykowany do kompleksowego zarządzania informacją przestrzenną w zakresie procedur planistycznych. Umożliwia skuteczne monitorowanie, archiwizowanie i analizowanie procesów związanych z miejscowymi planami zagospodarowania przestrzennego (MPZP) oraz Studium uwarunkowań i kierunków zagospodarowania przestrzennego. Moduł powinien zawierać następujące funkcjonalności:   * **Dostępność poprzez przeglądarkę internetową** – użytkownicy mogą korzystać z modułu bez konieczności instalacji dodatkowego oprogramowania. * **Zarządzanie rejestrem procedur planistycznych** – system umożliwia prowadzenie bazy procedur z podziałem na aktualne i archiwalne, zapewniając łatwy dostęp do danych oraz możliwość ich edycji i przeglądania na mapie w odniesieniu do działek ewidencyjnych. * **Prowadzenie rejestru procedur na wszystkich etapach** – system pozwala na śledzenie postępu każdej procedury planistycznej od momentu jej rozpoczęcia aż do zakończenia. * **Wprowadzanie informacji o procedurze planistycznej** – użytkownicy mogą dodawać i edytować szczegółowe dane dotyczące procedury dla wskazanej działki ewidencyjnej, w tym:   + Rodzaj procedury planistycznej,   + Nazwę procedury,   + Datę rozpoczęcia procedury,   + Numer procedury,   + Aktualny status,   + Opis procedury,   + Szczegółowy wykaz etapów procedury wraz z ich terminami realizacji. * **Automatyczne importowanie wniosków** – moduł umożliwia automatyczne wczytywanie złożonych wniosków dotyczących zmiany lub sporządzenia MPZP lub Studium, przypisując je do właściwych działek w granicach procedury. * **Integracja z systemem mapowym** – użytkownicy mogą wizualizować procedury planistyczne na mapie oraz analizować ich wpływ na otoczenie i istniejące uwarunkowania przestrzenne. * **Powiadomienia o statusie procedury** – moduł może generować automatyczne powiadomienia o zmianie statusu procedury planistycznej, co ułatwia bieżące monitorowanie procesów. * **Generowanie raportów** – system umożliwia tworzenie szczegółowych raportów z przeprowadzonych procedur planistycznych, uwzględniających wszystkie etapy oraz podjęte działania. * **Historia zmian i archiwizacja dokumentacji** – moduł przechowuje historię operacji wykonywanych na poszczególnych procedurach oraz umożliwia archiwizację dokumentów powiązanych z procesem planistycznym. |
| 3.4 | **Moduł – Akty Planowania Przestrzennego (APP).** Moduł Akty Planowania Przestrzennego (APP) jest częścią systemu GIS, umożliwiającą kompleksowe zarządzanie dokumentami planistycznymi w zakresie miejscowych planów zagospodarowania przestrzennego (MPZP) oraz studiów uwarunkowań i kierunków zagospodarowania przestrzennego (SUiKZP). Moduł wspiera prowadzenie rejestru aktów planowania przestrzennego oraz ich prezentację w formie tabelarycznej i mapowej.  Funkcjonalności modułu   1. Prowadzenie rejestru APP    * Ewidencja obowiązujących oraz archiwalnych aktów planowania przestrzennego,    * Możliwość dodawania, edytowania i usuwania danych,    * Prezentacja dokumentów w układzie tabelarycznym oraz mapowym. 2. Zarządzanie dokumentami i załącznikami    * Możliwość dodawania tekstów uchwał, rysunków MPZP oraz innych dokumentów planistycznych w formacie PDF, DOC, JPG, TIFF,    * Odczytywanie i pobieranie załączników bezpośrednio z poziomu systemu. 3. Wyszukiwanie i filtrowanie danych    * Możliwość wyszukiwania aktów planistycznych według numeru uchwały, daty uchwalenia, statusu, obszaru obowiązywania,    * Filtrowanie dokumentów według wybranych kryteriów,    * Możliwość przeglądania historycznych wersji MPZP i SUiKZP. 4. Generowanie dokumentów i raportów    * Automatyczne tworzenie wypisów i wyrysów z MPZP na podstawie danych przestrzennych,    * Generowanie zaświadczeń o obowiązującym zagospodarowaniu terenu,    * Eksport danych do różnych formatów (PDF, GML, SHP). 5. Integracja z innymi systemami    * Możliwość integracji z systemami ewidencji gruntów i budynków (EGiB),    * Automatyczna weryfikacja aktualnego przeznaczenia działek ewidencyjnych na podstawie MPZP,    * Integracja z krajowym rejestrem aktów planowania przestrzennego (Rejestr Urbanistyczny). |
| 3.5 | **Moduł – sprawy.** Moduł będący integralną częścią systemu GIS, przeznaczony do kompleksowego zarządzania informacją przestrzenną dotyczącą spraw, wniosków i decyzji administracyjnych związanych z zagospodarowaniem przestrzennym. Moduł oferuje następujące funkcjonalności:   * **Dostępność poprzez przeglądarkę internetową** – użytkownicy mają możliwość pracy w systemie bez konieczności instalacji dodatkowego oprogramowania. * **Prowadzenie rejestru spraw** - system umożliwia prowadzenie rejestru spraw. Sprawy muszą być powiązane z wnioskami i decyzjami. Wymagana jest integracja spraw z Systemem Obiegu Dokumentów. * **Prowadzenie rejestru wniosków** - system umożliwia prowadzenie rejestru wniosków. Wnioski muszą być powiązane z sprawami i decyzjami. Wymagana jest integracja spraw z Systemem Obiegu Dokumentów. * **Prowadzenie rejestru decyzji** – system umożliwia prowadzenie bazy danych decyzji w formie tabelarycznej i mapowej. Rejestr jest powiązany z działkami ewidencyjnymi, co pozwala na szybkie i intuicyjne zarządzanie danymi. Decyzje muszą być powiązane z sprawami i wnioskami. Wymagana jest integracja spraw z Systemem Obiegu Dokumentów. * **Możliwość zarządzania decyzji** – użytkownicy posiadają uprawnienia do aktualizacji danych w rejestrze, co pozwala na bieżące uzupełnianie i modyfikowanie informacji. * **Obsługa załączników** – moduł umożliwia dodawanie oraz odczytywanie załączników związanych z poszczególnymi decyzjami, co pozwala na przechowywanie kompletnych dokumentacji w jednym miejscu. * **Wyszukiwanie działek ewidencyjnych** – użytkownicy mogą szybko odnaleźć działki ewidencyjne poprzez różne kryteria wyszukiwania. System automatycznie odczytuje pełne informacje o zagospodarowaniu przestrzennym danej działki, co usprawnia proces analizy. * **Integracja z aplikacją dziedzinową dotyczącą miejscowych planów zagospodarowania przestrzennego (MPZP)** – system automatycznie weryfikuje aktualne przeznaczenie działki w oparciu o obowiązujące uchwały MPZP, co minimalizuje ryzyko błędów i usprawnia proces decyzyjny. * **Generowanie dokumentów** – moduł oferuje funkcję automatycznego generowania decyzjach na podstawie predefiniowanych szablonów. Dokumenty są gotowe do wydruku lub eksportu w formacie elektronicznym, co przyspiesza obsługę administracyjną. * **Zaawansowana analiza przestrzenna** – użytkownicy mogą korzystać z narzędzi analitycznych pozwalających na ocenę wpływu decyzji na otaczające środowisko i istniejącą zabudowę.   Dzięki powyższym funkcjonalnościom moduł **Decyzje** znacząco usprawnia proces zarządzania decyzjami administracyjnymi w kontekście zagospodarowania przestrzennego, zapewniając szybki dostęp do informacji, automatyzację kluczowych procesów oraz pełną integrację z innymi systemami GIS. |

### 1.4.4 Wymagania dotyczące digitalizacji danych

|  |  |
| --- | --- |
| Nr | Opis wymagania |
| 4.1. | **Digitalizacja Miejscowych Planów Zagospodarowania Przestrzennego (MPZP) 87 szt. oraz digitalizacja przystąpień dla dokumentów planistycznych w tym MPZP – 1 szt.**  **Zakres digitalizacji** Proces digitalizacji obejmuje zarówno aktualne, jak i archiwalne dokumenty planistyczne, w tym:   * **Opracowanie rejestru MPZP** zgodnie z wymogami Rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 26 października 2020 r. w sprawie zbiorów danych przestrzennych oraz metadanych dotyczących zagospodarowania przestrzennego. * **Utworzenie plików GML** dla obowiązujących Miejscowych Planów Zagospodarowania Przestrzennego (MPZP), uwzględniając ich zmiany. * **Tworzenie zbiorów danych przestrzennych** dla obowiązujących MPZP, zgodnie z obowiązującymi standardami.   **Źródła danych**  Digitalizacja MPZP zostanie przeprowadzona na podstawie materiałów źródłowych przekazanych przez Zamawiającego, obejmujących:   * Wykaz uchwał MPZP; * Rysunki planów w wersji analogowej,  oraz elektronicznej; * Teksty uchwał w wersji edytowalnej lub elektronicznej (skan dokumentu)   **Przetwarzanie dokumentów**   * Wykonawca zeskanuje do postaci rastrowej (JPG, PDF, TIFF) wszystkie rysunki MPZP przekazane przez Zamawiającego, które są dostępne jedynie w wersji analogowej lub których cyfrowe wersje są nieczytelne i nienadające się do wektoryzacji. * Digitalizacja wszystkich aktualnych i archiwalnych uchwał dotyczących MPZP do postaci cyfrowej zgodnej z wymogami Ustawy o Infrastrukturze Informacji Przestrzennej. * Kalibracja rastrów i zapis w formacie GeoTIFF (układ 2000), skadrowany do granic planu. * Wektoryzacja MPZP na podstawie skalibrowanego rastra, obejmująca utworzenie warstw:   + **MPZP zasięgi** (warstwa poligonowa), zawierająca atrybuty: ID, nazwa gminy, nazwa skrócona i pełna planu, numer uchwały, data uchwalenia, powierzchnia, typ uchwały, status, , numer i data Dziennika Urzędowego.   + **MPZP przeznaczenia terenu** (warstwa poligonowa) z atrybutami opisowymi: ID, numer uchwały, kod przeznaczenia (ustandaryzowany), symbol i opis przeznaczenia.   + **MPZP ustalenia dodatkowe punktowe, liniowe i powierzchniowe** (warstwy odpowiednio punktowa, liniowa i poligonowa) wraz z opisowymi atrybutami: ID, numer uchwały, kod obiektu (ustandaryzowany), symbol i opis przeznaczenia.   **Wymogi techniczne**   * Zachowanie reguł topologicznych – brak szczelin, nakładających się obiektów, duplikatów i niepoprawnych geometrii. * Dokładność wektoryzacji ≤ 0,5 mm w skali mapy. * Obiekty muszą być spójne topologicznie – przeznaczenia oraz ustalenia dodatkowe nie mogą wykraczać poza granicę zasięgu planu i powinny być dociągnięte do wierzchołków działek ewidencyjnych.   **Symbolizacja i wizualizacja**   * Wykonawca przygotuje **symbolizację i etykietowanie** warstw zgodnie z załącznikiem nr 1 do Rozporządzenia Ministra Rozwoju i Technologii z dnia 17 grudnia 2021 r. w sprawie zakresu projektu MPZP. * Symbolizacja zostanie zapisana do plików warstw (.qml/.qlr), uwzględniając zarówno standardowe oznaczenia, jak i dostosowanie do oryginalnych rysunków MPZP, uzgodnione z Zamawiającym. * Symbolika warstw wektorowych będzie **nieskalowalna (jednostki mapy)** – grubości linii będą dostosowywać się do zmiany skali.   **Produkty digitalizacji**   * Przetworzenie treści uchwał MPZP do postaci cyfrowej i ich powiązanie z wektorowymi elementami planu, umożliwiając automatyczne generowanie wypisów i zaświadczeń. * Import zdigitalizowanych danych do systemu GIS oraz przekazanie plików obejmujących:   + Warstwy wektorowe w układzie 2000, (granice planów, przeznaczenia terenu, obiekty powierzchniowe, liniowe i punktowe).   + Rastry w formacie GeoTIFF.   Dzięki temu procesowi wszystkie dane MPZP zostaną uporządkowane, ustandaryzowane i dostępne w postaci cyfrowej, zgodnej z obowiązującymi przepisami i wymogami technicznymi. |
| 4.2. | **Digitalizacja Studium Uwarunkowań i Kierunków Zagospodarowania Przestrzennego (Studium) – 5 szt.**  **Zakres digitalizacji**  Proces digitalizacji obejmuje zarówno aktualne, jak i archiwalne dokumenty planistyczne, w tym:   * **Opracowanie rejestru Studium** zgodnie z wymogami Rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 26 października 2020 r. w sprawie zbiorów danych przestrzennych oraz metadanych dotyczących zagospodarowania przestrzennego. * **Tworzenie zbiorów danych przestrzennych** dla obowiązującego Studium, zgodnie z obowiązującymi standardami.   **Źródła danych**  Digitalizacja Studium zostanie przeprowadzona na podstawie materiałów źródłowych przekazanych przez Zamawiającego, obejmujących:   * Wykaz uchwał Studium. * Rysunki studium w wersji analogowej,  oraz elektronicznej * Teksty uchwał w wersji edytowalnej lub elektronicznej (skan dokumentu)   **Przetwarzanie dokumentów**   * Wykonawca zeskanuje do postaci rastrowej (JPG, PDF, TIFF) wszystkie rysunki Studium przekazane przez Zamawiającego, które są dostępne jedynie w wersji analogowej lub których cyfrowe wersje są nieczytelne i nienadające się do wektoryzacji. * Digitalizacja aktualnej  uchwały dotyczącej Studium do postaci cyfrowej zgodnej z wymogami Ustawy o Infrastrukturze Informacji Przestrzennej. * Kalibracja rastrów i zapis w formacie GeoTIFF (układ 2000), skadrowany do granic studium. * Wektoryzacja Studium na podstawie skalibrowanego rastra, obejmująca utworzenie warstw:   + **Studium zasięgi** (warstwa poligonowa), zawierająca atrybuty: ID, nazwa gminy, nazwa skrócona i pełna planu, numer uchwały, data uchwalenia, powierzchnia, typ uchwały, status, , numer i data Dziennika Urzędowego.   + **Studium Kierunki - przeznaczenia terenu** (warstwa poligonowa) z atrybutami opisowymi: ID, numer uchwały, kod przeznaczenia (ustandaryzowany), symbol i opis przeznaczenia.   **Wymogi techniczne**   * Zachowanie reguł topologicznych – brak szczelin, nakładających się obiektów, duplikatów i niepoprawnych geometrii. * Dokładność wektoryzacji ≤ 0,5 mm w skali mapy. * Obiekty muszą być spójne topologicznie – przeznaczenia oraz ustalenia dodatkowe nie mogą wykraczać poza granicę zasięgu studium i powinny być dociągnięte do wierzchołków działek ewidencyjnych.   **Symbolizacja i wizualizacja**   * Symbolizacja zostanie zapisana do plików warstw (.qml/.qlr), uwzględniając zarówno standardowe oznaczenia, jak i dostosowanie do oryginalnych rysunków Studium, uzgodnione z Zamawiającym. * Symbolika warstw wektorowych będzie **nieskalowalna (jednostki mapy)** – grubości linii będą dostosowywać się do zmiany skali.   **Produkty digitalizacji**   * Przetworzenie treści uchwał Studium do postaci cyfrowej i ich powiązanie z wektorowymi elementami planu, umożliwiając automatyczne generowanie wypisów i zaświadczeń. * Import zdigitalizowanych danych do systemu GIS oraz przekazanie plików obejmujących:   + Warstwy wektorowe w układzie 2000, (granice planów, przeznaczenia terenu, obiekty powierzchniowe, liniowe i punktowe).   + Rastry w formacie GeoTIFF.   Dzięki temu procesowi wszystkie dane Studium zostaną uporządkowane, ustandaryzowane i dostępne w postaci cyfrowej, zgodnej z obowiązującymi przepisami i wymogami technicznymi. |
| 4.3. | **Digitalizacja rejestru decyzji o Warunkach Zabudowy (WZ) oraz decyzji o Ustaleniu Lokalizacji Inwestycji Celu Publicznego (ULICP)**  **Zakres digitalizacji**  Decyzje o Warunkach Zabudowy - 355 szt.  Decyzje o Ustaleniu Lokalizacji Inwestycji Celu Publicznego - 57 szt.  Proces digitalizacji obejmuje przetworzenie rejestrów wydanych decyzji o warunkach zabudowy (WZ) oraz decyzji o ustaleniu lokalizacji inwestycji celu publicznego (ULICP) do postaci cyfrowej, zgodnej z:   * **Ustawą o Infrastrukturze Informacji Przestrzennej**, * **Rozporządzeniem Ministra Infrastruktury z dnia 13 maja 2004 r.** w sprawie wzoru rejestru decyzji o warunkach zabudowy oraz wzorów rejestrów decyzji o ustaleniu lokalizacji inwestycji celu publicznego.   **Proces digitalizacji**   1. **Skanowanie decyzji**    * Przetworzenie decyzji wraz z załącznikami graficznymi (mapami) do formatu **PDF**. 2. **Kalibracja rastrów**    * Skalibrowanie skanów w celu zapisania ich w formacie **GeoTIFF** w układzie **PL-2000** 3. **Tworzenie warstwy wektorowej**    * Opracowanie warstwy wektorowej zawierającej **zasięgi decyzji** w odniesieniu do działek ewidencyjnych.    * Cyfryzacja będzie wykonywana na podstawie granic działek aktualnych na dzień wydania decyzji. 4. **Atrybuty opisowe**    * Każdy obiekt wektorowy zostanie wzbogacony o pełny zestaw informacji zgodny z rejestrem decyzji. 5. **Symbolizacja warstw**    * Opracowanie wizualizacji rozróżniającej decyzje **WZ** i **ULICP**. 6. **Powiązanie z dokumentami źródłowymi**    * Możliwość pobierania skanów decyzji bezpośrednio poprzez identyfikację obiektu na mapie.   **Format i sposób dostarczenia danych**  Zdigitalizowane dane zostaną **zaimportowane do Systemu** oraz przekazane w postaci:   * **Warstw wektorowych** w układzie **PL-2000** * **Rastrów** w formacie **GeoTIFF.** * **Skanów decyzji** w formacie **PDF**. |
| 4.4 | **Digitalizacja rejestrów gminnych z obszaru oraz digitalizacja uchwał:**   * Rejestr mienia gminnego - 25 szt. * Rejestr przydomowych oczyszczalni ścieków - 5 szt. * Rejestr zbiorników bezodpływowych - 9 szt. * Digitalizacja uchwał z zakresu ewidencji dróg gminnych publicznych - 10 szt. * Digitalizacja uchwał z zakresu obszarów aglomeracji - 1 szt.   Digitalizacja wszystkich aktualnych oraz archiwalnych ww. uchwał do postaci cyfrowej zgodnej z wymogami Ustawy o Infrastrukturze Informacji Przestrzennej. Digitalizacja do postaci cyfrowej zgodnej z wymogami Ustawy o Infrastrukturze Informacji Przestrzennej oraz Rozporządzenia Ministra Infrastruktury z dnia 13 maja 2004 r. w sprawie wzoru rejestru decyzji o warunkach zabudowy oraz wzorów rejestrów decyzji o ustaleniu lokalizacji inwestycji celu publicznego. Digitalizacja będzie obejmowała zeskanowanie treści decyzji do formatu pdf wraz z załącznikami graficznymi (mapami). Digitalizacja będzie obejmować proces kalibracji rastrów, wynikiem czego będą rastry zapisane w formacie Geotiff w układzie 2000 strefa 6.  Na podstawie skalibrowanych rastrów zostanie utworzona warstwa wektorowa zawierająca zasięgi poszczególnych decyzji w odniesieniu do działek ewidencyjnych (cyfryzację należy wykonać w stosunku do przebiegu granic aktualnych na dzień wydania decyzji). |

### 1.4.5 Wymagania dotyczące e-usług

#### 1 Wniosek o wydanie decyzji o warunkach zabudowy

|  |  |
| --- | --- |
| Nr | Opis wymagania |
| 5.1.1. | E-usługa musi umożliwiać uwierzytelnianie za pomocą usługi Węzła Krajowego. |
| 5.1.2. | E-usługa musi automatycznie zakładać konto podczas pierwszego logowania na podstawie danych pozyskanych z usługi Węzła Krajowego. |
| 5.1.3. | E-usługa musi umożliwiać podpisanie wniosku za pomocą Profilu Zaufanego. |
| 5.1.4. | E-usługa musi automatyczne przenosić dane z formularza wniosku  do rejestru wniosków i spraw systemu dziedzinowego. |
| 5.1.5. | E-usługa umożliwia automatyczną walidację danych wprowadzonych do  formularza wniosku poprzez weryfikację poprawności typów danych, zakresów  wprowadzonych danych, wymuszenie wypełnionych pól oznaczonych jako  obligatoryjne. Szczegółowy zakres formularza danych zostanie ustalony na etapie Analizy przedwdrożeniowej. |
| 5.1.6. | E-usługa musi umożliwiać wskazanie sposobu odbioru decyzji. |
| 5.1.7. | E-usługa musi wspierać wydawanie decyzji administracyjnych wraz z naliczaniem odpowiednich opłat za realizację sprawy. Wydawanie decyzji powinno odbywać się w systemie dziedzinowym. Decyzje muszą być rejestrowane w Systemie Obiegu Dokumentów. |
| 5.1.8. | E-usługa musi umożliwiać dodawanie załączników w postaci elektronicznej do  formularza wniosku. |
| 5.1.9. | E-usługa musi umożliwiać dokonanie płatności online, np. za pomocą KIR. |
| 5.1.10. | E-usługa musi być zintegrowana z Systemem Obiegu Dokumentów. |
| 5.1.11. | E-usługa musi być zintegrowana z modułem dziedzinowym i rejestrem wniosków. |
| 5.1.12. | E-usługa musi posiadać interfejs użytkownika zgodny z wytycznymi WCAG 2.1. |

#### 2 Wniosek o nadanie numeru porządkowego budynku

|  |  |
| --- | --- |
| Nr | Opis wymagania |
| 5.2.1. | E-usługa musi umożliwiać uwierzytelnianie za pomocą usługi Węzła Krajowego. |
| 5.2.2. | E-usługa musi automatycznie zakładać konto podczas pierwszego logowania na podstawie danych pozyskanych z usługi Węzła Krajowego. |
| 5.2.3. | E-usługa musi umożliwiać podpisanie wniosku za pomocą Profilu Zaufanego. |
| 5.2.4. | E-usługa musi automatyczne przenosić dane z formularza wniosku  do rejestru wniosków i spraw systemu dziedzinowego. |
| 5.2.5. | E-usługa umożliwia automatyczną walidację danych wprowadzonych do  formularza wniosku poprzez weryfikację poprawności typów danych, zakresów  wprowadzonych danych, wymuszenie wypełnionych pól oznaczonych jako  obligatoryjne. Szczegółowy zakres formularza danych zostanie ustalony na etapie Analizy przedwdrożeniowej. |
| 5.2.6. | E-usługa musi umożliwiać wskazanie sposobu odbioru decyzji. |
| 5.2.7. | E-usługa musi wspierać wydawanie decyzji administracyjnych wraz z naliczaniem odpowiednich opłat za realizację sprawy. Wydawanie decyzji powinno odbywać się w systemie dziedzinowym. Decyzje muszą być rejestrowane w Systemie Obiegu Dokumentów. |
| 5.2.8. | E-usługa musi umożliwiać dodawanie załączników w postaci elektronicznej do  formularza wniosku. |
| 5.2.9. | E-usługa musi umożliwiać dokonanie płatności online, np. za pomocą KIR. |
| 5.2.10. | E-usługa musi być zintegrowana z Systemem Obiegu Dokumentów. |
| 5.2.11. | E-usługa musi być zintegrowana z modułem dziedzinowym i rejestrem wniosków. |
| 5.2.12. | E-usługa musi posiadać interfejs użytkownika zgodny z wytycznymi WCAG 2.1. |

#### 3 Wniosek o wydanie wyrysu i wypisu z MPZP

|  |  |
| --- | --- |
| Nr | Opis wymagania |
| 5.3.1. | E-usługa musi umożliwiać uwierzytelnianie za pomocą usługi Węzła Krajowego. |
| 5.3.2. | E-usługa musi automatycznie zakładać konto podczas pierwszego logowania na podstawie danych pozyskanych z usługi Węzła Krajowego. |
| 5.3.3. | E-usługa musi umożliwiać podpisanie wniosku za pomocą Profilu Zaufanego. |
| 5.3.4. | E-usługa musi automatyczne przenosić dane z formularza wniosku  do rejestru wniosków i spraw systemu dziedzinowego. |
| 5.3.5. | E-usługa umożliwia automatyczną walidację danych wprowadzonych do  formularza wniosku poprzez weryfikację poprawności typów danych, zakresów  wprowadzonych danych, wymuszenie wypełnionych pól oznaczonych jako  obligatoryjne. Szczegółowy zakres formularza danych zostanie ustalony na etapie Analizy przedwdrożeniowej. |
| 5.3.6. | E-usługa musi umożliwiać wskazanie sposobu odbioru decyzji. |
| 5.3.7. | E-usługa musi wspierać wydawanie decyzji administracyjnych wraz z naliczaniem odpowiednich opłat za realizację sprawy. Wydawanie decyzji powinno odbywać się w systemie dziedzinowym. Decyzje muszą być rejestrowane w Systemie Obiegu Dokumentów. |
| 5.3.8. | E-usługa musi umożliwiać dodawanie załączników w postaci elektronicznej do  formularza wniosku. |
| 5.3.9. | E-usługa musi umożliwiać dokonanie płatności online, np. za pomocą KIR. |
| 5.3.10. | E-usługa musi być zintegrowana z Systemem Obiegu Dokumentów. |
| 5.3.11. | E-usługa musi być zintegrowana z modułem dziedzinowym i rejestrem wniosków. |
| 5.3.12. | E-usługa musi posiadać interfejs użytkownika zgodny z wytycznymi WCAG 2.1. |

#### 4 Wniosek o wydanie wyrysu i wypisu ze studium

|  |  |
| --- | --- |
| Nr | Opis wymagania |
| 5.4.1. | E-usługa musi umożliwiać uwierzytelnianie za pomocą usługi Węzła Krajowego. |
| 5.4.2. | E-usługa musi automatycznie zakładać konto podczas pierwszego logowania na podstawie danych pozyskanych z usługi Węzła Krajowego. |
| 5.4.3. | E-usługa musi umożliwiać podpisanie wniosku za pomocą Profilu Zaufanego. |
| 5.4.4. | E-usługa musi automatyczne przenosić dane z formularza wniosku  do rejestru wniosków i spraw systemu dziedzinowego. |
| 5.4.5. | E-usługa umożliwia automatyczną walidację danych wprowadzonych do  formularza wniosku poprzez weryfikację poprawności typów danych, zakresów  wprowadzonych danych, wymuszenie wypełnionych pól oznaczonych jako  obligatoryjne. Szczegółowy zakres formularza danych zostanie ustalony na etapie Analizy przedwdrożeniowej. |
| 5.4.6. | E-usługa musi umożliwiać wskazanie sposobu odbioru decyzji. |
| 5.4.7. | E-usługa musi wspierać wydawanie decyzji administracyjnych wraz z naliczaniem odpowiednich opłat za realizację sprawy. Wydawanie decyzji powinno odbywać się w systemie dziedzinowym. Decyzje muszą być rejestrowane w Systemie Obiegu Dokumentów. |
| 5.4.8. | E-usługa musi umożliwiać dodawanie załączników w postaci elektronicznej do  formularza wniosku. |
| 5.4.9. | E-usługa musi umożliwiać dokonanie płatności online, np. za pomocą KIR. |
| 5.4.10. | E-usługa musi być zintegrowana z Systemem Obiegu Dokumentów. |
| 5.4.11. | E-usługa musi być zintegrowana z modułem dziedzinowym i rejestrem wniosków. |
| 5.4.12. | E-usługa musi posiadać interfejs użytkownika zgodny z wytycznymi WCAG 2.1. |

#### 5 Wniosek o wydanie zaświadczenia z MPZP

|  |  |
| --- | --- |
| Nr | Opis wymagania |
| 5.5.1. | E-usługa musi umożliwiać uwierzytelnianie za pomocą usługi Węzła Krajowego. |
| 5.5.2. | E-usługa musi automatycznie zakładać konto podczas pierwszego logowania na podstawie danych pozyskanych z usługi Węzła Krajowego. |
| 5.5.3. | E-usługa musi umożliwiać podpisanie wniosku za pomocą Profilu Zaufanego. |
| 5.5.4. | E-usługa musi automatyczne przenosić dane z formularza wniosku  do rejestru wniosków i spraw systemu dziedzinowego. |
| 5.5.5. | E-usługa umożliwia automatyczną walidację danych wprowadzonych do  formularza wniosku poprzez weryfikację poprawności typów danych, zakresów  wprowadzonych danych, wymuszenie wypełnionych pól oznaczonych jako  obligatoryjne. Szczegółowy zakres formularza danych zostanie ustalony na etapie Analizy przedwdrożeniowej. |
| 5.5.6. | E-usługa musi umożliwiać wskazanie sposobu odbioru decyzji. |
| 5.5.7. | E-usługa musi wspierać wydawanie decyzji administracyjnych wraz z naliczaniem odpowiednich opłat za realizację sprawy. Wydawanie decyzji powinno odbywać się w systemie dziedzinowym. Decyzje muszą być rejestrowane w Systemie Obiegu Dokumentów. |
| 5.5.8. | E-usługa musi umożliwiać dodawanie załączników w postaci elektronicznej do  formularza wniosku. |
| 5.5.9. | E-usługa musi umożliwiać dokonanie płatności online, np. za pomocą KIR. |
| 5.5.10. | E-usługa musi być zintegrowana z Systemem Obiegu Dokumentów. |
| 5.5.11. | E-usługa musi być zintegrowana z modułem dziedzinowym i rejestrem wniosków. |
| 5.5.12. | E-usługa musi posiadać interfejs użytkownika zgodny z wytycznymi WCAG 2.1. |

#### 6 Wniosek o wydanie zaświadczenia ze studium

|  |  |
| --- | --- |
| Nr | Opis wymagania |
| 5.6.1. | E-usługa musi umożliwiać uwierzytelnianie za pomocą usługi Węzła Krajowego. |
| 5.6.2. | E-usługa musi automatycznie zakładać konto podczas pierwszego logowania na podstawie danych pozyskanych z usługi Węzła Krajowego. |
| 5.6.3. | E-usługa musi umożliwiać podpisanie wniosku za pomocą Profilu Zaufanego. |
| 5.6.4. | E-usługa musi automatyczne przenosić dane z formularza wniosku  do rejestru wniosków i spraw systemu dziedzinowego. |
| 5.6.5. | E-usługa umożliwia automatyczną walidację danych wprowadzonych do  formularza wniosku poprzez weryfikację poprawności typów danych, zakresów  wprowadzonych danych, wymuszenie wypełnionych pól oznaczonych jako  obligatoryjne. Szczegółowy zakres formularza danych zostanie ustalony na etapie Analizy przedwdrożeniowej. |
| 5.6.6. | E-usługa musi umożliwiać wskazanie sposobu odbioru decyzji. |
| 5.6.7. | E-usługa musi wspierać wydawanie decyzji administracyjnych wraz z naliczaniem odpowiednich opłat za realizację sprawy. Wydawanie decyzji powinno odbywać się w systemie dziedzinowym. Decyzje muszą być rejestrowane w Systemie Obiegu Dokumentów. |
| 5.6.8. | E-usługa musi umożliwiać dodawanie załączników w postaci elektronicznej do  formularza wniosku. |
| 5.6.9. | E-usługa musi umożliwiać dokonanie płatności online, np. za pomocą KIR. |
| 5.6.10. | E-usługa musi być zintegrowana z Systemem Obiegu Dokumentów. |
| 5.6.11. | E-usługa musi być zintegrowana z modułem dziedzinowym i rejestrem wniosków. |
| 5.6.12. | E-usługa musi posiadać interfejs użytkownika zgodny z wytycznymi WCAG 2.1. |

#### 7 Wniosek o sporządzenie MPZP

|  |  |
| --- | --- |
| Nr | Opis wymagania |
| 5.7.1. | E-usługa musi umożliwiać uwierzytelnianie za pomocą usługi Węzła Krajowego. |
| 5.7.2. | E-usługa musi automatycznie zakładać konto podczas pierwszego logowania na podstawie danych pozyskanych z usługi Węzła Krajowego. |
| 5.7.3. | E-usługa musi umożliwiać podpisanie wniosku za pomocą Profilu Zaufanego. |
| 5.7.4. | E-usługa musi automatyczne przenosić dane z formularza wniosku  do rejestru wniosków i spraw systemu dziedzinowego. |
| 5.7.5. | E-usługa umożliwia automatyczną walidację danych wprowadzonych do  formularza wniosku poprzez weryfikację poprawności typów danych, zakresów  wprowadzonych danych, wymuszenie wypełnionych pól oznaczonych jako  obligatoryjne. Szczegółowy zakres formularza danych zostanie ustalony na etapie Analizy przedwdrożeniowej. |
| 5.7.6. | E-usługa musi umożliwiać wskazanie sposobu odbioru decyzji. |
| 5.7.7. | E-usługa musi wspierać wydawanie decyzji administracyjnych wraz z naliczaniem odpowiednich opłat za realizację sprawy. Wydawanie decyzji powinno odbywać się w systemie dziedzinowym. Decyzje muszą być rejestrowane w Systemie Obiegu Dokumentów. |
| 5.7.8. | E-usługa musi umożliwiać dodawanie załączników w postaci elektronicznej do  formularza wniosku. |
| 5.7.9. | E-usługa musi umożliwiać dokonanie płatności online, np. za pomocą KIR. |
| 5.7.10. | E-usługa musi być zintegrowana z Systemem Obiegu Dokumentów. |
| 5.7.11. | E-usługa musi być zintegrowana z modułem dziedzinowym i rejestrem wniosków. |
| 5.7.12. | E-usługa musi posiadać interfejs użytkownika zgodny z wytycznymi WCAG 2.1. |

#### 8 Wniosek o zmianę aktu planowania przestrzennego

|  |  |
| --- | --- |
| Nr | Opis wymagania |
| 5.8.1. | E-usługa musi umożliwiać uwierzytelnianie za pomocą usługi Węzła Krajowego. |
| 5.8.2. | E-usługa musi automatycznie zakładać konto podczas pierwszego logowania na podstawie danych pozyskanych z usługi Węzła Krajowego. |
| 5.8.3. | E-usługa musi umożliwiać podpisanie wniosku za pomocą Profilu Zaufanego. |
| 5.8.4. | E-usługa musi automatyczne przenosić dane z formularza wniosku  do rejestru wniosków i spraw systemu dziedzinowego. |
| 5.8.5. | E-usługa umożliwia automatyczną walidację danych wprowadzonych do  formularza wniosku poprzez weryfikację poprawności typów danych, zakresów  wprowadzonych danych, wymuszenie wypełnionych pól oznaczonych jako  obligatoryjne. Szczegółowy zakres formularza danych zostanie ustalony na etapie Analizy przedwdrożeniowej. |
| 5.8.6. | E-usługa musi umożliwiać wskazanie sposobu odbioru decyzji. |
| 5.8.7. | E-usługa musi wspierać wydawanie decyzji administracyjnych wraz z naliczaniem odpowiednich opłat za realizację sprawy. Wydawanie decyzji powinno odbywać się w systemie dziedzinowym. Decyzje muszą być rejestrowane w Systemie Obiegu Dokumentów. |
| 5.8.8. | E-usługa musi umożliwiać dodawanie załączników w postaci elektronicznej do  formularza wniosku. |
| 5.8.9. | E-usługa musi umożliwiać dokonanie płatności online, np. za pomocą KIR. |
| 5.8.10. | E-usługa musi być zintegrowana z Systemem Obiegu Dokumentów. |
| 5.8.11. | E-usługa musi być zintegrowana z modułem dziedzinowym i rejestrem wniosków. |
| 5.8.12. | E-usługa musi posiadać interfejs użytkownika zgodny z wytycznymi WCAG 2.1. |

#### 9 Wniosek o zmianę do projektu aktu planowania przestrzennego

|  |  |
| --- | --- |
| Nr | Opis wymagania |
| 5.9.1. | E-usługa musi umożliwiać uwierzytelnianie za pomocą usługi Węzła Krajowego. |
| 5.9.2. | E-usługa musi automatycznie zakładać konto podczas pierwszego logowania na podstawie danych pozyskanych z usługi Węzła Krajowego. |
| 5.9.3. | E-usługa musi umożliwiać podpisanie wniosku za pomocą Profilu Zaufanego. |
| 5.9.4. | E-usługa musi automatyczne przenosić dane z formularza wniosku  do rejestru wniosków i spraw systemu dziedzinowego. |
| 5.9.5. | E-usługa umożliwia automatyczną walidację danych wprowadzonych do  formularza wniosku poprzez weryfikację poprawności typów danych, zakresów  wprowadzonych danych, wymuszenie wypełnionych pól oznaczonych jako  obligatoryjne. Szczegółowy zakres formularza danych zostanie ustalony na etapie Analizy przedwdrożeniowej. |
| 5.9.6. | E-usługa musi umożliwiać wskazanie sposobu odbioru decyzji. |
| 5.9.7. | E-usługa musi wspierać wydawanie decyzji administracyjnych wraz z naliczaniem odpowiednich opłat za realizację sprawy. Wydawanie decyzji powinno odbywać się w systemie dziedzinowym. Decyzje muszą być rejestrowane w Systemie Obiegu Dokumentów. |
| 5.9.8. | E-usługa musi umożliwiać dodawanie załączników w postaci elektronicznej do  formularza wniosku. |
| 5.9.9. | E-usługa musi umożliwiać dokonanie płatności online, np. za pomocą KIR. |
| 5.9.10. | E-usługa musi być zintegrowana z Systemem Obiegu Dokumentów. |
| 5.9.11. | E-usługa musi być zintegrowana z modułem dziedzinowym i rejestrem wniosków. |
| 5.9.12. | E-usługa musi posiadać interfejs użytkownika zgodny z wytycznymi WCAG 2.1. |

#### 10 Wniosek o wydanie zezwolenia na usunięcie drzew lub krzewów

|  |  |
| --- | --- |
| Nr | Opis wymagania |
| 5.10.1. | E-usługa musi umożliwiać uwierzytelnianie za pomocą usługi Węzła Krajowego. |
| 5.10.2. | E-usługa musi automatycznie zakładać konto podczas pierwszego logowania na podstawie danych pozyskanych z usługi Węzła Krajowego. |
| 5.10.3. | E-usługa musi umożliwiać podpisanie wniosku za pomocą Profilu Zaufanego. |
| 5.10.4. | E-usługa musi automatyczne przenosić dane z formularza wniosku  do rejestru wniosków i spraw systemu dziedzinowego. |
| 5.10.5. | E-usługa umożliwia automatyczną walidację danych wprowadzonych do  formularza wniosku poprzez weryfikację poprawności typów danych, zakresów  wprowadzonych danych, wymuszenie wypełnionych pól oznaczonych jako  obligatoryjne. Szczegółowy zakres formularza danych zostanie ustalony na etapie Analizy przedwdrożeniowej. |
| 5.10.6. | E-usługa musi umożliwiać wskazanie sposobu odbioru decyzji. |
| 5.10.7. | E-usługa musi wspierać wydawanie decyzji administracyjnych wraz z naliczaniem odpowiednich opłat za realizację sprawy. Wydawanie decyzji powinno odbywać się w systemie dziedzinowym. Decyzje muszą być rejestrowane w Systemie Obiegu Dokumentów. |
| 5.10.8. | E-usługa musi umożliwiać dodawanie załączników w postaci elektronicznej do  formularza wniosku. |
| 5.10.9. | E-usługa musi umożliwiać dokonanie płatności online, np. za pomocą KIR. |
| 5.10.10. | E-usługa musi być zintegrowana z Systemem Obiegu Dokumentów. |
| 5.10.11. | E-usługa musi być zintegrowana z modułem dziedzinowym i rejestrem wniosków. |
| 5.10.12. | E-usługa musi posiadać interfejs użytkownika zgodny z wytycznymi WCAG 2.1. |

## E-edukacja – szt.1 lic.

Przedmiotem zamówienia jest aktualizacja oraz dostawa licencji na oprogramowanie edukacyjne typu OPEN dla jednostek oświatowych oraz jednostki administracyjnej/ Gminnego Zespołu Ekonomiczno-Administracyjnego Szkół w Nozdrzcu (zwanego GZEAS) . Zamówienie obejmuje podniesienie wersji posiadanego systemu edukacyjnego do najnowszej wspieranej przez producenta wersji, wraz z integracją oraz instalacją systemu.

Aktualizacja obejmuje wszystkie moduły wchodzące w skład systemu edukacyjnego, w tym specjalizowane programy przeznaczone do obsługi edukacji w obszarach aktywności jednostek administracji, takich jak:

* Dziennik elektroniczny,
* e-Świadectwa,
* e-Sekretariat.

**Zakres funkcjonalności oprogramowania do realizacji dziennika elektronicznego**

Oprogramowanie musi zapewniać następujące funkcjonalności:

* Bieżąca kontrola frekwencji ucznia,
* Bieżąca kontrola ocen oraz analiza postępów w nauce,
* Otrzymywanie aktualnych informacji dotyczących spraw szkolnych i zachowania ucznia,
* Bezpośrednie wysyłanie wiadomości do nauczycieli,
* Obsługa systemu naboru elektronicznego do szkół (rekrutacja online),
* Możliwość zarządzania podziałem godzin w trybie online,
* Dostęp zdalny poprzez interfejs WWW.

**Licencjonowanie**

* Licencje muszą być dostarczone w ilości zgodnej z liczbą placówek edukacyjnych podległych jednostce administracyjnej oraz dla Gminnego Zespołu Ekonomiczno-Administracyjnego Szkół w Nozdrzcu

**Zakres usług wdrożeniowych** Koszty związane z instalacją, konfiguracją, optymalizacją oraz asystami stanowiskowymi są uwzględnione w następujących pozycjach specyfikacji usług:

* Integracja z platformą e-usług publicznych,
* Instalacja i konfiguracja na platformie e-usług publicznych.

Zamawiający oczekuje dostarczenia kompleksowego rozwiązania, obejmującego oprogramowanie oraz usługi wdrożeniowe, zgodnie z wymaganiami określonymi w  niniejszym opisie przedmiotu zamówienia.

### 1.5.1 Dziennik elektroniczny

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Pozycja dotyczy podniesienia wersji posiadanego systemu edukacyjnego do najnowszej wspieranej przez producenta wersji. 2. Aktualizacja ma dotyczyć wszystkich pozycji wchodzących w skład systemu – specjalizowane programy przeznaczone do obsługi edukacji - obszarów aktywności jednostek administracji (dziennik elektroniczny , e-Świadectwa, e-Sekretariat). 3. Oprogramowanie do realizacji „elektronicznego dziennika" - DE 4. Zakres funkcjonalności:    * bieżącą kontrolę frekwencji dziecka,    * bieżącą kontrolę ocen dziecka i analizę postępów w nauce,    * otrzymywanie aktualnych informacji o sprawach szkolnych i zachowaniu dziecka,    * bezpośrednie wysyłanie wiadomości wraz z załącznikami do Nauczycieli    * systemu naboru elektronicznego do szkół – rekrutacja    * podział godzin on-line    * dostęp zdalny poprzez interfejs WWW.    * Ilość licencji zgodna z ilością placówek:      + - Szkoła Podstawowa im. Kardynała Stefana Wyszyńskiego w Hłudnie        - Szkoła Podstawowa im. Aleksandra Fredry w Nozdrzcu        - Szkoła Podstawowa im. Świętego Jana Pawła II w Warze        - Szkoła Podstawowa Nr 1 im. Marszałka Józefa Piłsudskiego w Wesołej        - Szkoła Podstawowa im. Świętej Jadwigi Królowej Polski z Oddziałem Przedszkolnym        - Szkoła Podstawowa w Siedliskach | | | |
|  | Informacje ogólne | |
|  | Dla umożliwienia jednoznacznej interpretacji zakresu funkcjonalności dla systemu dziennika elektronicznego (DE) wyjaśnia się, że w każdym miejscu, w którym funkcjonalność związana jest z obszarem innym niż obowiązkowe zajęcia edukacyjne (lekcje) realizowane z klasami uczniów (np. zajęciami indywidualnymi, dodatkowymi, świetlicowymi, itd.), jest to jednoznacznie wskazane w jej opisie. | |
|  | Dziennik elektroniczny realizuje niżej wymienioną funkcjonalność dla uczniów ogólnokształcących szkół podstawowych w klasach 1-8 dla młodzieży prowadzących naukę w trybie dwusemestralnym. | |
|  | DE Obejmuje funkcjonalność umożliwiającą przeprowadzenie importu danych w następującym zakresie:   * + - dane osobowe uczniów - imię, nazwisko, adres, numer PESEL, data i miejsce urodzenia (format SOU)     - struktura organizacyjna szkoły: lista klas, lista nauczycieli, lista przedmiotów, schemat przydziałów czynności nauczycieli (powiązanie nauczyciel-przedmiot-klasa), format ASC XML | |
|  | W zakresie dostarczanej dokumentacji:   * + - udostępnienie każdemu zalogowanemu użytkownikowi instrukcji obsługi w serwisie dziennika elektronicznego. Instrukcja zawiera wyszukiwarkę za pomocą której użytkownik będzie w stanie łatwo odnaleźć interesujące go treści. | |
|  | Producent udziela dostępu do aplikacji na następujących polach eksploatacji:   * + - użytkowania wyłącznie przez jednostki objęte umową,     - używania aplikacji, przez co rozumie się uruchamianie, wyświetlanie, uzyskiwanie dostępu, wprowadzanie danych, zmienianie i usuwanie danych, przeglądanie danych,     - udostępniania aplikacji w ten sposób, aby każdy działający w imieniu lub z upoważnienia jednostek, o których mowa niniejszym zamówieniu mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym.   Producent przygotował i udostępnia użytkownikom regulamin świadczenia usługi w formie elektronicznej. | |
|  | DE jest dla rodziców i uczniów dostępny alternatywnie także przez aplikacje mobilne co najmniej dla aktualnych wersji systemu Android oraz iOS w zakresie prezentacji ocen, absencji, planu lekcji, terminarza wydarzeń szkolnych/tablicy ogłoszeń, korespondencji z rodzicami oraz możliwości przesyłania zdjęć do eLegitymacji. Dostępność aplikacji jest gwarantowana z chwilą udzielenia licencji może jednak zostać ograniczona w przypadku zmian polityki globalnych dostawców usług (operatorów sklepów Google Play i AppStore) co do warunków publikacji aplikacji w ich sklepach. | |
|  | Administrowanie systemem | |
|  | System posiada moduł administracyjny, do którego mają dostęp wyselekcjonowani w placówce szkolnej pracownicy. Moduł umożliwia dostosowanie systemu do potrzeb danej placówki poprzez włączenie/ wyłączanie wybranych opcji. | |
|  | Dziennik elektroniczny umożliwia założenie osobnych kont dla dowolnej liczby rodziców/opiekunów oraz uczniów. Każdy z nich posiada osobną wbudowaną w system i nie wymagającą konfiguracji dodatkowych narzędzi (np. kont e-mail) skrzynkę na wiadomości tekstowe i mieć zagwarantowaną poufność kontaktu z placówką szkolną. | |
|  | System pozwala na stworzenie przynajmniej dwóch osobnych kont rodzica/opiekuna przypisanych do danych indywidualnego ucznia. | |
|  | System umożliwia przyznanie wybranej grupie użytkowników (domyślnie administratorowi, fakultatywnie co najmniej każdemu nauczycielowi w szkole lub wychowawcom klas) uprawnień do tworzenia dowolnych grup uczniów:   * + - wewnątrzklasowych,     - między klasowych, złożonych z klas tego samego poziomu,     - między klasowych, złożonych z klas różnych poziomów (o ile mają te same daty semestrów). | |
|  | Podziały na grupy są dostępne w widoku planów lekcji oraz widoku lekcji zrealizowanych w danej szkole. Numeracja oraz kolejność uczniów w ramach takich grup nie ma wpływu na numerację i kolejność uczniów w klasie. Informacje o ocenach, tematach zajęć oraz frekwencji uczniów na zajęciach realizowanych w grupach są widoczne podczas prowadzenia zajęć grupy, jak i w dzienniku klas głównych, z których pochodzą uczniowie. | |
|  | System umożliwia administratorowi zablokowanie możliwości dodawania, wprowadzania zmian i usuwania danych dotyczących lekcji w wybranym dowolnie zakresie dat (np. cały pierwszy semestr, wybrany miesiąc lub inny zakres dat). Blokada może być włączana dla wybranych lub wszystkich klas oraz obejmować co najmniej następujące dane:   * + - oceny,     - frekwencję,     - zachowanie,     - zrealizowane lekcje. | |
|  | System umożliwia migrację uczniów pomiędzy klasami i grupami w dowolnym momencie roku szkolnego. Uczeń przenoszony lub skreślony zostaje w widoczny sposób oznaczony na liście dotychczasowej klasy - przekreślony (podobnie jak w dokumentacji papierowej, nie zostaje całkowicie usunięty z listy z chwilą skreślenia lub przeniesienia).  System posiada mechanizm (w postaci kreatora) usprawniający przenoszenie uczniów w obrębie danej szkoły. Mechanizm pozwala na skreślenie ucznia w dotychczasowych klasach wirtualnych, ustawiając przy tym odpowiednie daty skreśleń. | |
|  | System umożliwia dokonanie zmiany nauczyciela prowadzącego lekcje (w trakcie roku szkolnego), który automatycznie uzyska uprawnienia do kontynuacji pracy z klasą oraz do realizowanych przez jego poprzednika rozkładów materiałów nauczania. | |
|  | System umożliwia konfigurację widoku wybranych informacji na koncie rodzica i ucznia. Administrator ma możliwość definiowania opcjonalnych widoków dla rodziców co najmniej poprzez włączanie lub wyłączanie widoku:   * + - średniej ocen ucznia,     - zrealizowanych na zajęciach z klasą tematów lekcji,     - prezentacji uwag ucznia,     - prezentacji wyników egzaminów. | |
|  | System pozwala nałożyć lub zdjąć blokadę uzupełniania frekwencji przez nauczycieli w trakcie lekcji uczniom, którzy w tym czasie zostali przypisani do wycieczki (zgodnie wprowadzonym z harmonogramem wycieczki). | |
|  | System pozwala administratorowi stworzyć dodatkowe (poza zaimplementowanymi standardowo kategoriami – obecność, nieobecność, nieobecność usprawiedliwiona, spóźnienie, zwolnienie) kategorie frekwencji wg schematu:   * + - nazwa kategorii;     - sposób traktowania kategorii w statystyce (do jakiej grupy standardowych kategorii powinna być doliczona);     - kolor. | |
|  | System pozwala założyć dowolną liczbę jednostek w ramach szkoły  (w przypadku zespołu szkół). | |
|  | Funkcjonalności związane z prowadzeniem lekcji | |
|  | System umożliwia rodzicowi/opiekunowi ucznia dostęp przez interfejs www do następujących informacji:   * + - oceny dziecka z podziałem na okresy klasyfikacyjne,     - szczegóły związane z ocenami (kategorię, datę wpisu, nazwisko nauczyciela wpisującego ocenę do dziennika),     - absencję dziecka wraz z informacją nt. kategorii nieobecności,     - kalendarz wydarzeń klasowych,     - plan lekcji wraz z umieszczonymi w nim automatycznie przez system informacjami o zastępstwach, odwołaniu lub przeniesieniu lekcji,     - informacje o zadanej pracy własnej,     - szkolnej tablicy ogłoszeń,     - rejestru tematów które w danym okresie zostały zrealizowane w klasie (po odpowiednim skonfigurowaniu przez administratora dziennika w szkole),     - średniej ocen ucznia (po odpowiednim skonfigurowaniu przez administratora dziennika w szkole) | |
|  | System umożliwia rodzicowi/opiekunowi ucznia wysłanie wiadomości do dowolnego nauczyciela prowadzącego lekcje w danej szkole. Rodzic musi mieć możliwość dotarcia do informacji czy i kiedy wysłana przez niego wiadomość została przeczytana. | |
|  | System umożliwia dodawanie, usuwanie oraz modyfikację ocen oraz nieobecności na lekcjach. System jednocześnie prowadzi dla lekcji rejestr zmian co najmniej w zakresie ocen, nieobecności oraz zmiany podstawowych danych osobowych. Historia zmian zawiera widoczne następujące informacje:   * + - data zmiany/wprowadzenia/usunięcia informacji,     - imię i nazwisko oraz funkcja osoby zmieniającej,     - IP z którego dokonywano operacji,     - informacja, które dane zostały zmienione,     - jaka treść na jaką została zmieniona. | |
|  | System umożliwia nauczycielowi wcześniejsze zaplanowanie lekcji za pomocą specjalnego kreatora obejmującego możliwość wprowadzenia przed planowanym terminem lekcji tematu lekcji, dodanie notatki, dodanie linków do materiałów multimedialnych. W panelu administracyjnym jest możliwość zablokowania dla szkoły wglądu rodziców/uczniów w informacje  o zaplanowanych w ten sposób lekcjach. | |
|  | System zapewnia możliwość oceniania w sposób:   1. tradycyjny w skali 1-6, 2. oceniania kształtującego, 3. oceniania opisowego w edukacji wczesnoszkolnej, 4. za pomocą systemu mieszanego zawierającego pkt. 1-3, gdzie jednego ucznia w ramach jednych zajęć można oceniać jednocześnie kilkoma wybranymi sposobami. | |
|  | Każda ocena jest uzupełniona następującymi informacjami:  1. Obligatoryjnie, w sposób automatyczny przez system:   * imię i nazwisko osoby, która dodała ocenę do bazy danych  (w przypadku zastępstw powinna pojawić się osoba zastępująca), * dane nauczyciela mającego przydział do danej lekcji, * data fizycznego wpisania oceny do bazy danych, * data oceny, * kategoria oceny,   2. Fakultatywnie, po uzupełnieniu przez nauczyciela:   * komentarz nauczyciela do oceny, * indywidualnie dobrany do kategorii kolor, tak aby po kolorze użytkownicy mogli rozróżniać poszczególne kategorie  (np. sprawdzian – czerwony kolor, kartkówka – kolor żółty, itd.). | |
|  | System umożliwia pracę z wykorzystaniem różnych widoków przedstawiających listę ocen:   * + - widok ocen pogrupowanych wg kategorii,     - widok ocen posortowanych wg daty dodania do systemu DE oceny. | |
|  | System prezentuje wyliczoną średnią ważoną lub arytmetyczną w zależności od konfiguracji. Każdy nauczyciel indywidualnie może zdecydować o wyborze algorytmu wyliczania średniej na przedmiocie, którego uczy (tworząc odpowiednie kategorie oceniania i przypisując do nich wagi). | |
|  | 1. System umożliwia w zakresie frekwencji na lekcjach:    * + wpisanie uczniom nieobecności nieusprawiedliwionych,      + wpisanie nieobecności usprawiedliwionych,      + wpisanie spóźnienia,      + wpisanie zwolnienia z danej lekcji oraz zwolnienia w wybranym terminie,      + definiowanie własnych typów nieobecności oraz ich sposobu liczenia w statystykach frekwencji (np. podkategoria zawody sportowe w kategorii nieobecność). 2. System zawiera funkcję e-usprawiedliwienia – umożliwiającą wysłanie przez dowolnego rodzica/opiekuna ucznia wniosku o usprawiedliwienie jego nieobecności na lekcjach za pomocą dedykowanego formularza obejmującego:    * + informację o powodach nieobecności ucznia,      + informację o czasie usprawiedliwionej nieobecności (definiowanym co najmniej jako zakres dat lub zakres godzin lekcyjnych w ramach jednego dnia). 3. Usprawiedliwienie wysłane za pomocą modułu e-usprawiedliwienia powoduje:    * + automatyczną zmianę w dzienniku elektronicznym nieobecności nieusprawiedliwionych na usprawiedliwione we wskazanym we wniosku okresie,      + automatyczne wygenerowanie informacji zwrotnej do rodzica/opiekuna, potwierdzającej dokonanie usprawiedliwienia nieobecności we wskazanym okresie. 4. Dodatkowo system ma możliwość automatycznego usprawiedliwienia nieobecności w zadanym z wyprzedzeniem przez nauczyciela okresie (np. w sytuacji kiedy rodzic zgłosi, że przez najbliższych 14 dni uczeń nie będzie obecny z powodu choroby i wyśle odpowiednie usprawiedliwienie do DE, system każdą wpisaną po dacie otrzymania e-usprawiedliwienia nieobecność nieusprawiedliwioną usprawiedliwia w ramach zadanego okresu automatycznie). | |
|  | System umożliwia nauczycielowi dostęp do widoku, w którym będą wykazane braki w części dokumentacji, za którą odpowiada (prowadzone przez niego lekcje). Nauczyciel ma możliwość dotarcia do informacji o brakujących wpisach frekwencji i realizacji lekcji. W przypadku każdego braku nauczyciel może wyświetlić przynajmniej następujące szczegóły:   * + - data,     - numer lekcji,     - oddział,     - przedmiot. | |
|  | System umożliwia wygenerowanie zbiorczej informacji na temat konkretnego ucznia. W widoku tym znajdują się:   * + - wszystkie oceny uzyskane przez ucznia w bieżącym roku szkolnym  w trakcie lekcji z przedmiotów podlegających klasyfikacji,     - nieobecności na zajęciach z klasą,     - uwagi wysłane do rodzica przez nauczycieli wraz z informacją czy dany rodzic przeczytał daną uwagę,     - informacje o dacie i godzinie ostatniego logowania rodzica oraz ucznia przez stronę www. | |
|  | Dziennik elektroniczny umożliwia ocenianie zachowania w sposób tekstowy (wpisywanie uwag). W przypadku zastosowania punktowego oceniania zachowania system umożliwia skonfigurowanie słownika wzorców (nazwa + wartość punktowa, np. nieodpowiednie zachowanie na lekcji (-10 pkt), aktywność pozalekcyjna na rzecz szkoły (+20 pkt)). | |
|  | Dziennik elektroniczny posiada mechanizmy, umożliwiające wprowadzenie przez nauczycieli prowadzących obowiązkowe zajęcia edukacyjne (lekcje), rozkładów materiałów nauczania oraz korzystanie z biblioteki już przygotowanych.  W ramach dostarczanego systemu jest zagwarantowany dostęp do przynajmniej 100 przygotowanych i opracowanych rozkładów, w tym rozkładów pochodzących bezpośrednio od przynajmniej 3 różnych wydawców edukacyjnych (wpisanych przez pracowników wydawców oraz stosownie opisanych - wskazane pochodzenie/autorstwo rozkładu).  System jest wyposażony w moduł udostępniany wydawcom podręczników  i umożliwiający im wprowadzanie do systemu rozkładów materiału do oferowanych podręczników. System umożliwia nauczycielom dodawanie własnych rozkładów a następnie ich wielokrotne wykorzystywanie oraz dzielenie się nimi za pośrednictwem biblioteki rozkładów materiałów nauczania (baza RMN) na bazie regulaminu korzystania z bazy RMN, regulującego kwestie prawa autorskiego w udostępnianiu i kopiowaniu rozkładów, do których prawa posiadają wydawcy edukacyjni. | |
|  | System posiada moduł edukacji wczesnoszkolnej zawierający co najmniej:   * + - możliwość odnotowywania zajęć edukacji wczesnoszkolnej w trybie normalnych godzin lekcyjnych obowiązujących w szkole i w oparciu  o narzucony plan lekcji lub     - możliwość odnotowywania w ramach bloku lekcyjnego czasu trwania poszczególnych edukacji w systemie minutowym (bez konieczności ustalania sztywnego i powtarzalnego planu lekcji uwzględniającego wszystkie edukacje wchodzące w skład edukacji wczesnoszkolnej),     - słownik opisowych wyrażeń oceniających postępy ucznia składający się  z co najmniej 1000 wyrażeń podzielonych na poszczególne edukacje  i umiejętności (z możliwością modyfikacji i dostosowania przez wychowawcę, który stosuje ocenę opisową),     - możliwość wprowadzania frekwencji oraz tematów zajęć dla całego bloku edukacji wczesnoszkolnej (bez konieczności powtarzania wprowadzania tych danych dla każdej godziny lekcyjnej),     - możliwość odnotowania tematu dnia oraz jednocześnie tematów szczegółowych dla każdej edukacji realizowanej w danym dniu przez nauczyciela. | |
|  | System posiada dla lekcji zestaw następujących analiz związanych  z frekwencją, postępami w nauce, średnią ocen oraz klasyfikacjami:   * + - Oceny ucznia oraz frekwencję z podziałem na:       * klasy;       * jednostki szkolne w przypadku zespołów szkół;       * zakres czasowy (np. okres 1, okres 2, wybrany miesiąc);       * wybrany przedmiot;     - Klasyfikację śródroczną i roczną;     - Miesięczne zestawienia frekwencji;     - Frekwencję w konkretnym dniu i godzinie lekcyjnej. Zestawienie zawiera sumę obecności, nieobecności oraz procent obecności ogółem;     - Procentowe rankingi frekwencji z podziałem na oddziały oraz poszczególnych uczniów;     - Wykres nieobecności z podziałem na oddziały oraz jednostki szkolne;     - Wykres średniej ocen z podziałem na oddziały oraz jednostki szkolne;     - Miesięczny rozkład liczby poszczególnych ocen (1,2,3,4,5,6) z podziałem na oddziały i jednostki szkolne;     - Wykres ocen śródrocznych i rocznych;     - Wykaz uczniów z oceną niedostateczną oraz nieklasyfikowany;     - Zestawienie ocen zachowania;     - Średnią przedmiotów, klas oraz uczniów;     - Średnią ocen z wybranych przedmiotów dla ucznia lub klasy (np. średnia z przedmiotów zawodowych); | |
|  | System posiada moduł pozwalający na dokumentację wycieczek/ wyjść grupowych uczniów. Moduł pozwala na:   * + - możliwość tworzenia grup wycieczkowych składających się z dowolnej liczby uczniów pochodzących z różnych klas w szkole,     - możliwość wskazania kierownika wycieczki oraz opiekunów spośród wszystkich nauczycieli w szkole,     - możliwość dodania do wycieczki dowolnego uczestnika lub opiekuna spoza szkoły (uwzględnianych potem na wydruku karty wycieczki),     - możliwość wprowadzenia harmonogramu wycieczki obejmującego dokładny zakres dat i godzin zegarowych trwania wycieczki oraz jednocześnie wskazanie niezależnie ile godzin lekcyjnych, z jakich przedmiotów i z jakimi tematami zostanie zapisanych w dziennikach lekcyjnych wszystkich klas, z których uczniowie brali udział w wycieczce,     - przy każdej wskazanej do wprowadzenia do dziennika lekcji realizowanej w ramach wycieczki musi być możliwość oznaczenia czy powinna ona zostać doliczona do realizacji ramowego planu nauczania czy nie,     - możliwość uzupełnienia frekwencji na wycieczce z zajęć zaplanowanych w harmonogramie wycieczki. Uzupełnienie frekwencji z zajęć realizowanych na wycieczce powinno się odbywać na zbiorczym widoku z listą wszystkich uczniów uczestniczących w wycieczce (nawet jeśli pochodzą z różnych klas lub grup zajęciowych). Frekwencja powinna być traktowana jak wpisy frekwencji ze standardowych zajęć w szkole,     - generowanie gotowej karty wycieczki zgodnej z wzorem MEN.     - Moduł umożliwia odwoływanie lekcji wynikających z planu lekcji. W takim przypadku:       * W module Zastępstw zostaje wyświetlona informacja o zajęciach odwołanych - nie ma konieczności ponownego odwoływania zajęć klasy w tym module oraz dodawania nieobecności klasy na dzień wycieczki,       * Jeżeli odwołano zajęcia przez moduł Wycieczki, w planie lekcji klasy zostanie wyświetlone powiadomienie o odwołaniu zajęć,       * W kalendarzu wydarzeń klasowych musi zostać wyświetlone powiadomienie o odwołaniu zajęć,       * Zapisanie ucznia na wycieczkę blokuje możliwość sprawdzenia frekwencji temu uczniowi na lekcjach odbywających się w tym czasie w szkole. Funkcja ta jest konfigurowalna w ustawieniach DE, może być to zrealizowane za pomocą komunikatu o uczniu przypisanym do wycieczki. | |
|  | System udostępnia dyrektorowi dodatkowe informacje dotyczące pracy nauczycieli z uwzględnieniem:   * + - daty i godziny ostatniego logowania do systemu każdego z nauczycieli,     - co najmniej dla ocen w skali 1-6 liczby ocen z podziałem na kategorie wpisanych przez nauczyciela w wybranym okresie w trakcie prowadzonych przez niego lekcji,     - miesięcznego rozkładu w/w ocen z lekcji każdego nauczyciela. | |
|  | Dziennik umożliwia dyrektorowi placówki oraz nauczycielowi kontrolę realizacji rozkładu materiału nauczania dla każdego przedmiotu i każdej prowadzonej lekcji. System wskazuje dyrektorowi, które z zaplanowanych tematów zostały zrealizowane oraz kiedy. Dyrektor posiada także informacje o tematach, które zostały zrealizowane, ale nie należały do rozkładów materiałów nauczania. System ma także możliwość przypisania rozkładu materiału do grup wewnątrz i międzyoddziałowych, dzięki czemu możliwe będzie monitorowanie realizacji tematów i lekcji na zajęciach, w których stosowane są podziały na grupy. | |
|  | System posiada możliwość planowania zastępstw doraźnych dla lekcji, w tym:   * + - łączenia grup na zastępstwie (grup w ramach jednego oddziału lub grup z kilku oddziałów),     - dzielenia oddziałów na grupy na zastępstwie,     - przypisywanie dowolnego nauczyciela do realizacji zastępstwa,     - odwołania lekcji,     - przesunięcia lekcji,     - system umożliwia katalogowanie planowanych zastępstw według typu (co najmniej płatne/niepłatne/inne) oraz na żądanie generować zestawienia wszystkich zrealizowanych w danym miesiącu zastępstw wg typu i nauczyciela,     - informacje o planowanych zmianach (zastępstwach, przesunięciach lub odwołaniach) są nanoszone automatycznie na widok planu lekcji prezentowanego uczniom/rodzicom,     - system automatycznie weryfikuje, czy w trakcie planowania zastępstw podjęto działania dotyczące wszystkich uczniów zobowiązanych do uczestnictwa w pierwotnych zajęciach i nie dopuszcza do zatwierdzenia realizacji zastępstw, które nie obejmą wszystkich tych uczniów,     - z chwilą zaplanowania zastępstw, dla nauczycieli skierowanych do ich realizacji, zostają wysłane (poprzez wbudowany moduł wiadomości tekstowych) automatycznie powiadomienia o zmianach wprowadzonych w ich planach lekcji,     - umożliwia tworzenie dowolnych kategorii zastępstw oraz powodów nieobecności nauczycieli. System ma możliwość generowania na ich podstawie zestawień umożliwiających co najmniej monitorowanie godzin ponadwymiarowych nauczycieli,     - pozwala dodawać seryjne zastępstwa w przypadku nieobecności długoterminowych oraz pozwalać na seryjne odwoływanie zajęć,     - zapisanie kopii do pliku csv,     - umożliwia podgląd zastępstw pracownikowi sekretariatu. | |
|  | System zapewnia export danych dziennika lekcyjnego każdego oddziału, zajęć dodatkowych, zindywidualizowanej ścieżki kształcenia, nauczania indywidualnego, świetlicy i pedagoga do pliku XML zgodnego z obowiązującymi przepisami. Zadania eksportu danych muszą być kolejkowane. | |
|  | System zawiera funkcjonalność umożliwiającą dwustronną interakcję między użytkownikami w szkole poprzez możliwość przesyłania wiadomości tekstowych wewnątrz systemu (bez udziału zewnętrznych kont poczty elektronicznej). Obsługiwana funkcjonalność:   * + - możliwość przesyłania wiadomości tekstowych pomiędzy dowolnym pracownikiem dydaktycznym szkoły a rodzicami/opiekunami uczniów,     - możliwość przesyłania wiadomości tekstowych pomiędzy dowolnym pracownikiem dydaktycznym szkoły a uczniami,     - wiadomość tekstowa może zawierać linki do stron www,     - do wiadomości wysyłanych przez nauczycieli, sekretariat oraz w przypadku zadań domowych i e-usprawiedliwień jest możliwość dodania załącznika w formie pliku. | |
|  | System zawiera moduł umożliwiający dyrektorowi kontrolę wybranych parametrów związanych z realizacją lekcji poprzez otrzymywanie raportów:   * + - możliwość konfigurowania zakresu danych, które mają być przesyłane w raporcie;     - raporty są przesyłane automatycznie, po uprzednim skonfigurowaniu ich przez dyrektora;     - każdy dyrektor w szkole ma możliwość skonfigurowania dla siebie raportów generowanych w różnych terminach oraz z indywidualnie wybranym zestawem danych;     - w każdym przypadku konfiguracji podlega termin automatycznego przygotowania i dostarczenia na konto dyrektora każdego z w/w raportów (co najmniej poprzez wybór dnia tygodnia lub wyznaczenie dnia miesiąca, w którym regularnie ma być przygotowywany dany raport. Rytm generowania jest konfigurowany dla każdego raportu indywidualnie).   Zakres danych, które można otrzymać w raportach obejmuje:   * + - wykaz brakujących wpisów frekwencji i tematów zajęć (zestawienie braków przypadających na każdego nauczyciela) z zajęć z klasami,     - zestawienie imiennej listy uczniów, których absencja na zajęciach z klasą przekroczyła zdefiniowany procent (np. wskazujący na brak realizacji przez ucznia obowiązku szkolnego),     - zestawienie imiennej listy uczniów, których średnia semestralna spadła poniżej określonej wartości według przedmiotów (np. grożącej brakiem uzyskania promocji do kolejnej klasy),     - listę nauczycieli z informacją ile ocen wystawili. | |
|  | System automatycznie informuje wychowawcę klasy o zaleceniach wprowadzonych przez dyrektora (np. za pomocą wiadomości systemowej). | |
|  | Dokumentowanie zajęć innych niż lekcje | |
|  | System daje możliwość prowadzenia dokumentacji innych zajęć niż lekcje (obowiązkowe zajęcia edukacyjne) np. kół zainteresowań, zajęć sportowych, zajęć pomocy psychologiczno- pedagogicznej poprzez:   * + - umożliwienie stworzenia dziennika zajęć dla wybranej grupy uczniów (niekoniecznie z tej samej klasy),     - umożliwienie stworzenia planu zajęć,     - umożliwienie wprowadzenia tematów zajęć (również z wykorzystaniem listy stworzonej przez nauczyciela) oraz odnotowania frekwencji uczniów na zajęciach,     - umożliwienie dyrektorowi i szkolnemu administratorowi kontrolę liczby ilości zajęć dodatkowych prowadzonych w szkole oraz poprawność ich dokumentacji,     - umożliwienie oceniania postępów ucznia oraz wystawiania wniosków odnośnie dalszego uczestnictwa ucznia w zajęciach,     - umożliwienie zaplanowania przydzielenia zastępstwa doraźnego, przeniesienia zajęć na inny termin czy przesunięcia zajęć, a także oraz odwołania ich;     - umożliwienie eksportu dokumentacji do pliku XML zgodnego z przepisami MEN. | |
|  | System zapewnia możliwość dokumentowania nauczania indywidualnego poprzez:   * + - zdefiniowanie indywidualnego planu lekcji ucznia w oparciu o dowolny zakres czasu definiowany przez nauczyciela,     - system umożliwia zdefiniowanie dla każdego ucznia okresu skierowania go na nauczanie indywidualne oraz wskazanie zajęć, które będzie realizował w trybie indywidualnym oraz jednocześnie takich, z których ewentualnie został zwolniony,     - system uwzględnia dane o ocenach ucznia realizującego nauczanie indywidualne w statystykach klasy, do której przynależy (np. zestawieniach klasyfikacji),     - system wyświetla w jednym widoku wszystkich uczniów objętych nauczaniem indywidualnym z możliwością ich sortowania np. wg okresu objęcia nauczaniem indywidualnym,     - system umożliwia wprowadzenie zastępstw doraźnych, przeniesienia zajęć na inny termin oraz przesunięcia zajęć realizowanych w ramach nauczania indywidualnego; pozwala także na odwołanie takich zajęć. | |
|  | System umożliwia prowadzenie dokumentacji zindywidualizowanej ścieżki kształcenia poprzez:   * + - zdefiniowanie dla każdego ucznia okresu przyznania mu zindywidualizowanej ścieżki kształcenia,     - zdefiniowanie sposobu uczęszczania na dane zajęcia tj. określenie, na które zajęcia uczeń będzie uczęszczał indywidualnie, na które indywidualnie i z klasą, a z których zostanie zwolniony,     - uwzględnienie danych o ocenach ucznia realizującego zindywidualizowaną ścieżkę kształcenia w statystykach klasy, do której przynależy,     - umożliwienie stworzenia planu zajęć dla ucznia,     - umożliwienie zaplanowania przydzielenia zastępstw doraźnych, przeniesienia zajęć na inny termin oraz a, czy przesunięcia zajęć, a także odwołania ich,     - umożliwienie eksportu dokumentacji do formatu XML zgodnego z przepisami MEN. | |
|  | System posiada możliwość prowadzenia dziennika pracy świetlicy, który będzie umożliwiał:   * + - szczegółową ewidencję pobytu uczniów w świetlicy (system automatycznie proponuje godzinę przyjścia i wyjścia zgodnie z czasem systemowym komputera, pozwala także ją modyfikować);     - sprawdzenie aktualnej liczby uczniów w świetlicy;     - prezentowanie podsumowania dziennego oraz tygodniowego ilości godzin spędzonych w świetlicy oraz historii zapisów ucznia do świetlicy w porządku chronologicznym (z dokładnością do minut);     - prezentowania liczby uczniów obecnych w świetlicy w poszczególnych godzinach;     - jednoczesne prowadzenie dziennika przez kilku nauczycieli w różnych salach;     - zarejestrowanie planu pracy świetlicy, planu nauczycieli oraz wprowadzanie tematów zajęć;     - zapisanie dziennika do pliku XML zgodnego z przepisami MEN. | |
|  | System umożliwia prowadzenie dziennika pedagoga i psychologa szkolnego, które obejmują:   * + - dokumentowanie tygodniowego rozkładu swoich zajęć,     - dokumentowanie czynności przeprowadzonych w poszczególnych dniach,     - dokumentowanie informacji o kontaktach z osobami i instytucjami,     - dokumentowanie imion i nazwisk uczniów objętych różnymi formami pomocy,     - zapisanie kopii do pliku zgodnego z przepisami MEN. | |
|  | System zapewnia moduł wsparcia zdalnego nauczania, który obejmuje:   * + - Możliwość zintegrowania z Systemem dysku sieciowego nauczyciela (np. Google, Microsoft) polegającego co najmniej na możliwości (bez konieczności przechodzenia do niego i odrębnego logowania się):       * przesyłania uczniom plików (np. jako załącznika do pracy własnej),       * otrzymywania plików od uczniów (np. jako załącznika z rozwiązaniem prac własnych).     - Możliwość przygotowania oraz udostępnienia uczniom (na ich kontach w systemie) lekcji obejmujących:       * temat,       * materiały multimedialne (w formie plików z dysku sieciowego, linków do zasobów w internecie).     - Możliwość umieszczania w kalendarzu uczniów informacji o planowanych na dowolnych zewnętrznych platformach wideolekcjach (wraz z aktywnym linkiem umożliwiającym uczniom dołączanie do spotkania).     - Widok umożliwiający dyrektorowi wgląd w listę zaplanowanych w sposób opisany powyżej lekcji.     - Możliwość kontrolowania liczby prac własnych przydzielonych do lekcji uczniom w szkole. | |
|  | Pozostała funkcjonalność | |
|  | System posiada moduł ankietowania rodziców uczniów, uczniów oraz nauczycieli. Wyniki ankiet w sposób automatyczny są widoczne dla autora ankiety z możliwością eksportu danych do arkusza kalkulacyjnego np. Excel.  Dyrektor ma możliwość definiowania odbiorców ankiety z podziałem na co najmniej:   * + - rodzice uczniów,     - uczniowie,     - nauczyciele (z uwzględnieniem nauczycieli bez przydziałów, np. pedagog, nauczyciel świetlicy).   Stworzenie ankiety polega na wprowadzaniu przez przeglądarkę pytań oraz odpowiedzi, które potem wyświetlą się odbiorcom ankiety w postaci formularza internetowego umożliwiającego wypełnienie ankiety bezpośrednio na stronie internetowej. Rozwiązanie to nie jest oparte o zewnętrzne systemy do ankietowania ani zamieszczanie linku do ankiety zapisanej (treść ankiety oraz jej wyniki) gdzie indziej niż w bazie danych DE (jak np. moduł Google Forms - tak aby nie istniała potrzeba akceptacji zewnętrznego regulaminu korzystania z takich usług oraz przechowywania danych poza bazą danych DE).  Ankiety obsługują wprowadzenie co najmniej następujące typy pytań:   * + - Pytanie jednokrotnego wyboru;     - Pytanie wielokrotnego wyboru;     - Pytanie otwarte;     - Pytanie warunkowe;     - Skala ocen; | |
|  | System umożliwia wychowawcom klas odnotowywanie tematyki zebrań  z rodzicami uczniów oraz frekwencję rodziców na zebraniach (dla każdego ucznia informacja o obecności/nieobecności opiekuna na zebraniu). | |
|  | System posiada moduł ułatwiający dyrektorom monitorowanie stopnia realizacji podstawy programowej na podstawie wpisów tematów lekcji (z przypisanymi umiejętnościami z podstawy programowej). System jest wyposażony  w uniwersalny słownik podstawy programowej (autorstwa PCSS). | |
|  | Aplikacja do obsługi sekretariatu szkolnego | |
|  | Aplikacja jest wyposażona w bibliotekę gotowych szablonów oraz umożliwia wydruki najczęściej wystawianych zaświadczeń m.in. potwierdzenia spełniania obowiązku szkolnego i nauki, list uczniowskich, zestawień i raportów (np.: uczniowie wg rocznika i płci), zwolnienia z wychowania fizycznego i innych przedmiotów. | |
|  | Aplikacja umożliwia prowadzenie oraz wydruk rejestru legitymacji szkolnych. Umożliwia także eksport danych do pliku mLegitymacji ucznia (zgodnie ze standardem MEN). | |
|  | Umożliwia uzupełnianie i wydruk Księgi Ucznia i Księgi Ewidencji oraz eksport Ksiąg Ucznia i Ewidencji do pliku xml w formacie zgodnym z aktualnym rozporządzeniem MEN. | |
|  | Umożliwia prowadzenie rejestru wypadków uczniów. | |
|  | Umożliwia tworzenie zestawień zbiorczych dot. uczniów co najmniej:  wg roczników i płci, specjalnych potrzeb edukacyjnych, dysleksji, uczniów dowożonych do szkoły. | |
|  | Umożliwia wyszukiwanie i filtrowanie danych uczniów (np. wyszukanie ucznia po numerze PESEL, nazwisku, adresie). | |
|  | Umożliwia prowadzenie bazy kandydatów na przyszłych uczniów szkoły  i wspomagać proces naboru oraz prowadzenie archiwum kandydatów. | |
|  | Umożliwia użytkownikom tworzenie szablonów własnych pism i osadzanie  w nich wybranych danych, dotyczących uczniów, co najmniej:   * + - imienia, nazwiska, adresu, numeru identyfikacyjnego, daty i miejsca urodzenia,     - danych matki i ojca dziecka - adresu, imion i nazwisk,     - danych jednostki uczęszczania dziecka, informacji o aktualnym oddziale, numerze w dzienniku.   Przygotowane w ten sposób szablony są możliwe do użycia na zasadzie korespondencji seryjnej - po zaznaczeniu jednego lub wielu uczniów na liście aplikacja musi automatycznie przygotować i umożliwić wydruk dla każdego  z zaznaczonych uczniów indywidualnego pisma wypełnionego wskazanymi danymi. | |
|  | Umożliwia zastosowanie automatycznego mechanizmu promocji uczniów ze skutkiem dla dziennika elektronicznego i e-Sekretariatu. | |
|  | Umożliwia pracę kilku użytkowników jednocześnie, a także ustalenia dla każdego użytkownika indywidualnie praw do edycji konkretnych danych np.: danych w Księdze ucznia, danych kont użytkowników itp. | |
|  | Umożliwia eksport wybranych danych uczniów do plików w formacie PDF, CSV, XLSX, XML SOU do dalszego wykorzystania w innym oprogramowaniu. | |
|  | Umożliwia synchronizację zmian w danych dotyczących uczniów w ramach DE i Sekretariatu co najmniej w zakresie:   * + - aktualizacji danych osobowych uczniów w DE na podstawie danych wprowadzanych do Sekretariatu,     - aktualizacji przynależności uczniów do klasy/skreślenia z listy klasy  w Sekretariacie na podstawie zmiany w DE,     - aktualizacji przynależności uczniów do klasy na podstawie corocznej klasyfikacyjnej promocji uczniów przeprowadzonej w DE lub Sekretariacie. | |
|  | Umożliwia prowadzenie rejestru wydruków:   * + - dodawanie przez użytkownika ręcznie wpisów do rejestru     - konfigurację automatycznego dodawania wpisów do rejestru obejmującą co najmniej możliwość ustalenia wzorca numeracji wydruków zawierającego kolejny numer, miesiąc i rok wydruku oraz ustawienie dla każdej jednostki początkowego numeru wpisu. | |
|  | Umożliwia prowadzenie rejestru kart rowerowych w szkole podstawowej. | |
|  | System pozwala szkole obsłużyć proces tworzenia e-Legitymacji uczniów (zgodnie z rozporządzeniem MEN) oferując co najmniej:   * + - możliwość uzupełnienia niezbędnych danych pracownikowi sekretariatu  w kartotece ucznia (włącznie z możliwością dodania zdjęcia);     - możliwość przesłania przez rodzica cyfrowego zdjęcia do legitymacji  w systemie. Pracownik sekretariatu akceptuje przesłane zdjęcia po weryfikacji ich poprawności;     - pracownik sekretariatu może wygenerować pliki w formacie xml lub csv obejmujące kompletne dane niezbędne do wydruku e-Legitymacji dla pojedynczego ucznia lub grupy (może zaznaczyć uczniów na liście klasy lub wybrać wszystkich w klasie). | |
|  | Aplikacja do przygotowania i wydruku świadectw i arkuszy ocen. | |
|  | Udostępnia dyrektorowi i administratorowi widok statystyki liczby przygotowanych przez nauczycieli w danym momencie druków (świadectw lub arkuszy ocen) w stosunku do wszystkich, które muszą zostać przygotowane. | |
|  | Aplikacja posiada funkcję drukowania świadectw promocyjnych oraz ukończenia szkoły na specjalnym czystym giloszu świadectwa zgodnym  z aktualnym wzorem MEN. | |
|  | Aplikacja pobiera przynajmniej następujące dane z aplikacji DE:   * + - dane osobowe uczniów     - oceny końcowe i roczne. | |
|  | Aplikacja umożliwia import danych uczniów z formatu SOU. | |
|  | Aplikacja umożliwia podgląd świadectwa konkretnego ucznia przed jego wydrukowaniem w formie wizualnie zbieżnej z wyglądem świadectwa papierowego, na tle właściwego koloru gilosza (przy czym aplikacja nie uwzględnia indywidualnych oznaczeń blankietu nadawanych przez producenta gilosza). | |
|  | Aplikacja umożliwia przygotowanie i wydruk wszystkich stron arkuszy ocen zgodnych z aktualnym prawem. | |
|  | Aplikacja umożliwia podgląd arkusza ocen konkretnego ucznia przed jego wydrukowaniem w formie wizualnie zbieżnej z wyglądem wzoru ministerialnego dla arkuszy ocen uzupełnianych w postaci elektronicznej. | |
|  | Aplikacja posiada następujące funkcje:   * + - zakładanie grupy/klasy, w obrębie której każdemu uczniowi można dodać świadectwa i arkusze ocen z całego etapu edukacyjnego,     - wprowadzanie ocen na świadectwo za pomocą numerycznej klawiatury,     - posiada mechanizm automatycznie podpowiadający nauczycielowi podczas wypełniania świadectwa ukończenia szkoły dla młodzieży  (w szkole podstawowej lub ponadpodstawowej) oceny klasyfikacyjne  z przedmiotów zrealizowanych w trakcie całego etapu edukacyjnego (także na podstawie ocen wprowadzonych w system dla danej klasy w poprzednich latach),     - sortowanie listy uczniów względem numeru dziennika, nazwiska lub wyróżnienia czerwonym paskiem,     - możliwość definiowania nazwy szkoły, która zostanie automatycznie przeniesiona na wszystkie świadectwa i arkusze ocen,     - pomijanie drukowania przerywanych linii na świadectwie,     - wydruk na stronach klasyfikacji arkusza ocen adnotacji o realizacji programu nauczania dostosowanego do indywidualnych potrzeb  i możliwości ucznia z niepełnosprawnością intelektualną w stopniu lekkim,     - import danych o szczególnych osiągnięciach ucznia z dziennika elektronicznego (DE),     - słownik wyrazów, które nie mogą pozostać na końcu linii,     - słownik wyrażeń oceniających, ułatwiający nauczycielom przygotowanie śródrocznej i rocznej oceny opisowej dla klas edukacji wczesnoszkolnej  w standardowej szkole podstawowej wraz ze wskaźnikiem informującym nauczyciela ile miejsca na druku świadectwa pozostało w danym momencie (musi być także dostępna możliwość zmiany wielkości czcionki tworzonej oceny opisowej),     - możliwość importu z dziennika elektronicznego (jeśli została tam przygotowana) do modułu świadectwa śródrocznej i rocznej oceny opisowej, przygotowanej dla uczniów klas edukacji wczesnoszkolnej (klasy 1-3  w standardowej szkole podstawowej) oraz eksportu takiej oceny z modułu świadectw do dziennika elektronicznego jeśli została w nim przygotowana lub zmodyfikowana przez nauczyciela (celem zapewnienia tej samej treści oceny opisowej w dokumentacji - zarówno na świadectwie, w arkuszu ocen i dzienniku elektronicznym).     - zapis świadectwa do pliku zewnętrznego z którego możliwy jest ich wydruk bezpośrednio na drukarkę, a wykorzystanie oprogramowania do wydruku tego pliku nie pociąga za sobą konieczności zakupu dodatkowych licencji, np. format PDF,     - możliwość utworzenia słownika nazw przedmiotów funkcjonujących  w danej szkole, aby ułatwić proces uzupełniania świadectw i arkuszy ocen.     - możliwość tworzenia szablonów przedmiotów, rozumianych jako zestawy nazw przedmiotów, właściwe dla konkretnych oddziałów lub kierunków kształcenia     - umożliwienie skopiowania nazw przedmiotów rozszerzonych, pojawiających się na pierwszej stronie świadectwa na świadectwa wybranych uczniów danego oddziału. | |
|  | Podział godzin on-line | |
|  | DE umożliwia administratorowi szkoły (lub po przekazaniu odpowiednich uprawnień innym nauczycielom) wpisać plan lekcji szkoły lub zaimportować go z pliku asc xml. |
|  | Podział godzin jest zintegrowany z innymi modułami DE (w sposób opisany powyżej) dzięki czemu w sposób automatyczny widoczne są w nim dla wszystkich uprawnionych użytkowników wprowadzane zmiany (np. wynikające z zastępstw doraźnych). |
|  | Aktualny podział godzin prezentowany jest on-line zarówno nauczycielom jak  i rodzicom oraz uczniom. |
|  | Podział godzin obejmuje możliwość wpisania planu dyżurów międzylekcyjnych nauczycieli. |
|  | Aplikacja - generator planu lekcji |
|  | Generator planu lekcji dostarczany w wersji desktop, umożliwiający zautomatyzowane przygotowywanie planu lekcji dla szkoły oraz zaimportowanie go do DE (podział godzin on-line) |
|  | System umożliwia szybkie i efektywne układanie planów zajęć nauczycieli z uwzględnieniem czynników wpływających na efektywność prowadzonych zajęć, m.in.: zasad bezpieczeństwa i higieny pracy, organizacji, warunków lokalowych danej szkoły czy też potrzeb nauczycieli. |
|  | Aplikacja umożliwia import danych z arkusza organizacyjnego (asc xml) oraz modyfikację planu lekcji po zmianie arkusza organizacyjnego bez konieczności ponownego układania całości planu lekcji od początku. |
|  | System uwzględnia typowe dla organizacji pracy szkoły sytuacje np. podziału na grupy czy zajęć międzyoddziałowych. |
|  | System umożliwia dokonanie ręcznych modyfikacji ułożonego automatycznie planu. |
|  | System daje możliwość dopasowania planu do specyficznych wymagań narzuconych przez organizację szkoły np. warunki lokalowe i potrzeby nauczycieli.  Wskazywanie optymalnych miejsc, miejsc w których nie ma dostępnych sal, automatyczny dobór sali, zamiana sal bez konieczności zmiany planu itp. |
|  | System daje możliwość definiowania przy układaniu planu lekcji przez program odrębnych założeń dla każdego przedmiotu. |
|  | System zawiera sygnalizację niemożności ułożenia planu w wyniku wystąpienia konfliktu zadanych warunków, ze wskazaniem miejsca konfliktu. |
|  | System daje możliwość definiowania podziałów klas na różnego typu grupy. |
|  | System umożliwia kontrolę maksymalnej liczby godzin pracy nauczyciela  w ciągu jednego dnia. |
|  | System zapewnia równomierne obciążenie nauczycieli i uczniów  w poszczególnych dniach tygodnia. |
|  | System umożliwia definiowanie, minimalizowanie oraz automatyczne kontrolowanie liczby okienek nauczycieli, zarówno w ciągu jednego dnia, jak całego tygodnia. |
|  | System umożliwia drukowanie i zapisywanie planu w różnych definiowalnych formatach (np. xls, pdf). |
|  | System umożliwia obsługę sal szkolnych znajdujących się w różnych budynkach z uwzględnieniem czasu przejścia uczniów. |
|  | System posiada rozbudowaną funkcję cykli – możliwość wyboru, w którym semestrze (oraz tygodniu) ma się odbywać lekcja. |
|  | Aplikacja do obsługi biblioteki szkolnej |
|  | Dostarczony w modelu SaaS, dostępny dla wszystkich użytkowników przez przeglądarkę internetową (co najmniej Edge, Chrome, Safari, Firefox w aktualnych wersjach). Interfejs przygotowany w technologii RWD. |
|  | Integracja z dziennikiem elektronicznym:   * + - Import danych czytelników z systemu DE,     - Aktualizacja przypisania uczniów do klas – na początku roku szkolnego,     - Pracownik biblioteki ma dostęp do modułu wiadomości i ogłoszeń w systemie DE – może np. informować nauczycieli, uczniów i rodziców o zmianach godzin otwarcia biblioteki, przesyłać dodatkowe informacje,     - SSO – jednokrotne logowanie do dziennika elektronicznego oraz systemu bibliotecznego (płynne przejście z DE do aplikacji biblioteki). |
|  | Moduł pracownika biblioteki: |
|  | Dostęp do całej bazy BN. |
|  | Jeżeli w Bibliotece Narodowej zostanie zaktualizowana jakaś informacja w opisach, które wykorzystano w bibliotece szkolnej, to jest ona od razu uaktualniana w systemie. |
|  | Dodawanie egzemplarzy z autopsji (na bazie wcześniej stworzonych opisów). |
|  | Przy ręcznym dodawaniu więcej niż jednego egzemplarza, możliwe jest kopiowanie danych uzupełnionych dla pierwszego egzemplarza. |
|  | Obsługa formatu MARC21 – jeżeli format sugerowany przez BN zostanie zmieniony, to w systemie również zostanie to dostosowane. |
|  | Możliwość wyszukiwania pozycji po dowolnym polu z formatu MARC21. |
|  | Obsługa czytników kodów kreskowych (automatyczne generowanie kodów kreskowych dla każdego egzemplarza i czytelnika oraz możliwość przypisania już istniejących kodów do egzemplarza lub czytelnika). |
|  | Zestawienia i listy – możliwość utworzenia:   * + - Zestawienia bibliograficznego;     - Listy lektur;     - Listy podręczników; |
|  | Prowadzenie Skontrum |
|  | Prowadzenie księgi inwentarzowej oraz rejestru ubytków w systemie, z możliwością ich wydrukowania. |
|  | Obsługa różnych działów biblioteki (w tym również czytelni). |
|  | Wyszukiwanie i obsługa czytników kodów kreskowych (generowanie i wydruk kodów dla czytelników), możliwość wykorzystania (przypisania do czytelnika) istniejących już kodów kreskowych (np. z innych posiadanych przez niego kart). |
|  | Drukowanie etykiet – możliwość wydrukowania etykiet – pracownik decyduje o tym jakie, spośród dostępnych do wyboru, informacje znajdą się na etykiecie oraz w jakim rozmiarze etykiety zostaną wydrukowane. Etykiety mogą zostać wydrukowane na dowolnej drukarce. |
|  | Obsługa czytelników: |
|  | Akceptacja rezerwacji zgłoszonych przez czytelników (proces nie dzieje się automatycznie – pracowni biblioteki zawsze ma możliwość odrzucenia rezerwacji np. w przypadku gdy wie, że egzemplarz został zniszczony, a nie zdążył go ubytkować albo w sytuacji, gdy książka jest rezerwowana w tym samym momencie, gdy inny uczeń ją wypożycza). |
|  | Wyświetlanie list użytkowników zalegających ze zwrotem. |
|  | Wyświetlanie listy rezerwacji nieodebranych. |
|  | Pracownicy biblioteki decydują na jaki czas wypożyczane są książki i jaki jest ich limit liczbowy. |
|  | Pracownicy biblioteki decydują w jakim czasie czytelnik musi odebrać rezerwację i ile książek może maksymalnie zarezerwować. |
|  | Mimo ustanowienia limitów, ostateczna decyzja o dokonaniu rezerwacji, wypożyczenia egzemplarza, wykonania prolongaty zawsze należy do pracownika biblioteki. |
|  | Wysyłanie powiadomień o zbliżających się terminach zwrotów i innych do czytelników. |
|  | Moduł czytelnika: |
|  | Widok listy wypożyczonych i zarezerwowanych książek. |
|  | Możliwość zgłoszenia chęci rezerwacji książki. |
|  | Widok listy lektur. |
|  | Widok listy podręczników. |
|  | Aplikacja nabór elektroniczny |
|  | W części publicznej musi być dostęp do prezentacji oferty edukacyjnej placówek objętych Systemem Elektronicznej Rekrutacji, w tym do opisu oddziałów/grup. |
|  | Użytkownik rodzic/opiekun prawny musi mieć, bez konieczności logowania dostęp do prezentacji zasad naboru oraz terminarza rekrutacji. |
|  | Użytkownik rodzic/opiekun prawny musi mieć, bez konieczności logowania dostęp do plików i instrukcji obsługi systemu dla rodziców. |
|  | System musi umożliwiać dodawanie komunikatów i aktualności dla rodziców przez pracowników Organu Prowadzącego oraz pracownika komisji rekrutacyjnej. |
|  | Po wprowadzeniu miejscowości, ulicy i numeru domu System Elektronicznej Rekrutacji musi mieć możliwość wyszukania właściwej szkołę obwodową kandydata. |
|  | Dla użytkownika rodzic/opiekun prawny musi istnieć możliwość po zalogowaniu do złożenia zgłoszenia do szkoły obwodowej lub wniosku do wybranej placówki poprzez wprowadzenie wymaganych danych niezbędnych do złożenia wniosku takich jak dane osobowe i oznaczenie spełnianych kryteriów, zgodnie z zasadami rekrutacji. W przypadku spełniania poszczególnych kryteriów system umożliwi złożenie oświadczenia w ramach interaktywnych formularzy odzwierciedlających wzór oświadczenia, który funkcjonuje podczas danej rekrutacji. |
|  | Użytkownik rodzic/opiekun prawny na koniec musi mieć możliwość wygenerowania wniosku w formacie pdf. |
|  | Do czasu odbioru zgłoszenia/wniosku elektronicznego w placówce, użytkownik rodzic/opiekun prawny może go edytować i dokonać zmian np. w zakresie preferencji. |
|  | Użytkownik rodzic/opiekun prawny cały czas musi mieć możliwość monitorowania statusu zgłoszenia/wniosku w systemie. |
|  | Jeśli użytkownik rodzic/opiekun prawny zapomni hasła to system musi mieć udostępniony mechanizm przesłania nowego hasła do konta na wskazany w czasie rejestracji adres poczty elektronicznej. |
|  | Użytkownik rodzic/opiekun prawny o wynikach rekrutacji poinformowany zostanie poprzez wysłanie maila na wskazany we wniosku adres poczty elektronicznej. |
|  | Użytkownik rodzic/opiekun prawny musi mieć też możliwość dodatkowo złożyć potwierdzenie woli zapisu do wybranej placówki korzystając z formularza dostępnego z poziomu systemu, który należy podpisać profilem zaufanym. |
|  | Użytkownik rodzic/opiekun prawny musi mieć możliwość udostępnienia wniosku drugiemu rodzicowi, aby ten miał wgląd do wniosku oraz możliwość podpisania go profilem zaufanym. Udostępnienie powinno być dodatkowo zabezpieczone kodem weryfikacyjnym. |
|  | W Systemie Elektronicznej Rekrutacji musi istnieć opcja tworzenia przez placówki objęte systemem oddziałów/grup rekrutacyjnych wraz z ich opisem. |
|  | Organ prowadzący musi mieć możliwość kontrolowania wpisów związanych z utworzonymi oddziałami/grupami rekrutacyjnymi w zakresie podglądu i edycji wprowadzonych przez placówkę informacji. |
|  | Pracownik każdej placówki wskazanej we wniosku bez względu na kolejność preferencji musi mieć możliwość odebrania i potwierdzenia wniosku wraz z kryteriami. W przypadku zgłoszeń do szkół obwodowych w systemie, odebranie i potwierdzenie ma miejsce tylko przez szkołę wskazaną jako szkoła obwodowa. |
|  | System musi dawać możliwość podglądu wprowadzonej listy kandydatów obwodowych, w tym zaimportowania pliku w formacie XLS z listą kandydatów obwodowych. |
|  | Użytkownik rodzic/opiekun prawny musi mieć możliwość złożenia oświadczenia o zamieszkiwaniu w obwodzie szkoły jako załącznika do złożonego zgłoszenia w ramach formularza dostępnego z poziomu systemu, który należy podpisać profilem zaufanym. |
|  | System musi umożliwiać przyporządkowanie dzieci posiadających orzeczenie o potrzebie kształcenia specjalnego do oddziałów/grup rekrutacyjnych przeznaczonych dla dzieci z orzeczeniem w drodze indywidualnej decyzji dyrektora placówki wskazanej przez rodzica na liście preferencji. |
|  | System musi umożliwiać ustalenie kolejności przyjęć dzieci, które uzyskały tę samą liczbę punktów w procesie rekrutacji na podstawie spełnianych przez kandydata kryteriów przyjęć. |
|  | System Elektronicznej Rekrutacji musi umożliwiać tworzenie i przygotowania do publikacji list dzieci przyjętych i list dzieci nieprzyjętych. |
|  | System Elektronicznej Rekrutacji musi umożliwiać przeprowadzenia procesu rekrutacji uzupełniającej według zasad naboru z wykorzystaniem wszystkich mechanizmów wykorzystanych na pierwszym etapie rekrutacji. |
|  | System Elektronicznej Rekrutacji musi umożliwiać wysyłanie przez uprawnionych pracowników Organu Prowadzącego komunikatów do wszystkich użytkowników placówek, którzy mają założone konta w systemie. |
|  | Organ Prowadzący musi mieć możliwość pobierania z systemu raportów, zwierających takie informacje jak: liczba miejsc w oddziałach/grupach rekrutacyjnych, liczba zgłoszeń kandydatów obwodowych, liczba dzieci zakwalifikowanych i niezakwalifikowanych, liczba dzieci przyjętych i nieprzyjętych, informacja o spełnianych kryteriach przez kandydatów. |
|  | Organ Prowadzący może oraz pracownicy komisji rekrutacyjnej muszą mieć mieć dostęp do obsługi procesu symulacji przydziału. W zależności od nadanych uprawnień muszą mieć dostęp do generowania, podglądu oraz zatwierdzania symulacji, a także pobrania z widoku symulacji arkusza kalkulacyjnego z danymi zawartymi w raporcie. |
|  | Organ Prowadzący musi mieć możliwość w toku rekrutacji dokonywania korekt w ofertach placówek objętych elektronicznym systemem rekrutacji, w tym dodawania oddziałów/grup rekrutacyjnych oraz zmiany w zakresie liczby miejsc w oddziałach czy grupach. |
|  | Użytkownik rodzic/opiekun prawny musi mieć możliwość podpisania wniosku profilem zaufanym. |

### 1.5.2 Moduł finansowo-księgowy

System funkcjonujący zgodnie z ustawą o rachunkowości z uwzględnieniem specyfiki jednostek oświatowych do zarządzania i obsługi finansowo-księgowej. Wspomaga zarządzanie finansami, sprawozdawczość budżetową i finansową a także umożliwia szczegółową analizę danych i zwiększenie kontroli finansowej. Umożliwia prowadzenie rozrachunków jednostek oświatowych wraz z bieżącą kontrolą należności i zobowiązań, wraz z podstawową windykacją należności. Pozwana na obsługę obrotu gotówkowego w zakresie wielu niezależnych kas, a także na podstawie wprowadzonych dokumentów sprzedaży i zakupu - prowadzenie cząstkowego rejestru VAT.

System:

1. posiada jedną centralną bazę, dostępną przez Internet dla wszystkich podległych jednostek;
2. wspólna baza gromadzi dane o wszystkich jednostkach oświatowych, klasyfikacji budżetowej i zadaniach. Dane te są pobierane z jednego miejsca do wszystkich słowników w systemie;
3. plan kont ogranicza się do operacji gospodarczych i nie zawiera danych o kontrahentach, klasyfikacji budżetowej i zadaniach.

System umożliwia:

1. pobieranie danych kontrahentów automatycznie z systemu GUS;
2. automatyczne księgowanie dekretów płacowych na podstawie informacji z systemu płacowego;
3. oznaczanie statusów określających stan prac nad dokumentem (w trakcie opracowywania, gotowy);
4. tworzenie zestawień obejmujących dane wszystkich jednostek, zgodnie z nadanymi prawami;
5. generowanie Jednolitych Plików Kontrolnych (KR, WB, FA, VAT);
6. drukowane kilku dokumentów jednocześnie;
7. zapisywanie szablonów ustawień dla zestawień;
8. zdefiniowanie globalnych definicji sprawozdań budżetowych, finansowych a także wspólnego planu kont;
9. rejestrowanie czynności wykonywanych przez użytkowników w dzienniku zdarzeń.

**1.5.2.1 W zakresie dotyczącym obsługi finansowo-księgowej:**

1. modyfikowanie planu kont do własnych potrzeb (bez konieczności uwzględniania klasyfikacji budżetowej, zadania oraz kontrahenta) wraz z funkcją drukowania;
2. możliwość dekretacji w podziale na klasyfikację budżetową, kontrahenta, rodzaj planu i zadania;
3. dostęp do bazy kontrahentów ze wszystkich obszarów systemu;
4. niezależną numerację dokumentów w obrębie dziennika i automatyczną numerację dokumentów;
5. obsługę zamknięcia miesiąca i roku obrachunkowego;
6. dwustopniowe wprowadzanie dokumentów polegające na: zapisie w trybie możliwej modyfikacji, a następnie ich księgowania;
7. kontrolę bilansowania się dokumentu;
8. automatyczne tworzenie dokumentu księgowego na podstawie planu finansowego, faktur, raportów kasowych, wyciągów bankowych, not księgowych, wraz z możliwością drukowania dokumentu księgowego i jego dekretacji
9. możliwość sprawdzenia z poziomu dokumentu księgowego, danych dokumentów źródłowych (np. na fakturze zakupu);
10. automatyczne otwieranie nowego roku obrachunkowego (mechanizm tworzenia bilansu otwarcia, którego zapisy odpowiadają saldom kont w bilansie zamknięcia), wraz z możliwością przeglądania danych z kolejnych lat obrachunkowych;
11. tworzenie zestawień i wydruków (jednostkowo, zbiorczo, z wybranych jednostek):

* obrotów i sald oraz obrotów na koncie (wraz z możliwością przejścia z zestawienia obrotów i sald do obrotów na koncie, a następnie do pozycji dokumentu);
* kontrola realizacji planu;
* sprawozdań budżetowych: Rb-27S, Rb-27ZZ, Rb-28S, RB-30s, Rb-34S, Rb-Z, Rb-N, Rb-50, Rb-UZ wraz z eksportem do Besti@, a także Rb-23, Rb-27, Rb-28zestawień rozrachunkowych kontrahentów, sald i wezwań do zapłaty;
* sprawozdań finansowych wg rozporządzenia (bilans budżetowy rachunek zysków i strat (wariant porównawczy), zestawienie zmian w funduszu jednostki) z eksportem do Besti@; informacja dodatkowa do bilansu;
* sprawozdań finansowych wg załącznika nr 1 do ustawy (bilans, rachunek zysków i strat (wariant porównawczy)) wraz z zapisem roboczej wersji sprawozdań do pliku XML;
* zestawień z dokumentów źródłowych, zamówień;

1. uwzględnianie wprowadzonych wstępnie dokumentów w analizie konta księgowego i analizie wydatków oraz podczas porównywania z planem budżetowym;
2. kontrolę realizacji wydatków na sprawozdaniu Rb-28S (ostrzeżenie), oraz szybką analizę kwot wyliczonych na sprawozdaniach: Rb-27s, Rb-27, Rb-28, Rb-28s, Rb-30s, Rb-34s, Rb-Z, Rb-N;
3. grupową generację dokumentów księgowych z dokumentów źródłowych;
4. zapisywanie szablonów ustawień w zestawieniach;
5. prowadzenie raportów kasowych (RK) oraz dokumentów kasowych (KP, KW) dla kilku kas, wraz z możliwością drukowania;
6. tworzenie zestawienia wpłat i wypłat kasowych oraz zestawienia środków kasowych wraz z wydrukiem;
7. wprowadzanie wyciągów bankowych, wraz z możliwością importu wyciągów w formacie MT940 z banków (ING, PKO BP, PeKaO SA, Millenium, Bank Spółdzielczy z grupy BPS lub SGB)
8. podgląd i wydruk sald kontrahentów;
9. tworzenie not odsetkowych dla nieterminowych płatności dokumentów sprzedaży i należności z dokumentów PK, wraz z możliwością drukowania;
10. tworzenie zestawień: rozrachunkowych, not odsetkowych oraz wezwań do zapłaty;
11. obsługę eksportu przelewów z możliwością tworzenia paczek przelewów w układzie płatności podzielonej i zwykłej, a także z możliwością uwzględnienia pozycji z paczki przelewów w tworzonym wyciągu bankowym;
12. weryfikację danych kontrahenta w wykazie podatników VAT (KAS), na etapie tworzenia paczki przelewów;
13. wprowadzanie dokumentów sprzedaży i ich korekt wraz z możliwością wydruku, oraz dokumentów zakupu (wraz możliwością oznaczanie pozycji faktury zakupu współczynnikiem proporcji (art. 86 ustawy o VAT), a także sposobem opodatkowania (zakup związany ze sprzedażą));
14. tworzenie zestawienia dokumentów sprzedaży, zakupów, not księgowych wraz z wydrukiem;
15. kontrolowanie realizacji planu we wprowadzonym dokumencie zakupu;
16. obsługę faktur realizowanych płatnością podzieloną (split payment);
17. obsługę umów sprzedaży wraz z automatycznym generowaniem dokumentów sprzedaży;
18. obsługę rekompensat 40/70/100 euro za koszty odzyskiwania należności;
19. obsługę not księgowych własnych i obcych;
20. obsługę zaliczek (wnioski i rozliczenie zaliczki);
21. prowadzenie listy zamówień publicznych wraz z przypisywaniem zamówienia do dokumentu zakupu oraz tworzeniem zestawienia z realizacji zamówień a także danymi do druku ZP-SR;
22. prowadzenie ewidencji cząstkowej VAT i rejestru dokumentów sprzedaży i zakupu wraz z możliwością drukowania dla każdej jednostki;
23. możliwość tworzenia wielu wersji ewidencji VAT dla każdej jednostki;
24. tworzenie pliku JPK\_V7M (format ustrukturyzowany), wraz z możliwością określenia zawartości pliku (ewidencja z deklaracją, tylko deklaracja, tylko ewidencja) a także w celu złożenia (po raz pierwszy, korekta) oraz tworzenie pliku JPK\_V7M cząstkowego z danymi w części deklaracyjnej w groszach;
25. generowanie pliku PDF podsumowującego dla podatku od towarów i usług (rozliczenie podatku należnego i naliczonego), w ujęciu do pełnych złotych i w groszach;

**1.5.2.2 System do planowania i zatwierdzania organizacji oraz (wraz z systemem raportowania)**

System planowania i zatwierdzania organizacji (System) dostarcza jednostce samorządu terytorialnego funkcje ułatwiające gromadzenie, przechowywanie i przetwarzanie danych celem usprawnienia i przyspieszenia wykonywania codziennych obowiązków oraz uzyskania informacji umożliwiających podejmowanie optymalnych decyzji. Wspiera JST w obsłudze procesu planowania i zatwierdzania organizacji.

System:

1. korzysta z centralnego rejestru jednostek i użytkowników, w tym z centralnie definiowanej struktury jednostek sprawozdawczych;
2. jest wyposażony w centralne słowniki na potrzeby przygotowania projektu arkusza i projektu planu finansowego;
3. zapewnia na poziomie organu prowadzącego możliwość zatwierdzenia arkusza organizacyjnego przygotowanego w systemie oraz dalsze jego analizowanie.

System umożliwia:

1. centralne definiowanie warunków kontroli poprawnego opisu arkuszy przez dyrektora i sygnalizuje potencjalne nieprawidłowości w zakresie:

* wymaganej liczebności oddziałów w zależności od typu szkoły,
* liczebności grup na wybranych zajęciach (np. na zajęciach wychowania fizycznego, języków),
* maksymalnych wymiarów etatów nauczycielskich w zależności od stanowiska (np. dyrektor, nauczyciel przedmiotu),
* pensum bazowego dla wybranego stanowiska (np. bibliotekarza),
* minimalnego stażu pedagogicznego;

1. prowadzenie niezależnych od arkusza rejestrów oddziałów, pracowników i przedmiotów na poziomie jednostki oświatowej tak, aby możliwe było śledzenie niezmienności planów nauczania oddziałów w kolejnych latach cyklu nauczania;
2. możliwość opisania zajęć międzyoddziałowych, pozalekcyjnych oraz innych zajęć edukacyjnych;
3. dokonywanie wyboru nauczyciela pełniącego funkcję wychowawcy i opiekuna stażu z istniejącej listy nauczycieli;
4. budowanie planu nauczania dla wybranego oddziału szkolnego, również na cały cykl kształcenia;
5. kopiowanie planów nauczania tak, aby można było wykorzystać raz zdefiniowany plan nauczania dla różnych oddziałów;
6. wskazanie w planie nauczania godzin do dyspozycji dyrektora, godzin JST;
7. definiowanie godzin realizowanych w układzie tygodniowym, semestralnym i rocznym;
8. budowę planów nauczania dla szkół działających w układzie semestralnym;
9. kontrolę zgodności planów nauczania poszczególnych oddziałów z planami ramowymi poza szkołami artystycznymi;
10. rejestrację danych pracowników jednostek oświatowych w zakresie niezbędnym do budowy arkusza oraz wyliczenia kosztów organizacji na potrzeby projektu planu finansowego;
11. definiowanie przydziałów czynności nauczycieli, w tym w podziale na grupy i w ramach grup międzyoddziałowych;
12. rejestrację kilku niezależnych umów nauczyciela w tej samej jednostce oświatowej;
13. automatyczne wyliczanie średniorocznych wymiarów etatów nauczycieli na podstawie przydzielonych zajęć, na podstawie pensum zajęć oraz okresu ich prowadzenia;
14. wyliczanie wymiarów etatu nauczycieli prowadzących zajęcia z różnych pensów na podstawie uśrednionego pensum definiowanego na poziomie umowy nauczycielskiej;
15. definiowanie przewidzianych przez przepisy zniżek obowiązkowego wymiaru godzin;
16. tworzenie wydruku projektu arkusza (dokument zatwierdzający i/lub tzw. płachty);
17. tworzenie aneksów do arkusza;
18. przygotowanie przez jednostkę oświatową arkusza na nowy rok szkolny poprzez wykorzystanie danych arkusza z poprzedniego roku szkolnego;
19. budowę kompletnego projektu planu finansowego w obszarze dochodów   
    i wydatków budżetowych dla wszystkich typów jednostek oświatowych, w tym   
    z możliwością przeliczenia kosztów związanych z realizacją planowanej organizacji z arkusza organizacyjnego;
20. na podstawie zgromadzonych danych przygotowywanie wydruków dla poszczególnych jednostek oświatowych, jak i zbiorczo:

* projektu,
* wniosku o zmianę planu,

1. ułatwia automatyczną weryfikację poprawności sprawozdań budżetowych i sygnalizuje potencjalne nieprawidłowości. Mechanizm kontroluje powiązania pomiędzy poszczególnymi elementami sprawozdania Rb-27s i Rb-28s według następujących warunków:

* dla wykonania dochodów:
  + Dochody wykonane + (należności pozostałe do zapłaty - nadpłaty) = należności,
* dla wykonania wydatków:
  + Wydatki równe lub niższe niż plan,
  + Wydatki + zob. ogółem równe lub niższe niż plan,
  + Wydatki + zob. ogółem równe lub niższe niż zaangażowanie,
  + Zaangażowanie równe lub niższe niż plan albo równe lub wyższe od wydatków,
  + Zaangażowanie równe lub niższe niż plan.

1. umożliwia zbiorczą analizę zgromadzonych danych arkuszy organizacyjnych za pomocą MS Excel, w tym zapewniających możliwość analizy:

* liczby uczniów / oddziałów w każdym typie placówek, rodzaju oddziału, specjalności,
* nauczycielskich etatów przeliczeniowych w układzie jednostek oświatowych,
* etatów losowych i etatów wsparcia,
* specjalności nauczycieli,
* zgodności przydziałów z kwalifikacjami,
* zatrudnienia nauczycieli wg stopni awansu, pełnionych funkcji, nauczanych przedmiotów;

**1.5.2.3 Obsługa środków trwałych**

System wspierający prowadzenie ewidencji środków trwałych oraz wartości niematerialnych i prawnych dla jednostki oświatowej oraz centrum usług wspólnych. Umożliwia prowadzenie kartotek środków trwałych a także naliczanie rat amortyzacyjnych oraz ewidencję operacji specjalnych dla środków trwałych. System jest bezpośrednio powiązany z księgowością zapewniając natychmiastowy przepływ informacji i księgowanie dokumentów, eliminując tym samym konieczność wielokrotnego wprowadzania tych samych informacji.

System umożliwia:

1. prowadzenie ewidencji środków trwałych i wartości niematerialnych i prawnych;
2. przypisanie informacji dodatkowych do kartotek takich jak m.in. składowe ŚT, opis, dane techniczne;
3. wykonanie symulacji amortyzacji do końca okresu użytkowania;
4. rejestrowanie zwiększeń i zmniejszeń wartości środków trwałych wraz z możliwością stworzenia dokumentu księgowego;
5. zmianę wprowadzonej stawki amortyzacji;
6. tworzenie planu amortyzacji wg metody amortyzacji liniowej, degresywnej lub jednorazowej;
7. tworzenie listy naliczeń;
8. wycofywanie naliczonej amortyzacji;
9. wprowadzenie operacji likwidacji lub trwałego odłączenia składowej środków trwałych;
10. przypisanie indywidualnych kont księgowych dla kartotek środków trwałych i wartości niematerialnych i prawnych;
11. bezpośrednie księgowanie operacji specjalnych w księgowości, bez konieczności dwukrotnego wprowadzania tych samych informacji;
12. powiązanie dokumentu zakupu ze środkiem trwałym;
13. tworzenie zestawień wraz z zapisywaniem szablonów ustawień;
14. drukowanie dokumentów oraz zestawień.

**1.5.2.4 Obsługa płacowa podległych jednostek oświatowych**

System dostarcza funkcje ułatwiające naliczanie płac, uwzględniając specyficzne zasady naliczania wynagrodzeń nauczycieli. Uwzględnia obowiązujące przepisy prawne takie jak naliczanie składek na ubezpieczenia społeczne i zdrowotne, ustalanie zaliczki na podatek dochodowy od osób fizycznych.

System umożliwia:

**1.5.2.5 W zakresie dotyczącym obsługi płacowej**

1. pobieranie danych osobowych oraz danych dotyczące umów pracowniczych i cywilnoprawnych z systemu obsługującego kadry pracującego na wspólnej bazie danych;
2. prowadzenia wspólnych zasad naliczania płac we wszystkich podległych jednostkach;
3. sporządzanie i drukowanie list wypłat, comiesięcznych oraz sporadycznych, np. wypłata nagród, składników socjalnych;
4. przypisywanie kilku rozdziałów klasyfikacji budżetowej do jednej umowy pracownika (w sytuacji, kiedy pracownik realizuje etat w więcej niż jednym rozdziale);
5. aby na listach wypłat były wykazywane należne składniki wynagrodzenia lub świadczenia oraz naliczonych od nich składek na ubezpieczenia społeczne i ubezpieczenie zdrowotne, a także zaliczka na podatek dochodowy od osób fizycznych;
6. rejestrowanie i rozliczanie na liście płac potrąceń własnych pracownika, np. składka na Zw. Zaw., spłata pożyczki z KZP;
7. dokonywanie wyrównania wypłacanego wynagrodzenia za dowolne miesiące;
8. automatyczne wyliczanie godzin nadliczbowych pracowników niepedagogicznych;
9. rozliczać nieobecności dla umów o pracę i umów cywilnoprawnych;
10. eksportowanie:

* comiesięcznych dokumentów rozliczeniowych do ZUS za pomocą systemu „Płatnik”,
* wypłat i potrąceń w układzie klasyfikacji budżetowej do systemu księgowego,
* przelewów do bankowości elektronicznej,
* danych do Systemu Informacji Oświatowej;

1. tworzenie, na podstawie danych zgromadzonych w systemie, raportów i zestawień dla potrzeb analiz i sprawozdawczości z wybranej lub wielu jednostek;
2. dostarczanie danych niezbędnych do wypełniania sprawozdań GUS w zakresie danych o zatrudnieniu i czasie pracy;
3. dostarczanie danych do sporządzania przelewów oraz formularzy PIT (PIT-11, PIT-4R, PIT-8AR);
4. wygenerowanie formularzy IFT-1 i IFT-1R;
5. wysyłkę danych do systemu e-Deklaracje;
6. importowanie elektronicznych zwolnień lekarskich (e-ZLA) z portalu ZUS;
7. obsłużenie procesu Pracowniczych Planów Kapitałowych;
8. przygotowanie danych do naliczeń jednorazowego dodatku uzupełniającego;
9. import godzin ponadwymiarowych z dziennika elektronicznego i pliku XLS;
10. eksport przelewów do systemów bankowych;
11. wymianę e-Deklaracji;
12. eksport danych do Płatnika, GUS, SIO;
13. rejestr zmian.

**1.5.2.6 Jednorazowy Dodatek Uzupełniający Art.30**

System ułatwia JST wyliczenie wysokości dodatku uzupełniającego zgodnie z art.30a Karty Nauczyciela. Kwoty dodatków dla nauczycieli są przygotowane w podziale na stopnie awansu zawodowego dla poszczególnych jednostek. System umożliwia pozyskanie danych z programu do obsługi kadrowo-płacowej.

System umożliwia:

1. korzystanie z funkcjonalności pozwalających na wyznaczenie:

* średniego wynagrodzenia oraz średniorocznej struktury zatrudnienia,
* średnich wynagrodzeń nauczycieli na poszczególnych stopniach awansu zawodowego,
* kwot różnic między wynagrodzeniami należnym a faktycznie wypłaconym,
* podziału jednorazowego dodatku uzupełniającego między poszczególne placówki w podziale na stopnie awansu zawodowego;

1. gromadzenie danych pochodzących z systemu płacowego:

* liczbę etatów w podziale na miesiące,
* stopnie awansu zawodowego i placówki,
* faktycznie poniesione wydatki na wynagrodzenia nauczycieli – również w podziale na miesiące i stopnie awansu,
* współczynniki podziału niedopłaty (tj. osobista stawka wynagrodzenia zasadniczego);

1. wyżej wymienione metody obliczeń wynikające z zapisów w art. 30a Karty Nauczyciela winny być zgodne z Rozporządzeniem Ministra Edukacji Narodowej w sprawie sposobu opracowywania sprawozdania z wysokości średnich wynagrodzeń nauczycieli na poszczególnych stopniach awansu zawodowego w szkołach prowadzonych przez jednostki samorządu terytorialnego;
2. bieżącą kontrolę kompletności wprowadzanych danych;
3. bieżącą weryfikację poprawności;
4. bieżącą kontrolę kwoty niedopłaty (w poszczególnych miesiącach);
5. sporządzenie raportu dla RIO zgodnie ze wzorcem publikowanym przez MEN;
6. publikowanie wyników z przeprowadzonych analiz – kwot dodatków uzupełniających dla nauczycieli w poszczególnych placówkach;
7. jednostkom oświatowym zdalny dostęp do swoich danych płacowych, które zostały zgromadzone w aplikacji, oraz ich modyfikację lub sukcesywne uzupełnianie;
8. jednostkom oświatowym pobranie odpowiednich danych niezbędnych do przygotowania wypłat jednorazowego dodatku uzupełniającego dla nauczycieli zatrudnionych w tych jednostkach.

**1.5.2.7 Dotacje podręcznikowe**

System służy do gromadzenia informacji i wniosków o dotacje na zakup podręczników i materiałów ćwiczeniowych ze szkół prowadzonych i nieprowadzonych przez JST oraz do przygotowania zbiorczych wniosków i rozliczeń dotacji.

System umożliwia:

1. wypełnianie przez jednostki oświatowe elektronicznych formularzy będących odpowiednikiem formularzy ministerialnych „informacji” niezbędnych do pozyskania dotacji celowej na wyposażenie szkół w podręczniki, materiały edukacyjne i materiały ćwiczeniowe;
2. wypełnianie przez jednostki oświatowe nieprowadzone przez JST elektronicznych formularzy będących odpowiednikiem formularzy ministerialnych „informacji” oraz wniosków niezbędnych do pozyskania dotacji celowej na wyposażenie szkół w podręczniki, materiały edukacyjne i materiały ćwiczeniowe;
3. zablokowanie przez JST możliwości dokonywania zmian w informacjach i wnioskach, które wprowadziły jednostki oświatowe prowadzone i nieprowadzone przez JST;
4. automatyczne wygenerowanie przez JST zbiorczego wniosku o dotacje celowe na wyposażenie szkół w podręczniki, materiały edukacyjne i materiały ćwiczeniowe, na podstawie wprowadzonych przez jednostki oświatowe danych;
5. wypełnianie przez jednostki oświatowe prowadzone i nieprowadzone przez JST korekt „informacji” i wniosków;
6. zablokowanie przez JST możliwości dokonywania zmian w korektach do „informacji” i wniosków, które wprowadziły jednostki oświatowe prowadzone i nieprowadzone przez JST;
7. automatyczne wygenerowanie przez JST zbiorczej korekty wniosku o dotacje celowe, na podstawie wprowadzonych przez jednostki oświatowe danych;
8. przygotowanie rozliczeń wykorzystania dotacji celowej przez jednostki oświatowe prowadzone i nieprowadzone przez JST;
9. wygenerowanie przez JST zbiorczego rozliczenia wykorzystania dotacji celowej;
10. automatyczne sygnalizowanie przez system wykrytych możliwych nieprawidłowości i braków we wprowadzonych przez jednostki oświatowe danych;
11. zgodność wzorów dokumentów generowanych przez system z obowiązującymi przepisami;
12. automatyczne aktualizowanie ewentualnych zmian stawek dotacji celowej;
13. eksportowanie „informacji”, korekt i rozliczeń dotacji celowej jednostek oświatowych prowadzonych i nieprowadzonych przez JST do formatu „\*.xls”, według obowiązujących wzorów MEN;
14. eksportowanie w module dla JST zbiorczego wniosku, korekty i rozliczeń dotacji celowej do formatu „\*.xls”, według obowiązujących wzorów MEN;
15. podgląd aktualnych kwot dotacji.

**1.5.2.8 Obsługa rekrutacji i przyjęć do szkół podstawowych**

Oprogramowanie do rekrutacji wspiera pracowników JST, jednostek oświatowych oraz kandydatów i ich rodziców w procesie rekrutacji do szkół podstawowych. W ramach systemu wyświetlana jest oferta dla kandydatów. Dodatkowo system umożliwia wprowadzenie informacji o osobach przyjmowanych do jednostek w innym trybie niż rekrutacja.

**1.5.2.9 W zakresie dotyczącym naboru do szkół podstawowych**

1. stworzenie i opublikowanie internetowego informatora o ofercie szkół podstawowych; informator musi składać się z wizytówek poszczególnych szkół;
2. definiowanie obwodów przez szkoły podstawowe w oparciu o dane TERYT;
3. import danych o dzieciach zameldowanych na terenie JST z systemu ewidencji ludności;
4. dostęp do informacji o przebiegu rekrutacji na każdym etapie rekrutacji dla organu prowadzącego oraz poszczególnych szkół podstawowych;
5. rodzicowi/opiekunowi prawnemu kandydata, użytkownikom ze szkół oraz organu prowadzącego dostęp do podręcznika użytkownika zawierającego informacje w zakresie obsługi systemu; podręcznik powinien być możliwy do pobrania w pliku PDF, aby użytkownik mógł z niego korzystać w dowolnym momencie;
6. dokonywanie przez organ prowadzący korekt w planie naboru w trakcie całego okresu trwania procedury rekrutacyjnej;
7. dodanie do wniosku składanego elektronicznie załączników potwierdzających spełnianie przez kandydata kryteriów rekrutacyjnych poprzez wczytanie pliku ze skanem lub zdjęciem dokumentu;
8. opiekunowi samodzielne wpisanie hasła dostępu do konta;
9. organowi prowadzącemu na ustalanie wzoru wniosku o przyjęcie do szkoły;
10. automatyczne wskazanie szkoły obwodowej na podstawie adresu zamieszkania kandydata;
11. wskazanie przez opiekunów prawnych listy preferowanych szkół podstawowych (poza obwodowych), do których wnioskują o przyjęcie wraz z zaznaczeniem kolejności preferencji;
12. automatyczne przyjęcie do szkoły kandydatów z jej obwodu, których zgłoszenia zostały zaakceptowane;
13. dostęp do informacji o uczniach z obwodu oraz kandydatach spoza obwodu;
14. definiowanie stosowanych kryteriów naboru (w tym kryteriów automatycznych niewymagających wprowadzenia odpowiedzi przez osobę wypełniającą wniosek) oraz obliczanie liczby punktów z tytułu spełnienia określonych kryteriów określonych w zasadach rekrutacji;
15. organowi prowadzącemu przeprowadzenie serii próbnych przydziałów kandydatów, w trakcie których jest możliwość dokonywania zmian w planie naboru;
16. pobranie informacji w formie list o wynikach rekrutacji przez szkoły;
17. publikację wyników rekrutacji dla kandydatów za pośrednictwem Internetu;
18. powiadomienie kandydatów o statusie wniosku za pomocą poczty elektronicznej;
19. publikację na stronach internetowych informacji o pozostających wolnych miejscach;
20. przeprowadzenie procesu rekrutacji uzupełniającej, będącego powtórzeniem etapów rekrutacji właściwej;
21. wprowadzanie przez szkoły podstawowe informacji o kandydatach przyjmowanych do nich w ramach aktualizacji danych po zakończeniu procesu rekrutacji;
22. eksport list przyjętych w formacie \*.SOU w celu zasilenia bazy programów uczniowskich;
23. organowi prowadzącemu kontrolę stanu wykonania prac na kolejnych etapach rekrutacji przez wszystkie uczestniczące w procesie jednostki;
24. spełnianie określonych obowiązującym prawem wymogów w zakresie ochrony danych osobowych.

Terminy obsługi zgłoszeń: Ilekroć użyto miary czasu (godziny i dni) należy przez to rozumieć czas roboczy.

Zgłoszenia są przyjmowane i obsługiwane w czasie roboczym, tj. w dni robocze poniedziałek – piątek), z wyjątkiem dni ustawowo wolnych od pracy (niedziela, święta) od godziny 8:00 do 16:00.

Zgłoszenia, które wpłyną w czasie dni wolnych lub poza godzinami pracy traktujemy jakby wpłynęły w następny dzień roboczy.

## Obieg dokumentów – szt.35 lic.

Wymagania ogólne

1. EOD (Elektroniczny Obieg Dokumentów) musi realizować pełną funkcjonalność przewidzianą przepisami prawa dla systemu EZD.
2. EOD musi spełniać warunki określone dla systemu EZD w rozporządzeniu w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.
3. Jeśli jakaś czynność kancelaryjna jest obsługiwana przez EOD, to struktura systemu musi umożliwiać wykonywanie wszystkich wariantów tego zadania dopuszczalnych instrukcją kancelaryjną (np. dołączenie praktycznie dowolnej ilości dokumentów do sprawy – tzn. liczby na tyle dużej, by w praktyce nie napotkać ograniczeń systemu).
4. Moduły EOD muszą w szczególności:

* umożliwiać rozproszoną rejestrację wszelkiej korespondencji każdego typu wpływającej do Zamawiającego wraz z załącznikami oraz jej automatycznym numerowaniem i tworzeniem raportów i zestawień,
* umożliwiać wielostronicowe skanowanie dokumentów z poziomu aplikacji oraz rejestrowanie ich formy elektronicznej,
* umożliwiać rejestrację i nadzorowanie obiegu korespondencji wewnętrznej Zamawiającego (pomiędzy pracownikami i komórkami organizacyjnymi),
* udostępniać bazę nadawców i odbiorców korespondencji w celu sprawnej obsługi systemu i przeglądania korespondencji wg nadawców i odbiorców dać możliwość wielopoziomowej dekretacji wpływającej korespondencji z możliwością niezależnego kierowania oryginałów dokumentów i sporządzania dowolnej ilości ich kopii, tworzonych na dowolnym etapie ich obiegu. Każda z utworzonych kopii dokumentów powinna być nadzorowana. Ponadto powinien EOD dać możliwość dekretacji dokumentów jedynie „*do przeglądania*”,
* rejestrować każdą czynność związaną z poszczególnym dokumentem, np. w postaci historii i dać możliwość szybkiego odczytania tych informacji,
* posiadać możliwość nadania poleceń i terminów realizacji związanych z korespondencją oraz ich kontroli,
* posiadać możliwość przydzielania zadań samemu sobie oraz innym użytkownikom zgodnie z przydzielonymi uprawnieniami oraz umożliwiać nadzorowanie terminu i sposobu realizacji,
* posiadać możliwość tworzenia i przeglądania zadań, poleceń, ponagleń, przypomnień przypisanych do wielu pracowników oraz powiązania ich z dokumentem lub sprawą,
* posiadać możliwość udzielania zastępstw pracowników i pracy w zastępstwie,
* zapewniać jednoznaczne przypisanie odpowiedzialności za każdy z dokumentów,

1. EOD musi być w pełni transakcyjny i musi zabezpieczać dane przed zniszczeniem lub przypadkowym nadpisaniem w przypadku równoczesnego korzystania z tych danych przez wielu użytkowników.
2. EOD od strony technicznej musi zapewnić skalowalność w zakresie wydajności, pojemności oraz dołączania dodatkowych użytkowników i elementów infrastruktury sprzętowej.
3. EOD musi zapewnić możliwość rozbudowy warstw poprzez zwiększenie zasobów komputerów obsługujących warstwę poprzez rozbudowę pamięci, zwiększenie liczby procesorów, zwiększanie liczby maszyn oraz zwiększenie pojemności pamięci masowych.
4. EOD musi umożliwiać rozpraszanie repozytorium dokumentów w ramach jednego systemu elektronicznego obiegu dokumentów na wiele baz danych w różnych lokalizacjach (np. budynki urzędu, serwerownie).
5. EOD musi być zgodny z przepisami prawa, obowiązującymi na dzień ostatecznego odbioru systemu.
6. EOD musi posiadać mechanizm kontroli dostępu do usług pozwalający na dostęp do danej usługi ze względu na użytkownika oraz grupę (jednostkę organizacyjną) do której należy.
7. System musi być wyposażony w komunikator, pozwalający na wymianę wiadomości tekstowych w czasie rzeczywistym. Komunikator systemowy powinien zapewniać wymianę wiadomości zarówno między użytkownikami systemu jak i przekazywanie użytkownikowi komunikatów przez system.
8. EOD musi umożliwić wprowadzanie zmian kadrowych, urlopów i zastępstw bez konieczności modyfikacji ścieżek procedowania i umożliwia przekazanie osobie zastępującej części lub całości uprawnień osoby zastępowanej. Uprawnienia muszą być przekazane na określony czas.
9. EOD musi mieć możliwość integracji z usługą skrzynki e-doręczeń, EPUAP i powiązania spraw z Jednolitym Rzeczowym Wykazem Akt i implementacji podpisu elektronicznego.

## ePSZOK – szt.1 lic.

**Wymagania ogólne:**

1. Oprogramowanie - licencja typ OPEN - na jednostkę/Gminę.
2. System ma umożliwiać obsługę klientów Punktu Selektywnej Zbiórki Odpadów prowadzonego przez Gminę.
3. Moduł musi umożliwiać obsługę zadań związanych z ewidencją odpadów przyjmowanych w punkcie selektywnej zbiórki odpadów komunalnych (PSZOK) oraz prowadzenia szczegółowej ewidencji ilościowo jakościowej w zakresie odebranych odpadów.
4. Moduł musi być zaprojektowany w modelu trójwarstwowym:

* warstwa danych,
* warstwa aplikacji,
* warstwa prezentacji.

Powinien być obsługiwany przynajmniej przez dwie ogólnodostępne przeglądarki internetowe w aktualnych wersjach wspieranych przez producenta. Architektura systemu powinna umożliwiać pracę jedno i wielostanowiskową, zapewniać jednokrotne wprowadzanie danych tak, aby były one dostępne dla wszystkich użytkowników.

1. Moduł musi zapewniać weryfikację wprowadzanych danych w formularzach i kreatorach. Zapewnienie bezpieczeństwa danych zarówno na poziomie danych wrażliwych jak i komunikacji sieciowej powinno być przy zastosowaniu bezpiecznych protokołów sieciowych.
2. Moduł musi być zbudowany zgodnie z RWD i umożliwiać pracy na urządzeniach mobilnych (np. Laptop, Tablet, tel. komórkowy) podłączonych do sieci internetowej możliwością ograniczenia połączenia do określonych adresów IP.
3. W zakresie administrowania użytkownikami moduł powinien umożliwić wprowadzenie dowolnej ilość użytkowników i zdefiniować ich role (np.: administrator systemu, operator, kierownik, gmina) z określeniem zakresu czynności wykonywanych w systemie.
4. Moduł powinien wspierać zdalny odczyt z wag elektronicznych za pośrednictwem serwisu komunikującego się z elektroniką wagową (system w swojej funkcjonalności powinien przewidywać możliwość włączenia obsługi wag przy założeniu iż będzie taka możliwość techniczna).
5. Moduł powinien umożliwiać rejestrację danych klientów PSZOK,
6. Moduł w zakresie ewidencyjnym obsługi odbioru odpadów powinien umożliwić prowadzenie:

* rejestracji przyjęć odpadów do PSZOK (dane nieruchomości, dane transportującego, data, rodzaje odpadów, ilości i wagę poszczególnych rodzajów odpadów),
* ewidencji osób przekazujących odpady minimum w zakresie imię, nazwisko, oraz danych adresowych i kontaktowych w powiązaniu z ewidencją posesji z których są przyjmowane odpady,
* ewidencji nieruchomości z których są odbierane odpady (złożone deklaracje) minimum z zakresie adresu posesji, nr działki, identyfikacji karty mieszkańca w powiązaniu z ewidencją osób przekazujących odpady
* ewidencji przyjęć odpadów, umożliwiającą ewidencjonowanie:
  + daty i godziny oddania odpadów
  + danych osoby przekazującej odpady,
  + dane nieruchomości z której pochodzą odpady,
  + nr rej. pojazdu przywożącego odpady,
  + waga całkowitej oddanych odpadów,
* szczegółowej informacji o przyjmowanych rodzajach odpadów (nazwa i rodzaj odpadu, ilość/waga, jednostka materiałowa, magazyn składowania itp.).

1. Moduł musi umożliwić definicję rodzajów odpadów w zakresie nazwy, kod rodzaju odpadu oraz określania obowiązującego dla niego limitu i jego sposobu wyliczenia.
2. W zakresie określenia limitów odpadów powinna być możliwość definicji limitów na przyjmowane rodzaje odpadów obejmująca m.in.:

* okres obowiązywania limitu,
* wysokość limitu (wagowa lub ilościowa),
* określenie jednostka na którą przyznany jest limit (np. rok, kwartał, miesiąc) oraz liczba jednostek czasu w których ma być wyliczany (np. 1 rok, 1 kwartał, 4 miesiące),
* wybór sposobu uwzględniania jednostki czasu przy ustaleniu przekroczenia limitu – wg kalendarza (np., bieżący rok, miesiąc) lub wyliczane wstecz do daty ostatniego przekazywania odpadów,
* możliwość określenia stawki opłaty po przekroczeniu limitu.

1. Moduł powinien umożliwiać definicję dowolnej ilości magazynów, punktów przyjęć odpadów, adresów IP pozwalających na dostęp do aplikacji.
2. Moduł powinien współpracować z systemem do ewidencji opłat za gospodarowanie odpadami funkcjonującym w gminie z możliwością automatycznej weryfikacji danych osoby przekazującej odpady poprzez specjalistyczny serwis (usługa web service) systemu gminnego na podstawie kodu kreskowego, karty mieszkańca lub numeru PESEL i informowanie operatora minimum w zakresie informacji o złożeniu deklaracji i niezaleganiu z opłatami za odpady.   
   W celu usprawnienia wprowadzania danych system musi umożliwić po zidentyfikowaniu w systemie gminnym osoby oddającej odpady pobranie niezbędnych danych potrzebnych do wypełnienia formularza odbioru odpadów poprzez przekazanie danych przez web service systemu gminnego.
3. Moduł powinien umożliwić obsługę odpłatnego przyjęcia odpadów, z automatycznym wyliczeniem kwoty opłaty z uwzględnieniem określonych limitów i stawek obowiązujących przy ich przekroczeniu. System powinien wydrukować dokument z określeniem danych niezbędnych do uregulowania opłaty.
4. Kontrola zdefiniowanych limitów powinna być dokonywana w trakcie przyjmowania odpadów. System informuje użytkownika o fakcie przekroczenia limitu, wielkości przekroczenia oraz ewentualnej kwoty dopłaty.
5. Moduł musi umożliwić wydruk dokumentu potwierdzającego przyjęcie odpadów   
   z uwzględnieniem danych osoby oddającej oraz informacji o odebranych ilościach odpadów.
6. W zakresie składowania odpadów (magazyny) system powinien umożliwić:

* prowadzenie ewidencji magazynów (miejsc składowania poszczególnych odpadów)
* prowadzenie ewidencji stanów magazynowych dla poszczególnych rodzajów odpadów z uwzględnieniem automatyczne przeliczania stanów na podstawie przyjęć i przekazań odpadów,
* możliwość wprowadzania korekt stanów magazynowych.

1. Moduł powinien posiadać ewidencję przekazań odpadów obejmującą data przekazania, dane transportującego odpady, dane przyjmującego odpady, rodzaj odpadów, waga odpadów, metoda zagospodarowania.
2. Moduł powinien umożliwić wydruk potwierdzenia przekazania odpadów.
3. Moduł powinien zapewnić integrację z Bazą danych odpadowych (BDO) minimum w zakresie:
   * importu kontrahenta z BDO,
   * importu kodów odpadów z BDO
   * wglądu w Karty Ewidencji Odpadów Komunalnych z bazy BDO,
   * utworzenia nowej Karty Ewidencji Odpadów Komunalnych w bazie BDO,
   * wygenerowania Kart Ewidencji Odpadów Komunalnych w bazie BDO na podstawie poprzedniego roku,
   * aktualizacji Kart Ewidencji Odpadów Komunalnych w bazie BDO na podstawie przyjęć odpadów,
   * utworzenia Karty Przekazania Odpadu Komunalnego w bazie BDO na podstawie przekazania odpadów,
   * wglądu w Karty Przekazania Odpadów Komunalnych z bazy BDO.
4. W zakresie analizy danych system powinien umożliwiać:

* wgląd w historię przyjęć odpadów dla klienta i nieruchomości,
* wgląd w wykorzystanie limitów dla danej nieruchomości,
* podsumowanie przyjęć odpadów na poszczególne rodzaje odpadów w zadanym okresie czasu,
* podsumowanie przyjęć odpadów na poszczególne rodzaje odpadów w zadanym okresie czasu dla wybranego klienta lub nieruchomości,
* zestawienie przyjęć odpadów (łącznie lub na wskazany rodzaj odpadu) w poszczególnych dniach w zadanym okresie czasu,
* podsumowanie przekazań odpadów na poszczególne rodzaje odpadów w zadanym okresie czasu.
* raporty i zestawienia (przyjęcia wg odpadów, przyjęcia wg klientów, lista największych klientów, przekazania wg odpadów

1. Moduł powinien umożliwić założenia ewidencji podmiotów odbierających odpady z uwzględnieniem ich nr rejestrowego, nazwy, adres siedziby oraz adresu miejsca prowadzenia działalności w powiązaniu z BDO.
2. System powinien umożliwić przekazywanie zwrotnej informacji o odebranych odpadach do systemu gminnego odpowiedzialnego za naliczanie opłat za gospodarowanie odpadami w powiązaniu z posesją, z której zostały one odebrane. Użytkownik system gminnego powinien mieć wgląd w ilości odebranych odpadów, daty wizyt na PSZOK z poziomu kartoteki systemu dziedzinowego. Wymiana danych powinna odbywać się za pośrednictwem metod serwisu komunikacyjnego (web service) z możliwością wywołania przez operatora w dowolnym momencie funkcji przekazania danych do urzędu za określony okres. System może też przekazywać te dane bezpośrednio po zakończeniu odbioru odpadów od klienta.
3. Moduł powinien współpracować z czytnikami kodów kreskowych i pozwalać na odczytywanie aktualnych danych o klientach i nieruchomościach z bazy gminy na podstawie kodu kresowego (odczytywanego z naklejek z kodami kreskowymi lub kart mieszkańca).
4. Wykonawca musi zapewnić integrację z bazą gminy w zakresie weryfikacji klientów PSZOK (kontrola złożenia deklaracji, kontrola opłacenia należności za śmieci w gminie, informacja o zwolnieniach, np. o zadeklarowaniu kompostownika.
5. System musi zostać połączony z systemami dziedzinowymi, skąd powinien pobrać dane o osobach upoważnionych do oddawania odpadów do PSZOK oraz z systemem obsługi należności.

## eRada – szt.1 lic.

Wymagania minimalne:

|  |
| --- |
| 1. System do obsługi e-rady, transmisji obrad pozwalający na zdalne uczestniczenie w obradach osobom zainteresowanym. 2. Wszystkie poniższe funkcjonalności musza być zgodne z obowiązującymi przepisami prawa w opisanym zakresie (np. kodeksem cywilnym, kodeksem postępowania administracyjnego, ustawami i rozporządzeniami dot. stosowania podpisu elektronicznego, itd.) 3. Przygotowywanie i elektroniczna dystrybucja porządku obrad wraz z materiałami dla radnych poprzez konto użytkownika w systemie. 4. Funkcja importu porządku obrad bezpośrednio z pliku .docx, .doc (Word). 5. Możliwość dodawania dokumentów przez administratorów do wbudowanego w systemie repozytorium plików. 6. Możliwość dodawania do porządku obrad załączników w postaci elektronicznej takich jak projekty uchwał, załączniki do uchwał, mapy, prezentacje, itp. załączniki w formatach \*.doc, \*.docx, \*.pdf, \*.xls, \*.xlsx, \*.jpg, \*.jpeg, \*.bmp, \*.ppt, \*.pptx. 7. Możliwość eksportowania dokumentów z edytora aktów prawnych – Legislator do systemu obsługi Rady. 8. Możliwość dodawania linków do punktów w utworzonym posiedzeniu. 9. Możliwość dodawania prywatnych notatek do posiedzenia przez operatora oraz radnych. 10. Możliwość udzielania głosu i połączenia głosowego oraz video z zewnętrznymi obserwatorami obrad (mieszkańcami) celem umożliwienia im wypowiedzi/ zadania pytań, 11. Możliwością przyznawania głosu poszczególnym członkom, osobom zewnętrznym, kolejkowania głosu, śledzenia głosowań, itp. 12. Możliwość edytowania porządku obrad w trakcie posiedzeń. 13. Możliwość wydrukowania materiałów sesyjnych. 14. Możliwość zarządzania dokumentami dla radnych (publikacja, zapewnienie dostępu do dokumentów w wersji cyfrowej, potwierdzenie otrzymania, itp.). 15. Zarządzanie bazą kontaktów i wewnętrzną komunikacją między biurem rady, a radnymi z możliwością przesyłania wiadomości poprzez e-mail oraz SMS. Archiwizowanie przesyłanych wiadomości w systemie z możliwością sprawdzenia historii korespondencji. 16. Tworzenie głosowań jawnych (imiennych), zwyczajnych (tajnych), oraz specjalnych (np. do przeprowadzania różnego rodzaju wyborów). 17. Możliwość tworzenia głosowań z własnymi odpowiedziami. 18. Możliwość zabezpieczenia głosowań kodem PIN ustalonym przez administratora oraz jego wyświetlenie na ekranie prezentacyjnym podczas głosowania. 19. Możliwość automatycznego i ręcznego sprawdzenia listy obecności radnych z możliwością ręcznej modyfikacji tej listy, na wypadek spóźnień czy wcześniejszych wyjść. 20. Generowanie raportu obecności z informacją o obecności radnych w poszczególnych punktach porządku obrad. 21. Sprawdzanie obecność w trakcie posiedzenia w formie głosowania. 22. Możliwość złożenia przez radnego interpelacji w formie elektronicznej. 23. Brak możliwości oddawania głosu przez osoby oznaczone jako nieobecne na posiedzeniu. 24. Prezentacja wyników głosowań na urządzeniach wszystkich osób biorących udział w głosowaniach. 25. Możliwość zabezpieczenia głosowania na podstawie adresu IP z którego będą przyjmowane glosy – zewnętrzny adres sieci urzędowej, w celu wyeliminowania możliwości oddania głosów przez osoby przebywające poza urzędem. 26. Dostęp do systemu za pomocą urządzeń mobilnych oraz komputerów umożliwiający:  * sprawdzenie kalendarium posiedzeń nadchodzących oraz archiwalnych, * przeglądanie porządków obrad i wyników głosowań, * pobieranie i przeglądanie załączników, * głosowanie (oddawanie głosów) w czasie rzeczywistym podczas posiedzenia poprzez wybór jednego z 3 przycisków: „za”, „przeciw”, „wstrzymuję się”. * zgłaszanie się do dyskusji i przeglądanie listy osób planujących wypowiedź w danej sprawie w czasie rzeczywistym podczas posiedzenia. * funkcję wewnętrznego komunikatora dla radnych.  1. Elektroniczna i interaktywna obsługa posiedzeń poprzez:  * elektroniczną rejestrację radnych zgłaszających się do dyskusji nad projektami uchwał i innymi materiałami będącymi przedmiotem obrad, * elektroniczną rejestracje wniosków formalnych, * elektroniczną obsługę głosowań podczas sesji (głosowania jawne imienne), * prezentację porządku obrad oraz dostęp do załączników w czasie posiedzenia, * możliwość dynamicznej modyfikacji porządku obrad oraz materiałów na posiedzenia z automatycznym odświeżaniem zmian na urządzeniach radnych, * prezentację przedmiotu głosowania, listy osób uprawnionych do głosowania i wyników głosowania w czasie posiedzenia, * dynamiczne zarządzanie listą gości, którym udziela się głosu podczas posiedzenia, * możliwość ustawienia czasu wypowiedzi oraz wyświetlanie w czasie posiedzenia licznika czasu wypowiedzi i komunikatu o przekroczeniu czasu wypowiedzi, * zatwierdzanie uchwał, * przygotowanie projektów protokołu z posiedzeń z automatycznym przekazywaniem wyników głosowań, * rejestrację dźwięku w systemie informatycznym z możliwością transkrypcji dźwięku na tekst przy wykorzystaniu zewnętrznego oprogramowania, * rejestrację dźwięku w systemie informatycznym wraz ze scenariuszem prezentującym punkty porządku obrad oraz wypowiadające się przy tych punktach osoby z możliwością odsłuchania konkretnej wypowiedzi po wybraniu jej ze scenariusza, * umożliwienie poprzez sieć Internet dostępu mieszkańcom i podmiotom zainteresowanym do transmisji z posiedzenia (na żywo). * możliwość nagrywania obrad rady oraz ich bieżącej prezentacji w systemach streamingowych lub na ogólnie dostępnych portalach np. youtube, lub na stronie własnej Urzędu.  1. Możliwość tworzenia wewnętrznego rejestru uchwał oraz jego automatyczne publikowanie dla mieszkańców i podmiotów zainteresowanych. 2. Możliwość integracji z systemami zewnętrznymi Zamawiającego – Wykonawca zobowiązuje się udostępnić API umożliwiające integracje w zakresie przesyłania danych dostępnych w systemie do obsługi Rady. 3. Integracja z systemem eBOM celem prezentacji treści i umożliwienia dostępu do usługi bezpośrednio z systemu eBOM. 4. System obsługiwany będzie przez laptopy z systemem Windows lub urządzenia mobilne z systemem android nie starszym niż wersja 4.4. 5. Automatyczna transkrypcja dźwięku nagrania sesji na tekst w ramach systemu eRada w formacie odpowiednim do tworzenia napisów do sesji. 6. Możliwość ustawienia głosowania w ten sposób, ze wybór jest jednej z dwóch lub więcej opcji/możliwości. 7. Możliwość określenia trybu głosowania na: głosowanie zwykłą większością głosów, głosowanie bezwzględną większością głosów, głosowanie bezwzględną większością głosów ustawowego składu rady, głosowanie kwalifikowaną większością. 8. Automatyczne zamknięcie i zapisanie listy głosowań po zagłosowaniu przez wszystkich radnych. 9. Możliwość zamknięcia głosowania przez administratora w sytuacji, gdy radny obecny na posiedzeniu nie bierze udziału w głosowaniu. 10. Możliwość określenia grup użytkowników oraz nadania im stosownych uprawnień; 11. Możliwość udostępniania wszystkim radnym, jak również pojedynczym adresatom, np. tylko członkom danej komisji, komunikatów, które niekoniecznie muszą dotyczyć posiedzeń czy sesji wraz z udostępnieniem dowolnych plików tzw. „Informator”. 12. Możliwość podglądu przez administratora w historię odczytu posiedzenia, jak i dołączonych dokumentów, załączników do porządku obrad, komunikatów przez poszczególnych radnych. 13. Możliwość sprawdzenia przez administratora aktywności użytkowników i ilości logowań, kiedy się one odbywały, ostatnia aktywność w systemie użytkownika, ostatnie logowanie.   System powinien być kompatybilny ze sprzętem opisanym w punkcie System do transmisji obrad Rady Gminy - sprzęt.   1. Transmisje mają być zintegrowane z systemem do obsługi Rady w zakresie Automatycznego wyświetlania w transmisji informacji o:    1. aktualnie przemawiającej osobie    2. aktualnie omawianym punkcie z porządku obrad    3. uruchomionym głosowaniu i temacie tego głosowania    4. wynikach głosowania    5. o trwającej przerwie    6. nazwie instytucji i dacie posiedzenia 2. System ma zapewniać możliwość automatycznego przewinięcia archiwalnego nagrania wideo do wybranego przez oglądającego punktu porządku obrad. 3. Automatyczne kadrowanie mówcy w momencie udzielenia głosu w systemie do obsługi Rady. 4. Podczas okresu obowiązywania gwarancji wymagana jest transmisja oraz archiwizacja nagrań z sesji o minimalnej jakości 720p poprzez serwery Wykonawcy. 5. Integracja systemu obsługi rady z systemem konferencyjnym.    1. Zgłoszenie chęci zabrania głosu:       1. Chęć zgłoszenia do głosu przez radnego musi być możliwa z poziomu tabletu oraz pulpitu konferencyjnego;       2. Zgłoszenie z poziomu tabletu spowoduje pojawienie się radnego na liście osób chętnych do zabrania w systemie obsługi rady oraz zaświecenie wskaźnika LED na szyjce mikrofonu przypisanym do radnego w kolorze innym niż kolor aktywnego mikrofonu;       3. Zgłoszenie z poziomu pulpitu konferencyjnego spowoduje zaświecenie wskaźnika LED na szyjce mikrofonu przypisanym do radnego w kolorze innym niż kolor aktywnego mikrofonu oraz umieszczenie radnego na liście osób chętnych do zabrania głosu w dyskusji;    2. Udzielenie radnemu zgody na zabranie głosu:       1. Udzielenie zgody na głos jest możliwe z poziomu aplikacji do obsługi rady dla administratora oraz poprzez aplikację na urządzeniu przewodniczącego;       2. Udzielenie głosu spowoduje zmianę koloru wskaźnika LED umieszonego na szyjce mikrofonu na kolor inny niż w przypadku chęci zabrania głosu oraz aktywuje mikrofon;    3. Wykonawca dostarczy zamawiającemu aplikację do integracji wraz z danymi uwierzytelniającymi, którą zamawiający będzie mógł samodzielnie zainstalować na dowolnym urządzeniu z systemem Windows. 6. Wymagania dodatkowe:    1. Publikacja materiałów sesyjnych oraz wyników przeprowadzonych głosowań w Internecie w oparciu o infrastrukturę techniczną Wykonawcy.    2. Przechowywanie danych na serwerach znajdujących się na terytorium Rzeczypospolitej Polskiej.    3. Udostępnienie kopii zapasowej oprogramowania oraz danych wprowadzonych przez Zamawiającego na żądanie Zamawiającego.    4. Montaż oraz parametryzacja wszystkich urządzeń po stronie Wykonawcy w siedzibie Zamawiającego. |

## Monitoring środowiska – szt. 1 zestaw

|  |
| --- |
| Pozycja dotyczy wdrożenia systemu monitoringu środowiskowego obejmującego bieżące pomiary następujących czynników szkodliwych: PM2,5, PM10, PM1 w lokalizacjach na terenie powiatu. Dodatkowo prowadzone będą pomiary temperatury, wilgotności, ciśnienia atmosferycznego. Dane zbierane z czujników publikowane będą na portalu eBOM oraz będą udostępniane w formie danych surowych, otwartych wszystkim zainteresowanym stronom. Przewiduje się udostępnienie danych okresowych na portalu eBOM. System składał się będzie z trzech stacji pomiarowych oraz zintegrowanego z nimi systemu informatycznego (aplikacja dostępna w chmurze) zapewniającego ich analizę i publikację. Ponadto dane z czujników będą prezentowane w ujęciu geograficznym na podkładach mapowych.  Urządzenie pomiarowe/czujniki zapewnią pomiary:   * temperatury w zakresach przynajmniej od -30 °C do +60°C  oraz dokładnością co najmniej 0,5’C; * wilgotności powietrza przynajmniej w zakresach od 0-100 % wilgotności  względnej przy dokładności ±3%; * ciśnienia atmosferycznego nad poziomem morza, przeliczony z wartości podawanych przez urządzenie z uwzględnieniem wysokości na jakiej zostanie zamontowany – zakres min. 700-1200hPa oraz dokładności 1 hPa * pyłu zawieszonego PM1.0 w zakresie pomiarowym 0 – 500 μg/m³  z dokładnością pomiarową ±10 μg/m³; * pyłu zawieszonego PM2.5 w zakresie pomiarowym 0 – 1000 μg/m³  z dokładnością pomiarową ±10%; * pyłu zawieszonego PM10 w zakresie pomiarowym 0 – 1000 μg/m³  z dokładnością pomiarową ±10%;   System pomiaru obejmował będzie czujniki do pomiaru jakości powietrza, system monitorowania w postaci platformy informacyjnej wizualizującej wyniki pomiarów w czasie rzeczywistym oraz aplikacji mobilnej. Systemy dostępne w wielu wersjach językowych. W ramach projektu założono instalację 3 punktów pomiarowych.  **Czujniki do pomiaru jakości powietrza**  1.  Komunikacja z serwerem wykonawcy gromadzącym i udostępniającym informacje z czujników za pomocą sieci GSM.  2.  Urządzenie pomiarowe/czujniki zapewnią pomiary:  -   temperatury w zakresach przynajmniej od -40 °C do +80°C  oraz dokładnością co najmniej 0,5’C;  -   wilgotności powietrza przynajmniej w zakresach od 0-100 % wilgotności  względnej przy dokładności ±3%;  -   ciśnienia atmosferycznego nad poziomem morza, przeliczony z wartości podawanych przez urządzenie z uwzględnieniem wysokości na jakiej zostanie zamontowany – zakres min. 700-1200hPa, dokładność 1 hPa;  -   pyłu zawieszonego PM 1.0 w zakresie pomiarowym 0 – 500 μg/m³  z dokładnością pomiarową ±10 μg/m³;  -   pyłu zawieszonego PM2.5 w zakresie pomiarowym 0 – 1000 μg/m³  z dokładnością pomiarową ±10 μg/m³;  -   pyłu zawieszonego PM10 w zakresie pomiarowym 0 – 1000 μg/m³  z dokładnością pomiarową ±10 μg/m³;  3.  Urządzenia muszą wykazywać niepewność wskazań średnich dobowych stężenia pomiędzy dwoma urządzeniami na poziomie maksimum 10% dla pyłów PM2.5 i PM10.  4.  Sensory muszą zostać poddane, przed ich montażem oraz w czasie ich eksploatacji, kalibrowaniu z urządzeniem posiadającym wykazaną równoważność do metody referencyjnej badań pyłu zawieszonego w powietrzu.  5.  Urządzenia muszą posiadać zasilanie z sieci energetycznej 230V/110V i posiadać kabel zasilający o długości min. 2.5 metra wyposażony w USB lub wtyczkę sieciową.  6.  Urządzenia muszą zostać zamontowane w sposób nieinwazyjny, zapewniający brak ingerencji w elewację czy też inne elementy budynków np. elewację i stolarkę okienną/drzwiową.  7.  Urządzenia muszą posiadać możliwość przeniesienia do innej lokalizacji.  8.  Urządzenia muszą posiadać min. 24-miesięczną gwarancję sprzętową na całość urządzeń pomiarowych.  9.  Urządzenia muszą posiadać wbudowany system powiadamiania kolorem diody w zależności od stanu jakości powietrza. Kolory wyświetlane na diodach czujnika muszą być kompatybilne z tymi wyświetlanymi na platformie internetowej i w aplikacjach mobilnych.  10.   Urządzenia powinny posiadać system podgrzewania powietrza przed pomiarem w celu wyeliminowanie wpływu wilgotności na pomiary stężenia pyłów w powietrzu. W konstrukcji urządzenia musi zostać przewidziany element kondycjonujący próbkę powietrza przed pomiarem, w celu podgrzania jej powyżej punktu rosy.  11.   Urządzenia powinny zapewniać stopień ochrony na poziomie min IP 34. Obudowa urządzenia musi być odporna na warunki zewnętrzne i być przystosowana do pracy w trudnych warunkach atmosferycznych. Wskazana obudowa z aluminium, stali nierdzewnej itp.  12.   Temperatura pracy urządzeń musi wynosić przynajmniej od -40 °C do +80°C.  13.   Maksymalny pobór mocy czujnika to max 2,5 W  14.   Roczny pobór mocy nie może przekraczać 11 kWh.  15.   Urządzenie powinno być przeznaczone do montowania na wysokości od 1,5 do 8 metrów nad poziomem ziemi.  16.   Masa urządzenia nie może być większa niż 500 gram ze względu na planowane miejsce instalacji urządzeń.  17.   Wymiary urządzenia nie mogą być większe niż 140/140/140 mm nie licząc ewentualnej zewnętrznej anteny nadawczej ze względu na planowane miejsce instalacji urządzeń.  **Systemu monitorowania jakości powietrza:**  1.  Wykonawca zapewni bezpłatny dostęp do ogólnodostępnej platformy informacyjnej wizualizującej wyniki pomiarów w czasie rzeczywistym. Platforma internetowa musi być obsługiwana w polskiej i angielskiej wersji językowej.  2.  Platforma musi być dostosowana dla osób niepełnosprawnych (słabowidzących, osób z dysfunkcją wzrokową)  3. Dane pomiarowe (PM1, PM2.5, PM10, temperatura, wilgotność, ciśnienie) muszą być aktualizowane minimum co 5 minut i wizualizowane na platformie internetowej oraz w aplikacji mobilnej.  4.  Wykonawca zapewni darmową aplikację mobilną, prezentującą wyniki pomiarów w czasie rzeczywistym dostępne dla minimum 2 systemów operacyjnych: Android (Google Play) i IOS (App Store) z zasięgiem przynajmniej ogólnopolskim. Aplikacja mobilna musi być obsługiwana w polskiej i angielskiej wersji językowej.  5.  Wykonawca zapewni dostęp do widget-u pozwalającego na publikację danych na wskazanych przez Zamawiającego stronach www.  6.  Platforma internetowa oraz aplikacja mobilna musi zapewnić dane pomiarowe dotyczące pyłów PM1, PM2.5, PM10 oraz dane pogodowe: temperatura, wilgotność, ciśnienie i siła wiatru.  7.  Dane z sensorów (dane pomiarowe) muszą być zgodne z europejskim wskaźnikiem jakości powietrza CAQI (Common Air Quality Index). Prezentacja tych danych w skali CAQI musi być wizualizowana w platformie informacyjnej oraz w aplikacjach mobilnych.  8.  Na ogólnodostępnej platformie oraz w aplikacjach mobilnych musi zostać zapewniony dostęp do danych historycznych z ostatnich 24 godzin (PM1, PM2.5, PM10, temperatura, wilgotność, ciśnienie).  9.  Na platformie internetowej oraz w aplikacjach mobilnych mają być prezentowane prognozy zanieczyszczenia powietrza na kolejne 24 godziny ze sprawdzalnością na poziomie minimum 80%. Prognozowana wartość zanieczyszczenia powietrza ma być prezentowana w skali CAQI (forma liczbowa oraz graficzna) w odniesieniu do skali kolorystycznej stosowanej do wizualizacji wyników pomiarów. Zamawiający zapewnia sobie możliwość zweryfikowania sprawdzalności prognozy zanieczyszczeń powietrza.  10.  Wykonawca zapewni możliwość generowania raportów, zawierających dane dotyczące stężeń pyłów (PM1, PM2.5, PM10) oraz dane pogodowe (temperatura, wilgotność, ciśnienie) w cenie abonamentu dostępne w wersji online w indywidualnym panelu klienta. System musi posiadać możliwość generowania wyników pomiarów w formie tabel i wykresów dla poszczególnych parametrów i określonych ram czasowych tj. raporty dobowe, tygodniowe, miesięczne, roczne.  11.   Wykonawca na platformie internetowej oraz w aplikacjach mobilnych musi prezentować dane dotyczące sponsora czujnika tj. jego nazwę oraz jego logo (logotyp/herb). Ponadto Wykonawca musi zapewnić interaktywny link umożliwiający przekierowanie na wskazaną przez Zamawiającego stronę internetową (stronę internetową sponsora czujnika).  12.   System monitorowania jakości powietrza musi zapewnić dostęp do API z danymi pomiarowymi.  13. Platforma musi być dostosowana dla osób niepełnosprawnych (słabowidzących, osób z dysfunkcją wzrokową). |

## 

## System eWoda – szt. 1

**Rozwiązanie musi spełniać następujące wymagania funkcjonalne:**

1. System musi być dostosowany do specyfiki jednostek organizacyjnych gminy, zakładów komunalnych i wodociągowych poprzez specjalistyczne funkcjonalności oraz integrację z pozostałymi systemami dziedzinowymi.
2. System gwarantuje m.in. natychmiastowy dostęp do informacji o odbiorcach, strukturze sieci oraz parametrach rozliczania. Automatycznie obsługuje cały proces sprzedaży od zawarcia umowy z klientem, wprowadzenia do systemu odczytów z liczników, wystawienia faktur zgodnie z zatwierdzoną taryfą oraz przyjętym sposobem rozliczania do umieszczenia tych faktur w eBOM z możliwością ich zapłaty przez klienta.
3. System musi umożliwiać obejrzenie w eBOM szczegółów dokumentów, pozycji, wartości, ewentualnych odsetek czy nadpłat, podgląd własnych rozrachunków, podgląd naliczeń, podgląd stanów liczników, możliwość zgłoszenia nowego odczytu, możliwość pobrania odpowiednich formularzy i dokumentów, możliwość zgłoszenia awarii,
4. System musi umożliwiać połączenie eBOM z obiegiem dokumentów. Zapis procedur organizacyjnych za pomocą obiegu dokumentów - określenie czynności sekwencyjnych, równoległych i warunkowych, które muszą być zrealizowane wraz z określeniem komórki lub osoby odpowiedzialnej i terminu realizacji.
5. System musi posiadać wspólną z systemem finansowo-księgowym kartotekę płatników-odbiorców zawierającą minimum: dane adresowe, dane bankowe, rodzaje odbiorców, dane dotyczące zawartych umów z klientem.
6. Kartoteka płatników-odbiorców musi umożliwiać jej wydruk oraz filtrowanie według: kodu odbiorcy, nazwiska, adresu, nazwy (ogólne pole), adresu posesji (punktu odbioru mediów) oraz obsługiwać filtrowanie i sortowanie wg wybranego pola z listy.
7. System musi posiadać kartotekę zawierającą minimum: numer punktu odbioru, numer książki z liczbą porządkową, numer (identyfikator) inkasenta, adres punktu, opis punktu, dane niezbędne do naliczenia opłaty za dostawę wody i odbiór ścieków zarówno w odniesieniu do opłat ustalanych na podstawie odczytów wodomierzy jak i opłat ryczałtowych oraz opłat stałych w powiązaniu z wybraną taryfą, dane dotyczące wodomierzy z uwzględnieniem czy jest to wodomierz główny czy podlicznik.
8. W zakresie odczytów radiowych system powinien ewidencjonować dane z układów pomiarowych umożliwiające automatyzację procesu zdalnego odczytu bez konieczności ręcznego przyporządkowania odczytów do poszczególnych układów pomiarowych.
9. System powinien umożliwiać eksport danych ewidencjonowanych układów pomiarowych w formacie zgodnym z oferowanym systemem do zdalnego odczytu.
10. Po wykonaniu importu danych z systemu zdalnego odczytu powinna być możliwość automatycznego naliczenia opłat dla grupy odbiorców, których układy pomiarowe zostały odczytane. Operator systemu powinien mieć możliwość wyselekcjonowania odbiorców dla których nie zostały wykonane odczyty.
11. System musi posiadać kartotekę liczników zawierającą: kod dodatkowy licznika, numer fabryczny licznika, numer układu pomiarowego dla zdalnych odczytów, średnica, typ licznika, ile cyfr licznika, data zabudowy licznika, data legalizacji licznika, numer plomby licznika, numer wskaźnika licznika, historię wskazań (odczytów), zużycie licznika z wymiany, średnia wartość zużycia.
12. System musi umożliwiać operacje na punktach: wymiana wodomierza, wymiana spowodowana legalizacją lub uszkodzeniem, naliczanie średniego zużycia, zapamiętywanie odczytu starego wodomierza (doliczanie do faktury), przegląd wymian wodomierzy, przeniesienie punktu na inny, renumeracja pozycji w książce.
13. System musi umożliwiać rejestrację odczytów umożliwiając: pokazywanie danych wprowadzanego punktu/odbiorcy, zbiorcze wprowadzanie odczytów dla punktów odbiorcy, całej książki, doliczanie zużycia z wymiany, obliczanie średniego zużycia w przypadku uszkodzenia licznika, obliczanie bieżącego zużycia, pokazywanie informacji o relacjach: punkt nadrzędny/podlicznik, przegląd odczytów dla bieżącego punktu, przegląd i drukowanie odczytów dla odbiorcy, informowanie użytkownika o odchyleniach od średniego zużycia (np. powyżej 30%).
14. System musi umożliwiać wystawianie faktur, w szczególności musi uwzględniać: wystawianie faktur dla pojedynczego odbiorcy, wpisywanie daty wystawienia i płatności, spisywanie uwag do faktury, możliwość modyfikacji wzoru wydruku faktury (logo, rozmieszczenie), uwzględnianie na fakturze: zaległości odbiorcy, nadpłaty odbiorcy, należnych odsetek za wpłaty po terminie, kosztów upomnienia, drukowanie kodów kreskowych, zatwierdzenie bądź anulowanie faktury, wystawianie zbiorcze faktur: dla książki, przeglądanie wystawionych faktur, zestawienie wystawionych faktur, wystawianie raportu dla banków dotyczących wystawionych faktur, tworzenie raportu poleceń zapłaty.
15. System powinien zapewnić tworzenie i wydruk rejestrów sprzedaży wraz z zapisem jego do formatu (struktury) JPK\_VAT, JPK\_V7M oraz JPK\_V7K.
16. System musi umożliwiać rozliczenie odbiorcy dla faktur od podanej daty wystawienia oraz za zadany przez użytkownika okres.
17. System musi umożliwiać współpracę z przenośnymi terminalami inkasenckimi minimum w zakresie zbierania odczytów oraz wystawiania faktur (współpraca z zestawem inkasenckim terminal Psion WA MX 2MB RS/TTL oraz drukarką przenośną MEFA-12 lub równoważnym zestawem).
18. System powinien umożliwiać automatyczną wysyłkę wystawionych faktur na wskazany adres email.
19. System powinien umożliwiać import odczytów z zewnętrznych systemów odczytujących (nakładki radiowe).
20. System powinien umożliwiać wykonie analizy kompletności i poprawności odczytów.
21. System powinien umożliwiać generowanie faktur na podstawie zaimportowanych odczytów.
22. System powinien umożliwiać zapisanie faktur sprzedaży w formacie pdf i wysyłka ich e-mailem (e-faktury).
23. System powinien przechowywać oryginał oraz kopie faktur sprzedaży w formie elektronicznej (format pdf) a także Przeglądanie faktur, zapłat w eBOM .
24. Moduł powinien umożliwiać przygotowywanie raportu TransGUS do GUS-u.
25. System powinien umożliwiać wysyłanie komunikatów SMS oraz e-mail do odbiorców zarówno indywidualnie jak i do wybranej grupy odbiorców. Powinna być możliwość selekcji odbiorców na podstawie miejscowości, trasy, określonej grupy odbiorców, dat dokonania odczytu lub braku odczytu w zadanym okresie, wystawienia faktury w danym okresie. Operator systemu może następnie wprowadzić treść komunikatu i przesłać ją do wybranej grupy.

## 1.11 Strona WWW – szt.1

|  |
| --- |
| Celem zadania jest dostosowanie strony urzędu do obowiązujących standardów dostępności. Wymaga się dostosowania strony co najmniej do standardu WCAG 2.1. Usługa obejmuje główną stronę gminy oraz stronę Biuletynu Informacji Publicznej.  Modernizacja istniejącej strony <https://nozdrzec.pl/>. Optymalizacja strony pod kontem Dostępności Plus (audyt www), uruchomienie modułu szukaj. Integracja z lektorem migania on-line (wideo tłumacz języka migowego), aktualizacja deklaracji dostępności dla www, informacje ETR, uzupełnienie opisu alternatywnego <img>=<alt>   1. Audyt (1) dostępności strony internetowej (zgodność z wymaganiami WCAG 2.1. AA określonymi w tabeli załączonej do ustawy. Wymagania te pokrywają się z pkt 9, 10 i 11 normy EN 301 549 V2.1.2 lub równoważnej (DZIENNIK USTAW 2019 R. POZ. 848 ).  * Wykonawca musi posiadać uprawnienia wymagane przez ustawę o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych z dnia 4 kwietnia 2019 r * Stronę należy dokładnie zbadać, aby zidentyfikować problemy dostępności. * Raport z audytu eksperckiego zawiera wyszczególnienie wszystkich znalezionych niezgodności wraz z sugestiami ich poprawy. * Raport określa stan w jakim znajduje się serwis w chwili badania, oraz sugestie do spełnienia wymogów WCAG na poziomie A, AA, AAA. * Na podstawie audytu (raportu) wykonawca musi zaplanować działania naprawcze i je wdrożyć. * Audyt (2) kontrolny powtórnie weryfikuje wszystkie niezgodności wykazane w raporcie. * Po wykonaniu audytu kontrolnego Zamawiający otrzymuje końcowy raport zgodności ze standardami WCAG (np. wystawienie Certyfikatu).  1. Dostępna strona to znaczy taka strona, na której każdy może się zapoznać z jej zawartością i wykonać na niej wszystkie zadania: 2. na dowolnej aplikacji klienckiej, np. przeglądarce, czytniku ekranu, 3. na dowolnym urządzeniu, np. laptopie, smartfonie, monitorze brajlowskim, 4. z dowolnego połączenia, np. bardzo wolnego, 5. w każdych warunkach, np. w hałasie, w jasnym oświetleniu, o zmroku. 6. Zamawiający: 7. będzie posiadał wiedzę czy osoby niepełnosprawne mogą korzystać ze strony internetowej lub serwisu mobilnego i czy treści w nich zamieszczone są dla nich widoczne, 8. zyska pewność czy osoby niedowidzące mogą w sposób intuicyjny dostać się do kluczowych informacji, oraz czy mają dostęp do niezbędnych funkcjonalności swojego serwisu, 9. będzie miał pewność, że formularze kontaktowe zawarte na stronie są funkcjonalne. 10. Sporządzenie/aktualizacja deklaracji dostępności dla strony głównej i strony z BIP. 11. Przygotowanie opisu działalności podmiotu za pomocą polskiego języka migowego.(Ustawa z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami zobowiązuje każdą instytucje i jednostkę publiczną do posiadania opisu działalności podmiotu za pomocą polskiego języka migowego.). 12. Przygotowanie informacji spełniające załażenia ETR (Tekst łatwy do czytania). 13. Integracja z lektorem migania on-line (wideo tłumacz języka migowego). 14. Wymaga się zgodności strony co najmniej ze standardem WCAG 2.1 na poziomie AA z wyłączeniem audiodeskrypcji.  1.12 Szkolenia TiK typ II – 160 godzin **Wymagania minimalne dla szkoleń TIK typ II – 160 godzin zegarowych**  1. Wykonawca w ramach wdrożenia przeprowadzi instruktaże dla wskazanych użytkowników.  2. Instruktaże prowadzone będą w języku polskim zgodnie z organizacją opisaną w Planie Szkoleń, przyjętym przez Zamawiającego.  3. W ramach instruktaży dla liderów użytkowników, Wykonawca przekaże uczestnikom pełną wiedzę niezbędną do poprawnego użytkowania funkcjonalności Systemu.  4. Instruktaże dla użytkowników należy przeprowadzić w formie instruktaży grupowych, w formie warsztatów (praca przy komputerach).  5. Instruktaże grupowe winny się odbywać w podziale na grupy zawodowe nie więcej niż 5 osobowe. Każda grupa w wymiarze czasu co najmniej 8 godzin zegarowych/dziennie.  6. Dla przeprowadzenia instruktaży grupowych Zamawiający nieodpłatnie zapewni Wykonawcy 5 stanowisk roboczych (pochodzących z zamówienia w ramach niniejszego projektu) i odpowiednie pomieszczenie wraz z infrastrukturą transmisji danych umożliwiającą dostęp do Systemu. Odpowiedzialność za przygotowanie stanowisk do przeprowadzenia instruktaży leży po stronie Wykonawcy.  7. Instruktaże dla administratorów Systemu przeprowadzone zostaną w jednej grupie.  8. Wykonawca przeprowadzi szkolenia dla Użytkowników systemu w ciągu wskazanych/ustalonych dni szkoleniowych.  9. Przeprowadzenie instruktaży zostanie potwierdzone protokołem sporządzonym w dwóch jednobrzmiących egzemplarzach, po jednym dla Zamawiającego i Wykonawcy, zawierającym:  nazwę i tematykę i czas trwania szkolenia,   * 1. datę i miejsce szkolenia,   2. imienną listę osób uczestniczących w szkoleniu,   3. imię i nazwisko oraz specjalizację osób prowadzących szkolenie.   10. Protokół z przeprowadzenia instruktaży podlegać będzie zatwierdzeniu przez Zamawiającego |

# **CZEŚĆ II – SPRZĘT i INFRASTRUKTURA**

## Zestawienie zakresu dostaw i usług dla części II

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| LP | NAZWA | Min. Gwarancja  (m-ce) | Typ/ Rodzaj gwarancji | Ilość | JM |
|  | Oprogramowanie do backupu | 24 | Producenta | 1 | lic. |
|  | Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa | 24 | Producenta | 1 | lic. |
|  | Serwer | 36 | Producenta | 1 | szt. |
|  | Firewall - klaster | 36 | Producenta | 2 | szt. |
|  | Centralny system logów | 36 | Producenta | 1 | szt. |
|  | Zestaw komputerowy z oprogramowaniem | 36 | Producenta | 15 | szt. |
|  | Laptopy | 36 | Producenta | 20 | szt. |
|  | Centralny UPS | 36 | Producenta | 1 | szt. |
|  | Agregat | 36 | Producenta | 1 | szt. |
|  | System do transmisji obrad Rady Gminy - sprzęt | 36 | Wykonawcy/ producenta | 1 | kpl. |
|  | Wodomierze | 36 | Wykonawcy/ producenta | 296 | szt. |
|  | Przepływomierz | 36 | Wykonawcy/ producenta | 2 | szt. |
|  | Instalacja i konfiguracja (Platforma sprzętowa) | 12 | Wykonawcy | 250 | RBH |
|  | Dokumentacja techniczna | Nd. | Nd. | 20 | RBH |
|  | Szkolenia TiK typ I | Nd. | Nd. | 120 | RBH |
|  | Opracowanie procedur bezpieczeństwa informacji i przetwarzania danych | Nd. | Nd. | 120 | RBH |

**Zakres obejmuje:**

1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji.
2. Urządzenia, które nie są montowane w szafach teleinformatycznych np.: komputery powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego.
3. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
4. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
5. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.
6. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchcordy miedziane kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
7. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).
8. Instalacja, konfiguracja i wdrożenie dostarczonego oprogramowania
9. systemu wykonywania backupu i archiwizacji danych.
10. systemu serwerowego wraz z niezbędnymi usługami opisanymi
11. oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn.
12. monitorowania i analizy cyberbezpieczeńśtwa - SOC (SIEM/SOAR).
13. zarządzania infrastrukturą IT.
14. Rejestracja oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Wnioskodawcy)
15. Opracowanie dokumentacji powykonawczej
16. Asysta stanowiskowa.

## Wymagania ogólne dla urządzeń i oprogramowania infrastruktury

* całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
* całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana wcześniej;
* Ogólne zasady równoważności rozwiązań:

W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie   
w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Urzędu. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, uwzględnić niezbędną asystę pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.

Wykonawca odpowiedzialny jest za dostawę w pełni funkcjonujących rozwiązań opisanych w niniejszym załączniku, w tym jeżeli jest konieczne, pozyskanie niezbędnych informacji do realizacji zamówienia, zawarcie koniecznych umów itp. Portale, które zostaną uruchomione dzięki realizacji tego projektu, na których znajdować się będą oferowane e-usługi, będą spełniały wszystkie obowiązkowe wytyczne określone w dokumencie WCAG 2.1.

## Wymagania gwarancyjne

* O ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona gwarancja oparta na gwarancji producenta rozwiązania; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany, jako podjęcie działań diagnostycznych   
  i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
* Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Wnioskodawcy), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
* Gwarantowany czas naprawy nie może być dłuższy niż 10 dni roboczych.   
  W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
* Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Wnioskodawcy.

## Licencja na system Backupu – szt. 1 lic.

Wymagania minimalne

|  |  |  |
| --- | --- | --- |
| |  |  | | --- | --- | | System przeciwdziałania cyberzagrożeniom, oferująca możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi.   1. System musi umożliwić odbieranie logów z urządzeń sieciowych oraz wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding. 2. System musi zapewnić agentów XDR na stacje końcowe umożliwiających im pobieranie pełnych danych telemetrycznych hostów, których chronią i przesłanie tych danych do systemu centralnego w celu dalszej korelacji i analizy behawioralnej. W przypadku wykrycia zagrożenia agenci muszą umożliwiać automatyczną i dostosowaną do kontekstu reakcje, m.in. na blokowanie bądź izolację sieciową złośliwego oprogramowania.    1. Agent musi posiadać możliwość dodawania i usuwania reguł wbudowanego firewalla obejmując m.in. blokowanie i odblokowywanie poszczególnych procesów bądź reguł dotyczących ruchu sieciowego stanowiące reakcję na wykryte zagrożenie.    2. Agent musi pobierać oraz aktualizować na bieżąco listę zainstalowanego oprogramowania.    3. System w przypadku wykrycia techniki ataku ukierunkowanego na podatną aplikację w celu zablokowania ataku musi umożliwiać zatrzymanie procesu aplikacji oraz zapewnić dostęp do danych dowodowych obejmujących nazwę chronionego systemu, system operacyjny, tożsamość użytkownika, nazwę procesu, dokładną komendę uruchamiającą złośliwy proces wraz parametrami i znacznik czasowy.    4. System musi obsługiwać scenariusz uwzględniający ocenę prawdopodobieństwa materializacji się wykrytego zagrożenia, gdzie w przypadku, gdy wyliczone przez system prawdopodobieństwo ataku jest wysokie proces zostanie zablokowany, natomiast w pozostałych przypadkach, gdy jest ono średnie bądź niskie zostanie on zamrożony z możliwością ponownego wznowienia przez operatora.    5. System musi posiadać możliwość dostosowania reakcji na zagrożenie w zależności od rodzaju zasobu, który chroni, przykładowo, jeżeli zagrożenie dotyczyć będzie procesu na stacji roboczej proces zostanie automatycznie zablokowany jednakże w przypadku, gdy to samo zagrożenie dotyczyć będzie serwera świadczącego usługi w sieci publicznej proces pozostanie uruchomiony z jednoczesną blokadą publicznego ruchu przychodzącego. 3. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI; 4. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych. 5. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiający ich podział na poszczególne pola, na podstawie, których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie. 6. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie. 7. Proces normalizacji musi wspierać następujące typy składni:  CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych. 8. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware. 9. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy. 10. System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku, gdy będzie to konieczne przywrócić jedną z poprzednich wersji. 11. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg” znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX. 12. Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni, w której te logi są przesyłane. Przykładowo, jeżeli logi są przesyłane w standardzie CEF system dobierze odpowiedni parser, w przypadku, gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora. 13. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej. 14. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zwartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo, jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku, gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B. 15. Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie. 16. System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów. 17. Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielenia ich składowania na osobny serwer i dedykowane zasoby dyskowe. 18. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej. 19. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych. 20. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach. 21. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne. 22. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa. 23. Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące, jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. „Kliknięcie” na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów. 24. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej. 25. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług. 26. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły. 27. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego. 28. Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje: 29. nowe zasoby wykryte w sieci, 30. typy wykrytych zasobów (np.: serwer lub stacja robocza), 31. zastosowane na nich zabezpieczenia, 32. usługi z którymi się komunikują, 33. nowe usługi wykryte na zasobie, 34. komunikację do usług wykrytych na zasobie. 35. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację. 36. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora. 37. Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi, której ta komunikacja dotyczy. 38. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników:     1. fqdn,     2. e-mail,     3. nazwa pliku,     4. ścieżka do pliku,     5. hash,     6. adres IP,     7. klucz rejestru,     8. cmd. 39. System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (<https://www.misp-project.org/>). 40. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu). 41. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”). 42. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych. 43. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory. 44. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwanym wynikiem analizy jest lista niezgodności, (np: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu). 45. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT. 46. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu. 47. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie. 48. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności: 49. id techniki, 50. taktykę, 51. platformy których dotyczy, 52. potencjalne źródła, 53. opis zagrożenia, 54. mityzację, 55. sposób detekcji, 56. referencje. 57. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów. 58. Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy). 59. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum: 60. rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych, 61. rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów, 62. rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji, 63. rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów. 64. System uczenia maszynowego musi posiadać wbudowane mechanizmy niewymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA). 65. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP, na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji. 66. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np.: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet). 67. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role. 68. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację. 69. System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać: 70. sprasowane pola oraz ich wartości, 71. listy referencyjne, 72. atrybuty użytkowników z Active Directory, 73. atrybuty komputerów z Active Directory, 74. bazę wskaźników kompromitacji (IOC), 75. informacje z elektronicznej dokumentacji, 76. anomalie w zachowaniu użytkowników (UBA), 77. anomalie w zachowaniu zasobów (EBA), 78. podatności na zasobach, 79. wyniki analizy konfiguracji, 80. techniki MITRE ATT&CK®, 81. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić: 82. wykrycie dowolnej treści w logach, 83. wykrycie zmiany jednego z kilku pól, 84. wykrycie zaniku wiadomości, 85. wykrycie nowej wartości pola w zadanym okresie czasu, 86. wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności, 87. wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu, 88. wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu, 89. wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa, 90. wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu, 91. wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu, 92. wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa, 93. wykrycie ilości uruchomionych procesów w zadanym okresie czasu, 94. wykrycie skanowania portów. 95. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić: 96. wykrycie wystąpienia wartości pola na wybranej liście, 97. wykrycie niewystępowania wartości pola na wybranej liście, 98. wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku, z którego został uruchomiony), 99. wykrycie niewystąpienia pary wartości na wybranej liście 100. (np.: nazwa użytkownika wraz aplikacją, z którą się wcześniej nie łączył). 101. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić: 102. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory, 103. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory, 104. wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta). 105. wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins), 106. wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej. 107. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić: 108. wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory, 109. wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory, 110. wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej. 111. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić: 112. wykrycie czy źródłowy adres IP nie jest oznaczony w systemie, jako wskaźnik kompromitacji; 113. wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie, jako wskaźnik kompromitacji; 114. wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie, jako wskaźnik kompromitacji; 115. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić: 116. wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu, 117. wykrycie połączenia do usługi przez nieautoryzowanego użytkownika, 118. wykrycie nieautoryzowanej usługi na serwerze, 119. wykrycie nieautoryzowanego połączenia do usługi na serwerze, 120. wykrycie nieautoryzowanego połączenia z serwera usług, 121. wykrycie nieautoryzowanego połączenia do sieci Internet. 122. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić: 123. wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, 124. wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware, 125. wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejecie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie, 126. wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN. 127. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić: 128. wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, 129. wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware, 130. wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejecie komputera przez cyberprzestępcę lub złośliwe oprogramowanie, 131. wykrycie anomalii związanych z procesami uruchamianymi na serwerach. 132. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić: 133. wykrycie skanowania portów z zasobu posiadającego krytyczne podatności, 134. wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności, 135. wykrycie zdarzeń o wysokim „severity” na zasobach posiadającego krytyczne podatności, 136. wykrycie zdarzeń o wysokim „severity” do zasobów posiadających krytyczne podatności. 137. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na: 138. wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków, 139. wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł nie spełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny. 140. Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić: 141. wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, 142. wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, 143. wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie. 144. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.: 145. wykrycie anomalii na koncie uprzywilejowanym użytkownika, 146. wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej, 147. wykrycie wielu typów anomalii na komputerze z krytyczną podatnością, 148. wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi, 149. wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny. 150. System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać: 151. sparsowane pola oraz ich wartości, 152. atrybuty użytkowników z Active Directory, 153. atrybuty komputerów z Active Directory, 154. informacje z elektronicznej dokumentacji. 155. Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po: 156. adresie IP, 157. koncie domenowym użytkownika, 158. strefie bezpieczeństwa, 159. zakresie adresów IP. 160. Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop” umożliwiającą m.in. na zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej. 161. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze. 162. Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in. 163. wszystkie skorelowane zdarzenia, 164. korespondencja pocztowa, 165. załączniki z próbkami lub dowodami, 166. wskaźniki kompromitacji (IoC), 167. informacje pozyskane z innych systemów. 168. System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielenia uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora. 169. Dla obsługiwanych zdarzeń system powinien umożliwiać automatyczne pozyskanie informacji z innych systemów oraz bazując na uzyskanej od nich odpowiedzi automatycznie zmieniać ich status, np.: na podstawie pozyskanego wskaźnika kompromitacji (IoC) zmienić status zdarzenia na incydent bezpieczeństwa. 170. Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane: 171. identyfikację celu i źródła zagrożenia, 172. nazwę oraz adres IP źródła zagrożenia, 173. rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza, 174. lokalizację z które pochodzi zagrożenie np.: Internet, 175. strefę bezpieczeństwa, z której pochodzi zagrożenie, 176. prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło, 177. wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification), 178. nazwę oraz adres IP celu zagrożenia, 179. zabezpieczenia lokalne chroniące cel zagrożenia, 180. strefę bezpieczeństwa, w której znajduje się cel zagrożenia. 181. Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku, gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall). 182. Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami. Przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem. 183. Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie: 184. nazwy zasobu, 185. rodzaju zasobu, 186. ważności zasobu dla organizacji, 187. rodzaj przetwarzanych informacji, 188. usług, które ten zasób świadczy, 189. lokalizację użytkowników, którzy z niego korzystają, 190. usługi z których zasób korzysta. 191. System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi uwzględniać m.in. dostępność operatora, jego obciążenia oraz parametry zasobu, którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Na przykład: zdarzenie przypisane do krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych. 192. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to: 193. nowe zdarzenie – jako zdarzenie zarejestrowane w systemie, 194. segregacja – segregacja i kwalifikacja zdarzeń, 195. incydent bezpieczeństwa – zdarzenie zakwalifikowane, jako incydent bezpieczeństwa, 196. fałszywy alarm – zdarzenie zakwalifikowane, jako fałszywy alarm, 197. zdarzanie obsłużone – zdarzenie, które zostało obsłużone w systemie. 198. System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa” do statusu „zdarzenie zamknięte”, ale zablokować zmianę ze statusu „incydent bezpieczeństwa” na status „fałszywy alarm”. 199. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi. 200. System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia, z którym są grupowane oraz synchronizować z nim statusy. Dla zdarzeń przetwarzanych przez operatora, zmiana statusu głównego zdarzenia musi wymusić zmianę statusu pozostałych. Na przykład: zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne. Na liście zdarzeń oraz w podglądzie każdego zdarzenia powinna się pojawić informacja o zdarzeniach z nim powiązanych. 201. Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowane w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi). Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów. 202. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów. 203. W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Na przykład:, jeżeli w obsługiwanym zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi wskaźnikami typu FQDN oraz HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów. 204. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell), na skonfigurowanie nowych integracji z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API. 205. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na: 206. podgląd aktywności zagrożonego zasobu na linii czasu, 207. w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku, 208. w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu, 209. podgląd reguły korelacyjnej, która wygenerowała zdarzenie, 210. w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis, 211. listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich, 212. gotowe i proste w użyciu filtry rozszerzajcie analizę zdarzeń o:  * listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po, * listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym,  1. gotowe i proste w użyciu filtry rozszerzajcie analizę logów o:  * listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym, * listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.  1. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących: 2. warunki powiadomień,  * zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi, * zdarzeń o przekroczonych czasach SLA o definiowalny okres, * zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA, * zdarzeń, których priorytet osiągnął określoną wartość, * zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, * zdarzeń na których doszło do naruszenia bezpieczeństwa, * zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną, * zdarzeń realizujących zdefiniowaną usługę, * zdarzeń przetwarzających sklasyfikowane informację, * zdarzeń przetwarzanych na krytycznych zasobach,  1. odbiorców powiadomień, w tym:  * operatora, któremu zostało przydzielone zdarzenie, * właściciela zasobu na którym wystąpiło zdarzenie, * zespół obsługi, który odpowiada za obsługę zdarzeń, * właściciela usługi, która jest realizowana na zasobie, na którym wystąpiło zdarzenie, * podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną.  1. kanały powiadomień, m.in. e-mail, sms, komunikator, 2. zastosowanie mechanizmów grupowania:  * grupowanie wielu powiadomień w jednej wiadomości, * ograniczenie liczby wierszy powiadomienia do określonej wartości.  1. System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach: 2. utworzenia nowego zdarzenia z określonym priorytetem, 3. utworzenia nowego zdarzenia na zasobie krytycznym, 4. utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę, 5. utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe, 6. utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej, 7. modyfikacji przydzielonego operatorowi zdarzania przez innego operatora, 8. zamknięcia przydzielonego operatorowi zdarzania przez innego operatora, 9. przejęcia przydzielonego operatorowi zdarzania przez innego operatora. 10. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego: 11. wybór raportu, który ma zostać wysłany, 12. zdefiniowanie jego tytułu, 13. zdefiniowanie cyklu, w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny, 14. możliwość ograniczenia cyklu do dni powszednich, 15. określenie daty przesłania pierwszego raportu, 16. możliwości ograniczenia okresu, przez jaki raport będzie przesyłany, do:  * zdefiniowanej daty końcowej, * określnej liczby raportów,  1. określenie odbiorców raportu. 2. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook). 3. Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka, jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczą dla podatności wymagających obsługi priorytet w oparciu o następujące parametry: 4. strefę bezpieczeństwa, w której została wykryta podatność, 5. prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie, 6. rodzaj zasobu, którego dotyczy ta podatność, 7. ważność tego zasobu dla organizacji, 8. przetwarzane na tym zasobie informacje, np.: dane osobowe, 9. usługi realizowane przez ten zasób, np.: DNS, 10. wartość parametrów CVSS dla podatności, np.: „*Confidentiality Impact*” = High, 11. poprawność konfiguracji zasobu, na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł, 12. szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet. 13. W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi, jaki i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji. 14. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach: 15. wyliczonym priorytecie podatności, 16. aktualnym statusie obsługi, 17. ważności zasobu na którym została wykryta, 18. adresie IP tego systemu, 19. parametrów SLA związanych z tym statusem, 20. przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe, 21. parametrach CVSS, np.: lista podatności których „Access Complexity (AC)” = „low” oraz „Access Vector (AV) = „Network”. 22. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach: 23. przekroczenia czasu reakcji o określony czas np.: o godzinę, 24. możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji, 25. przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe, 26. przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym, 27. przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę, 28. przekroczenia czasu obsługi zdarzeń zakwalifikowanych, jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe, 29. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych, 30. przekroczenia czasu obsługi zdarzeń zakwalifikowanych, jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę, 31. przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe, 32. przekroczenia czasu reakcji dla podatności na zasobie krytycznym, 33. przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę, 34. Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących: 35. warunki powiadomień,  * podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi, * podatności o przekroczonych czasach SLA o definiowalny okres, * podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA, * podatności, których priorytet osiągnął określoną wartość, * zdarzeń realizujących zdefiniowaną usługę, * zdarzeń przetwarzających sklasyfikowane informację, * zdarzeń przetwarzanych na krytycznych zasobach,  1. odbiorców powiadomień, w tym:  * operatora, któremu została przydzielona podatność, * właściciela zasobu, na którym wystąpiła podatność, * zespół obsługi, który odpowiada za obsługę podatności, * właściciela usługi, na która jest realizowana na zasobie, na którym wystąpiła podatność, * podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną.  1. kanały powiadomień, m.in. e-mail, sms, komunikator, 2. zastosowanie mechanizmów grupowania:  * grupowanie wielu powiadomień w jednej wiadomości, * ograniczenie liczby wierszy powiadomienia do określonej wartości.  1. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku, gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach: 2. przydzielenia nowej podatności do obsługi z określonym priorytetem, 3. przydzielenia nowej podatności do obsługi na zasobie krytycznym, 4. przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę, 5. przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe, 6. modyfikacji przydzielonej operatorowi podatności przez innego operatora, 7. zamknięcia przydzielonej operatorowi podatności przez innego operatora, 8. przejęcia przydzielonej operatorowi podatności przez innego operatora. 9. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na: 10. wybór raportu, który ma zostać wysłany, 11. zdefiniowanie jego tytułu, 12. zdefiniowanie cyklu, w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny, 13. możliwość ograniczenia cyklu do dni powszednich, 14. określenie daty przesłania pierwszego raportu, 15. określenie okresu, przez jaki będą one przesyłane, poprzez:  * zdefiniowanie daty końcowej, * bez daty końcowej, * określenie liczby raportów,  1. określenie odbiorców raportu. 2. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard’u”, tj. dostosowywać zakres i prezentacje danych do potrzeb zalogowanego użytkownika. 3. System musi pozwalać na tworzenie dedykowanych dashboard’ów obejmujących: 4. zestaw wykresów dla bieżącego użytkownika, 5. zestaw wykresów dla wybranego użytkownika, 6. zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu, 7. zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center). 8. System musi zapewniać zestaw predefiniowanych dashboard’ów obejmujących następujące wykresy: 9. wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia:  * ilość zdarzeń nowych i niesklasyfikowanych, * ilość zdarzeń sklasyfikowanych, jako incydenty bezpieczeństwa, * ilość zdarzeń sklasyfikowanych, jako fałszywe alarmy,  1. wykres przedstawiający skale zagrożeń, który uwzględnia:  * ilość zasobów krytycznych, na których są obsługiwane zdarzenia, * ilość zasobów niekrytycznych, na których są obsługiwane zdarzenia,  1. wykres przedstawiający źródła zagrożeń, który uwzględnia:  * ilość nowych zdarzeń dotyczących użytkowników, * ilość podjętych zdarzeń dotyczących użytkowników, * ilość nowych zdarzeń dotyczących zasobów, * ilość podjętych zdarzeń dotyczących zasobów,  1. wykres przedstawiający poziom zagrożeń, który uwzględnia:  * ilość nowych zdarzeń w podziale na priorytety, * ilość podjętych zdarzeń w podziale na priorytety,  1. wykres przedstawiający czas obsługi zagrożeń, który uwzględnia:  * ilość zdarzeń zarejestrowanych w bieżącym dniu, * ilość zdarzeń zarejestrowanych w ostatnim tygodniu, * ilość zdarzeń zarejestrowanych w ostatnim miesiącu, * ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu,  1. wykres przedstawiający zagrożone usługi, który uwzględnia:  * ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia, * ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia, * wykres przedstawiający zagrożone dane, który uwzględnia: * ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje, * ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje, * ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje, * ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,  1. wykres przedstawiający skale podatności, który uwzględnia:  * ilość zasobów krytycznych, na których są obsługiwane podatności, * ilość zasobów niekrytycznych, na których są obsługiwane podatności,  1. wykres przedstawiający czas obsługi podatności, który uwzględnia:  * ilość podatności zarejestrowanych w bieżącym dniu, * ilość podatności zarejestrowanych w ostatnim tygodniu, * ilość podatności zarejestrowanych w ostatnim miesiącu, * ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu,  1. wykres przedstawiający wagę podatności, który uwzględnia:  * ilość nowych podatności w podziale na priorytety, * ilość podjętych podatności w podziale na priorytety,  1. Nawigacja w ramach „Dashboard’u” musi wspierać opcję typu „Drill down” w następującym zakresie: 2. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, 3. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej podatności musi przenieść operatora systemu do listy tych podatności z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości, których dotyczy wykres, 4. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej użytkowników (UBA) musi przenieść operatora systemu do listy tych użytkowników z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości, których dotyczy wykres, 5. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zasobów (EBA) musi przenieść operatora systemu do listy tych zasobów z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości, których dotyczy wykres, 6. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych zdarzeń korelacyjnych musi przenieść operatora systemu do listy prezentującej te zdarzenia z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości, których dotyczy wykres, 7. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych logów musi przenieść operatora systemu do listy prezentującej te logi z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości, których dotyczy wykres. 8. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli. 9. Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów (UEBA), mechanizmy reakcji/ scenariusze reakcji (SOAR). Zamawiający nie zaakceptuje systemu, który wykorzystuje mechanizmy typu open source np.: Elastic Search, OSSIM, Snort, The Hive, AlienVault itd. lub został stworzony przez modyfikację oprogramowania otwartego. 10. W celach weryfikacji zgodności produktu z wymaganiami, musi być on dodatkowo oferowany przez autoryzowanego dystrybutora, dostarczającego produkty z obszaru cyberbezpieczeństwa na rynku polskim, który w przypadku jakichkolwiek wątpliwości Zamawiającego, związanych z wymaganymi funkcjonalności będzie mógł je potwierdzić lub im zaprzeczyć. 11. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem. 12. Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencje nie może nakładać limitów w tym zakresie. 13. Produkt musi umożliwiać równoczesną pracę, co najmniej 5 operatorów oraz obsługiwać 200 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności. 14. Dla wszystkich źródeł objętych licencją oraz stanowiących jednocześnie komputery bądź serwery licencja produktu musi uwzględniać możliwość wykorzystania dedykowanych agentów XDR. 15. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów. 16. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet. 17. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x). 18. Dostarczone rozwiązanie musi być objęte 24 miesięcznym wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia niestanowiące błędu krytycznego lub poważnego).  * Wykonawca udzieli Zamawiającemu wieczystej (perpetual), nieograniczonej czasowo licencji na zakupiony System. |  | |

## Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa – szt.1 lic.

|  |
| --- |
| System przeciwdziałania cyberzagrożeniom, oferująca możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi.   1. System musi umożliwić odbieranie logów z urządzeń sieciowych oraz wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding. 2. System musi zapewnić agentów XDR na stacje końcowe umożliwiających im pobieranie pełnych danych telemetrycznych hostów, których chronią i przesłanie tych danych do systemu centralnego w celu dalszej korelacji i analizy behawioralnej. W przypadku wykrycia zagrożenia agenci muszą umożliwiać automatyczną i dostosowaną do kontekstu reakcje, m.in. na blokowanie bądź izolację sieciową złośliwego oprogramowania.    1. Agent musi posiadać możliwość dodawania i usuwania reguł wbudowanego firewalla obejmując m.in. blokowanie i odblokowywanie poszczególnych procesów bądź reguł dotyczących ruchu sieciowego stanowiące reakcję na wykryte zagrożenie.    2. Agent musi pobierać oraz aktualizować na bieżąco listę zainstalowanego oprogramowania.    3. System w przypadku wykrycia techniki ataku ukierunkowanego na podatną aplikację w celu zablokowania ataku musi umożliwiać zatrzymanie procesu aplikacji oraz zapewnić dostęp do danych dowodowych obejmujących nazwę chronionego systemu, system operacyjny, tożsamość użytkownika, nazwę procesu, dokładną komendę uruchamiającą złośliwy proces wraz parametrami i znacznik czasowy.    4. System musi obsługiwać scenariusz uwzględniający ocenę prawdopodobieństwa materializacji się wykrytego zagrożenia, gdzie w przypadku, gdy wyliczone przez system prawdopodobieństwo ataku jest wysokie proces zostanie zablokowany, natomiast w pozostałych przypadkach, gdy jest ono średnie bądź niskie zostanie on zamrożony z możliwością ponownego wznowienia przez operatora.    5. System musi posiadać możliwość dostosowania reakcji na zagrożenie w zależności od rodzaju zasobu, który chroni, przykładowo, jeżeli zagrożenie dotyczyć będzie procesu na stacji roboczej proces zostanie automatycznie zablokowany jednakże w przypadku, gdy to samo zagrożenie dotyczyć będzie serwera świadczącego usługi w sieci publicznej proces pozostanie uruchomiony z jednoczesną blokadą publicznego ruchu przychodzącego. 3. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI; 4. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych. 5. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiający ich podział na poszczególne pola, na podstawie, których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie. 6. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie. 7. Proces normalizacji musi wspierać następujące typy składni:  CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych. 8. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware. 9. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy. 10. System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku, gdy będzie to konieczne przywrócić jedną z poprzednich wersji. 11. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg” znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX. 12. Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni, w której te logi są przesyłane. Przykładowo, jeżeli logi są przesyłane w standardzie CEF system dobierze odpowiedni parser, w przypadku, gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora. 13. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej. 14. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zwartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo, jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku, gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B. 15. Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie. 16. System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów. 17. Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielenia ich składowania na osobny serwer i dedykowane zasoby dyskowe. 18. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej. 19. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych. 20. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach. 21. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne. 22. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa. 23. Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące, jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. „Kliknięcie” na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów. 24. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej. 25. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług. 26. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły. 27. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego. 28. Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje: 29. nowe zasoby wykryte w sieci, 30. typy wykrytych zasobów (np.: serwer lub stacja robocza), 31. zastosowane na nich zabezpieczenia, 32. usługi z którymi się komunikują, 33. nowe usługi wykryte na zasobie, 34. komunikację do usług wykrytych na zasobie. 35. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację. 36. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora. 37. Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi, której ta komunikacja dotyczy. 38. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników:     1. fqdn,     2. e-mail,     3. nazwa pliku,     4. ścieżka do pliku,     5. hash,     6. adres IP,     7. klucz rejestru,     8. cmd. 39. System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (<https://www.misp-project.org/>). 40. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu). 41. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”). 42. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych. 43. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory. 44. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwanym wynikiem analizy jest lista niezgodności, (np: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu). 45. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT. 46. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu. 47. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie. 48. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności: 49. id techniki, 50. taktykę, 51. platformy których dotyczy, 52. potencjalne źródła, 53. opis zagrożenia, 54. mityzację, 55. sposób detekcji, 56. referencje. 57. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów. 58. Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy). 59. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum: 60. rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych, 61. rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów, 62. rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji, 63. rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów. 64. System uczenia maszynowego musi posiadać wbudowane mechanizmy niewymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA). 65. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP, na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji. 66. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np.: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet). 67. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role. 68. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację. 69. System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać: 70. sprasowane pola oraz ich wartości, 71. listy referencyjne, 72. atrybuty użytkowników z Active Directory, 73. atrybuty komputerów z Active Directory, 74. bazę wskaźników kompromitacji (IOC), 75. informacje z elektronicznej dokumentacji, 76. anomalie w zachowaniu użytkowników (UBA), 77. anomalie w zachowaniu zasobów (EBA), 78. podatności na zasobach, 79. wyniki analizy konfiguracji, 80. techniki MITRE ATT&CK®, 81. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić: 82. wykrycie dowolnej treści w logach, 83. wykrycie zmiany jednego z kilku pól, 84. wykrycie zaniku wiadomości, 85. wykrycie nowej wartości pola w zadanym okresie czasu, 86. wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności, 87. wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu, 88. wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu, 89. wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa, 90. wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu, 91. wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu, 92. wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa, 93. wykrycie ilości uruchomionych procesów w zadanym okresie czasu, 94. wykrycie skanowania portów. 95. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić: 96. wykrycie wystąpienia wartości pola na wybranej liście, 97. wykrycie niewystępowania wartości pola na wybranej liście, 98. wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku, z którego został uruchomiony), 99. wykrycie niewystąpienia pary wartości na wybranej liście 100. (np.: nazwa użytkownika wraz aplikacją, z którą się wcześniej nie łączył). 101. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić: 102. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory, 103. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory, 104. wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta). 105. wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins), 106. wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej. 107. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić: 108. wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory, 109. wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory, 110. wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej. 111. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić: 112. wykrycie czy źródłowy adres IP nie jest oznaczony w systemie, jako wskaźnik kompromitacji; 113. wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie, jako wskaźnik kompromitacji; 114. wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie, jako wskaźnik kompromitacji; 115. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić: 116. wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu, 117. wykrycie połączenia do usługi przez nieautoryzowanego użytkownika, 118. wykrycie nieautoryzowanej usługi na serwerze, 119. wykrycie nieautoryzowanego połączenia do usługi na serwerze, 120. wykrycie nieautoryzowanego połączenia z serwera usług, 121. wykrycie nieautoryzowanego połączenia do sieci Internet. 122. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić: 123. wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, 124. wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware, 125. wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejecie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie, 126. wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN. 127. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić: 128. wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, 129. wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware, 130. wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejecie komputera przez cyberprzestępcę lub złośliwe oprogramowanie, 131. wykrycie anomalii związanych z procesami uruchamianymi na serwerach. 132. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić: 133. wykrycie skanowania portów z zasobu posiadającego krytyczne podatności, 134. wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności, 135. wykrycie zdarzeń o wysokim „severity” na zasobach posiadającego krytyczne podatności, 136. wykrycie zdarzeń o wysokim „severity” do zasobów posiadających krytyczne podatności. 137. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na: 138. wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków, 139. wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł nie spełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny. 140. Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić: 141. wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, 142. wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, 143. wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie. 144. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.: 145. wykrycie anomalii na koncie uprzywilejowanym użytkownika, 146. wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej, 147. wykrycie wielu typów anomalii na komputerze z krytyczną podatnością, 148. wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi, 149. wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny. 150. System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać: 151. sparsowane pola oraz ich wartości, 152. atrybuty użytkowników z Active Directory, 153. atrybuty komputerów z Active Directory, 154. informacje z elektronicznej dokumentacji. 155. Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po: 156. adresie IP, 157. koncie domenowym użytkownika, 158. strefie bezpieczeństwa, 159. zakresie adresów IP. 160. Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop” umożliwiającą m.in. na zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej. 161. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze. 162. Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in. 163. wszystkie skorelowane zdarzenia, 164. korespondencja pocztowa, 165. załączniki z próbkami lub dowodami, 166. wskaźniki kompromitacji (IoC), 167. informacje pozyskane z innych systemów. 168. System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielenia uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora. 169. Dla obsługiwanych zdarzeń system powinien umożliwiać automatyczne pozyskanie informacji z innych systemów oraz bazując na uzyskanej od nich odpowiedzi automatycznie zmieniać ich status, np.: na podstawie pozyskanego wskaźnika kompromitacji (IoC) zmienić status zdarzenia na incydent bezpieczeństwa. 170. Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane: 171. identyfikację celu i źródła zagrożenia, 172. nazwę oraz adres IP źródła zagrożenia, 173. rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza, 174. lokalizację z które pochodzi zagrożenie np.: Internet, 175. strefę bezpieczeństwa, z której pochodzi zagrożenie, 176. prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło, 177. wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification), 178. nazwę oraz adres IP celu zagrożenia, 179. zabezpieczenia lokalne chroniące cel zagrożenia, 180. strefę bezpieczeństwa, w której znajduje się cel zagrożenia. 181. Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku, gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall). 182. Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami. Przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem. 183. Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie: 184. nazwy zasobu, 185. rodzaju zasobu, 186. ważności zasobu dla organizacji, 187. rodzaj przetwarzanych informacji, 188. usług, które ten zasób świadczy, 189. lokalizację użytkowników, którzy z niego korzystają, 190. usługi z których zasób korzysta. 191. System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi uwzględniać m.in. dostępność operatora, jego obciążenia oraz parametry zasobu, którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Na przykład: zdarzenie przypisane do krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych. 192. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to: 193. nowe zdarzenie – jako zdarzenie zarejestrowane w systemie, 194. segregacja – segregacja i kwalifikacja zdarzeń, 195. incydent bezpieczeństwa – zdarzenie zakwalifikowane, jako incydent bezpieczeństwa, 196. fałszywy alarm – zdarzenie zakwalifikowane, jako fałszywy alarm, 197. zdarzanie obsłużone – zdarzenie, które zostało obsłużone w systemie. 198. System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa” do statusu „zdarzenie zamknięte”, ale zablokować zmianę ze statusu „incydent bezpieczeństwa” na status „fałszywy alarm”. 199. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi. 200. System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia, z którym są grupowane oraz synchronizować z nim statusy. Dla zdarzeń przetwarzanych przez operatora, zmiana statusu głównego zdarzenia musi wymusić zmianę statusu pozostałych. Na przykład: zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne. Na liście zdarzeń oraz w podglądzie każdego zdarzenia powinna się pojawić informacja o zdarzeniach z nim powiązanych. 201. Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowane w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi). Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów. 202. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów. 203. W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Na przykład:, jeżeli w obsługiwanym zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi wskaźnikami typu FQDN oraz HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów. 204. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell), na skonfigurowanie nowych integracji z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API. 205. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na: 206. podgląd aktywności zagrożonego zasobu na linii czasu, 207. w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku, 208. w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu, 209. podgląd reguły korelacyjnej, która wygenerowała zdarzenie, 210. w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis, 211. listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich, 212. gotowe i proste w użyciu filtry rozszerzajcie analizę zdarzeń o:  * listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po, * listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym,  1. gotowe i proste w użyciu filtry rozszerzajcie analizę logów o:  * listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym, * listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.  1. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących: 2. warunki powiadomień,  * zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi, * zdarzeń o przekroczonych czasach SLA o definiowalny okres, * zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA, * zdarzeń, których priorytet osiągnął określoną wartość, * zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, * zdarzeń na których doszło do naruszenia bezpieczeństwa, * zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną, * zdarzeń realizujących zdefiniowaną usługę, * zdarzeń przetwarzających sklasyfikowane informację, * zdarzeń przetwarzanych na krytycznych zasobach,  1. odbiorców powiadomień, w tym:  * operatora, któremu zostało przydzielone zdarzenie, * właściciela zasobu na którym wystąpiło zdarzenie, * zespół obsługi, który odpowiada za obsługę zdarzeń, * właściciela usługi, która jest realizowana na zasobie, na którym wystąpiło zdarzenie, * podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną.  1. kanały powiadomień, m.in. e-mail, sms, komunikator, 2. zastosowanie mechanizmów grupowania:  * grupowanie wielu powiadomień w jednej wiadomości, * ograniczenie liczby wierszy powiadomienia do określonej wartości.  1. System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach: 2. utworzenia nowego zdarzenia z określonym priorytetem, 3. utworzenia nowego zdarzenia na zasobie krytycznym, 4. utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę, 5. utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe, 6. utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej, 7. modyfikacji przydzielonego operatorowi zdarzania przez innego operatora, 8. zamknięcia przydzielonego operatorowi zdarzania przez innego operatora, 9. przejęcia przydzielonego operatorowi zdarzania przez innego operatora. 10. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego: 11. wybór raportu, który ma zostać wysłany, 12. zdefiniowanie jego tytułu, 13. zdefiniowanie cyklu, w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny, 14. możliwość ograniczenia cyklu do dni powszednich, 15. określenie daty przesłania pierwszego raportu, 16. możliwości ograniczenia okresu, przez jaki raport będzie przesyłany, do:  * zdefiniowanej daty końcowej, * określnej liczby raportów,  1. określenie odbiorców raportu. 2. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook). 3. Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka, jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczą dla podatności wymagających obsługi priorytet w oparciu o następujące parametry: 4. strefę bezpieczeństwa, w której została wykryta podatność, 5. prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie, 6. rodzaj zasobu, którego dotyczy ta podatność, 7. ważność tego zasobu dla organizacji, 8. przetwarzane na tym zasobie informacje, np.: dane osobowe, 9. usługi realizowane przez ten zasób, np.: DNS, 10. wartość parametrów CVSS dla podatności, np.: „*Confidentiality Impact*” = High, 11. poprawność konfiguracji zasobu, na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł, 12. szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet. 13. W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi, jaki i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji. 14. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach: 15. wyliczonym priorytecie podatności, 16. aktualnym statusie obsługi, 17. ważności zasobu na którym została wykryta, 18. adresie IP tego systemu, 19. parametrów SLA związanych z tym statusem, 20. przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe, 21. parametrach CVSS, np.: lista podatności których „Access Complexity (AC)” = „low” oraz „Access Vector (AV) = „Network”. 22. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach: 23. przekroczenia czasu reakcji o określony czas np.: o godzinę, 24. możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji, 25. przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe, 26. przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym, 27. przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę, 28. przekroczenia czasu obsługi zdarzeń zakwalifikowanych, jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe, 29. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych, 30. przekroczenia czasu obsługi zdarzeń zakwalifikowanych, jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę, 31. przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe, 32. przekroczenia czasu reakcji dla podatności na zasobie krytycznym, 33. przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę, 34. Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących: 35. warunki powiadomień,  * podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi, * podatności o przekroczonych czasach SLA o definiowalny okres, * podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA, * podatności, których priorytet osiągnął określoną wartość, * zdarzeń realizujących zdefiniowaną usługę, * zdarzeń przetwarzających sklasyfikowane informację, * zdarzeń przetwarzanych na krytycznych zasobach,  1. odbiorców powiadomień, w tym:  * operatora, któremu została przydzielona podatność, * właściciela zasobu, na którym wystąpiła podatność, * zespół obsługi, który odpowiada za obsługę podatności, * właściciela usługi, na która jest realizowana na zasobie, na którym wystąpiła podatność, * podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną.  1. kanały powiadomień, m.in. e-mail, sms, komunikator, 2. zastosowanie mechanizmów grupowania:  * grupowanie wielu powiadomień w jednej wiadomości, * ograniczenie liczby wierszy powiadomienia do określonej wartości.  1. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku, gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach: 2. przydzielenia nowej podatności do obsługi z określonym priorytetem, 3. przydzielenia nowej podatności do obsługi na zasobie krytycznym, 4. przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę, 5. przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe, 6. modyfikacji przydzielonej operatorowi podatności przez innego operatora, 7. zamknięcia przydzielonej operatorowi podatności przez innego operatora, 8. przejęcia przydzielonej operatorowi podatności przez innego operatora. 9. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na: 10. wybór raportu, który ma zostać wysłany, 11. zdefiniowanie jego tytułu, 12. zdefiniowanie cyklu, w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny, 13. możliwość ograniczenia cyklu do dni powszednich, 14. określenie daty przesłania pierwszego raportu, 15. określenie okresu, przez jaki będą one przesyłane, poprzez:  * zdefiniowanie daty końcowej, * bez daty końcowej, * określenie liczby raportów,  1. określenie odbiorców raportu. 2. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard’u”, tj. dostosowywać zakres i prezentacje danych do potrzeb zalogowanego użytkownika. 3. System musi pozwalać na tworzenie dedykowanych dashboard’ów obejmujących: 4. zestaw wykresów dla bieżącego użytkownika, 5. zestaw wykresów dla wybranego użytkownika, 6. zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu, 7. zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center). 8. System musi zapewniać zestaw predefiniowanych dashboard’ów obejmujących następujące wykresy: 9. wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia:  * ilość zdarzeń nowych i niesklasyfikowanych, * ilość zdarzeń sklasyfikowanych, jako incydenty bezpieczeństwa, * ilość zdarzeń sklasyfikowanych, jako fałszywe alarmy,  1. wykres przedstawiający skale zagrożeń, który uwzględnia:  * ilość zasobów krytycznych, na których są obsługiwane zdarzenia, * ilość zasobów niekrytycznych, na których są obsługiwane zdarzenia,  1. wykres przedstawiający źródła zagrożeń, który uwzględnia:  * ilość nowych zdarzeń dotyczących użytkowników, * ilość podjętych zdarzeń dotyczących użytkowników, * ilość nowych zdarzeń dotyczących zasobów, * ilość podjętych zdarzeń dotyczących zasobów,  1. wykres przedstawiający poziom zagrożeń, który uwzględnia:  * ilość nowych zdarzeń w podziale na priorytety, * ilość podjętych zdarzeń w podziale na priorytety,  1. wykres przedstawiający czas obsługi zagrożeń, który uwzględnia:  * ilość zdarzeń zarejestrowanych w bieżącym dniu, * ilość zdarzeń zarejestrowanych w ostatnim tygodniu, * ilość zdarzeń zarejestrowanych w ostatnim miesiącu, * ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu,  1. wykres przedstawiający zagrożone usługi, który uwzględnia:  * ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia, * ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia, * wykres przedstawiający zagrożone dane, który uwzględnia: * ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje, * ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje, * ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje, * ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,  1. wykres przedstawiający skale podatności, który uwzględnia:  * ilość zasobów krytycznych, na których są obsługiwane podatności, * ilość zasobów niekrytycznych, na których są obsługiwane podatności,  1. wykres przedstawiający czas obsługi podatności, który uwzględnia:  * ilość podatności zarejestrowanych w bieżącym dniu, * ilość podatności zarejestrowanych w ostatnim tygodniu, * ilość podatności zarejestrowanych w ostatnim miesiącu, * ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu,  1. wykres przedstawiający wagę podatności, który uwzględnia:  * ilość nowych podatności w podziale na priorytety, * ilość podjętych podatności w podziale na priorytety,  1. Nawigacja w ramach „Dashboard’u” musi wspierać opcję typu „Drill down” w następującym zakresie: 2. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres, 3. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej podatności musi przenieść operatora systemu do listy tych podatności z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości, których dotyczy wykres, 4. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej użytkowników (UBA) musi przenieść operatora systemu do listy tych użytkowników z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości, których dotyczy wykres, 5. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zasobów (EBA) musi przenieść operatora systemu do listy tych zasobów z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości, których dotyczy wykres, 6. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych zdarzeń korelacyjnych musi przenieść operatora systemu do listy prezentującej te zdarzenia z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości, których dotyczy wykres, 7. „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych logów musi przenieść operatora systemu do listy prezentującej te logi z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości, których dotyczy wykres. 8. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli. 9. Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów (UEBA), mechanizmy reakcji/ scenariusze reakcji (SOAR). Zamawiający nie zaakceptuje systemu, który wykorzystuje mechanizmy typu open source np.: Elastic Search, OSSIM, Snort, The Hive, AlienVault itd. lub został stworzony przez modyfikację oprogramowania otwartego. 10. W celach weryfikacji zgodności produktu z wymaganiami, musi być on dodatkowo oferowany przez autoryzowanego dystrybutora, dostarczającego produkty z obszaru cyberbezpieczeństwa na rynku polskim, który w przypadku jakichkolwiek wątpliwości Zamawiającego, związanych z wymaganymi funkcjonalności będzie mógł je potwierdzić lub im zaprzeczyć. 11. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem. 12. Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencje nie może nakładać limitów w tym zakresie. 13. Produkt musi umożliwiać równoczesną pracę, co najmniej 5 operatorów oraz obsługiwać 200 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności. 14. Dla wszystkich źródeł objętych licencją oraz stanowiących jednocześnie komputery bądź serwery licencja produktu musi uwzględniać możliwość wykorzystania dedykowanych agentów XDR. 15. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów. 16. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet. 17. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x). 18. Dostarczone rozwiązanie musi być objęte 24 miesięcznym wsparciem producenta lub producentów. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia niestanowiące błędu krytycznego lub poważnego).   Wykonawca udzieli Zamawiającemu wieczystej (perpetual), nieograniczonej czasowo licencji na zakupiony System. |

## Serwer – szt.1

Wymagania minimalne:

|  |
| --- |
| **Obudowa**   * Typu RACK, wysokość 2U; * Szyny umożliwiające wysunięcie serwera z szafy stelażowej; * Możliwość zainstalowania 12 dysków twardych hot plug 3,5”; * Zainstalowane fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych; * Zainstalowane 10 szt. dysków SSD 1,92TB Hot-Plug * Możliwość zainstalowania dysku M.2 NVMe;   **Płyta główna**   * Dwuprocesorowa; * Wyprodukowana i zaprojektowana przez producenta serwera; * Możliwość instalacji procesorów 60-rdzeniowych; * Zainstalowany moduł TPM 2.0; * 6 złącz PCI Express w tym:   + 4 fizyczne złącza o prędkości x16, minimum 2 generacji 5;   + 2 fizyczne złącza o prędkości x8; * 32 gniazda pamięci RAM; * Obsługa minimum 8 TB pamięci RAM DDR5; * Wsparcie dla technologii:   + Memory Scrubbing;   + ECC; * Możliwość instalacji 2 dysków M.2 na płycie głównej lub dedykowanej karcie producenta. Dyski nie mogą zajmować klatek dla dysków hot-plug.   **Procesory**   * Dwa procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86\_64; * Osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base 246 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany w konfiguracji dwuprocesorowej dla dowolnego producenta serwera na stronie <http://spec.org/cpu2017/results/cpu2017.html>.   **Pamięć RAM**   * 256 GB pamięci RAM; * DDR5 Registered 4800MT/s;   **Kontrolery LAN**  Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:   * 2x 1Gbit Base-T; * 2x 10Gbit SFP+, wszystkie porty obsadzone modułami MMF LC; * Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28   **Kontrolery I/O**   * Kontroler SAS RAID dla dysków wewnętrznych posiadający 4GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania;   **Porty**   * Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; * 1 porty USB 3.0 wewnętrzne; * 2 porty USB dostępne z tyłu serwera; * 2 porty USB na panelu przednim; * Opcjonalny port serial * Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.   **Zasilanie, chłodzenie**   * Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy minimum 900W; * Redundantne wentylatory hotplug.   **Zarządzanie**   * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;   + informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:     - karty rozszerzeń zainstalowane w dowolnym  slocie PCI Express;     - procesory CPU;     - pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;     - status karty zarządzającej serwera;     - wentylatory;     - bateria podtrzymująca ustawienia BIOS płyty głównej;     - zasilacze; * Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:   + Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;   + Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;   + Dostęp poprzez przeglądarkę Web, SSH;   + Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;   + Zarządzanie alarmami (zdarzenia poprzez SNMP);   + Możliwość przejęcia konsoli tekstowej;   + Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);   + Obsługa serwerów proxy (autentykacja);   + Obsługa VLAN;   + Możliwość konfiguracji parametru Max. Transmission Unit (MTU);   + Obsługa protokołów TLS 1.2, SSL v3;   + Obsługa protokołu LDAP;   + Synchronizacja czasu poprzez protokół NTP;   + Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej; * Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); * Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.   **Wspierane OS**   * Microsoft Windows Server 2025, 2022, 2019; * VMWare vSphere 8.0; * Suse Linux Enterprise Server 15; * Red Hat Enterprise Linux 9, 8; * Microsoft Hyper-V Server 2025, 2022, 2019.   **Gwarancja**   * 3 lata gwarancji producenta serwera w trybie on-site. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej; * Funkcja zgłaszania usterek i awarii sprzętowych poprzez założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; * Firma serwisująca musi posiadać ISO 9001:2000 lub równoważna na świadczenie usług serwisowych; * Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; * Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite   **Dokumentacja, inne**   * Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; * Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; * W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; * Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; * Zgodność z normami:RoHS, WEEE oraz CE lub równoważnymi. * Serwer będzie przeznaczony nie tylko dla Urzędu Gminy Nozdrzec, ale również będzie służył podniesieniu bezpieczeństwa w Gminnym Ośrodku Pomocy Społecznej. |

## Firewall – klaster – szt.2

**Wymagania minimalne**

|  |
| --- |
| Wymagania Ogólne  System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania, co najmniej 4 administratorów do poszczególnych instancji systemu.  System wspiera protokoły IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego.   Redundancja, monitoring i wykrywanie awarii   1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.   Interfejsy, Dysk, Zasilanie:   1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:  * 16 portami Gigabit Ethernet RJ-45. * 8 gniazdami SFP 1 Gbps. * 4 gniazdami SFP+ 10 Gbps.  1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 2. System Firewall pozwala skonfigurować, co najmniej 200 interfejsów wirtualnych, definiowanych, jako VLAN’y w oparciu o standard 802.1Q. 3. System realizujący funkcję Firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności minimum 480 GB. 4. System jest wyposażony w zasilanie AC. 5. Parametry wydajnościowe: 6. W zakresie Firewall’a obsługa nie mniej niż 2.8 mln. jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę. 7. Przepustowość Stateful Firewall: nie mniej niż 38 Gbps dla pakietów 512 B. 8. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps. 9. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 30 Gbps. 10. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps. 11. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.5 Gbps. 12. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.   **Funkcje Systemu Bezpieczeństwa:**  W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).   Polityki, Firewall   1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.  * Amazon Web Services (AWS). * Microsoft Azure. * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. * Kubernetes.   Połączenia VPN   1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:  * Wsparcie dla IKE v1 oraz v2. * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19, 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.  1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:  * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.   Routing i obsługa łączy WAN  W zakresie routingu rozwiązanie zapewnia obsługę:   1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.   Funkcje SD-WAN   1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).   Zarządzanie pasmem   1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.   Ochrona przed malware   1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.   Ochrona przed atakami   1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.   Kontrola aplikacji   1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).   Kontrola WWW   1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.   Uwierzytelnianie użytkowników w ramach sesji   1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.   Zarządzanie   1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.   Logowanie   1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.   Testy wydajnościowe oraz funkcjonalne   1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.   Serwisy i licencje  W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:  a)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.  Gwarancja oraz wsparcie   1. Gwarancja: System musi być objęty serwisem gwarancyjnym, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu wykonawca musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.   Opisy do wymagań ogólnych   1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.   Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym. |

## Centralny system logów – szt.1

Wymagania minimalne

|  |
| --- |
| **Wymagania Ogólne**  W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.  Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia, na co najmniej następujących hypervisorach:  VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).  **Interfejsy, Dysk:**   1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności min. 1 TB.   Parametry wydajnościowe:   1. System musi być w stanie przyjmować minimum 5 GB logów na dzień. 2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.   W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane, co najmniej poniższe funkcje:  **Logowanie**   1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować, co najmniej:   a. Listę najczęściej wykrywanych ataków.  b. Listę najbardziej aktywnych użytkowników.  c. Listę najczęściej wykorzystywanych aplikacji.  d. Listę najczęściej odwiedzanych stron www.  e. Listę krajów, do których nawiązywane są połączenia.  f. Listę najczęściej wykorzystywanych polityk Firewall.  g. Informacje o realizowanych połączeniach IPSec.   1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 2. Komunikacja systemów bezpieczeństwa, (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa, co najmniej z wykorzystaniem UDP/514 oraz TCP/514. 3. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.   **Raportowanie**  W zakresie raportowania system musi zapewniać:   1. Generowanie raportów, co najmniej w formatach: PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Funkcję definiowania własnych raportów. 4. Możliwość spolszczenia raportów. 5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.   **Korelacja logów**  W zakresie korelacji zdarzeń system musi zapewniać:   1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia, co najmniej dla następujących kategorii zdarzeń:  * Malware. * Aplikacje sieciowe. * Email. * IPS. * Traffic. * Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.   **Zarządzanie**   1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.   a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.   1. System musi umożliwiać zdefiniowanie, co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.   Serwisy i licencje  Wsparcie: System musi być objęty serwisem przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. |

## Zestaw komputerowy z oprogramowaniem – szt.15

Wymagania minimalne

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa komponentu | Wymagane minimalne parametry techniczne komputerów |
|  | Komputer | Komputer fabrycznie wbudowany w obudowę monitora. Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. |
|  | Obudowa | Obudowa typu All-in-One z możliwością zabezpieczenia fizycznego przez metalową linkę typu Kensington Lock oraz umożliwiająca beznarzędziową wymianę pamięci RAM.  Wyposażona w listwę montażową w standardzie VESA 100x100.  Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem MTM, PN, numerem seryjnym |
|  | Podstawa | Podstawa umożliwiająca regulację jednostki w zakresie co najmniej:   * pochylenie przód tył od -5 do 20 stopni * swivel w zakresie 45 stopni w każdą stronę * pivot w zakresie 90 stopni * regulację wysokości w do 110 mm |
|  | Chipset | Dostosowany do zaoferowanego procesora |
|  | Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Płyta główna wyposażona w min. 3 złącza M.2 z czego 2 dedykowane dla dysku SSD PCIe. Płyta główna wyposażona w min. 2 sloty pamięci RAM DDR5. |
|  | Procesor | Procesor dedykowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark - Multithread Rating wynik co najmniej 25000 pkt. według wyników opublikowanych na stronie <https://www.cpubenchmark.net/cpu_list.php>  Wynik nie starszy niż 90 dni od daty złożenia oferty. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. |
|  | Pamięć operacyjna | Min. 16GB RAM,  Możliwość rozbudowy do min. 64GB  Jeden slot pozostawiony wolny |
|  | Dysk twardy | Min 512GB M.2 PCIe, wspierający sprzętowe szyfrowanie dysku OPAL, zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. Możliwość instalacji drugiego dysku SSD M.2 |
|  | Karta graficzna | Zintegrowana karta graficzna z procesorem. |
|  | Matryca | Min. 23,8” IPS o rozdzielczości min. FHD 1920x1080  Jasność typowa min. 250 cd/m²  Kontrast typowy min. 1300:1  Typowy czas reakcji matrycy maksymalnie 14ms  Odświeżanie min. 60Hz  Gamut min. 99% sRGB  Sprzętowa funkcja redukująca emisję światła niebieskiego  Kąty widzenia poziomo/pionowo min. 178/178 stopni |
|  | Multimedia | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.  Wbudowane dwa głośniki o mocy min. 3W każdy  Wbudowane dwa mikrofony.  Kamera min. 5MP zintegrowana z obudową komputera, z mechaniczną zasłoną obiektywu, funkcją logowania za pomocą rozpoznawania twarzy oraz możliwością regulacji pochylenia w zakresie od -20 do 20 stopni. |
|  | Sieć | Karta sieciowa LAN obsługująca prędkości 10/100/1000 Wbudowana karta sieci bezprzewodowej, pracująca w standardzie AX  Bluetooth min. 5.1 |
|  | Porty/złącza | Z tyłu obudowy:   * 1 x USB 3.2 typu C Generacji 2; * 3 x USB 3.2 typu A Generacji 1; * 1 x HDMI combo; * 1x DisplayPort 1.4; * 1x RJ-45;   Z boku obudowy:   * 3x USB 3.2 typu A Generacji 2; * 1x złącze audio combo;   Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |
|  | Klawiatura/mysz | Przewodowa USB: klawiatura w układzie US + mysz z rolką |
|  | Zasilacz | Energooszczędny zasilacz o mocy nie większej niż 180W oraz sprawności na poziomie min. 90%. |
|  | Ergonomia | Głośność jednostki w konfiguracji oferowanej lub wyższej mierzona zgodnie z normą ISO 7779 lub równoważną oraz wykazana zgodnie z normą ISO 9296 lub równoważną w trybie jałowym (IDLE) ma wynosić maksymalnie 22dB |
|  | System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych.  2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego.  3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim.  4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.  5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe.  6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.  7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.  8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.  9. Wbudowany system pomocy w języku polskim.  10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).  11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.  12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.  13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.  14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.  15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.  16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".  17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.  18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.  19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.  20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.  21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.  22.Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.  23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."  24. Wbudowany mechanizm wirtualizacji typu hypervisor."  25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.  26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.  27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.  28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).  29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.  30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.  31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.  32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM  33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.  34. Możliwość tworzenia wirtualnych kart inteligentnych.  35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu  (Secure Boot)  36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.  37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.  38. Mechanizmy logowania w oparciu o:   * 1. Login i hasło,   2. Karty inteligentne i certyfikaty (smartcard),   3. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),   4. Certyfikat/Klucz i PIN,   5. Certyfikat/Klucz i uwierzytelnienie biometryczne.   39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5  40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.  41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń.  43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń. |
|  | BIOS | Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:   * modelu komputera, * numerze seryjnym, * numerze inwentarzowym (AssetTag), * MAC Adres karty sieciowej, * wersji BIOS, * dacie produkcji BIOS, * zainstalowanym procesorze, * zainstalowanej pamięci RAM, * urządzeniach podłączonych do portów M.2.   Możliwość z poziomu Bios:   * wyłączenia/włączenia selektywnego (pojedynczo) portów USB, * wyłączenia karty sieciowej, * wyłączenia karty audio, * wyłączenia funkcji Wake on LAN, * wyłączenia wirtualizacji, * wyłączenia modułu TPM.   - możliwość ustawienia portów USB w jednym z dwóch trybów:   1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB, 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej.   - ustawienia hasła: administratora, Power-On, dysku twardego,  - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan),  - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii,  - zdefiniowania sekwencji bootowania, z uwzględnieniem PXE, zewnętrznych nośników, dysku twardego,  - załadowania optymalnych ustawień Bios,  bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. |
|  | Zintegrowany System Diagnostyczny | Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający wykonanie diagnostyki następujących podzespołów:   * test pamięci RAM, * test dysku twardego, * test portów USB, * test płyty głównej, * test procesora.   Wizualna lub dźwiękowa sygnalizacja w przypadku uszkodzenia bądź błędów któregokolwiek z powyższych podzespołów komputera.  Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie:   * PC: Producent, model, * BIOS: Wersja, data wydania, producent, * Procesor : Nazwa, taktowanie, liczba rdzeni, liczba wątków, pamięć cache L1, L2, L3, * Pamięć RAM : Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny, taktowanie, * Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy, producent.   System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera. |
|  | Certyfikaty i standardy | Dla producenta sprzętu:   * ISO 9001 lub równoważny; * ISO 14001 lub równoważny; * ISO 50001 lub równoważny;   Dla komputera:   * Deklaracja zgodności CE lub równoważna; * TUV Rheinland Low Blue Light lub równoważna; * TUV Rheinland Flicker Free lub równoważna; * MIL-STD-810H lub równoważna; |
|  | Bezpieczeństwo | * Złącze typu Kensington Lock; * Moduł TPM 2.0 z certyfikacją TCG; * Czujnik otwarcia obudowy; |
|  | Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji. |
|  | Oprogramowanie | Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczną weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. |
|  | Gwarancja i wsparcie techniczne | Świadczona w miejscu użytkowania sprzętu (on-site). Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej:   * fabrycznej konfiguracji urządzenia, * rodzaju gwarancji, * dacie wygaśnięcia gwarancji, * aktualizacjach.   Zaawansowana diagnostyka urządzenia i oprogramowania dostępna na stronie producenta komputera. |
|  | Pakiet biurowy | Pakiet biurowy spełniający następujące wymagania techniczne:  Licencja wieczysta  Wymagania odnośnie interfejsu użytkownika:   * pełna polska wersja językowa interfejsu użytkownika, * prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych; * oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: * posiada kompletny i publicznie dostępny opis formatu, * w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy); * do aplikacji musi być dostępna pełna dokumentacja w języku polskim;   Pakiet zintegrowanych aplikacji biurowych musi zawierać:   * edytor tekstów, * arkusz kalkulacyjny, * narzędzie do przygotowywania i prowadzenia prezentacji, * narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),  1. Edytor tekstów musi umożliwiać:  * edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, * wstawianie oraz formatowanie tabel, * wstawianie oraz formatowanie obiektów graficznych, * wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), * automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, * automatyczne tworzenie spisów treści, * formatowanie nagłówków i stopek stron, * śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie, * nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, * określenie układu strony (pionowa/pozioma), * wydruk dokumentów, * wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, * zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, * wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem,  1. Arkusz kalkulacyjny musi umożliwiać:  * tworzenie raportów tabelarycznych, * tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, * tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, * tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, WebService), * obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych, * tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, * wyszukiwanie i zamianę danych, * wykonywanie analiz danych przy użyciu formatowania warunkowego, * nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, * nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, * formatowanie czasu, daty i wartości finansowych z polskim formatem, * zapis wielu arkuszy kalkulacyjnych w jednym pliku, * zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013, 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, * zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji;  1. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:  * przygotowywanie prezentacji multimedialnych, * prezentowanie przy użyciu projektora multimedialnego, * drukowanie w formacie umożliwiającym robienie notatek, * zapisanie jako prezentacja tylko do odczytu, * nagrywanie narracji i dołączanie jej do prezentacji, * opatrywanie slajdów notatkami dla prezentera, * umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, * umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, * odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, j) możliwość tworzenia animacji obiektów i całych slajdów, * prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, * pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, 2010 i 2013, 2016;  1. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:  * pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, * przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, * filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, * tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, * automatyczne grupowanie poczty o tym samym tytule, * tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, |
|  | Program antywirusowy | **Administracja zdalna w chmurze**   1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.   **Ochrona stacji roboczych**   1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:     * tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,     * tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,     * tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,     * tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,     * tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.   **Ochrona serwera**   1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.   Dodatkowe wymagania dla ochrony serwerów Windows:   1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.   Dodatkowe wymagania dla ochrony serwerów Linux:   1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.   **Ochrona urządzeń mobilnych opartych o system Android**   1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:    * usunięcie zawartości urządzenia,    * przywrócenie urządzenie do ustawień fabrycznych,    * zablokowania urządzenia,    * uruchomienie sygnału dźwiękowego,    * lokalizację GPS. 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:    * nazwę aplikacji,    * nazwę pakietu,    * kategorię sklepu Google Play,    * uprawnienia aplikacji,    * pochodzenie aplikacji z nieznanego źródła. |

## Laptop – szt.20

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa komponentu | Wymagane minimalne parametry techniczne komputerów |
|  | Typ | Komputer przenośny. |
|  | Procesor | Procesor ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, o wydajności liczonej w punktach równej minimum 17000 na podstawie wyników Passmark CPU Mark z dnia XYZ opublikowanych na stronie <http://www.cpubenchmark.net/> . Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. |
|  | Pamięć operacyjna RAM | Min. 16GB DDR5 pracującej w trybie dual channel.  Możliwość rozbudowy pamięci do min. 64GB. |
|  | Parametry pamięci masowej | M.2 512 GB SSD PCIe 4.0 x4 NVMe.  Przygotowana, wolna zatoka do rozbudowy komputera o dodatkowy dysk SSD. |
|  | Karta graficzna | Zintegrowana karta graficzna z procesorem. |
|  | Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki stereo 2x2W, port słuchawek i mikrofonu typu COMBO, kamera video 1080p z mechaniczną zasłoną obiektywu oraz obsługująca logowanie za pomocą danych biometrycznych z obsługą między Windows Hello, dwa mikrofony z funkcją wygłuszania niechcianych odgłosów tła, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute). |
|  | Obudowa | Wykonana z metali lekkich lub kompozytów (np. aluminium, duraluminium, włókno węglowe, włókno szklane, PC-ABS) charakteryzujących się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych. Obudowa o podwyższonej odporności spełniająca normy MIL-STD-810H lub równoważne. |
|  | Płyta główna | Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny urządzenia. |
|  | Bezpieczeństwo | Moduł fTPM 2.0 lub dTPM 2.0.  Slot typu Kensington. Komputery wyposażone w złącze Noble Lock muszą zostać zaoferowane z adapterem ze złącza Noble Lock komputera do Kensington.  Dysk systemowy zawierający partycję recovery umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
|  | Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji). |
|  | BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:   * wersji BIOS, * nr seryjnym komputera, * typie procesora, * ilości pamięci RAM.   Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:   * Możliwość ustawienia hasła administratora; * Możliwość ustawienia hasła dysku twardego; * Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS; * Możliwość włączenia/wyłączenia bootowania z USB oraz PXE; * Możliwość Wyłączania/Włączania: karty sieciowej, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, USB; |
|  | Bezpieczeństwo – System Diagonstyczny | Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia błędów zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. Działający nawet w przypadku uszkodzenia dysku twardego. System obsługiwany za pomocą myszy lub klawiatury, umożliwiający wykonanie minimum następujących czynności diagnostycznych:  1. Wykonanie testu komponentów w zakresie przyspieszonym lub rozszerzonym z możliwością wyboru algorytmów testowania oraz liczby cykli testowych do przeprowadzenia. System diagnostyczny powinien umożliwiać wykonanie testu następujących komponentów:   * pamięci ram, * procesora, * pamięci masowej, * płyty głównej.   2. Identyfikację jednostki i jej komponentów w następującym zakresie:   * urządzenie (producent, model, numer seryjny), * bios (producent, wersja oraz data wydania), * procesor (nazwa, taktowanie, ilości pamięci cache), * pamięć ram (ilość zainstalowanej pamięci ram, producent), * dysk twardy (producent, model, numer seryjny, pojemność). |
|  | Ekran | Matowy, matryca IPS min. 14” max. 16” 16:10 z podświetleniem w technologii LED, rozdzielczość min. WUXGA 1920x1200, jasność min. 300 nits, kąt otwarcia pokrywy ekranu min. 180 stopni. |
|  | Interfejsy / Komunikacja | - 2x USB 3.2 typu A;  - 1x ThunderBolt 4;  - 1x USB 3.2 typu C;  - 1x HDMI;  - 1x złącze audio combo;  - 1x RJ-45;  - 1x czytnik kart SD wbudowany lub w formie przejściówki USB;  Nie dopuszcza się osiągnięcia wymaganych portów USB poprzez zastosowanie przejściówek. |
|  | Karta sieciowa WLAN | Wbudowana karta sieciowa, pracująca w standardzie min. Wi-Fi 6E 11ax.  Bluetooth min. 5.3. |
|  | Klawiatura | Klawiatura odporna na zalanie cieczą, układ US, wyposażona w min. 2 tryby podświetlania przycisków (włączone, wyłączone). |
|  | Czytnik linii papilarnych | Czytnik linii papilarnych wbudowany w klawiaturę lub przycisk zasilania. Przycisk zasilania znajdujący się poza obrysem klawiatury, celem uniknięcia przypadkowego naciśnięcia. Nie dopuszcza się umiejscowienia przycisku włączania np. w górnym rzędzie klawiatury. |
|  | Akumulator | O pojemności min. 45Wh. |
|  | Zasilacz | Zasilacz zewnętrzny USB-C min. 65W. |
|  | Certyfikaty, oświadczenia i standardy | Dla producenta sprzętu należy dostarczyć certyfikat:  - ISO 9001 lub równoważny;  - ISO 14001 lub równoważny;  - ISO 50001 lub równoważny;  Dla komputera: - Deklaracja zgodności CE lub równoważna; |
|  | Waga | Waga startowa urządzenia nie większa niż 1.75kg według karty katalogowej producenta. |
|  | System operacyjny | System operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych.  2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego.  3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim.  4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.  5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe.  6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.  7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.  8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.  9. Wbudowany system pomocy w języku polskim.  10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).  11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.  12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.  13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.  14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.  15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.  16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".  17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.  18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.  19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.  20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.  21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.  22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.  23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."  24. Wbudowany mechanizm wirtualizacji typu hypervisor."  25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.  26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.  27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.  28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).  29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.  30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.  31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.  32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM.  33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.  34. Możliwość tworzenia wirtualnych kart inteligentnych.  35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu  (Secure Boot).  36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.  37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.  38. Mechanizmy logowania w oparciu o:  a. Login i hasło,  b. Karty inteligentne i certyfikaty (smartcard),  c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  d. Certyfikat/Klucz i PIN,  e. Certyfikat/Klucz i uwierzytelnienie biometryczne.  39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5  40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.  41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń.  43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń. |
|  | Oprogramowanie do aktualizacji sterowników | Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczną weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralną bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. |
|  | Gwarancja i wsparcie techniczne | Gwarancji świadczonej w miejscu użytkowania (on-site).  Bezpłatna infolinia w języku polskim, funkcjonująca minimum w godzinach 9:00 – 16:00 oraz obsługująca zgłoszenia serwisowe i oferująca wsparcie techniczne w zakresie co najmniej:  - wsparcia technicznego dla zakupionego sprzętu,  - weryfikacji konfiguracji fabrycznej zakupionego sprzętu,  - weryfikacji statusu gwarancji zakupionego sprzętu.  Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej:  - fabrycznej konfiguracji urządzenia,  - rodzaju gwarancji,  - dacie wygaśnięcia gwarancji,  - aktualizacjach.  Diagnostyka sprzętowa dostępna na stronie internetowej producenta |
|  | Pakiet biurowy | Pakiet biurowy spełniający następujące wymagania techniczne:   * Licencja wieczysta; * Wymagania odnośnie interfejsu użytkownika: * pełna polska wersja językowa interfejsu użytkownika, * prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych; * oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: * posiada kompletny i publicznie dostępny opis formatu, * w skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy); * do aplikacji musi być dostępna pełna dokumentacja w języku polskim;   Pakiet zintegrowanych aplikacji biurowych musi zawierać:   * edytor tekstów, * arkusz kalkulacyjny, * narzędzie do przygotowywania i prowadzenia prezentacji, * narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),   + - 1. Edytor tekstów musi umożliwiać: * edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, * wstawianie oraz formatowanie tabel, * wstawianie oraz formatowanie obiektów graficznych, * wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), * automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, * automatyczne tworzenie spisów treści, * formatowanie nagłówków i stopek stron, * śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie, * nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, * określenie układu strony (pionowa/pozioma), * wydruk dokumentów, * wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, * zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, * wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem,   + - 1. Arkusz kalkulacyjny musi umożliwiać: * tworzenie raportów tabelarycznych, * tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, * tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, * tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, WebService), * obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych, * tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, * wyszukiwanie i zamianę danych, * wykonywanie analiz danych przy użyciu formatowania warunkowego, * nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, * nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, * formatowanie czasu, daty i wartości finansowych z polskim formatem, * zapis wielu arkuszy kalkulacyjnych w jednym pliku, * zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010 i 2013, 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, * zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji;   + - 1. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: * przygotowywanie prezentacji multimedialnych, * prezentowanie przy użyciu projektora multimedialnego, * drukowanie w formacie umożliwiającym robienie notatek, * zapisanie jako prezentacja tylko do odczytu, * nagrywanie narracji i dołączanie jej do prezentacji, * opatrywanie slajdów notatkami dla prezentera, * umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, * umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, * odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, j) możliwość tworzenia animacji obiektów i całych slajdów, * prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, * pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, 2010 i 2013, 2016;   + - 1. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: * pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, * przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, * filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, * tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, * automatyczne grupowanie poczty o tym samym tytule, * tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, |
|  | Program antywirusowy | **Administracja zdalna w chmurze**   1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.   **Ochrona stacji roboczych**   1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:     * tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,     * tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,     * tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,     * tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,     * tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.   **Ochrona serwera**   1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.   Dodatkowe wymagania dla ochrony serwerów Windows:   1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.   Dodatkowe wymagania dla ochrony serwerów Linux:   1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.   **Ochrona urządzeń mobilnych opartych o system Android**   1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:    * usunięcie zawartości urządzenia,    * przywrócenie urządzenie do ustawień fabrycznych,    * zablokowania urządzenia,    * uruchomienie sygnału dźwiękowego,    * lokalizację GPS. 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:    * nazwę aplikacji,    * nazwę pakietu,    * kategorię sklepu Google Play,    * uprawnienia aplikacji,    * pochodzenie aplikacji z nieznanego źródła. |

## Centralny UPS – szt.1

|  |  |  |
| --- | --- | --- |
| Lp. | Opis wymagań techniczno-funkcjonalnych | Wartość minimalna |
|  | Technologia | VFI (true on-line, podwójne przetwarzanie energii) |
|  | Budowa | Beztransformatorowa, prostownik IGBT.  UPS musi być wyposażony w podwójny tor zasilający niezależny dla prostownika i Bypassu. |
|  | Moc znamionowa | 30 kVA / 30kW |
|  | Wyjściowy współczynnik mocy (PF) | 1,0 |
|  | Współczynnik mocy wejściowej 0.99. | 0,99 |
|  | Napięcie wejściowe trójfazowe | 400 VAC 3F + N |
|  | Tolerancja napięcia wejściowego przy obciążeniu 100%; bez przechodzenia na baterie | 172 – 287 Vac (L-N) |
|  | Zakres częstotliwości wejściowej | Wymagana 40-70 Hz |
|  | Sprawność AC-AC w trybie pracy  on-line z obciążeniem 100% | nie mniejsza niż 96% |
|  | Tryb pracy ECO mode, zapewniający podwyższoną sprawność zasilacza | Wymagany |
|  | Możliwość rozbudowy mocy w  okresie eksploatacji | Do minimum 8 sztuk w układzie pracy równoległej |
|  | Montażu modułu pracy równoległej w oferowanej jednostce | Wymagane – pozwala na dołączenie kolejnej jednostki. |
|  | Napięcie wyjściowe trójfazowe | 400 VAC 3F + N |
|  | Częstotliwość wyjściowa | 50/60Hz (programowalna) |
|  | Zintegrowane bezprzerwowe  przełączniki obejściowe (by-pass) | Statyczny przełącznik (SCR) oraz  ręczny rozłącznik serwisowy |
|  | Zewnętrzny bezprzerwowy Bypass serwisowy | Wymagany Bypass bezprzerwowy w postaci jednego przełącznika, z informacją o położeniu dla zabezpieczenia falownika UPS przed uszkodzeniem w przypadku nieprawidłowego użycia. |
|  | Wejście komunikacyjne na UPS do podłączenia sygnalizacji położenia przełącznika zewnętrznego Bypassu serwisowego, dla ochrony falownika UPS przed przypadkowym przełączeniem | Wymagane |
|  | Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie  chroniące baterie przed głębokim rozładowaniem. | Wymagane, wraz z funkcją restingu baterii |
|  | Możliwość regulacji prądu ładowania baterii z poziomu panelu LCD w UPS-ie. | Wymagane – podać maksymalną wartość prądu ładowania baterii |
|  | Czas podtrzymania | 6 minut przy obciążeniu 30kW |
|  | Minimalna pojemność zainstalowanych akumulatorów liczona jako: Ilosc akumulatorów \* pojemność pojedynczego akumulatora \* napięcie pojedynczego akumulatora [V\*Ah] | 8 640 Ah\*V |
|  | Moduł baterii | Baterie muszą być umieszczone w obudowie UPS. Należy stosować baterie szczelne AGM VRLA o żywotności 10-12 lat. Każdy łańcuch baterii zabezpieczony niezależnym rozłącznikiem bezpiecznikowym. |
|  | Autonomia pracy zasilacza UPS przy pracy z baterii podawana w minutach na panelu LCD zasilacza | Wymagane |
|  | W przypadku uszkodzenia pojedynczych  akumulatorów w stosie, wymagana  poprawna praca urządzenia ze zmniejszonym łańcuchem baterii | Wymagane, poprzez konfigurację, zmianę długości łańcucha baterii 30-40 sztuk |
|  | Stabilizacja napięcia wyjściowego w  stanie ustalonym | ± 1% |
|  | Stabilizacja napięcia wyjściowego w stanie nieustalonym | ± 3% |
|  | Stabilność częstotliwości  wyjściowej: | bez synchronizacji: ± 0,05 Hz |
|  | Współczynnik szczytu | 3:1 |
|  | Minimalne przeciążenie falownika w trybie pracy normalnej | 115% przez 60 minut  130% przez 10 minut  150% przez 1 minutę  >150% - 0,2 sek |
|  | Panel sterujący z wyświetlaczem dotykowym oraz sygnalizacją diodową i akustyczną | Wymagane |
|  | Złącze interfejsów | SNMP, Dry Contact In/OUT, Modbus RTU, RS485 |
|  | Karta sieciowa SNMP wbudowana w UPS. | Wymagane |
|  | Interfejs EPO (do wyłącznika ppoż.) | Wymagane – zestyk NO oraz NC. UPS zintegrowany z systemem ppoż budynku. |
|  | Diagnostyka parametrów urządzenia  UPS i baterii | Automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-a i z wykorzystaniem oprogramowania do zarządzania i monitorowania UPS |
|  | Dedykowane oprogramowanie do wysyłania SMS | Wymagane |
|  | Poziom hałasu w odległości 1m | < 50 dBA |
|  | Rejestr zdarzeń | Dziennik zdarzeń w UPS-ie + komunikaty serwisowe |
|  | Możliwość regulacji z panelu sterującego tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu | Wymagane |
|  | Monitorowanie stanu baterii i czasu autonomii | Stan baterii + dostępna autonomia mierzona w czasie rzeczywistym |
|  | UPS wyposażony w dotykowy, kolorowy wyświetlacz zabezpieczony hasłem przed ingerencją osób postronnych | Wymagane |
|  | UPS wyposażony w programowany tryb pracy ECO mode o podwyższonej sprawności z możliwością zaprogramowania dni tygodnia oraz godzin w jakich UPS przechodzi automatycznie w tryb oszczędnej pracy o podwyższonej sprawności. | Wymagane |
|  | UPS wyposażony w funkcję automatycznego czyszczenia z możliwością zaplanowania okresowego samoczynnego załączenia się tej funkcji. | Wymagane |
|  | UPS wyposażony w zdalny wyłącznik REPO | Wymagane – dostawa po stronie dostawcy UPS. |
|  | Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa ,kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE | Wymagane zarówno dla zasilacza UPS jak i baterii |
|  | Producent zasilacza UPS z siedzibą w Polsce, posiadający biuro dystrybucji i serwisu na terenie kraju. | Wymagane |
|  | Rozłączniki manewrowe | Zasilacz UPS powinien być wyposażony w komplet rozłączników pozwalających na bezpieczne włączenie i wyłączenie UPS-a. Wymaga się co najmniej czterech rozłączników zamontowanych na UPS: zasilanie prostownika, zasilanie bypass, bypass serwisowy, rozłącznik wyjściowy z UPS. |
|  | Podłączenie zasilania i odbiorów | Podłączenie okablowania z tyłu zasilacza, z możliwością podłączenia dwóch oddzielnych torów do zasilania prostownika i bypassu wewnętrznego. |
|  | UPS powinien posiadać funkcję umożliwiającą samo dociążenie bez podłączania dodatkowych odbiorników w celu przetestowania podzespołów pod pełnym obciążeniem w trakcie każdej wizyty serwisu. | Wymagane |
|  | Zasilacz wyposażony w kółka transportowe pozwalające na łatwe przemieszczanie w czasie konserwacji | Wymagane |
|  | Wymiary UPS nie większe niż (S x G x W) | 300 x 850 x 1250 mm (+/-5%) |
|  | Instrukcja w języku polskim | Wymagane |

## Agregat – szt.1

|  |
| --- |
| 1. Moc wg PN-ISO 8528 lub równoważnej (+/-5%): PRP min. 60 kVA / 48 kW  LPT (SB) min. 70 kVA / 56 kW 2. Napięcie nominalne: 3x 400 VAC / 50 Hz 3. Prędkość obrotowa: 1500 obr/min 4. Klasa regulacji (ISO 8528-5) lub równoważna: G2 5. Regulator silnika: elektroniczny 6. Agregat obudowany i wyciszony o głośności nie większej niż 70 dB z 7 metrów 7. Obudowa wykonana z profili stalowych, ocynkowanych, malowanych proszkowo 8. Maksymalne wymiary obudowy nie większe niż 2500 x 1000 x 1700 mm (D x S x W) 9. Zbiornik paliwa – min. 100l. 10. Drzwi serwisowe po obu stronach obudowy + 1 drzwi do panelu sterowania 11. Dostęp do chłodnicy poprzez przy pomocy zdejmowanego panelu 12. Spawana, stalowa rama agregatu wyposażona w zbiornik paliwa na 12 godzin pracy z pełnym obciążeniem 100% PRP 13. Zamki i okucia obudowy wykonane ze stali nierdzewnej 14. Dwa wskaźniki poziomu paliwa: - analogowy, widoczny na zewnątrz obudowy, - cyfrowy na panelu sterowania z możliwością wyprowadzenia zdalnego odczytu 15. Wlew paliwa na obudowie, zabezpieczony na klucz 16. Możliwość dotankowania podczas pracy agregatu 17. Agregat wyposażony w układ podgrzewania cieczy chłodzącej umożliwiający start zespołu w niskich temperaturach. Układ podgrzewania musi posiadać termostat umożliwiający regulację zadanej temperatury 18. Tłumiki wibroizolacyjne pomiędzy ramą, a zespołem silnikiem i prądnicą 19. Tłumik wydechu 20. Agregat z bieżącej produkcji, nowy 21. Pompa do spuszczania oleju silnikowego 22. Spalanie silnika Diesla nieprzekraczające 17 l/h przy 100% obciążenia PRP 23. Zalecane przez producenta silnika przeglądy nie częściej niż co 500 motogodzin. 24. Konstrukcja prądnicy: synchroniczna, samowzbudna, samoregulująca, bez-szczotkowa, jednołożyskowa 25. Sprawność prądnicy przy 100% PRP min 88,5 % 26. Panelu automatyki wyposażony w sterownik mikroprocesorowy z cyfrowym wyświetlacz LCD oraz diody sygnalizujące tryb pracy agregatu oraz sieci 27. Panel automatyki posiadający minimum 7 wejść binarnych, 7 wyjść binarnych, 3 wejścia analogowe 28. Panel sterowania przygotowany do pracy w trybach: ręcznym, automatycznym i testowym. 29. Możliwość zastosowania komunikacji zdalnej SNMP oraz MODBUS RTU 30. Wejście do podania sygnału startu i stopu z zewnętrznego układu SZR 31. Możliwość sterowania zewnętrznym układem SZR 32. Menu sterownika w języku polskim 33. Historia zdarzeń sterownika min. 100 wpisów 34. Agregat wyposażony w wyłącznik 3-biegunowy |

## System do transmisji obrad Rady Gminy – sprzęt – 1 kpl.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Zestaw sprzętowy dla 19 osób (15 radnych w tym Przewodniczący, Wójt, Sekretarz, Skarbnik, pracownik obsługi)  System transmisji z obrad (2 kamery, komputer do transmisji, monitor, montaż po stronie Wykonawcy)   1. Kamera do transmisji IP – 2 sztuki    1. Praca w standardzie TCP/IP,    2. przetwornik 1/2.8” STARVIS,    3. obiektyw w zakresie 5-80 mm,    4. zoom optyczny 16x,    5. protokoły sieciowe: IPv4, SSL, RTSP, DHCP, UPnP,    6. zasilenie PoE    7. ONVIF. 2. Centrala system konferencyjnego – 1 szt.    1. Jednostka sterująca systemu konferencyjnego.       1. Funkcjonalność i parametry techniczne:          1. Kontrola otwartych mikrofonów pozwalająca wybrać minimum 4 otwarte mikrofony          2. Wbudowany rejestrator dźwięku może nagrywać dyskusję w formacie MP3 do pamięci wewnętrznej lub pamięci USB          3. Napięcie zasilania sieciowego od 100 do 240 VAC ± 10%          4. Maks. od 1,6 A (100 VAC) do 0,7 A (240 VAC)          5. Liczba pulpitów dyskusyjnych na jednostkę sterującą minimum 40          6. Minimalna częstotliwość próbkowania 44,1 kHz          7. Maksymalna waga 3.4 kg          8. Materiał metal lakierowany          9. Metoda montażu stołowy lub w szafie typu Rack 19”          10. Wymiary maksymalne (wys. X szer. X gł.) 45 x 483 x 300          11. Temperatura pracy od 5 do 45°C          12. Złącza umieszczone na obudowie:              1. Z przodu jednostki:   Minimum 1 x złącze USB   * + - 1. Z tyłu jednostki:          1. Minimum 1 x wyjście analogowe          2. Minimum 1 x wejście analogowe          3. Minimum 1 x złącze Ethernet RJ45 do komunikacji       2. Kontrola dyskusji odbywa się poprzez wybór jednego z dostępnych trybów dyskusji:          1. Tryb otwarty - uczestnicy mogą mówić, naciskając przycisk na swoim mikrofonie. Gdy maksymalna liczba otwartych mikrofonów zostanie osiągnięta, następny uczestnik, który naciśnie przycisk swojego mikrofonu, zostanie dodany do listy oczekujących. Pierwszy uczestnik z listy oczekujących będzie mógł mówić, gdy zostanie wyłączony któryś z aktywnych mikrofonów          2. Tryb z wyciszaniem - uczestnicy mogą wyciszać się wzajemnie przez włączanie swojego mikrofonu. Gdy maksymalna liczba otwartych mikrofonów zostanie osiągnięta, następny uczestnik, który naciśnie przycisk na swoim mikrofonie, zdezaktywuje mikrofon, który był najdłużej aktywny (mikrofon, który posiada przewodniczący nie jest uwzględniany w liczbie otwartych mikrofonów i dlatego nie może go wyciszyć żaden inny uczestnik).          3. Tryb aktywacji głosowej - uczestnicy mogą aktywować swoje mikrofony, mówiąc do nich. Mikrofon może być czasowo wyciszony poprzez naciśnięcie i przytrzymanie przycisku mikrofonu.  1. Zestaw mikrofonowy – 1 szt.   **Minimalne parametry techniczne**   |  |  | | --- | --- | | **Nazwa** | Parametr | | Typ urządzenia | zestaw mikrofonu bezprzewodowego | | Częstotliwość nośna | 672- 692 MHz | | Pasmo przenoszenia | 50- 18 000 Hz | | Kanały wejściowe | 1 | | THD | < 0.5 % | | Dynamika | 120 dB | | Stosunek S/ N RF | 105 dB | | Dopuszcz. temp. otoczenia | 0- 40 °C | | Moc nadajnika | < 25 mW/ 2.5 mW (EIRP) | | Zasięg | ≈ 50 m | | Nadajnik, zasilanie | 2 x 1.5 V bateria AA | | Nadajnik, głębokość | 52 mm | | Nadajnik, wysokość | 52 mm | | Nadajnik, głębokość | 275 mm | | Nadajnik, waga | 235 g | | Odbiornik, wyjścia audio | 350 mV/ 10 kΩ (6.3 mm) 25 mV/ 10 kΩ (XLR, sym.) | | Odbiornik, zasilanie | z doł. zasilacza | | Odbiornik, szerokość | 152 mm | | Odbiornik, wysokość | 38 mm | | Odbiornik, głębokość | 120 mm | | Odbiornik, waga | 482 g | | Odbiornik, złącza | 1 x 6.3 mm, niesym. 1 x XLR, sym. |  1. Mikrofon konferencyjny bezprzewodowy – 19 szt./Jednostki konferencyjne (pulpity dyskusyjne) –    1. Szyjka mikrofonu o długości minimum 480 mm oraz minimum jednym przegubie.    2. Przycisk aktywacji mikrofonu musi umożliwiać uczestnikowi włączanie/wyłączanie mikrofonu lub (w zależności od trybu aktywacji mikrofonu) zgłoszenie chęci wypowiedzi. Wokół, nad lub od spodu przycisku musi znajdować się podświetlany wskaźnik LED informujący o aktywnym mikrofonie (preferowany kolor czerwony).    3. Wbudowane 3,5 mm stereofoniczne gniazdo słuchawkowe    4. Odporność na zakłócenia z sieci GSM    5. Sygnalizacja świetlna umieszczona na szyjce mikrofonowej wskazująca włączenie i żądanie zabrania głosu (np. pierścień lub wskaźniki LED w dwóch kolorach – preferowany zielony oraz czerwony)    6. Szeregowa topologia połączeń, każdy z pulpitów musi posiadać gniazdo przelotowe.    7. Wbudowany wysokiej jakości głośnik    8. Możliwość konfiguracji dowolnego pulpitu jako jednostki przewodniczącego lub dostarczenie pulpitu dedykowanego dla przewodniczącego.    9. Pasmo przenoszenia urządzenia obejmuje zakres częstotliwości od 200 Hz do 12,5 kHz    10. Impedancja obciążenia słuchawek > 8 Ω < 1 k Ω    11. Maksymalne wymiary urządzenia bez mikrofonu (wys. X szer. X gł.) 65 x 210 x 150 mm    12. Ciężar ok. 1 kg    13. Materiał plastik, metal    14. Temperatura pracy od 0 do 35°C |

## Szkolenia TiK typ I – 120 godzin

**Wymagania minimalne dla szkoleń TIK typ I**

|  |
| --- |
| Szkolenia/Asysta stanowiskowa ma obejmować 120 godzin szkoleniowych w ujęciu max. 8 godzin na jeden dzień. Całość powinna się zamknąć w okresie 15 dni i ma dotyczyć autorskiego rozwiązania zrealizowanego w ramach podmiotowego wdrożenia.  Asysta musi zostać podzielona na bloki dziedzinowe:   * Blok pierwszy (10 dni – 80 godzin) musi zostać przeprowadzony w centrum kompetencyjnym (poza terenem Zamawiającego) i mieć na celu zapoznanie uczestników z elementami technologicznymi, które składają się na całość autorskiego rozwiązania. * Blok drugi (5 dni – 40 godziny) musi zostać przeprowadzony w miejscu instalacji (Urzędzie Gminy) i musi ściśle dotyczyć podstawowych procedur administracyjnych, które są typowe dla codziennej pracy administratora celem zapewnienia poprawnej pracy rozwiązania sprzętowego jako platformy teleinformatycznej na potrzeby rozwiązania związanego z oprogramowaniem systemu.   Zakres asysty stanowiskowej:   * Architektura serwerowa; * Architektura macierzowa; * Architektura sieci LAN; * System wirtualizacji danych; * System backupu i replikacji danych; * Administrowania i obsługi systemu operacyjnego (domena, usługa katalogowa) z zakresu zaoferowanego rozwiązania – oprogramowanie domenowe. * Punkt styku z Internetem – firewall.   Asysta musi być warunkiem dopuszczający do przekazania rozwiązania technicznego do wykorzystania produkcyjnego.  Asysta stanowiskowa musi zostać odebrana i zatwierdzona protokołem odbioru sygnowanym przez obie strony projektu tj. wykonawcę oraz użytkownika końcowego. |

## Opracowanie procedur bezpieczeństwa informacji i przetwarzania danych

W ramach realizacji przedmiotu zamówienia Wykonawca dostarczy oraz wdroży Kompleksowy System Zarządzania Bezpieczeństwem Informacji (KSZBI). Usługa obejmuje analizę, projektowanie, implementację i szkolenie związane z wdrożeniem SZBI w jednostce. Celem usługi jest zwiększenie ochrony danych i informacji w organizacji na poziomie technicznym oraz organizacyjnym, zapewnienie zgodności z obowiązującymi przepisami prawnymi, poprawa ogólnego poziomu bezpieczeństwa informacji zgodnie z normami wyrażonymi w PN ISO/IEC 27001 lub równoważnymi w załączeniu KSZBI zawierać będzie co najmniej:

Dokumentacja zarządzania systemem zarządzania bezpieczeństwem informacji (uwzględniająca poniższe zagadnienia):

– Zasady dotyczące korzystania z systemu zakres, zasoby, ciągłe doskonalenie;

– Procedury przeprowadzania audytów, zawierających wskazanie częstotliwości audytów, sposobu przygotowywania i zatwierdzania ich planów, sposobu ich przeprowadzania oraz dokumentowania i raportowania ich wyników.

– Procedury działań korygujących w przypadku niezgodności z wymaganiami systemu zarządzania.

– Procedury wprowadzania działań zapobiegawczych w przypadku wystąpienia sytuacji mogącej prowadzić do niezgodności z wymaganiami systemu zarządzania.

Dokumentacja dotycząca zabezpieczeń systemu zarządzania bezpieczeństwem informacji w obszarach (uwzględniająca poniższe zagadnienia):

* Zasady bezpiecznego przetwarzania informacji przez pracowników
* Zabezpieczenie stacji roboczych
* Zasady klasyfikacji informacji i postępowania z informacjami klasyfikowanymi
* Zasady zarządzania dostępem do informacji, w tym nadawania, modyfikacji, odbierania uprawnień oraz przeglądu uprawnień
* Zasady zarządzania dostępem do usług informatycznych, w tym usług sieciowych
* Zarządzanie mechanizmami uwierzytelniającymi, w tym hasłami
* Zasady publikacji informacji
* Zasady wymiany danych z podmiotami zewnętrznymi
* Zasady wewnętrznej wymiany danych
* Zasady postępowania z nośnikami informacji, w tym składowanie i wymiana nośników oraz niszczenie informacji zapisanych na nośnikach
* Zasady wprowadzania zmian w przetwarzaniu informacji, w szczególności z wykorzystaniem systemów informatycznych, z uwzględnieniem testowania bezpieczeństwa wprowadzanych rozwiązań
* Wytyczne w zakresie utrzymania dokumentacji zabezpieczeń i systemów informatycznych
* Zasady zgłaszania podatności w mechanizmach przetwarzających informacje
* Zasady postępowania w przypadku incydentu naruszenia bezpieczeństwa informacji
* Zasady kontroli bezpieczeństwa informacji.

Zamawiający wymaga by KSZBI zawierał:

* + 1. Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwanej „SZBI”), w skład której wchodzą następujące dokumenty:
  1. Polityka Bezpieczeństwa Informacji;
  2. Polityka ochrony danych osobowych;
  3. Instrukcja zarządzania systemem informatycznym;
  4. Polityka zarządzania ciągłością działania;
  5. Procedura zarządzania incydentami cyberbezpieczeństwa
  6. Analiza ryzyka w zakresie Bezpieczeństwa Informacji;
     1. W ramach dokumentacji SZBI ujęte zostaną następujące procedury:
        1. procedury korzystania z urządzeń mobilnych
        2. procedury pracy zdalnej
        3. postępowanie z nośnikami
        4. procedury kontroli dostępu
        5. zabezpieczenie pomieszczeń i obiektów
        6. procedury czystego biurka
        7. procedury czystego ekranu
        8. procedury kopii zapasowych
        9. procedury ochrony logów
        10. bezpieczeństwo komunikacji
        11. zarządzanie bezpieczeństwem sieci
        12. przesyłanie informacji
        13. plany ciągłości działania
        14. procedury zarządzania incydentami
        15. prywatność i ochrona danych osobowych
        16. szacowanie ryzyka w obszarze bezpieczeństwa informacji.

Szczegółowa zawartość dokumentacji zostanie określona w zależności od stanu faktycznego odpowiadającego strukturze i zasobom Zleceniodawcy w oparciu o wzajemne ustalenia dokonane we współpracy pomiędzy Stronami oraz wszelkich innych informacji uzyskanych w trakcie realizacji Umowy mogących mieć wpływ na treść dokumentacji. Doradztwo dotyczące czynności wdrażających dokumentację nastąpi po przekazaniu Zleceniodawcy przez Zleceniobiorcę całości dokumentacji KSZBI.

## Instalacja i konfiguracja (Platforma sprzętowa) – 250 RBH

|  |  |  |
| --- | --- | --- |
| Usługi informatyczne w zakresie wdrożenia, konserwacji  i serwisu sprzętu informatycznego oraz oprogramowania. | | |
|  | Usługi | Celem prac jest przygotowanie środowiska teleinformatycznego – platformy sprzętowej, na potrzeby realizacji elementów Zintegrowanego Systemu Informatycznego i cyberbezpieczeństwa, dla świadczonych e-usług. Zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie.  Część sprzętowa powinna zostać oparta na rozbudowie istniejącego systemie wirtualizacji i backupu zasobów IT.  Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania wdrożenia, migracji do nowego środowiska itp. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa i wymagań Zamawiającego.  Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia. |
|  | Montaż i fizyczne uruchomienie systemu | Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach, co najmniej w zakresie:   1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach RACK w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji. 2. Rozbudowa istniejących zasobów sprzętowych. 3. Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego. 4. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń. 5. Podłączenie całości rozwiązania do infrastruktury Zamawiającego. 6. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu. 7. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów. 8. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym). 9. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające). 10. Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ miedzy innymi celem:     1. Stworzenia połączeń sieci LAN pomiędzy przełącznikami.     2. Podłączenia urządzeń serwerowo-macierzowych (serwery, macierze) do przełączników sieci LAN.     3. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie, co najmniej n+1.     4. Połączenia musza wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami. |
|  | Instalacja i konfiguracja oprogramowania | 1. Instalacja i konfiguracja istniejącego oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji. Zamawiający posiada licencje jedną wolną licencję na wirtualizator firmy Vmware. 2. Instalacja i konfiguracja oprogramowania do systemu wykonywania backupu i archiwizacji danych działającego na serwerze backupu. 3. Instalacja oprogramowania systemu serwerowego wraz z niezbędnymi usługami oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Zamawiającego). 4. Instalacja i konfiguracja systemów operacyjnych dla serwerów wirtualnych. 5. Zarządzania infrastrukturą IT 6. Instalacja i konfiguracja oprogramowania do monitorowania i analizy cyberbezpieczeństwa (SIEM/SOAR). |
|  | Konfiguracja przełączników/sieci LAN: | Re/Konfiguracja przełączników w zakresie:   * 1. Przeprowadzenie audytu obecnej topologii oraz konfiguracji.   2. Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych, aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym).   3. Jeśli jest to konieczne – Zamawiający oczekuje rekonfiguracji adresacji IP w danych strefach (readresacja urządzeń, serwerów, komputerów leży po stronie Wykonawcy)   4. Zamawiający wymaga skonfigurowania polityk ruchu pomiędzy strefami na dostarczonych urządzeniach firewall - klaster.   5. Konfiguracja sieci VLAN na wszystkich przełącznikach – konfiguracja propagacji sieci VLAN.   6. Konfiguracja routingu pomiędzy sieciami VLAN na centralnym urządzeniu firewall - klaster;   7. Zamawiający wymaga aby wszystkie sieci VLAN (L2) zostały rozpięte na warstwie L2 na urządzeniu firewall – (połączenie TRUNK).   8. Testowanie obsługi ruchu sieciowego.   9. Testowanie skuteczności zabezpieczeń. |
|  | Konfiguracja elementów bezpieczeństwa sieciowego. | Konfiguracja/Modernizacja konfiguracji UTM dla nowych urządzeń w zakresie.   1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. 2. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta. 3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email) 4. Włączenie dostarczonego urządzenia do sieci LAN urzędu – stworzenie klastera HA. 5. Konfiguracja dostarczonych systemów Firewall:    1. Konfiguracja podstawowych parametrów    2. Konfiguracja translacji adresów NAT    3. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, macierze, itp.    4. Konfiguracja inspekcji określonych protokołów sieciowych;    5. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall;    6. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;    7. Testowanie działania bramy 6. Konfiguracja modułów należących do systemu wykrywania włamań IPS:    1. Konfiguracja podstawowych parametrów    2. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań;    3. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego;    4. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;    5. Testowanie działania ochrony IPS 7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL.    1. Przypisanie adresu IP do zarządzania.    2. Konfiguracja inspekcji protokołów HTTP, HTTPS; SMTP, FTP, POP3    3. Definicja reguł filtrowania/blokowania    4. Integracja z systemem domenowym w celu weryfikacji nawiązywania połączenia poprzez nazwę użytkownika z domeny. 8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej. 9. Konfiguracja uwierzytelniania w oparciu o dostarczony moduł uwierzytelnienia. 10. Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla: dedykowanych, stworzonych na przelaniach sieci VLAN. 11. W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (moduł uwierzytelnienia), nie zaś o adresy IP, czy MAC 12. W każdej instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaże Zamawiający) dla każdej z poniższych funkcjonalności:     1. kontrola dostępu - zapora ogniowa klasy Stateful Inspection     2. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar     3. ochrona przed atakami - Intrusion Prevention System [IPS/IDS]     4. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.     5. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)     6. kontrola pasma oraz ruchu [QoS, Traffic shaping]     7. Kontrola aplikacji oraz rozpoznawanie ruchu P2P     8. Ochrona przed wyciekiem poufnej informacji (DLP)     9. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL)     10. Inspekcja ruchu SSL     11. Ochrony przez atakami na stacje klienckie     12. Kontrola pasma 13. Konfiguracja szyfrowanych tuneli VPN (IPSec) pomiędzy lokalizacjami zdalnymi. 14. Konfiguracja logowania i raportowania. |
|  | Serwer | Zamawiający wymaga instalacji i konfiguracji dostarczonego serwera celem stworzenia bazy sprzętowej repliki dla istniejącego klastra niezawodnościowego i wydajnościowego stworzonego na bazie istniejących serwerów i oprogramowania do wirtualizacji. |
|  | Backup | W ramach projektu przewiduje się wykorzystanie istniejącego serwera backupu (Fujitsu PY RX2540 M7) oraz NAS na miejsce przechowywanie backupu.  Na serwerze backupu należy zainstalować oprogramowanie do trzymania kopi zapasowych (Hardened repository), które jest wspierane przez zaoferowany system backupu. Zarządzanie środowiskiem backupem ma mieć miejsce z poziomu maszyny wirtualnej z jednego centralnego miejsca, tego samego jak dla serwerów wirtualizacyjnych.  System musi zostać podłączony do macierzy produkcyjnej, musie posiadać lokalne repozytoria danych na przestrzeni dyskowej, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na połowie zasobu dyskowego.  Dostarczony serwer ma zostać użyty do przechowywania repliki on-line maszyn wirtualnych na lokalna platformę wirtualizacyjną – odmiejscowiona lokalizacja.  Takie podejście ma gwarantować zabezpieczenie kluczowych węzłów sieciowych (serwerów wirtualnych) na dwa sposoby tj. plik off-line maszyny wirtualnej oraz kopia on-line replikowania asynchronicznie według harmonogramu.  Wykonywanie backupu musi być powiązane z procedurą sprawdzania poprawności jego wykonania oraz automatycznym raportowaniem do jednostki administracyjnej.  Oprogramowanie backupu musi obsługiwać również system NAS i chmurę, gdzie będzie można skorzystać z replikacji danych – przesłania backupu dyskowego na zasób zdalny.  Mechanizm podłączenia   1. Konfiguracja i podłączenie serwera backupu do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy. 2. Konfiguracja i podłączenie serwera backupu do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN. 3. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q. |
|  | Logiczny schemat rozbudowywanego systemu backup – stan docelowy. | |
|  | Macierz  dyskowa | Istniejąca macierz musi być wykorzystywana do gromadzenia i przechowywania „danych produkcyjnych” – wykorzystywanych przez oprogramowanie dostarczone w projekcie jak i już istniejące w tym oprogramowanie dziedzinowe.  Ilość i wielkość udziałów dyskowych udostępnionych dla serwerów np.: wirtualizacyjnych zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej. Macierz należy zintegrować z istniejącym rozwiązaniem firmy Fujitsu – model DX60S5. |
|  | UPS, Agregat. | W ramach niniejszego postępowania Zamawiający wymaga podłączenia, skonfigurowania i uruchomienia zaoferowanych urządzeń UPS i Agregat do sieci elektrycznej Urzędu celem zabezpieczenia pomieszczenia serwerowni. Wszystkie koszty z tym związane np.: modernizacji istniejącej instalacji elektrycznej muszą zostać przewidziane i uwzględnione w ofercie Wykonawcy. |
|  | Migracja danych | Dotyczy przeniesienia obecnie wykorzystywanych i rozbudowywanych systemów informatycznych na nowe dostarczone rozwiązanie sprzętowe z wykorzystaniem wirtualizacji zasobów.  Dane (systemy dziedzinowe) musza zostać przeniesione na nowe zasoby serwerowo-macierzowe. Zakres migracji zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej.  Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej min. w pełnym zakresie danych i rejestrów systemów dziedzinowych. |
|  | Rekonfiguracja środowiska wirtualizacyjnego. | Zamawiający wymaga rekonfiguracji środowiska wirtualizacyjnego, co najmniej w zakresie:   1. Aktywacja licencji oprogramowania wirtualizacyjnego na stronie producenta – jeżeli jest taka potrzeba. 2. Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 3. Przygotowanie macierzy do podłączenia do systemu wirtualizacji – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 4. Instalacja oprogramowania wirtualizacyjnego na dostarczonym serwerze. 5. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów. 6. Konfiguracja i podłączenie serwera wirtualizacyjnego do zasobu dyskowego. Zamawiający wymaga (jeżeli to możliwe) takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy. 7. Konfiguracja i podłączenie serwera wirtualizacyjnego do sieci LAN. Zamawiający wymaga, aby serwer wirtualizacyjny był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN. 8. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q. 9. Przygotowanie replikacji wirtualnych maszyn ze środowiska produkcyjnego do zapasowego. 10. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym – jeżeli jest wymagane.. 11. Konfiguracja klastra wysokiej dostępności:     1. Konfiguracja mechanizmów HA – w przypadku awarii węzła klastra wirtualne maszyny, które są na nim uruchomione muszą zostać przeniesione na sprawny węzeł klastra bez ingerencji użytkownika.     2. Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn.     3. Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera. 12. Weryfikacja działania klastra wysokiej dostępności. 13. Migracja istniejącej infrastruktury do środowiska wirtualnego. 14. Konfiguracja uprawnień w środowisku wirtualizacyjnym – integracja z usługą katalogową 15. Konfiguracja powiadomień o krytycznych zdarzeniach (email). |
|  | Rekonfiguracja systemu zarządzania kopiami zapasowymi. | 1. Instalacja i rekonfiguracja oprogramowania zarządzającego wykonywaniem kopii zapasowych na serwerze backupu (wgranie licencji). 2. Aktywacja oraz instalacja niezbędnych licencji. 3. Konfiguracja stacji zarządzającej. 4. Dołączenie klientów do system backupu. 5. Zdefiniowanie zadań backupu oraz przypisanie do nich harmonogramu automatycznego wykonywania:    1. kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące;    2. kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy;    3. kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu;    4. kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową;    5. musi istnieć możliwość odtworzenia:       1. całej wirtualnej maszyny;       2. dysku wirtualnej maszyny;       3. pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa); 6. Zdefiniowanie powiadomień o przebiegu zadania (Zamawiający wymaga skonfigurowania powiadomień na wskazany adres email zawierających, co najmniej:    1. Nazwę zadania backupu;    2. Status zakończenia zadania backupu /Powodzenie, niepowodzenie/;    3. Długość trwania zadania backupu;    4. Ilość zapisanych na taśmie danych. 7. Zdefiniowanie powiadomień na wskazany adres email o zdarzeniach:    1. Błąd urządzenia;    2. Uszkodzenie wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi;    3. Brak miejsca w wewnętrznej bazie danych systemu zarządzania kopiami zapasowymi;    4. Konieczność przeprowadzenia oczyszczania wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi;    5. Zdarzenia dotyczące licencji;    6. Zapełnienia mail-slotu. 8. Uruchomienie testowych zadań backupu. 9. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień email. 10. Uruchomienie testowych zadań odtworzenia danych. 11. Miejscem przechowywania kopii zapasowych jest:     1. serwer backupu.,     2. na etapie wdrożenia należy ustalić czasy RPO (okresu czasu przez jaki dane mogą być utracone w wyniku awarii) i RTO (okresu czasu w ciągu, którego system, który uległ awarii powinien zostać przewrócony) z Zamawiającym. 12. Do serwera backupu należy podłączyć istniejąca macierz, oraz system NAS.   System musi zostać podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na serwerze backupu. |
|  | Oprogramowanie do monitorowania i analizy cyberbezpieczeństwa (SIEM/SOAR) | 1. Proces wdrożenia systemu określony powinien zostać zrealizowany zgodnie z opisanymi niżej wytycznymi oraz zatwierdzonym harmonogramem, umożliwiając efektywne wdrożenie rozwiązania w okresie 3 miesięcy. 2. Proces wdrożeniowy podzielony zostanie na obszary: 3. Obszar Analizy, zakładający stworzenie elektronicznej dokumentacji organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji (budowa kontekstu organizacji). 4. Obszar Detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowania modułu SIEM. 5. Obszar Reakcji, zakładający podłączenie i konfigurację mechanizmów wspomagających proces automatyzacji reakcji na wykryte zdarzenia, incydenty bezpieczeństwa i podatności w ramach zainstalowania modułu SOAR. 6. Obszar Analizy ma na celu identyfikację potencjalnych cyber zagrożeń oraz możliwych konsekwencji, na jakie narażona jest organizacja. Zakres prac powinien uwzględniać kolejno: 7. Pracę z konsultantem (w zakresie m.in. wprowadzenia do metodyki, uzupełnienia ankiety przedwdrożeniowej oraz przygotowania i zatwierdzenia harmonogramu prac). 8. Uruchomienie systemu w infrastrukturze zamawiającego, w tym:  * konsultacje w przygotowaniu infrastruktury Zamawiającego do instalacji systemu, * przygotowanie przez Zamawiającego połączenia zdalnego, * instalację lub import maszyny wirtualnej typu „software appliance”, * aktywację licencji, * wstępną konfigurację, * import/wprowadzenie tabeli adresacji znaczących stref bezpieczeństwa, wymaganych przez mechanizmy wykrywania (np.: sieci serwerów, sieci DMZ, sieci LAN).  1. Podłączenie głównego źródła zdarzeń opisującego komunikację sieciową, w tym:  * przekierowanie logów opisujących transmisje sieciową (traffic) z zapór sieciowych (Firewall) na kolektor systemu, * uruchomienie reguł wykrywania.  1. Prace audytowe, w tym:  * pasywną analizę transmisji sieciowej:   + o ruch z/do serwerów webowych i aplikacyjnych,   + o ruch z/do serwerów baz danych,   + o ruch z/do serwerów pocztowych,   + o ruch z/do kontrolerów domenowych,   + o ruch z/do serwerów usług podstawowych (m.in. DNS/NTP),   + o ruch z/do zasobów zidentyfikowanych na bazie charakterystyki i wolumenu ruchu oraz możliwości identyfikacji aplikacji. * konsultacje w ramach otrzymanych wyników, * zebranie danych audytowych wymaganych do sporządzenia raportu.  1. Analizę podatności, w zakresie:  * integracji po API ze wskazanym przez zamawiającego komercyjnym skanerem/ skanerami podatności lub zainstalowanie skanera podatności typu open source, * przygotowanie reguł priorytetów i importu krytycznych podatności.  1. Przygotowanie dynamicznego raportu audytowego w oparciu o dostępne w systemie narzędzia elektronicznej dokumentacji i szacowania ryzyka obejmującego analizę prawdopodobieństwa przełamania zabezpieczeń organizacji. Raport powinien zawierać:  * zidentyfikowane zagrożenia oraz prawdopodobieństwo ich wystąpienia, * potencjalne wektory ataków dla wykrytych zagrożeń, * wizualizacja graficzna wykrytych źródeł zagrożeń oraz wektorów ataków, * rekomendacja zabezpieczeń, * zidentyfikowane zagrożenia związane z podatnościami oraz prawdopodobieństwo wykorzystania ich do przełamania zabezpieczeń.  1. Obszar Detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń. Zakres prac powinien uwzględniać kolejno: 2. Podłączenie (przekierowanie przez Zamawiającego do systemu) źródeł zdarzeń i ich dalszą konfigurację w systemie. Kluczowe źródła zdarzeń obejmują:  * zapory sieciowe w punkach styku z siecią Internet (Firewall brzegowy), * sieciowe systemy bezpieczeństwa dedykowane do wykrywania incydentów bezpieczeństwa (np.: Sandbox, IDP/IPS, AntySpam), * centralne systemy, dedykowane do kontroli złośliwego oprogramowania na stacjach końcowych/Serwerach, umożliwiające wykrywanie aktywności złośliwego oprogramowania (np.: AntyWirus, EDR), * kontroler domenowy oraz system zarządzania dostępem uprzywilejowanym, * systemy detekcji anomalii w przepływach lub zdarzeniach (np.: NBA), * system SIEM, * źródła, muszą zostać powiązane z parserami, pozwalającymi na detekcję zgodną z wbudowanymi w system regułami korelacji.  1. Adaptację reguł profilowych, pozwalających na dostosowanie zdarzeń do zasobów, których dotyczą. 2. Podłączenie reguł detekcji. 3. Podłączenie i konfiguracja mechanizmów UEBA:  * integracja z Active Directory, * adaptacja profili użytkowników UBA, * adaptacja profili hostów EBA, * import reguł bezpieczeństwa UEBA, uruchomienie procesu uczenia.  1. Obszar Reakcji ma na celu uruchomienie i dostrojenie mechanizmów automatyzacji w działaniach reagowania na wykryte zagrożenia bezpieczeństwa. Zakres prac powinien uwzględniać: 2. Import gotowych scenariuszy obsługi. 3. Konfigurację zespołów obsługi, celem właściwej adresacji podatności oraz zdarzeń wymagających obsługi. 4. Konfigurację mechanizmów powiadamiania. 5. Usługa konsultacji powdrożeniowej, świadczona przez dedykowanego inżyniera w ramach okresu wsparcia musi w szczególności uwzględniać: 6. przygotowanie i modyfikację formularzy raportów; 7. tworzenie i edycję parserów; 8. przygotowywanie nowych reguł bezpieczeństwa; 9. modyfikację dostępnych reguł i ich dostrojenie; 10. wsparcie w procesie aktualizacji systemu; 11. tworzenie i edycję nowych scenariuszy reakcji; 12. tworzenie i dostosowanie dashboardów danych. 13. Wykonawca musi zapewnić usługę obejmującą proces aktualizacji oprogramowania oraz kontekstu systemu (dotyczy to zwłaszcza bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji). Dostęp do centralnej usługi aktualizacyjnej ma pozwalać na automatycznie wyświetlanie i pobieranie z poziomu interfejsu systemu dostępnych aktualizacji. Dla pobranych w procesie aktualizacji reguł oraz parserów musi być dostępne wersjonowanie, pozwalające uruchomić nową wersję reguły korelacyjnej oraz parsera z poziomu interfejsu systemu. Automatyczne wersjonowanie ma umożliwiać wczytanie starszej wersji reguły lub parsera, a zmiana reguł i parserów musi być możliwa z poziomu graficznego systemu.   Wykonawca zapewni bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla maksymalnie 5 osób i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez producenta systemu/ systemów. Szkolenia mogą odbyć się w formie zdalnej. |
|  | Testowanie i modyfikacja parametrów infrastruktury sieciowej. | 1. Testowanie mechanizmów bezpieczeństwa klastra wirtualizacyjnego. 2. Testowanie wydajności przesyłu i zapisu danych do środowiska LAN. 3. Testowanie mechanizmów replikacji danych. 4. Testowanie dostępu publicznego do zasobów. 5. Testy wydajnościowe połączeń pochodzących z Internetu i wychodzących z zasobów lokalnych do Internetu 6. Testowanie autoryzowanego dostępu do wewnętrznych zasobów. 7. Wprowadzanie koniecznych modyfikacji konfiguracji urządzeń sieciowych po przeprowadzonych testach. |
|  | Asysty stanowiskowe | Asysta stanowiskowa ma obejmować 16 godzin szkoleniowych w ujęciu 8 godzin na jeden dzień. Całość powinna się zamknąć w okresie 2 dni i ma dotyczyć autorskiego rozwiązania zrealizowanego w ramach podmiotowego wdrożenia.  Asysta musi być warunkiem dopuszczający do przekazania rozwiązania technicznego do wykorzystania produkcyjnego.  Asysta stanowiskowa musi zostać odebrana i zatwierdzona protokołem odbioru sygnowanym przez obie strony projektu tj. wykonawcę oraz użytkownika końcowego. |
|  | Termin wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji. | Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą.  Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszego dnia roboczego następującego po pracach wdrożeniowo – instalacyjnych w godzinach od 8.00 do 15.30.  W tym czasie przedstawiciel Wykonawcy:   * zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji. * dokona prezentacji działania sytemu dla pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności:  1. zastosowanej technologii serwerów 2. zastosowanej technologii pamięci masowej 3. wirtualizacji 4. systemu backupu 5. zastosowanych rozwiązań aplikacyjnych   Wykonawca zapewni również wparcie techniczne ze strony inżynierów w okresie trwania realizacji projektu. Wsparcie polegałoby na pomocy zdalnej lub telefonicznej przy rozwiązaniu problemów, które ewentualnie pojawią się podczas eksploatacji ww. rozwiązania. |
|  | Opracowanie dokumentacji powykonawczej | Zamawiający wymaga opracowania dokumentacji technicznej powykonawczej.   1. Konfiguracja urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację). 2. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały. 3. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały. 4. JHasHasła dostępowe do dostarczonych i zainstalowanych systemów. |

## Wodomierze – szt. 296

## Wodomierze – szt. 296

Przedmiotem zamówienia jest dostawa i montaż 296 szt. wodomierzy z wybudowanym modułem radiowym z systemem odczytu zdalnego, zgodnych z określonymi wymaganiami technicznymi i eksploatacyjnymi o minimalnym progu rozruchu dla pomiaru zużycia wody – 0,75 l/h.

Celem wdrożenia jest zapewnienie nowoczesnej, zdalnej obsługi pomiaru zużycia wody oraz integracja systemu z istniejącymi infrastrukturami informatycznymi zamawiającego.

1. **Zakres dostawy**

W ramach realizacji zamówienia przewidziana jest dostawa wodomierzy statycznych DN20 R≥250, Q3-4 L-130/DN 15 R≥250 Q3 – 2,5 L-110, według zapotrzebowania Zamawiającego, wyposażonych w moduł radiowy WMBus oraz LoRaWAN, Dodatkowo każdy wodomierz zostanie zaopatrzony w plombę wodomierzową zatrzaskową z indywidualną numeracją. Dostawca dostarczy dokumentację obejmującą dokumentację techniczną, karty katalogowe, certyfikaty oraz dokumentację oprogramowania.

1. **Wymagania techniczne wodomierzy**

Wodomierze muszą posiadać statyczny układ pomiarowy, pozbawiony części ruchomych, co zapewni długotrwałą i bezawaryjną pracę. Konstrukcja wodomierza powinna być niezależna od przewodności elektrycznej wody, a jego obudowa wykonana z mosiądzu, posiadającego stosowne atesty higieniczne do kontaktu z wodą pitną. Wodomierze powinny być odporne na temperatury w zakresie od +5°C do +55°C, a ich liczydła powinny być wyposażone w elektroniczny wyświetlacz o minimalnym zakresie wskazań 999999,999 m3.

1. **Integracja i funkcjonalność systemu**

System odczytu zdalnego musi umożliwiać bieżące monitorowanie zużycia wody, identyfikację przepływów wstecznych, wykrywanie ingerencji oraz przekroczeń parametrów granicznych. Moduły radiowe powinny obsługiwać komunikację dwukierunkową zgodną z LoRaWAN oraz Wireless M-Bus, zapewniając wysoką jakość przesyłu danych oraz ich szyfrowanie. Wodomierze muszą być kompatybilne z systemem inkasenckim oraz umożliwiać integrację z platformą zarządzającą SPIDAP Cloud.

1. **Wymagania dotyczące szczelności i trwałości**

Korpus wodomierza powinien posiadać oznaczenia materiałowe oraz numer seryjny, umożliwiające jednoznaczną identyfikację. Klasa szczelności obudowy powinna odpowiadać IP68, a liczydło być odporne na zaparowanie i zanieczyszczenia. System pomiarowy nie może być wypełniony żywicą, lecz umożliwiać rozłożenie na elementy poddawane recyklingowi.

1. **Wymagania normatywne** Wodomierze muszą spełniać wymagania norm:

* EN-ISO 4064-1÷5:2014(E) lub równoważna – wodomierze do wody zimnej pitnej i wody gorącej,
* OIML R49:2013 – wodomierze przeznaczone do pomiaru zimnej wody pitnej i wody ciepłej,
* Dyrektywa 2014/32/EC Parlamentu Europejskiego dotycząca przyrządów pomiarowych,
* EN 13757-4:2019 – komunikacja bezprzewodowa M-Bus,
* WELMEC 7.2 – zasady metrologiczne dla urządzeń pomiarowych lub równoważne.

1. **Wymagania dotyczące systemu odczytu radiowego** S

System powinien umożliwiać odczyt danych w trybach wM-Bus i LoRaWAN, zapewniając pełną rejestrację danych pomiarowych i diagnostycznych. Wodomierze powinny obsługiwać mechanizm adaptacyjnej regulacji transmisji danych (ADR), a dane powinny być szyfrowane zgodnie z OMS3 encryption 5.

1. **Oprogramowanie i wsparcie techniczne** D

Dostawca zobowiązany jest do dostarczenia oprogramowania inkasenckiego SPIDAP Mobile oraz jego integracji z platformą SPIDAP Cloud. System powinien zapewniać harmonogramowanie zadań, analizę zużycia oraz eksport danych do plików CSV. Oprogramowanie powinno być zgodne z systemami operacyjnymi Android oraz posiadać wsparcie dla komunikacji NFC i Bluetooth.

**Dostawca zapewni wsparcie techniczne, szkolenie użytkowników oraz bieżące aktualizacje systemu. Wszystkie urządzenia muszą być fabrycznie nowe, posiadać aktualne certyfikaty legalizacyjne oraz gwarancję na co najmniej 5 lat.**

## 5.12 Przepływomierz – szt. 2

Zamawiający zamierza dokonać opomiarowania zrzutu ścieków na oczyszczalniach ścieków w Nozdrzcu i Siedliskach za pomocą przepływomierzy elektromagnetycznych do pomiaru przepływu cieczy w zamkniętych instalacjach rurociągowych bezciśnieniowych. Zamawiający zamierza również dokonać opomiarowanie wody przeznaczonej do płukania filtrów na Stacji Uzdatniania Wody w Wesołej. Zakres pomiarowy przepływomierzy: 60-2 000 l/min. Dokładność pomiaru: ± 0,5 %. Zakres ciśnienia procesowego: maks. 16 bar Zakres temperatury procesowej: 0-60 °C

Pomiar przepływ cieczy przewodzących czystych i zanieczyszczonych, agresywnych i obojętnych chemicznie oraz przewodzących mieszanin i pulp.

Przedmiotem zamówienia jest dostawa i montaż przepływomierza elektromagnetycznego DN 65 (urządzenie pomiarowe służące do mierzenia przepływu objętościowego cieczy przewodzących (np. wody, ścieków, cieczy technologicznych) w rurociągach o nominalnej średnicy DN 65 (czyli 65 mm). Urządzenie musi zapewniać precyzyjny pomiar objętościowy przepływu wody czystej i uzdatnionej.

### 5.12.1 Model – 6 DN 65

Wymagania techniczne obejmują:

* Średnica nominalna DN 65,
* Zakres pomiarowy Qmin - Qmax dostosowany do warunków eksploatacyjnych zamawiającego,
* Dokładność pomiaru zgodna z normami EN ISO 4064 lub równoważnymi,
* Obudowa i elementy pomiarowe odporne na korozję,
* Interfejs komunikacyjny kompatybilny z systemem LoRaWAN lub M-Bus,
* Certyfikaty i atesty do stosowania w instalacjach wodociągowych.

### 5.12.2 Model – 6 DN 100

Wymagania techniczne obejmują:

* Średnica nominalna DN 100,
* Zakres pomiarowy Qmin - Qmax dostosowany do warunków eksploatacyjnych zamawiającego,
* Dokładność pomiaru zgodna z normami EN ISO 4064 lub równoważnymi,
* Obudowa i elementy pomiarowe odporne na korozję,
* Interfejs komunikacyjny kompatybilny z systemem LoRaWAN lub M-Bus,
* Certyfikaty i atesty do stosowania w instalacjach wodociągowych.

Przez równoważne rozwiązanie uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową

UWAGA:

**Dostawca zobowiązuje się do dostarczenia urządzenia wraz z dokumentacją techniczną, atestami oraz instrukcją eksploatacyjną.**