**Załącznik nr 1**

**Szczegółowy opis przedmiotu zamówienia (SOPZ)**

**czerwiec 2022**

Spis treści

[1. Wymagania ogólne dla urządzeń i oprogramowania sieciowego. 3](#_Toc98765523)

[2. Wymagania gwarancyjne. 3](#_Toc98765524)

[3. Miejsce instalacji sprzętu i oprogramowania/systemu. 3](#_Toc98765525)

[4. Ubezpieczenie sprzętu 4](#_Toc98765526)

[5. Zestawienie zakresu dostaw i usług. 4](#_Toc98765527)

[5.1. Serwery – szt. 2 – wymagania minimalne. 7](#_Toc98765528)

[5.2. Macierz– szt.1 – wymagania minimalne. 10](#_Toc98765529)

[5.3. Backup NAS – szt. 1 – wymagania minimalne 13](#_Toc98765530)

[5.4. Domena 13](#_Toc98765531)

[5.5. Oprogramowanie do wirtualizacji – szt.1 – wymagania minimalne. 16](#_Toc98765532)

[5.6. Oprogramowanie do e-usług – eNależności 17](#_Toc98765533)

[5.7. Oprogramowanie do e-usług – PSZOK 20](#_Toc98765534)

[5.8. Elektroniczny Obieg Dokumentów 20](#_Toc98765535)

[5.9. Aplikacja mobilna – Gmina 52](#_Toc98765536)

[5.10. Przełączniki sieciowe - szt. 2 – wymagania minimalne 53](#_Toc98765537)

[5.11. Firewall - szt. 1 – wymagania minimalne 55](#_Toc98765538)

[5.12. Usługi wdrożenia i konfiguracji oprogramowania 60](#_Toc98765539)

[5.13. Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania 61](#_Toc98765540)

[5.14. Diagnoza cyberbezpieczeństwa 76](#_Toc98765541)

## Wymagania ogólne

## dla urządzeń i oprogramowania sieciowego.

* całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
* całość sprzętu musi być nowa, nie używana wcześniej;

## dla oprogramowania i aplikacji mobilnych

* Wykonawca wykona przedmiot zamówienia zgodnie ze wszystkimi wytycznymi WCAG 2.1 o których mowa w załączniku do Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.
* Warunkiem odbioru serwisu i dokonania płatności jest spełnienie wymogów wskazanych w załączniku do Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.
* Zamawiający zastrzega sobie prawo do zlecenia zewnętrznego audytu spełnienia wymagań WCAG 2.1.

## Wymagania gwarancyjne.

**Sprzęt**

* o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona min. roczna gwarancja (chyba, że zapisy szczegółowe stanowią inaczej) 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;
* wszystkie dostarczane moduły muszą pochodzić od producenta urządzeń sieciowych i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu;

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące się w dalszej części SOPZ.

## Miejsce instalacji sprzętu i oprogramowania/systemu.

* Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części załącznika na 1, w budynkach urzędu w miejscach wskazanych przez Zamawiającego.

1. Ubezpieczenie sprzętu

Wykonawca zobowiązany jest do dostawy sprzętu komputerowego wraz z ubezpieczeniem na okres 12 m-cy. Koszty ubezpieczenia należy ująć w cenie oferowanego sprzętu.

Sprzęt musi zostać ubezpieczony do 100% jego wartości księgowej brutto.

Ubezpieczenie nie może przewidywać franszyzy, integralnej i udziału własnego ze strony Zamawiającego.

Polisa ubezpieczeniowa powinna zostać wystawiona na rzecz Zamawiającego.

Dostarczony sprzęt powinien zostać objęty ubezpieczeniem od wszelkich ryzyk zgodnie z poniższymi założeniami:

1. Przedmiotem ubezpieczenia jest sprzęt elektroniczny stacjonarny zainstalowany na stałe w

miejscu ubezpieczenia oraz sprzęt przenośny, pod warunkiem, że wiek sprzętu elektronicznego stacjonarnego i sprzętu przenośnego nie przekracza 5 lat.

1. Sprzęt przenośny używany poza lokalem na terenie Rzeczypospolitej Polskiej jest objęty ochroną w przypadku jego utraty wskutek kradzieży z włamaniem, jeżeli został skradziony z samochodu, gdy:
   1. pojazd posiadał twardy dach (jednolitą sztywną konstrukcję),
   2. został prawidłowo zamknięty na wszystkie możliwe zabezpieczenia znajdujące się w pojeździe,
   3. był zaparkowany w zamkniętym garażu lub na parkingu strzeżonym (jeżeli kradzież z włamaniem nastąpiła w godzinach 22.00 - 6.00),
   4. ubezpieczony przedmiot był przechowywany wewnątrz pojazdu w sposób uniemożliwiający zobaczenie go z zewnątrz, np. w bagażniku.
2. Zakres ubezpieczenia:
3. Od wszystkich ryzyk z rozszerzeniem o użytkowanie mobilne w tym m.in.:
   1. utrata bądź ubytek wartości ubezpieczonego sprzętu nastąpiły z powodu jego zniszczenia lub uszkodzenia w wyniku nieprzewidzianego wypadku uniemożliwiającego dalsze spełnianie zamierzonych funkcji.
   2. utrata sprzętu nastąpiła wskutek kradzieży z włamaniem, rabunku, dewastacji i wandalizmu.
4. Do szkód objętych ubezpieczeniem zalicza się m.in. szkody wynikłe w następstwie:
5. działania człowieka:
   1. niewłaściwej obsługi sprzętu, tj. nieostrożności, zaniedbania, niewłaściwego użytkowania,
   2. braku kwalifikacji, błędu operatora itp.;
   3. świadomego i celowego zniszczenia przez osoby trzecie, pracowników i współpracowników ubezpieczającego (jednak z zastosowaniem klauzuli reprezentantów),
6. kradzieży z włamaniem, rabunku, wandalizmu i dewastacji. Ubezpieczyciel ponosi odpowiedzialność także za szkody powstałe wskutek kradzieży z pojazdu lub kradzieży całego pojazdu wraz ze sprzętem.
7. ognia (w tym działania dymu, sadzy itp.) oraz polegające na osmaleniu, przypaleniu, a także w wyniku wszelkiego rodzaju eksplozji, implozji, uderzenia piorunu bezpośrednio i pośrednio na przedmiot ubezpieczenia, upadku statku powietrznego oraz w akcji ratunkowej
8. wody, tj. zalania wodą z urządzeń wodno – kanalizacyjnych, powodzi, wylewu wód podziemnych, a także czynników atmosferycznych w postaci mrozu, śniegu, deszczu wilgoci, pary wodnej itp.
9. wiatru, gradu, lawiny, obsunięcia i zapadania się ziemi, huraganu, trzęsienia ziemi,
10. zbyt wysokiego lub zbyt niskiego napięcia albo całkowitego zaniku napięcia w sieci instalacji elektrycznej, szkód przepięciowych i pochodnych powstałych w związku z uderzeniem pioruna,
11. sprzęt elektroniczny ubezpieczony jest również w zakresie szkód spowodowanych przez upadek.
12. Dodatkowe rozszerzenie dotyczące ochrony sprzętu nie podłączonego na stanowisku pracy lub podczas przerwy w eksploatacji.

## Zestawienie zakresu dostaw i usług.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa** | **Długość gwarancji (minimum) [m-ce]** | **Ilość** | **Jednostka miary** | **Uwagi** |
|  | Serwery | 12 (kryterium oceny) | 2 | Szt. | *S*erwery jako podstawa do uruchomienia kolejnych wirtualnych maszyn przeznaczonych dla poszczególnych systemów dziedzinowych |
|  | Macierz | 12 (kryterium oceny) | 1 | Szt. | Pozycja dotyczy zakupu macierzy dyskowej, produkcyjnej, na której składowane i przetwarzane będą dane systemów dziedzinowych pozwalających na świadczenie e-usług i pracę zdalną. Parametry urządzenia: 2 kontrolery dostępowe 2-portowe, 6 dysków HDD min. 4 TB, 4 dyski SSD SAS min. 1 TB, |
|  | Backup NAS + 6HDD x 6TB | 12 (kryterium oceny) | 1 | Szt. | Urządzenia NAS do tworzenia kopii będzie odpowiadać za nadzór nad procesami backupu i archiwizacji kopii zapasowych danych. Będzie to kolejny poziom bezpieczeństwa danych.  Parametry serwera: min 6HDD x 6TB |
|  | Domena | 12 (kryterium oceny) | 1 | Szt. | Pozycja uwzględnia koszty systemu operacyjnego niezbędnego do funkcjonowania serwerów wirtualizacji i backupu oraz koszty licencji dostępowych (CAL) dla użytkowników (50 licencji). Zakup jest niezbędny do zapewnienia dostępu i funkcjonowania całej planowanej infrastruktury. |
|  | Oprogramowanie do wirtualizacji | 12 (kryterium oceny) | 1 | Szt. | Oprogramowanie do wirtualizacji niezbędne do uruchomienia maszyn wirtualnych na zakupionym serwerze. Oprogramowanie konieczne do zapewnienia warunków pracy zdalnej i świadczenia e-usług publicznych przez gminę. |
|  | Oprogramowanie do e-usług - Należności | 12 (kryterium oceny) | 1 | Szt. | Pozycja uwzględnia zakup licencji na portal umożliwiający mieszkańcom gminy zdalne załatwianie spraw związanych z podatkami i innymi należnościami wobec JST. Portal e-Należności będzie zintegrowany z systemami dziedzinowymi oraz aplikacją mobilną. Będzie miał postać portalu www dostępnego przez przeglądarkę. Pozycja nie uwzględnia kosztów zakupu licencji na system podatki. Gmina posiada już to oprogramowanie. |
|  | Oprogramowanie do e-usług - PSZOK | 12 (kryterium oceny) | 1 | Szt. | Pozycja uwzględnia zakup licencji na portal umożliwiający mieszkańcom gminy zdalne załatwianie spraw związanych z deklaracjami śmieciowymi, gospodarką odpadami oraz należnościami wobec JST związanymi z tymi sprawami. Portal będzie zintegrowany z systemami dziedzinowymi oraz aplikacją mobilną. Będzie miał postać portalu www dostępnego przez przeglądarkę. Pozycja nie uwzględnia kosztów zakupu licencji na system podatki. Gmina posiada już to oprogramowanie. |
|  | Elektroniczny Obieg Dokumentów | 12 (kryterium oceny) | 1 | Szt. | W ramach pozycji przewiduje się zakup licencji do elektronicznego obiegu dokumentów wraz z instruktażem dla użytkowników oraz gwarancją na okres 12 m-cy. Oprogramowanie pozwoli na wdrożenie EOD w JST i na pracę zdalną pracownikom z zapewnionym dostępem do dokumentacji. Tym samym zwiększy cyfryzację Urzędu i poziom bezpieczeństwa danych. |
|  | Aplikacja mobilna - Gmina | 12 (kryterium oceny) | 1 | Szt. | Aplikacja winna być dostępna na urządzenia przenośne. Aplikacja pozwoli na kontakt i zdalną obsługę spraw mieszkańców, niezależnie od miejsca ich przebywania. Dzięki wykorzystaniu urządzeń mobilnych i technologii typu push umożliwi przekazywanie mieszkańcom informacji o stanie ich spraw, aktualności dotyczących gminy, decyzji, itp. Zwrotnie mieszkaniec będzie mógł również, przy jej wykorzystaniu załatwić swoje sprawy w urzędzie. |
|  | Przełączniki sieciowe (24 porty)+4 uplink 10G | 12 (kryterium oceny) | 2 | Szt. | Dwa przełączniki sieciowe 24-portowe z uplinkiem 4G. Urządzenia te posłużą do połączenia serwerów i macierzy z infrastrukturą sieci LAN. |
|  | Firewall | 12 (kryterium oceny) | 1 | Szt. | Urządzenie Firewall UTM do zarządzania ruchem w całej sieci LAN i będące zabezpieczeniem tej sieci przed dostępem z zewnątrz. Jednocześnie urządzenie to pozwoli na zarządzanie pracownikami pracującymi zdalnie i bezpieczne udostępnianiem im zasobów gminnych. Zakup jest konieczny do odpowiedniego zabezpieczenia funkcjonowania całego systemu |
|  | Usługi wdrożenia i konfiguracji oprogramowania | 12 | 185 | godz. | Usługa dotyczy wdrożenia i konfiguracji dostarczonego oprogramowania. |
|  | Instalacja i konfiguracja | 12 | 100 | Godz. | Usługi doradcze związane z wdrożeniem platformy sprzętowej (wirtualizacyjnej), migracją danych z dotychczasowych urządzeń, ustaleniem i skonfigurowaniem zasad bezpieczeństwa sieciowego, montaż urządzeń, instruktaż z zakresu wdrożonych rozwiązań dla służb informatycznych w urzędzie. Dla całości usług przewidziano ok. 100 godz.,  Zakres usługi   * Instalacja urządzeń serwerowych i komputerowych. * Migracja danych. * Konfiguracja całego systemu wirtualizacyjnego. * Konfiguracja polityk sieciowych i bezpieczeństwa. * Testy systemu. |
|  | Diagnoza cyberbezpieczeństwa | 12 | 1 | Szt. | Pozycja dotyczy przeprowadzenia diagnozy bezpieczeństwa zgodnie z wymaganiami konkursu programu "Cyfrowa Gmina", |

## Serwery – szt. 2 – wymagania minimalne.

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Parametr lub warunek | | Minimalne wymagania |
| 1 | Obudowa | | -Typu Rack, wysokość max. 2U;  -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack. Możliwość montażu ramienia porządkującego przewody. |
| 2 | Płyta główna | | -Dwuprocesorowa, wyprodukowana i zaprojektowana przez producenta serwera, możliwość instalacji procesorów 18-rdzeniowych;  -Sumarycznie minimum 6 złącz PCI Express, w tym minimum 3 złącza o prędkości minimum PCI Express x16 generacji 3;  -Aktywne wszystkie złącza PCI-e.  -Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug;  -Zainstalowany moduł TPM 2.0 kompatybilny z systemem operacyjnym Windows Server 2022; |
| 3 | Procesory | | - Zainstalowane dwa procesory 8-rdzeniowe w architekturze x86 taktowane podstawowym zegarem o częstotliwości min. 3,2 GHz, osiągające wynik w testach wydajności SPECrate2017\_int\_base min. 121 pkt. przy konfiguracji z dwoma procesorami dla dowolnej platformy dwuprocesorowej producenta serwera, który jest oferowany w postępowaniu przez Wykonawcę. Wymagane jest aby do oferty był załączony PDF ze strony spec.org. z wynikami testów wydajnościowych.  Nie dopuszcza się procesorów o innej ilości rdzeni fizycznych z uwagi na optymalizację kosztową licencjonowania aplikacji i systemów operacyjnych; |
| 4 | Pamięć RAM | | -Zainstalowane 256 GB pamięci RAM DDR4 typu Registered, 2933Mhz w kościach o pojemności 32 GB;  -Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC;  -12 gniazd pamięci RAM na płycie głównej, obsługa minimum 768 GB pamięci RAM; |
| 5 | Kontrolery dyskowe, I/O | | -Zainstalowany kontroler SAS 3.0 RAID 0,1,5,10,50; |
| 6 | Dyski twarde | | -Zainstalowane min. 2 dyski SSD o pojemności 480 GB każdy, DWPD min.0,9, dyski Hotplug;  -Minimum 4 wnęki dla dysków twardych Hotplug 3,5”; |
| 7 | Inne napędy zintegrowane | | -Możliwość montażu napędu optycznego typu DVD-RW; |
| 8 | Kontrolery LAN | | -Wbudowana w płytę główną karta 2 x 1Gbit/s ze wsparciem iSCSI, niezajmująca slotu PCI Express;  -Dodatkowa osobna karta sieciowa 2 x 10 Gbit/s SFP+; |
| 9 | Kontrolery I/O | | -Zainstalowana karta SAS HBA wyposażona w dwa zewnętrze porty SFF 8644;  -Wraz z serwerem należy dostarczyć min. 2 szt. kabli SAS (8644-8644) o długości min. 1m każdy; |
| 10 | Porty | | -zintegrowana karta graficzna ze złączem VGA;  -7x USB 3.0, w tym minimum 2 na panelu przednim, minimum 1 wewnętrzne; |
| 11 | | Zasilanie, chłodzenie | -Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy maksymalnej 800W każdy;  -Redundantne wentylatory;  -Dwa kable zasilające C13-C14 o długości min. 4m każdy; |
| 12 | | Zarządzanie | -Wbudowane diody informacyjne informujące o stanie serwera;  -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 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; * Dostęp poprzez przeglądarkę Web; * 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); * Możliwość pobrania darmowego oprogramowania zarządzającego i diagnostycznego wyprodukowanego przez producenta serwera umożliwiającego 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 itd.); * Zainstalowana, dedykowana dla potrzeb karty zarządzającej pamięć flash o pojemności minimum 16 GB; * Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB); * Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania; * Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; * 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 (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji; * Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń); * Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą; * Karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email). Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera; |
| 13 | | Wspierane OS | * Windows Server 2022, Windows Server 2019, Windows Server 2016, Suse, RHEL, Vmware 6.7 U3, 7.0 U1; |
| 14 | | Gwarancja | - gwarancja producenta serwera w trybie onsite z czasem reakcji w miejscu instalacji sprzętu najpóźniej w następnym dniu roboczym od zgłoszenia usterki;  -Dostępność części zamiennych przez 5 lat od momentu zakupu serwera;  -Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera– jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji;  - Zgłoszenia serwisowe w języku polskim na dedykowany nr infolinii serwisowej producenta serwera;  - Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera |
| 15 | | Dokumentacja, inne | -Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji  -Ogólnopolska, telefoniczna, polskojęzyczna infolinia/linia techniczna producenta serwera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji. |

## Macierz– szt.1 – wymagania minimalne.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa podzespołu** | **Minimalne wymagania** |
|  | Obudowa, możliwości rozbudowy macierzy | 1) System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks 2U w tej szafie.  2) Obudowa pojedynczego modułu rozwiązania – półka dyskowa, moduł kontrolerów -musi zawierać układ nadmiarowy dla modułów zasilania i chłodzenia umożliwiający wymianę tych elementów w razie awarii bez konieczności wyłączania macierzy  3) Macierz musi posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii/macierzy;  4) Macierz nie może zawierać elementów typu bateria/akumulator wymagających jakiegokolwiek reżimu obsługowego: wymiana, przełączanie, ładowanie (np. nie dopuszcza się podtrzymania bateryjnego cache kontrolerów itp.) ;  5) Rozbudowa o dodatkowe moduły dyskowe (półki dyskowe) dla obsługiwanych dysków musi odbywać się wyłącznie poprzez zakup takich modułów tj. bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy;  6) Moduły (półki dyskowe) dla rozbudowy o dodatkowe dyski i przestrzeń dyskową muszą zapewniać możliwość instalacji co najmniej 24 dysków twardych 2,5” w półce o zajętości instalacyjnej nie większej niż 2U w szafach przemysłowych standardu 19”;  7) Macierz musi umożliwiać obsługę i rozbudowę do co najmniej 96 dysków twardych w jednym urządzeniu (zarządzane przez parę kontrolerów)  8) Połączenia pomiędzy półkami dyskowymi muszą zapewniać brak pojedynczego punktu awarii; |
|  | Pojemność | 1) System musi umożliwiać instalację dysków wykonanych w technologii hot-plug i wyposażonych w podwójny interfejs SAS,  2) Zainstalowane 4 szt. dysków SSD-SAS 12G o pojemności min. 960GB  3) Zainstalowane 6 szt. dysków NL-SAS 12G o pojemności min. 4TB |
|  | Kontrolery | 1) System musi obsługiwać 2 kontrolery pracujące w układzie nadmiarowym typu active-active i bez konieczności stosowania zewnętrznych połączeń kablowych pomiędzy nimi, z minimum 8GB pamięci podręcznej Cache w każdym kontrolerze, wymaga się dostarczenia minimum 2 kontrolerów;  2) W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik;  3) Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia.  4) Macierz musi pozwalać na wymianę kontrolera RAID bez utraty danych zapisanych na dyskach nawet w przypadku konfiguracji z jednym kontrolerem RAID;  5) W układzie z zainstalowanymi dwoma kontrolerami RAID zawartości pamięci podręcznej obydwu kontrolerów musi być identyczna tzw. cache mirror.  6) Każdy z kontrolerów RAID musi posiadać dedykowane min. 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością 1 Gb/s - dla zdalnej i lokalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy |
|  | Interfejsy | 1) Oferowana macierz musi być dostarczona w konfiguracji z minimum 2 portami iSCSI 10G na każdy kontroler macierzy, do podłączenia serwerów; |
|  | Poziomy RAID | Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: 0, 1,1+0, 5, 5+0, 6 |
|  | Wspierane dyski | Oferowany model macierzy musi wspierać dyski:  1) dyski SAS wykonane w technologii hot-plug o pojemnościach o prędkościach obrotowych 10000 obrotów na minutę,  2) dyski NL-SAS (NearLine SAS) wykonane w technologii hot-plug o prędkości obrotowej min 7200 obrotów na minutę,  3) dyski SSD SAS wykonane w technologii hot-plug;  3) interfejsy obsługiwanych dysków muszą być wyposażone w minimum 2 porty pracujące w reżimie full-duplex (jednoczesna transmisję danych przez dwa porty)  4) Macierz musi wspierać mieszaną konfigurację dysków SSD, SAS i NearLine SAS w obrębie pojedynczego modułu obudowy  5) Macierz musi wspierać mechanizm automatycznej przedawaryjnej migracji zapisów i składowanych danych na dysk zapasowy.  6) Macierz musi wspierać technologię energooszczędne typu Drive Spin Down lub wyłączanie dysków nieaktywnych w trybie ręcznym i automatycznym z wykorzystaniem mechanizmu typu ‘time scheduler’ czyli w zadanym i/lub powtarzalnym oknie czasowym.  7) Macierz musi umożliwiać definiowanie i obsługę dysków zapasowych tzw. hot-spare w trybach:  - hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID  - hot-spare dla zabezpieczania dowolnej grypy dyskowej RAID.  8) Macierz musi pozwalać na skonfigurowanie dowolnego dysku hot-plug dostarczonego w rozwiązaniu do roli dysku zapasowego jak w pkt.7  9) W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. BackLessCopy) |
|  | Opcje software’owe | 1) Macierz musi być wyposażona w system kopii migawkowych (snapshot) z licencją na minimum 1024 kopie migawkowych.  2) Macierz musi wspierać Microsoft Volume ShadowCopy Services (VSS)  3) Macierz musi umożliwiać zdefiniowanie min. 1024 woluminów (LUN)  4) Macierz musi umożliwiać podłączenie logiczne z serwerami i stacjami poprzez minimum 4 ścieżki;  5) Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego i kontrolerów RAID bez konieczności wyłączania macierzy lub bez konieczności wyłączania ścieżek dla podłączonych stacji/serwerów;  6) Macierz musi umożliwiać rozproszenie alokacji danych dla pojedynczego woluminu LUN na maksymalnej liczbie obsługiwanych dysków HDD.  7) Oferowany model macierzy musi obsługiwać mechanizmy Thin Provisioning (przy zainstalowanych 2 kontrolerach) czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy – wymagana jest obsługa minimum 64 pól ThinProvisioning w rozwiązaniu.  8) Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacji:  - zmiana rozmiaru woluminu,  - zmiana poziomu RAID,  - zmiana technologii dysków dla danej grupy RAID,  - dodawanie nowych dysków do istniejącej grupy dyskowej,  9) Macierz musi posiadać wsparcie dla systemów operacyjnych: MS Windows Server, SuSE Linux, RedHat Linux, Oracle Linux, Oracle VM, HP-UX, IBM AIX, SUN Solaris, Vmware, Citrix XEN Server  10) Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem)  11) Macierz musi obsługiwać woluminy logiczne o maksymalnej pojemności minimum 128 TB.  12) Wraz z macierzą należy dostarczyć oprogramowanie lub moduły programowe typu plug-in pozwalające na integracje macierzy w środowiskach Vmware w zakresie obsługi mechanizmów: Vmware VAAI, Vmware MultiPath IO – z subskrypcją do bezpłatnej aktualizacji w całym okresie obowiązywania gwarancji  13) Wraz z macierzą należy zapewnić wsparcie dla mechanizmów Off-loaded Data Transfer i Space Reclamation w środowiskach MS Windows  14) Wraz z macierzą należy zapewnić subskrypcję na bezpłatną aktualizację (możliwość bezpłatnego pobrania ze stron internetowych producenta) oprogramowania wewnętrznego macierzy w całym okresie obowiązywania gwarancji |
|  | Konfiguracja, zarządzanie | 1) Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.  2) Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI |
|  | Gwarancja i serwis | 1. Całe rozwiązanie musi być objęte gwarancją producenta z czasem przyjazdu inżyniera serwisu producenta na miejsce użytkowania najpóźniej w następnym dniu roboczym od zgłoszenia usterki do organizacji serwisowej producenta macierzy. 2. Serwis gwarancyjny musi obejmować dostęp do bezpłatnych poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia. 3. Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązania bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy oraz do kolejnych wersji oprogramowania zarządzającego w okresie minimum 2 lat. 4. System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez szyfrowany protokół. 5. Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych |

## Backup NAS – szt. 1 – wymagania minimalne

|  |
| --- |
| * Procesor osiągający w teście CPU Mark na stronie <https://www.cpubenchmark.net/cpu_list.php> wartość min. 5200 punktów * Prędkość odczytu, min. 450.00 MB/sek * Prędkość zapisu min. 450.00 MB/sek * Wbudowany interfejs 1Gbit/s z min. czterema portami RJ-45 oraz funkcją agregacji łączy * Możliwość zainstalowania karty SSD M.2 lub 10GbE * Pamięć RAM min. 4GB (możliwość rozbudowy do min. 32 GB w min 2 slotach) * Ilość kieszeni dysków min. 8 (możliwość rozbudowy do 12 dysków z wykorzystaniem jednostki rozszerzającej lub równoważnie obudowa na 12 dysków) * Obudowa 19 cali max. 2U z szynami do montaży w szafie teleinformatycznej * Port USB 3.0 min. 2 szt. * Port eSATA min 1 szt. * Obsługiwane typy dysków:   + 3,5” SATA HDD   + 2,5” SATA HDD   + 2,5” SATA SSD * Obsługiwany poziom RAID:   + Basic   + JBOD   + [RAID 0](https://www.komputronik.pl/search-filter/7071/serwer-nas-z-raid-0)   + RAID 1   + RAID 10   + [RAID 5](https://www.komputronik.pl/search-filter/7071/serwer-nas-z-raid-5)   + RAID 6 * Urządzenie musi zostać dostarczone z min. 6 szt. dysków twardych o pojemności min 6TB. * Wsparcie dla środowisk wirtualizacji takich jak VMware, Citrix oraz Microsoft Hyper-V. * Wbudowany serwer FTP z funkcjami SSL, TLS. * Obsługa Windows AD, LDAP oraz Domain Trust. * Ochrona za pomocą funkcji kopii zapasowych, jednostek LUN, migawek, klonowania i synchronizacji danych. * Panel użytkownika i oprogramowanie dostępne w pełnej polskiej wersji językowej. * Wbudowane systemy zabezpieczeń sieciowych, antywirus, szyfrowanie AES256bit oraz dwustopniowe uwierzytelnianie użytkowników. * Urządzenie musi być wyposażone w zintegrowane rozwiązanie do tworzenia kopii zapasowych dla serwerów fizycznych z systemem Windows/Linux, komputerów z systemem Windows, serwerów plików rsync/SMB oraz maszyn wirtualnych VMware vSphere/Microsoft Hyper-V. * Urządzenie musi posiadać centralny interfejs zarządzania służący do monitorowania stanu wszystkich zadań tworzenia kopii zapasowych, zużycia pamięci masowej i transmisji danych historycznych. * Oprogramowanie do backupu musi umożliwiać szybkie przywracanie plików, całych maszyn fizycznych i maszyn wirtualnych. |

## Domena

|  |
| --- |
| Licencje na serwerowy system operacyjny – szt. 2  Licencje na serwerowy system operacyjny muszą uprawniać do zainstalowania serwerowego systemu operacyjnego 2 oferowanych serwerach fizycznych lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego na każdym z 2 oferowanych serwerów fizycznych. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanych serwerach.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.   1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:    1. pozwalają na zmianę rozmiaru w czasie pracy systemu,    2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,    3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,    4. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:     1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,     2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o:     1. Login i hasło,     2. Karty z certyfikatami (smartcard),     3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:     1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,     2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:   Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.   * 1. Zdalna dystrybucja oprogramowania na stacje robocze.   2. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej   3. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:   Dystrybucję certyfikatów poprzez http  Konsolidację CA dla wielu lasów domeny,  Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.   * 1. Szyfrowanie plików i folderów.   2. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).   3. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.   4. Serwis udostępniania stron WWW.   5. Wsparcie dla protokołu IP w wersji 6 (IPv6),   6. Wsparcie dla algorytmów Suite B (RFC 4869),   7. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,   8. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:   Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  Obsługi 4-KB sektorów dysków  Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)   1. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 2. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 4. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 5. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 6. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.   Licencje dostępowe:  Wymaga się, aby oferowane licencje dla systemu operacyjnego umożliwiały korzystanie z zasobów dla 50 użytkowników (50 licencji dostępowych). |

## Oprogramowanie do wirtualizacji – szt.1 – wymagania minimalne.

|  |
| --- |
| Licencja dla 2 serwerów fizycznych posiadających 2 procesory z gwarancją utrzymania aktualnej wersji przez okres min. 1 roku,   1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych 2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. 3. Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji. 4. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym winno obsłużyć   i wykorzystać procesory fizyczne i pamięć RAM objęte przedmiotem postępowania.   1. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych. 2. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. 3. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 4. z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM. 5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. 6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. 7. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. 8. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. 9. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami. 10. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2012, Windows Server 2019, Windows Server 2022, Windows 10, Windows 11, SLES, RHEL, Solaris, OS/2, NetWare, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu SCO OpenServer, SCO Unixware, Mac OS X. 11. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. 12. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. 13. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. 14. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. 15. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. 16. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. 17. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. 18. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. 19. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. 20. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. 21. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). 22. Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewni~~a~~ć stosowanie deduplikacji dla kopii zapasowych. Mechanizm winien zapewni~~a~~ć możliwość wykonywania spójnych kopii zapasowych serwerów aplikacyjnych oraz replikację kopii zapasowych. 23. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. 24. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie. 25. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. |

## Oprogramowanie do e-usług – eNależności

|  |
| --- |
| Portal przeznaczony do prezentacji i obsługi rozliczeń należności pomiędzy Gminą a jej mieszkańcami. Portal ma służyć do realizacji e-usług z obszaru eNależności.  Wymagania minimalne:   1. System musi umożliwiać zalogowanemu użytkownikowi dostęp bezpośredni do danych z systemów dziedzinowych użytkowanych przez Zamawiającego w zakresie określonym w poniższymi wymaganiami z możliwością dokonywania zapłat za pośrednictwem systemu płatności elektronicznych, również na urządzeniach mobilnych. Wymaganie to może być zrealizowane przez responsywny interfejs i/lub aplikację mobilną. W szczególności integracja musi objąć moduły systemu dziedzinowego w zakresie systemów rozliczających opłaty za gospodarowanie odpadami komunalnymi, systemu Finansowo Księgowego (FK) oraz systemów podatkowych funkcjonujących w urzędzie. Wymiana danych musi przebiegać poprzez bezpieczne, szyfrowane połączenie za pośrednictwem serwisów komunikacyjnych. W ramach wdrożenia systemu wymagane jest scalenie baz danych modułów systemu dziedzinowego w obrębie jednej instancji bazy danych celem możliwości świadczenia usług związanych z regulowaniem różnych należności. 2. Dostęp do modułu musi być zapewniony poprzez bezpieczne logowanie przez autoryzację z wykorzystaniem powszechnie dostępnego profilu zaufanego (<https://pz.gov.pl>) za pośrednictwem krajowego węzła identyfikacji elektronicznej. 3. Wymiana danych musi być zabezpieczona. Przy nieprawidłowych danych metoda nie powinna się wykonać i musi zostać zwrócony stosowny komunikat z błędem. 4. Implementacja mechanizmów polegających na automatyzacji wymiany danych pomiędzy modułem a systemem dziedzinowym. Dostępność aktualnych danych nie może dodatkowo angażować operatorów systemów dziedzinowych. 5. Udostępnianie danych użytkownika musi następować wyłącznie po zalogowaniu się użytkownika na jego indywidualne konto. 6. Moduł musi zapewniać wizualizację danych za pomocą tabel i pól informacyjnych pogrupowanych ze względu na obszary, których dotyczą dla każdej kartoteki w obszarach:    1. podatki lokalne (rolny, leśny, od nieruchomości),    2. podatek od środków transportu,    3. ewidencja opłat za gospodarowanie odpadami komunalnymi,    4. system FK (w podziale na różne rodzaj opłat). 7. Dane do wizualizacji muszą być pobierane automatycznie z bazy systemów dziedzinowych za pośrednictwem usług serwisu SOAP uruchomionego w systemie Gminy. Dostęp do serwisu jest szyfrowany i zabezpieczony certyfikatem. Dane udostępniane są tylko w odniesieniu do konta danego podatnika i po jego uwierzytelnieniu za pośrednictwem profilu zaufanego. 8. Zakres danych do prezentacji dla poszczególnych systemów dziedzinowych musi obejmować co najmniej:    1. dla podatku od środków transportowych:       1. wykaz pojazdów zgodnie ze złożoną deklaracją,       2. sprawdzenia zobowiązań wobec gminy w zakresie opłat za podatek od środków transportowych,       3. podgląd dokumentów (deklaracji, decyzji, innych pism przechowywanych w aktówce elektronicznej) dotyczących karty podatkowej danego podatnika z możliwością ich automatycznego pobrania w formie elektronicznej (w przypadku dokumentów „tradycyjnych” elektroniczna kopia w formacie pdf, a w przypadku dokumentu elektronicznego oryginał),    2. podatków i opłat (podatek rolny, leśny, od nieruchomości):       1. stan posiadania podatnika,       2. naliczony podatek (wymiar podatku),       3. stan zobowiązań wobec gminy z tytułu podatków (rolnego, leśnego, od nieruchomości),       4. podgląd dokumentów (deklaracji, decyzji, informacji podatkowych, wystawionych zaświadczeń, innych pism) dotyczących karty podatkowej danego podatnika z możliwością ich automatycznego pobrania (w przypadku dokumentów „tradycyjnych” elektroniczna kopia w formacie pdf, a w przypadku dokumentu elektronicznego oryginał),    3. ewidencji opłat za gospodarowanie odpadami komunalnymi:       1. dane ze złożonych deklaracji,       2. wysokość wystawionych przypisów / kwot do zapłaty,       3. stan zobowiązań wobec Urzędu z tytułu rozliczeń za odpady komunalne,       4. podgląd dokumentów (deklaracji, decyzji, informacji o wysokości opłat, innych pism) dotyczących karty danego podatnika z możliwością ich automatycznego pobrania (w przypadku dokumentów „tradycyjnych” elektroniczna kopia w formacie pdf, a w przypadku dokumentu elektronicznego oryginał),    4. systemu FK: 9. wysokości należności fakturowanych w obrębie systemu finansowo-księgowego, 10. informacja o źródle pochodzenia opłaty (numer faktury lub decyzji, numer konta w systemie FK, terminy płatności oraz wysokość należnej kwoty do zapłaty z wyliczonymi na dany dzień należnymi odsetkami, opisu płatności). 11. Moduł musi umożliwiać przejrzystą prezentację należności z uwzględnieniem sald poszczególnych rat, terminów ich płatności oraz wysokości odsetek wraz z kosztami upomnień. 12. Moduł musi zapewniać wyliczanie ogólnej kwoty należności. 13. Moduł musi generować automatycznie informacje z systemów dziedzinowych o dokonanych wpłatach i dawać możliwość przeglądania zobowiązań wg. zbliżających się terminów zapłaty należności. 14. Moduł musi umożliwiać dokonywanie wpłat zarówno dla użytkowników zalogowanych, jak i tych którzy nie posiadają konta na Portalu. W przypadku użytkowników niezalogowanych identyfikacja ich dokonywana jest na podstawie numeru z dokumentu ustalającej dane zobowiązanie i system wypełnia dowód wpłaty tylko w zakresie opisu należności i podania odpowiedniego konta, na które należy dokonać zapłatę. 15. System musi posiadać możliwość zintegrowania z co najmniej z dwoma systemami płatniczymi. Systemy płatnicze powinny posiadać zezwolenie Komisji Nadzoru Finansowego na świadczenie usług płatniczych w charakterze krajowej instytucji płatniczej lub realizować bezpośrednie płatności z konta płatnika na rachunek urzędu. 16. System musi pozwalać na wnoszenie opłat za pośrednictwem systemu płatności elektronicznych w sposób umożliwiający wygenerowanie płatności na wybraną należność i jej opłacenie, lub na zaznaczenie kilku rat należności i zapłacenie ich jednym przelewem. 17. System musi dawać możliwość sortowania wyświetlanych danych rosnąco lub malejąco względem wyświetlanych parametrów należności. 18. Możliwość wyszukiwania lub filtrowania należności według ich rodzajów, typów, dat. 19. Możliwość przeglądu operacji księgowych już zrealizowanych tzn. opłaconych (wpłaty, zwroty, przeksięgowania). 20. Przegląd operacji księgowych już zrealizowanych na należnościach (wpłaty, zwroty, przeksięgowania) z wyszczególnionym informacji na jakie należności została zaksięgowana oraz salda pozostałego do zapłaty. 21. Jeśli należność jest płatna w ratach (np. należności podatkowe, opłaty za gospodarowanie odpadami należności rozłożone na raty) system musi przedstawiać klientowi informację, którą ratę kwota płatności stanowi. 22. System musi posiadać mechanizmy kontroli i bezpieczeństwa chroniące użytkowników przed kilkukrotnym wniesieniem płatności z tego samego tytułu. System musi generować komunikaty informujące i/lub ostrzeżenia wizualne dla użytkownika podczas próby ponownego zlecenia płatności dla należności, dla których płatność została zlecona za pośrednictwem Portalu, a transakcja jeszcze jest przetwarzana. 23. System musi dawać możliwość wydrukowania wypełnionego polecenia przelewu bankowego dla zaznaczonej należności. 24. System musi dawać możliwość wysyłania przypomnień o terminie płatności za pośrednictwem systemu komunikacji elektronicznej z interesantem, w tym: możliwość zaznaczenia, ile dni przed terminem płatności powinna być wysłana informacja przypominająca, (wymagane kanały komunikacji elektronicznej: email, sms, komunikat push na aplikację mobilną). 25. Wygenerowane płatności zlecone za pośrednictwem systemu, ale jeszcze nie zaksięgowane muszą zawierać informacje takie jak: nr konta bankowego na które została przelana płatność, kwota i data zlecenia, status zlecenia oraz data wykonania.   Poniższe funkcjonalności mają zapewnić możliwość wysyłania przez system spersonalizowanych komunikatów do użytkowników. Mogą być realizowane przez aplikację eNależności lub przed inne rozwiązanie współpracujące z nią.   1. System ma zapewnić możliwość przesyłania spersonalizowanych komunikatów do petentów urzędu generowanych na podstawie zdarzeń występujących w systemach dziedzinowych oraz komunikatów wprowadzonych „ręcznie” przez administratora systemu. 2. System powinien posiadać jedną wspólna kartotekę komunikatów zawierającą informację o treści komunikatu, źródło jego pochodzenia, dacie zapisania do rejestru, identyfikację odbiorcy, datę i godzinę wysłania, datę ważności komunikatu oraz identyfikację kanału którym został on przesłany. 3. Administrator systemu musi mieć dostępny edytor wzorów treści dla określonych typów komunikatów oraz wybranego kanału dystrybucji. 4. W systemie powinny być dostępne kanały komunikacyjne za pośrednictwem SMS-a, e-maila oraz komunikatu push aplikacji mobilnych. 5. Wysyłanie komunikatów powinno być wykonywane wg. kryteriów (kalendarzy) określonych przez administratora dla każdego kanału oddzielnie. 6. System powinien współpracować z modułami dziedzinowymi w zakresie powiadamia co najmniej o:    1. Zbliżającym się terminie płatności zobowiązania    2. Przypomnienie o zaległościach    3. Wystawienie nowego dokumentu dla użytkownika na portalu (decyzja, zaświadczenie, informacja itp.)    4. Dokonanie księgowania na koncie podatnika (zaksięgowanie wpłaty, przeksięgowanie nadpłat, dokonanie przypisu lub odpisu należności, wystawienie upomnienia) 7. Zbliżającym się termin wywozu odpadów z podaniem rodzajów odbieranych odpadów 8. Przesyłanie powiadomień wybranym przez użytkownika kanałem z uwzględnieniem wybranej przez niego tematyki i terminarza odbywa się automatycznie. |

## Oprogramowanie do e-usług – PSZOK

|  |
| --- |
| System ma umożliwiać obsługę klientów Punktu Selektywnej Zbiórki Odpadów prowadzonego przez Gminę.  System musi zostać połączony z systemami dziedzinowymi, skąd powinien pobrać dane o osobach upoważnionych do oddawania odpadów do PSZOK oraz z systemem obsługi należności.  Wymagania minimalne wobec systemu:   1. Rejestracja danych klientów PSZOK 2. Rejestracja przyjęć odpadów do PSZOK (dane nieruchomości, dane transportującego, data, rodzaje odpadów, ilości i wagę poszczególnych rodzajów odpadów), 3. Definiowanie, bieżące przeliczanie i egzekwowanie limitów ilości na poszczególne rodzaje odpadów. W zależności od ustawień możliwe jest blokowanie przyjęć w przypadku przekroczenia limitu na odpad dla danej nieruchomości bądź naliczenie opłaty wg przyjętego cennika dla ilości ponad limit. 4. Integracja 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. Rejestracja przekazań odpadów z PSZOK 6. Prowadzenie stanów magazynowych PSZOK dla poszczególnych rodzajów odpadów, 7. Integracja z systemem BDO 8. Przeliczanie i raportowanie wykorzystania limitów dla poszczególnych nieruchomości 9. Wgląd w historię przyjęć dla poszczególnych klientów i nieruchomości 10. Raporty i zestawienia (przyjęcia wg odpadów, przyjęcia wg klientów, lista największych klientów, przekazania wg odpadów) 11. Współpraca z czytnikami kodów kreskowych pozwalająca na odczytywanie aktualnych danych o klientach i nieruchomościach z bazy gminy na podstawie kodu kresowego (odczytywanego z naklejek z kodami kreskowymi lub kart mieszkańca). 12. Współpraca z wagami elektronicznymi w zakresie automatycznego przenoszenia bieżącego odczytu z wagi. 13. Definiowanie użytkowników z różnymi poziomami uprawnień: Administrator, Kierownik, Gmina, Operator. 14. Możliwość definicji dowolnej ilości magazynów, punktów przyjęć odpadów, adresów IP pozwalających na dostęp do aplikacji. 15. Aplikacja zbudowana zgodnie z wymogami RWD, dostępna na dowolnym urządzeniu wyposażonym w przeglądarkę internetową (Komputer PC, Laptop, Tablet, tel. komórkowy). |

## Elektroniczny Obieg Dokumentów

|  |
| --- |
| Głównym celem zamówienia jest dostarczenie rozwiązania klasy EZD , które służyć będzie Zamawiającemu do realizacji zadań wynikających z instrukcji kancelaryjnej oraz wspierać działalność Zamawiającego w różnych obszarach biznesowych. Dostarczony System Elektronicznego Obiegu Dokumentów (SEOD) będzie obsługiwał obieg korespondencji, prowadzenie spraw. SEOD będzie możliwy do integracji w przyszłości z innymi systemami dzięki posiadanym interfejsom komunikacyjnym.  SEOD musi posiadać budowę modułową pozwalającą na wsparcie zadań jednostki we wskazanych zakresach.  SEOD musi posiadać interfejsy komunikacyjne, rozumiane jako specyfikacje wytycznych, jak powinna przebiegać interakcja między komponentami programowymi, na styku z aplikacjami zewnętrznymi.  SEOD w ramach zamówienia powinien zostać zintegrowany z:   * elektroniczną platformą usług administracji publicznej ePUAP, * Platformą Elektronicznego Fakturowania PEF, * Elektronicznym Nadawcą (aplikacja udostępniana przez Pocztę Polską), * Innymi wskazanymi w dokumencie.   Wymagania technologii systemu SEOD:   * SEOD ma działać w dowolnej sieci komputerowej TCP/IP, * Interfejs użytkownika oparty na przeglądarkach internetowych, * Serwer bazy danych musi być możliwy do rozdzielenia od serwera aplikacji, * SEOD winien zapewnić wysoki poziom bezpieczeństwa danych i użytkowania systemu, * SEOD musi działać w modelu trójwarstwowym, * SEOD ma mieć strukturę modułową, * SEOD musi pozwalać na wykonywanie kopii bezpieczeństwa, * SEOD musi zapewniać jednoznaczne przypisanie odpowiedzialności za każdy z dokumentów, * SEOD musi zapewniać jednoznaczną i niepodważalną identyfikację użytkowników pracujących w systemie,   Wymagania warstwy technologicznej:   1. SEOD ma działać w dowolnej sieci komputerowej TCP/IP, 2. SEOD musi działać w modelu trójwarstwowym, 3. SEOD musi pracować na stacji klienckiej poprzez przeglądarki internetowe, Google Chromie, Mozilla Firefox. 4. SEOD musi zapewniać jednoznaczną i niepodważalną identyfikację użytkowników pracujących w systemie, 5. SEOD nie może ograniczać ilości użytkowników którym założono konta SEOD. 6. SEOD musi obsługiwać i przetwarzać dokumenty elektroniczne (pliki je zawierające) w taki sposób, aby nie naruszać ich spójności i integralności oraz zachować ich oryginalną treść. 7. Usterka stacji roboczej w trakcie pracy w systemie nie może spowodować niestabilności pracy systemu dla pozostałych użytkowników. 8. Uprawnienia pracowników w aplikacji muszą być niezależne od systemu uprawnień systemu plików lub systemu operacyjnego lub zastosowanej bazy danych i muszą być tylko i wyłącznie realizowane przez aplikację. 9. Graficzny interfejs użytkownika Systemu (GUI) SEOD musi:    1. być oparty o typowe w systemach internetowych komponenty graficznych interfejsów użytkowników (tj. menu, listy, przyciski, linki, formularze itp.);    2. być wyposażony w pomoc kontekstową;    3. być polskojęzyczny;    4. umożliwiać obsługę polskich liter;    5. umożliwiać użytkownikowi zmianę interfejsu poprzez wybór z listy dostępnych w aplikacji;    6. umożliwiać użytkownikowi zdefiniowanie i wykorzystanie skrótów klawiszowych do wywoływania często użytkowanych funkcji; 10. SEOD musi umożliwiać użytkownikowi zdefiniowanie ekranu powitalnego (startowego), jego układu oraz umieszczenie na nim np. odnośników do stron zewnętrznych. 11. posiadać widok indywidualny, w ramach którego prezentowane będą te informacje, za które odpowiedzialny jest dany użytkownik. Widok ten musi udostępniać informacje o dokumentach prowadzonych przez użytkownika, dla których to dokumentów termin zakończenia realizacji już minął lub termin zakończenia realizacji zadania mija za określoną w konfiguracji systemowej liczbę dni kalendarzowych; 12. wyróżniać na zestawieniach dla użytkownika, dokumentów ze zbliżającym się terminem realizacji oraz terminem, który upłynął; 13. w celu zwiększenia ergonomii wyszukiwania informacji SEOD powinien wyświetlać elementy na listach: pism, spraw i zapewnić możliwość szybkiej filtracji danych oraz sortowania danych; 14. SEOD musi umożliwić definiowanie i wykorzystywanie wartości domyślnych oraz słownikowych dla wybranych pól w formularzach systemowych w miejscach, gdzie wykorzystanie wartości domyślnych znacznie usprawni pracę.; 15. w ramach interfejsu Użytkownik musi posiadać możliwość korzystania ze wszystkich funkcjonalności systemu, które są dla niego udostępnione zgodnie z przypisanymi mu uprawnieniami, 16. uwierzytelnianie użytkowników ma następować na podstawie jednoznacznie przydzielonego identyfikatora (loginu) i hasła, SEOD nie pozwala na przydzielenie tego samego identyfikatora innej osobie. 17. w systemie są rejestrowane wszystkie operacje użytkowników na dokumentach ze wskazaniem nazwy użytkownika, daty operacji, typu operacji. Informacje te są prezentowane użytkownikowi przeglądającemu dokument na żądanie, 18. SEOD musi uniemożliwiać wprowadzanie i modyfikację danych dokumentów i interesantów w sposób anonimowy, 19. SEOD musi posiadać zabezpieczenia danych przed niepowołanym dostępem, dzięki możliwości przydzielania zakresu uprawnień poszczególnym użytkownikom i grupom użytkowników, 20. SEOD musi umożliwiać jednoczesny dostęp do danych przez wielu użytkowników, z ochroną tych danych przed utratą spójności lub zniszczeniem, 21. hasła muszą być przechowywane w systemie w postaci zaszyfrowanej, 22. SEOD ma posiadać mechanizmy bezpieczeństwa polegające na automatycznym generowaniu i weryfikacji sum kontrolnych dla każdego z plików dołączonych w aplikacji przez użytkownika i umożliwiać potwierdzenie jego wiarygodności, 23. SEOD musi zapewniać automatyczne wylogowanie użytkownika po określonym przez administratora czasie bezczynności stacji roboczej, 24. Wykonawca powinien dostarczyć narzędzie służące do wykonywania automatycznej oraz ręcznej kopii zapasowej modułu. Przy kopii automatycznej administrator ma mieć możliwość zdefiniowania konkretnego terminu wykonania kopii lub terminu powtarzającego się cyklicznie. Narzędzie to ma umożliwiać wykonywanie co najmniej dwóch rodzajów kopii:     1. pełną kopię bezpieczeństwa (kopia, która umożliwia przywrócenie systemu wraz z wszystkimi ustawieniami, z bazą danych oraz dokumentami);     2. różnicową kopię (aktualizuje kopię pełną o dane, które uległy zmianie).   **Wymagania warstwy funkcjonalnej:**   1. modułowość aplikacji, 2. rozbudowany system uprawnień i system prowadzenia rejestrów, 3. obsługa obszaru: pism przychodzących, wychodzących, spraw i innych zdefiniowanych w opisach modułów. 4. obsługa obszaru zadań przydzielanych użytkownikom w związku ze sprawami i ad hoc, 5. obsługa podpisu elektronicznego, 6. archiwum zakładowe, 7. udostępnianie kalendarzy, 8. rezerwacje zasobów jednostki, 9. powiadomienia,   **Szczegółowe wymagania warstwy funkcjonalnej:**   1. możliwość elektronicznego obiegu dokumentów wewnątrz poszczególnych działów, komórek, referatów, 2. możliwość organizacji dokumentów w oparciu o klasyfikacje, 3. rejestracja korespondencji na poziomie rejestrów centralnych pism przychodzących wraz z automatyczną prezentacją fragmentów rejestrów dotyczących komórek oraz pracowników – komórkom oraz pracownikom, 4. automatyczne zasilenie dzienników wydziałowych rejestrów przesyłek przychodzących z rejestru centralnego, 5. automatyczne zasilenie dziennika udostępnianego stanowisku merytorycznemu, po dekretacji na to stanowisko, z wydziałowych rejestrów przesyłek przychodzących, 6. rejestracja korespondencji wychodzącej na poziomie pracowników wraz z automatyczną prezentacją stanowiskom kancelarii wysyłkowych utworzonego w taki sposób rejestru centralnego. 7. automatyczna numeracja pism i spraw, 8. możliwość uzupełnienia podstawowych metadanych dokumentów o metadane dodatkowe za pomocą edytora metadanych, 9. możliwość przyjęcia dokumentu do obiegu z różnych źródeł np. skan dokumentu, poczta e-mail, plik wgrany do systemu w różnych formatach (formaty biurowe, format PDF), plik dodany ręcznie do systemu, e-PUAP, 10. możliwość rejestracji dokumentu bez formy źródłowej: rejestracja jedynie metadanych opisujących przesyłkę, 11. możliwość wersjonowania tzn. śledzenie poszczególnych wersji dokumentów z możliwością przywrócenia wersji poprzedniej, 12. możliwość rejestracji pliku źródłowego w dowolnym formacie, bez ograniczeń, 13. zapewnienie wizualizacji plików w formatach pdf, doc i docx bez potrzeby posiadania na komputerze aplikacji do przeglądania plików tego rodzaju 14. możliwość odtworzenia ścieżki obiegu dokumentu i sprawy wraz z wykazem wszystkich wykonanych na nich czynnościach, z oznaczeniem kto i kiedy wykonał czynność, 15. możliwość wyświetlenia treści dowolnego pliku źródłowego, wymogiem jest posiadanie zainstalowanej na stanowisku przeglądarki plików danego rodzaju, 16. SEOD musi posiadać funkcjonalność podpisu elektronicznego, umożliwiający: weryfikację podpisu elektronicznego oraz podpisywanie dokumentów za pomocą podpisu elektronicznego, analogicznie wymóg dotyczy PZ, 17. SEOD musi posiadać model uprawnień nadawanych grupom użytkowników, dotyczący poszczególnych funkcji, modułów, rodzajów dokumentów. 18. SEOD musi zostać zintegrowany z pocztą elektroniczną i dawać możliwość automatycznego wysyłania i przyjmowania dokumentów, co najmniej MS Outlook i Mozilla Thunderbird oraz zawierać wbudowanego klienta poczty elektronicznej. Integracja ze wskazanymi programami pocztowymi musi umożliwiać automatyczne pobranie do systemu wytypowanych wiadomości poczty odebranych i wysłanych w wymienionych programach. Wbudowany klient poczty musi umożliwiać edytowanie oraz wysyłkę maila wraz z załącznikami bezpośrednio z systemu SEOD , wysyłkę w trybie DW oraz UDW. 19. Musi być możliwe automatyczne zarejestrowanie maila który został wcześniej wysłany w jednym z wyżej wskazanych programów pocztowych. 20. SEOD musi umożliwiać generowanie podstawowych statystyk/raportów dotyczących ilości dokumentów, dat, itd., 21. SEOD musi umożliwiać wskazywanie pism i spraw do których użytkownik powinien mieć szybki dostęp i umieszczanie ich na dedykowanej odrębnej liście. 22. SEOD musi zawierać jedną wspólną kartotekę interesantów, stanowiącą słownik dla wszystkich adresatów, nadawców, stron spraw, i innych przypadków użycia interesantów w dokumentacji przetwarzanej w aplikacji. Ewidencja pracowników jednostki prowadzona w module administracyjnym musi automatycznie zasilać kartotekę interesantów. 23. Ewidencja interesantów musi zawierać co najmniej:     1. Rozróżnienie interesantów na osoby fizyczne i instytucje.     2. W przypadku instytucji, wskazanie pracownika reprezentującego instytucję, w tym imię, nazwisko, stanowisko, dział, telefony, faksy, e-mail oraz określenie oddziałów (jednostek podległych) instytucji.     3. Informację o żądaniu otrzymywania albo nieotrzymywania korespondencji poprzez platformę ESP.     4. Dane adresowe, w tym możliwość określenia wielu adresów ze wskazaniem które są korespondencyjnym. Dane adresowe muszą zawierać co najmniej: imię, nazwisko, nazwę firmy/instytucji, nazwę skróconą, ulicę, nr budynku, nr lokalu, skrytkę pocztową, kod pocztowy, pocztę, miejscowość, adres do korespondencji, dane kontaktowe (nr telefonu, nr faksu e-mail), identyfikator interesanta na platformie ePUAP. 24. SEOD musi zapewnić przyporządkowanie interesantów do uprzednio zdefiniowanych grup w celu późniejszego wykorzystania w modułach systemu. 25. Logowanie się do systemu musi być możliwe tylko dla zdefiniowanych użytkowników. 26. SEOD umożliwia uwierzytelnianie i autoryzację użytkowników i w efekcie zalogowanie do aplikacji:     1. Poprzez podanie przez użytkownika pary login i hasło;     2. Poprzez dane udostępnione z domeny (Active Directory). 27. W odniesieniu do każdego użytkownika, SEOD musi prezentować wszystkie stanowiska aktualnie przyporządkowane danemu użytkownikowi, niezależnie od przyczyny przyporządkowania. 28. W ewidencji użytkowników, w odniesieniu do każdego użytkownika, SEOD musi prezentować datę i czas ostatniego logowania do aplikacji. 29. SEOD musi zapewnić prowadzenie bazy interesantów jednostki. 30. SEOD musi posiadać bazę interesantów wykorzystywaną na potrzeby prowadzenia spraw, rejestracji pism, prowadzenia rejestrów. 31. Baza musi być automatycznie uzupełniania w momencie tworzenia pism, spraw o dane interesantów wprowadzane przez pracowników. 32. SEOD musi udostępniać możliwość rejestracji danych interesanta tylko w przypadku posiadania takiego uprawnienia. 33. SEOD musi umożliwiać konfigurację polegająca na zdefiniowaniu wymagalności i kontroli unikalności danych NIP, PESEL, Regon. 34. SEOD musi pozwalać na ustawienie automatycznej zmiany przy rejestracji interesanta, pierwszej wprowadzonej litery na dużą. 35. SEOD musi umożliwiać zablokowanie lub odblokowanie możliwości wprowadzania danych interesantów niezgodnych z bazą Teryt. 36. SEOD musi umożliwiać zdefiniowanie domyślnie pojawiających się na formularzach rejestracji danych, dotyczących interesantów, np. nazwa miejscowości, kod pocztowy, województwa. 37. SEOD musi umożliwiać uprawnionym pracownikom zmianę danych interesantów. Zmiana danych musi być możliwa w dwóch trybach - korekty albo aktualizacji. W trybie korekty, dane interesanta użyte w jakiejkolwiek dokumentacji muszą ulec zmianie odpowiednio do zmian wprowadzonych w ewidencji. W trybie aktualizacji, nowe dane mają być używane tylko w stosunku do nowej dokumentacji wprowadzonej do aplikacji po zmianach wprowadzonych do ewidencji. SEOD musi informować w kontekście dokumentów zarejestrowanych z użyciem poprzednich danych adresowych, że dane zostały zmienione i nie jest to ich najnowsza wersja. 38. SEOD musi umożliwiać pracownikom:     1. Zarządzanie ewidencją interesantów.     2. Tworzenie interesanta na podstawie danych innego interesanta.     3. Odnajdywanie podobnych interesantów oraz ich scalanie.     4. Wydruk zakresu przetwarzanych w aplikacji danych osobowych, wobec danych osób fizycznych, zgodnie z wytycznymi GIODO w tym zakresie.     5. Podgląd całej dokumentacji związanej ze wskazanym interesantem, z poziomu ewidencji interesantów.     6. Generację raportu z informacjami: kto, kiedy, w jakim zakresie dodał, usunął, zmodyfikował dane wskazanego interesanta.     7. Eksport/import danych wskazanego interesanta do/z pliku HML. 39. SEOD musi umożliwiać wykorzystanie słownika danych adresowych we wszystkich formularzach dotyczących danych adresowych. 40. SEOD musi przechowywać historię zmian danych interesanta wraz z informacją, kto, kiedy i jakie dane zmienił, i umożliwiać określenie danych nieaktualnych. 41. Aplikacja, w przypadku korzystania z zasobu słownika danych adresowych, po wskazaniu miejscowości, nr budynku i ewentualnie ulicy, musi automatycznie podpowiadać wartość kodu pocztowego, w tym także w przypadku miejscowości, które nie posiadają ulic albo współdzielą kod pocztowy z inną miejscowością. 42. SEOD nie może uzależniać określenia danych adresowych interesanta od istnienia odpowiednich danych w słowniku danych adresowych. 43. SEOD musi umożliwiać ustawienie domyślnego wyrażenia zgody na przetwarzanie danych osobowych. 44. SEOD musi umożliwiać rejestrowanie informacji o przekazywaniu/udostępnianiu danych osobowych osób fizycznych. 45. SEOD musi zawierać słownik numerów identyfikacyjnych interesantów, z możliwością przyporządkowania wprowadzonej do niego pozycji do: osoby, jednostki, osoby+jednostki, jednostki+jednostki powiązanej. 46. SEOD musi umożliwiać konfigurację powiązań osób, instytucji oraz wskazanie ich funkcji w instytucji oraz poza instytucją. 47. ESOD musi zapewniać zarządzanie wydrukami i wzorcami (szablonami) dokumentów. 48. SEOD musi umożliwiać administratorowi prowadzenie ewidencji szablonów dokumentów oraz wydruków, w tym co najmniej dodawanie, aktualizacje. 49. SEOD musi umożliwiać administratorowi import do aplikacji szablonów dokumentów z edytora tekstowego, co najmniej MS Word. 50. SEOD musi współpracować z co najmniej pakietem MS Office na poziomie przygotowania i edycji dokumentów. SEOD powinien umożliwiać otwarcie dokumentu w MS Office z poziomu Systemu. 51. SEOD musi pozwalać na utworzenie szablonu na podstawie innego szablonu. 52. Szablony dokumentów mają służyć do tworzenia treści pism wychodzących do interesantów oraz być wykorzystywane w tworzeniu treści dokumentów wprowadzanych do rejestrów wewnętrznych. 53. SEOD musi umożliwiać generowanie dokumentów na podstawie szablonów pism używanych obecnie przez Zamawiającego. 54. SEOD musi umożliwiać administratorowi konfigurowanie zawartości szablonów dokumentów dostępnych w systemie. Szablony dokumentów będą składać się z treści stałych przypisanych do szablonu (z możliwością zmiany w momencie tworzenia treści z szablonu) jak i znaczników przyjmujących w trakcie generacji odpowiednią wartość pochodząca z bazy danych (zmiennych), wg uznania administratora. 55. Znaczniki możliwe do wykorzystania we wzorach /szablonach dokumentów to co najmniej:     1. Kod graficzny zawierający identyfikator dokumentu.     2. Data.     3. Znak sprawy.     4. Dane autora pisma.     5. Lista interesantów powiązanych ze sprawą (strony sprawy).     6. Znaczniki umożliwiające rozmieszczenie danych adresowych interesantów w układzie zmieniającym się w zależności od osoby dla której tworzy się dokument: znacznik osoby do której **adresowane jest** pismo, znacznik osoby o której **wspomina się** w piśmie (strony głównej postępowania), lista osób będących informowanymi o piśmie: strony zainteresowane.     7. SEOD musi automatycznie podstawiać i zmieniać zawartość danych adresowych, o których mowa w punkcie wyżej w zależności od tego dla kogo tworzy się egzemplarz pisma. 56. Pliki dokumentów wygenerowane na podstawie szablonu mają być projektem/szkicem dokumentu, generowanie pliku dokumentu musi odbywać się w systemie, a jego dalsza obróbka z poziomu aplikacji zintegrowanej w której automatycznie otworzy się wygenerowany plik (co najmniej MS Word). 57. SEOD musi umożliwiać edycję plików dokumentów w formatach obsługiwanych przez MS Word bezpośrednio z poziomu systemu bez konieczności ich ponownego załączania do bazy danych. 58. Plik dokumentu wygenerowany na podstawie szablonu, musi być automatycznie wprowadzany do formularza dokumentu, a jednocześnie SEOD musi umożliwiać jego lokalny zapis. 59. SEOD musi udostępniać zestawy gotowych raportów (wydruków możliwych do wygenerowania na poszczególnych stronach systemu) zawierających zestawienia wygenerowane na podstawie prezentowanych danych. 60. SEOD ma umożliwiać generację wydruków dostępnych w systemie do pliku w formacie PDF, TXT, RTF, XPS, ODT, Excel, CSV oraz XLS. 61. ESOD musi zapewnić prowadzenie dzienników pism wpływających, wychodzących, spraw oraz opisywanie ich metadanymi. 62. SEOD zarówno dla dokumentów wpływających, jak i wychodzących oraz dokumentów wewnętrznych musi umożliwiać opatrywanie dowolną liczbą metadanych dodatkowych. Administrator musi mieć możliwość tworzenia dowolnej liczby typów dokumentów poprzez przypisanie im odpowiednio spreparowanego formularza, umożliwiającego wprowadzenie odpowiedniego zestawu metadanych. 63. SEOD musi wersjonować dokumentację, w tym zapamiętywać wszystkie informacje dotyczące starszych wersji dokumentacji. Musi być możliwość zapoznać się ze starszą wersją dokumentacji i ewentualnie użyć jej, jako nowej wersji. 64. SEOD powinien umożliwić dodawanie uwag/komentarzy do dokumentu na każdym etapie jego obiegu. SEOD powinien posiadać możliwość przechowywania historii wprowadzanych uwag/komentarzy. 65. SEOD powinien umożliwić kierownictwu opatrywanie uwagami/komentarzami dokumentów podwładnych. 66. SEOD musi umożliwiać uprawnionym użytkownikom: 67. edycję parametrów dokumentacji i w efekcie stworzenie jej nowej wersji, 68. udostępniać informacje o wszystkich egzemplarzach (kopiach) dokumentów wpływających. 69. SEOD musi blokować edycję parametrów dokumentu przekazanego do zatwierdzenia lub skierowanego do wysłania lub już wysłanego, co dotyczy także używania starszej wersji jako nowej. 70. SEOD musi umożliwiać stworzenie wersji roboczej dokumentu wychodzącego i dołączania jej do sprawy, jednakże wersja robocza dokumentu może być dostępna tylko jej twórcy na zestawieniach dokumentów wychodzących, natomiast ma być widoczna dla osoby mającej dostęp do sprawy. 71. SEOD musi umożliwiać prowadzenie postępowania z dokumentami ewidencjonowanymi i metadanymi zgodnie z wymogami określonymi w obowiązujących przepisach prawa. 72. SEOD musi umożliwiać przeglądanie danych opisujących dokumenty i sprawy, mieszczących się w zakresie przewidzianym dla ich minimalnego opisu Systemie Elektronicznego Zarządzania Dokumentacją. Ponadto, SEOD musi udostępniać uprawnionemu użytkownikowi możliwość edycji i uzupełniania tych danych. 73. SEOD musi posiadać predefiniowane rejestry typu: Dziennik podawczy pism przychodzących, Rejestr Przesyłek Wychodzących, Rejestry Spraw, Rejestry Notatek, czyli prezentować widok domyślny w aplikacji, z możliwością zmiany tego widoku przez użytkownika zalogowanego. 74. SEOD musi posiadać definiowalne rejestry: dokumentów wewnętrznych, pism przychodzących, przesyłek wychodzących, spraw. 75. SEOD musi zapewniać prowadzenie dzienników podawczych jednostki. 76. SEOD musi umożliwiać uprawnionemu użytkownikowi rejestrację przesyłek przychodzących w dziennikach podawczych jednostki, zarówno złożonej/nadesłanej w formie tradycyjnej (papierowej) jak i elektronicznej, zgodnie z wymogami instrukcji kancelaryjnej obowiązującej Zamawiającego. SEOD musi umożliwiać przetworzenie dokumentacji w formie tradycyjnej do postaci wtórnego dokumentu elektronicznego (odwzorowania cyfrowego). 77. SEOD musi umożliwiać automatyczne generowanie potwierdzenia przyjęcia przesyłki przychodzącej. 78. SEOD musi zapewnić wielostopniową dekretację oraz możliwość zwrotu przesyłek do miejsc otrzymania. 79. SEOD musi zapewnić tworzenie spraw na podstawie przesyłek, dołączanie ich do spraw już prowadzonych (również zbiorczo), pozostawienie bez rozpatrywania, bezpośrednio z poziomu przesyłki utworzenie odpowiedzi do interesanta (z pominięciem etapu zakładania sprawy). 80. Utworzenie odpowiedzi do interesanta (z pominięciem etapu zakładania sprawy) z poziomu przesyłki wpływającej musi polegać na przejściu do utworzenia automatycznie z pisma przychodzącego, odpowiedzi z automatycznym przekopiowaniem tematu, danych interesanta z metadanych przesyłki wpływającej. 81. SEOD musi pozwalać na utworzenie na podstawie metadanych przesyłki pozycji w rejestrach wewnętrznych. 82. SEOD musi zapewniać definiowanie wielu dzienników podawczych, numerację w obrębie rejestru oraz rejestracje prowadzoną równolegle przez wielu użytkowników. 83. SEOD musi zapewnić predefiniowany widok (domyślny) na Dziennik podawczy pism przychodzących wraz z możliwością późniejszego samodzielnego zdefiniowania widoczności kolumn w rejestrze. 84. SEOD musi umożliwiać definiowanie szablonów ułatwiających rejestrację pism, ich gromadzenie w dedykowanym słowniku i udostępnianie dla danego dziennika (rejestru). 85. Szablony muszą być możliwe do wyposażenia w domyślne dekretacje. 86. SEOD musi umożliwiać podczas rejestracji pism kopiowanie załączonego interesanta w celu wykorzystania w następnym piśmie. 87. SEOD musi umożliwiać rejestrację dat: nadania, wpływu, daty przesyłki. 88. Nawigacja podczas rejestracji powinna być możliwa co najmniej za pomocą myszki i klawiatury. 89. SEOD musi umożliwiać pracownikowi wskazanie szablonu rejestracji z listy lub jeżeli formularz wniosku udostępniony przez urząd był opatrzony kodem kreskowym: wyszukanie szablonu za pomocą odczytania kodu z wniosku przez skaner kodów kreskowych. 90. SEOD musi umożliwiać podczas rejestracji, usunięcie jednym przyciskiem wszystkich już wprowadzonych na formularzu danych. 91. SEOD musi umożliwić przygotowanie szablonów dla pism o wspólnych cechach i wprowadzenie cech domyślnych: temat pisma, klasyfikacja dodatkowa tematyczna, domyślna dekretacja, domyślny termin załatwienia. 92. SEOD musi zapewnić możliwość przygotowania szablonu dedykowanego do rejestracji pism wymagających wielostopniowych zatwierdzeń (faktury do zapłaty). 93. SEOD musi prezentować w odniesieniu do pisma wymagającego wielostopniowych zatwierdzeń (faktura do zapłaty): dane osoby dokonującej zatwierdzenia, datę i godzinę zatwierdzenia oraz możliwość wykonania i prezentacji podsumowującej: zatwierdzenia merytorycznego, formalnego i rachunkowego oraz zatwierdzenia do realizacji opłaty. 94. Upoważnione osoby muszą mieć możliwość zarządzania słownikiem szablonów, wprowadzania nowych, zdejmowania ich z listy widocznych dla użytkowników podczas rejestracji. Musi istnieć możliwość wprowadzenia do słownika szablonu utworzonego na podstawie innego już istniejącego. 95. Musi istnieć możliwość przypisania szablonu do konkretnego rejestru pism przychodzących. 96. Ponieważ dane z pism przychodzących mają posłużyć również do zasilania rejestrów wewnętrznych, musi istnieć w szablonach możliwość określenia jaka data będzie przekazywana do rejestru: nadania pisma, czy wpływu. 97. Ponieważ na podstawie pisma przychodzącego ma być możliwe utworzenie odpowiedzi, z pominięciem rejestracji sprawy, w szablonie musi być możliwe wskazanie rodzaju pisma tworzonego w odpowiedzi. 98. Utworzony szablon musi być możliwy do zmiany danych podczas rejestracji pisma lub nie, co ma wynikać z definicji szablonu. 99. SEOD musi umożliwiać w szablonie wskazanie domyślnej dekretacji lub nie. 100. SEOD musi umożliwiać zawsze podczas rejestracji pisma wskazanie osoby do której będzie dekretacja oryginału. 101. SEOD musi udostępniać możliwość wskazania w szablonie listy osób do których pismo będzie kierowane w trybie do wiadomości. Lista ta w zależności od definicji użytego szablonu będzie prezentowana lub nie pracownikowi rejestrującemu pismo. 102. SEOD w momencie i w związku z rejestracją przesyłki przychodzącej, musi generować unikalny identyfikator przydzielany danej przesyłce i służący do jej identyfikacji w aplikacji. Jednocześnie, SEOD musi generować kod graficzny zawierający w swojej treści unikalny identyfikator. Proces rejestracji wspierany przez aplikację musi przewidywać możliwość naniesienia kodu graficznego i unikalnego identyfikatora na odwzorowanie cyfrowe oraz oryginał tradycyjny przesyłki, bez konieczności edycji odwzorowania cyfrowego. 103. SEOD musi mieć możliwość umieszczania na wydruku z w/w kodem graficznym, identyfikatora w formie numerycznej, numeru wpływu z dziennika podawczego, daty wpływu oraz nazwy Zamawiającego i imienia i nazwiska osoby która dokonała rejestracji, w formie nadruku na etykietę naklejaną na dokument. 104. SEOD musi umożliwiać pełną rejestrację przesyłki przychodzącej w dwu ścieżkach:      1. Czynności opisu przesyłki i tworzenie odwzorowania cyfrowego odbywa się łącznie, w jednym kroku.      2. Czynności opisu przesyłki i tworzenia odwzorowania cyfrowego są podzielone na odrębne kroki, tj. najpierw wstępne opisanie przesyłki, generacja unikalnego identyfikatora i wydruku z kodem graficznym, następnie odwzorowanie cyfrowe i dokończenie opisu. 105. SEOD musi umożliwiać wstępną rejestrację przesyłki przychodzącej ograniczoną do wprowadzenia daty wpływu, wygenerowania wydruku zawierającego kod graficzny, numer i datę wpływu. W tym wypadku uprawniony użytkownik musi mieć możliwość dokończenia rejestracji. 106. SEOD musi umożliwiać rejestrowanie przesyłek przychodzących, których pracownicy rejestrujący nie otwierają. Użytkownik merytoryczny musi mieć możliwość dokończenia rejestracji. 107. SEOD musi umożliwiać w trakcie rejestracji powiązywanie w dowolnej liczbie z opisem przesyłki przychodzącej (na etapie wypełniania formularza) wybranych interesantów (z ewidencji interesantów). 108. SEOD musi umożliwiać rejestrację pisma głównego i załączników oraz odróżniać je graficznie. 109. SEOD musi prezentować w rejestrze przesyłek ilościowe podsumowanie załączników dla każdej z przesyłek z możliwością przejścia do ich szczegółów. 110. SEOD musi umożliwiać użytkownikowi jednoczesne powiązywanie wielu plików (załączników), do formularza rejestracji przesyłki przychodzącej. Powiązanie musi następować poprzez zaznaczenie wielu plików z dysku i automatyczne przepisanie ich nazw do nazw załączników nadawanych w systemie. Nie może istnieć ograniczenie do pojedynczego wprowadzania wielu plików do formularza. 111. SEOD musi również umożliwiać rejestrowanie odrębnie poszczególnych załączników: opisywanie każdego po kolei przez wskazywanie pojedynczych plików i odnotowanie dowolnej nazwy każdego załącznika, czyli nazwy nie pochodzącej z nazwy pliku na dysku. 112. Załączniki wprowadzone w każdy z powyższy sposób muszą być prezentowane graficznie w jednej sekcji formularza. 113. SEOD musi próbować automatycznie rozpoznać interesanta (twórcę i nadawcę) i dołączyć do formularza przesyłki przychodzącej na podstawie:informacji o koncie/skrytce nadawcy w platformie ESP interesanta, spośród interesantów już zarejestrowanych w ewidencji. Jeśli rozpoznany interesant nie zostanie odnaleziony w ewidencji (np. nadesłał przesyłkę pierwszy raz), SEOD musi automatycznie go wprowadzić do ewidencji i dołączyć do formularza. Jeśli automatyczne rozpoznanie nie będzie możliwe, SEOD musi pozwolić na jego rejestrację. 114. Procedura rejestracji przesyłki przychodzącej musi umożliwiać użytkownikowi rejestrującemu jednoczesne wskazanie wielu odbiorców wewnętrznych, którym przesyłka ma zostać przekazana. Przesyłki mogą być przekazywane zarówno stanowiskom jak i komórkom, z oznaczeniem kto otrzymuje dokument będący oryginałem, a kto dostaje go w trybie do wiadomości. 115. SEOD musi pozwalać na weryfikację podpisu elektronicznego w każdym momencie, również przed rejestracją przesyłki przychodzącej, bez konieczności uruchamiania dodatkowego zewnętrznego oprogramowania. SEOD musi weryfikować podpisy w standardzie XAdES oraz profil zaufany ePUAP. 116. SEOD musi umożliwiać pozostawienie przesyłki przychodzącej bez rozpatrzenia oraz przywrócenie jej do rozpatrzenia. 117. SEOD musi umożliwiać przekazywanie i obieg dokumentacji wewnątrz, pomiędzy komórkami organizacyjnymi i pracownikami. 118. SEOD powinien zarządzać pełnym cyklem obiegu dokumentów – od przyjęcia korespondencji w Biurze Obsługi Interesanta do wydania decyzji administracyjnej. 119. SEOD musi automatycznie zasilać wydziałowe dzienniki przesyłek przychodzących z zewnątrz, przesyłek wychodzących na zewnątrz, dokumentacji wewnętrznej przesyłanej między komórkami i stanowiskami. Dzienniki musza być dostępne do podglądu dla każdej komórki organizacyjnej. Dzienniki wydziałowe muszą być wycinkiem Dzienników urzędowych dotyczącym danej komórki. 120. SEOD musi umożliwiać generację dzienników wydziałowych w różnych układach, co najmniej:      1. tylko dokumentacja przychodząca do danej komórki,      2. tylko dokumentacja wychodząca z danej komórki,      3. tylko dokumentacja przychodząca z innych komórek (pisma nie będące pismami pochodzącymi z zewnątrz ale korespondencją wymienianą miedzy wydziałami) w układzie chronologicznym. Dokumentacja przychodząca musi być oddzielnie prezentowana od dokumentacji wychodzącej z/do komórki. 121. Książka wydziałowa w Systemie SEOD musi rozróżniać pisma wpływające i wypływające do/z komórek organizacyjnych. 122. SEOD musi umożliwiać generację wydruku dziennika wydziałowego w wybranym układzie. 123. SEOD musi umożliwiać wielopoziomową dekretację w pionie oraz w poziomie. 124. Musi być możliwe utworzenie szablonu (formatki) rejestracji pisma wpływającego z już domyślnie wprowadzoną dekretacją. 125. Musi być możliwe utworzenie szablonu (formatki) rejestracji pisma wpływającego bez domyślnie wprowadzonej dekretacji. Użytkownik podczas rejestracji musi mieć możliwość dekretacji i musi mieć możliwość uzyskania informacji o obciążeniu poszczególnych stanowisk. 126. Każdy z użytkowników biorących udział w dekretacji musi mieć możliwość wykonywania dekretacji w pojedynczym dokumencie oraz zbiorczych. 127. Dekretacje zbiorcze muszą polegać na wskazaniu odbiorcy i oznaczaniu poszczególnych pism które będą do niego kierowane. 128. Dekretacja pisma musi być zakończona przekazaniem pisma do osoby/komórki z możliwym wydrukiem. 129. SEOD musi umożliwiać opatrzenie pisma treścią dekretacji i złożenie podpisu elektronicznego. 130. SEOD musi udostępniać narzędzie do obiegu formatki akceptacji faktur i prezentować kto i kiedy zatwierdził fakturę merytorycznie, rachunkowo i dokonał zatwierdzenia do zapłaty. 131. SEOD musi umożliwiać przekazanie dokumentacji dowolnej liczbie pracowników lub komórek organizacyjnych lub oznaczanie jako przekazanych jednostkom organizacyjnym Zamawiającego niepracującym w aplikacji. Pracownik dekretujący musi mieć możliwość wskazania, który z wybranych odbiorców, jest merytoryczny a którzy pełnią funkcje pomocnicze w kontekście danej dokumentacji (do wiadomości). Do odbiorcy merytorycznego trafia oryginał dokumentu. 132. Dokumentacja przekazana do komórki organizacyjnej, musi trafiać do kierownika komórki, do dalszej dekretacji, natomiast dokumentacja przekazana bezpośrednio do stanowiska musi trafić do tego stanowiska. 133. SEOD musi automatycznie przydzielać kierownikom poszczególnych komórek dokumentację przekazaną na komórkę do dalszej dekretacji. Dokumentacja ta ma być prezentowana na odrębnym zestawieniu. 134. Dekretacja musi umożliwiać nadanie terminów realizacji wg uznania pracownika dekretującego. 135. SEOD musi umożliwiać stanowisku któremu przydzielono dokumentację, wycofanie jej do osoby która ją dekretowała (również w przypadku dekretacji wielostopniowej). Wycofanie musi być możliwe w każdym momencie przed założeniem sprawy lub oznaczeniem dokumentacji jako nietworzącej akt sprawy. 136. SEOD musi umożliwiać jednoczesną dekretację w stosunku do kilku dokumentacji, z wyborem stanowisk, komórek, . 137. Po otrzymaniu dokumentacji do merytorycznego rozpatrzenia, w przypadku braku opatrzenia danej dokumentacji obowiązkowymi metadanymi, SEOD musi automatycznie poinformować użytkownika o braku odpowiednich danych i konieczności ich uzupełnienia. 138. SEOD musi zapewnić obsługę odpowiedzi kierowanej do interesanta. 139. SEOD musi umożliwiać uprawnionemu użytkownikowi akceptację wstępną i ostateczną odpowiedzi do interesanta (dokumentacji), w tym wielopoziomową w pionie oraz w poziomie z uwzględnieniem posiadanych uprawnień, wraz z podpisaniem elektronicznym. 140. SEOD musi domyślnie podpowiadać użytkownikowi osobę bezpośredniego przełożonego jako akceptującego dokumenty. 141. SEOD musi pozwalać użytkownikowi na budowanie własnej listy osób akceptujących, poprzez wskazanie ich ze struktury organizacyjnej. Osoby wskazane muszą być zapamiętywane na takiej liście, musi być również możliwe usunięcie ich z listy. Tak przygotowana lista musi być prezentowana użytkownikowi podczas kierowania kolejnych pism do akceptacji. 142. SEOD musi pozwalać akceptującemu na: zmiany w dokumencie, podpisanie dokumentu, oznaczenie go jako niezaakceptowanego, akceptację, skierowanie pisma do kolejnych osób do akceptacji i to zarówno w sytuacja gdy bieżąca osoba akceptująca zaakceptowała dokument jak i gdy go nie zaakceptowała. 143. SEOD nie może umożliwiać pracownikowi przydzielającemu wycofanie dokumentacji przekazanej do akceptacji, ta czynność musi być wykonana z inicjatywy osoby która dostała dokument do akceptacji. Autor dokumentu musi mieć po zwrocie dokumentu z akceptacji możliwość wskazania nowego pracownika akceptującego. 144. SEOD na żądanie użytkownika musi informacje kto i kiedy dokonał akceptacji. 145. Pracownik będący autorem otrzymujący zwrotnie zaakceptowany już dokument, musi mieć możliwość ponownego skierowania go do akceptacji, do wysyłki bądź np. Odłączenia go od sprawy. 146. SEOD musi pozwalać na wskazanie go jako systemu EZD w jednostce i w związku z tym musi zapewniać obsługę składów chronologicznych. 147. SEOD musi posiadać funkcje umożliwiające przejście na w pełni elektroniczne prowadzenie spraw. 148. SEOD musi umożliwiać prowadzenie w jednostce składów chronologicznych oraz składów nośników. SEOD musi umożliwiać administratorowi tworzenie składów chronologicznych dla pism wpływających i dla pism wysyłanych. 149. SEOD musi umożliwiać administratorowi zdefiniowanie, nazwy składu, jego rodzaju, zakresu odwzorowania korespondencji w nim umieszczonej. 150. Numeracja w składach ma być automatyczna. 151. W odniesieniu do każdego ze zdefiniowanych składów musi być możliwe oznaczenie sposobu przyjmowania na stan składu: automatyczne czy ręczne. 152. Oznaczenie „ręcznego” przyjęcia na stan składu musi umożliwiać zarejestrowanie pozycji w składzie, a w następnym kroku odnotowanie przez pracownika fizycznie prowadzącego skład przyjęcia na stan składu. 153. Oznaczenie „automatycznego” przyjęcia na stan składu musi umożliwiać zarejestrowanie pozycji w składzie z jednoczesnym oznaczeniem pozycji jako już widniejącej fizycznie na stanie składu. 154. SEOD musi nadawać każdej przesyłce przyjętej do składu numer w składzie. 155. Jeżeli do składu przyjmowana jest korespondencja która posiada np. załączniki, to musi być możliwe umieszczenie ich w innym składzie niż pismo przewodnie. 156. Numer w składzie musi wynikać z numeracji nadanej przesyłce w składzie. Nie może to być numer taki sam jak numer wynikający z numeracji w Rejestrze Przesyłek Wpływających lub Rejestrze Przesyłek Wychodzących. SEOD musi zapewnić wzajemne wskazanie (powiązanie) na siebie obu numerów. 157. SEOD musi zapewniać osobie prowadzącej skład możliwość przeglądania pozycji składów z podziałem na poszczególne składy. 158. SEOD musi zapewnić osobie prowadzącej skład widok na wszystkie pisma w danym składzie i prezentować na zestawieniu jej udostępnianym: numer w składzie, numer w rejestrze źródłowym (przesyłek przychodzących lub wychodzących) z możliwością sortowania widoku po obydwu polach. 159. SEOD musi zapewniać obsługę wypożyczeni ze składu, wycofanie pozycji ze składu. 160. SEOD musi zapewniać dla każdej przesyłki możliwość wydruku etykiety przesyłki ze składu. 161. Przyjęcie na stan składu musi oznaczać automatyczne umieszczenie (przypisanie logiczne) pisma do otwartego pudła. 162. Brak otwartego pudła nie może powodować nieprzyjęcia pozycji do składu. Pozycje nieprzypisane do pudła, w momencie otwarcia pudła obsługującego dany rodzaj składu muszą automatycznie zostać przypisane do odpowiedniego pudła. 163. SEOD musi pozwalać w zależności od pracownika obsługującego zamknięcie pudła i odnotowanie otwarcia kolejnego pudła oraz odnotowanie zapakowania pudła po którym następuje określenie i wyświetlenie w systemie skrajnych numerów z rejestru składów znajdujących się w pudle, dat skrajnych przesyłek oraz liczby pism na stanie pudła wraz z możliwością wydruku etykiety na pudło. 164. SEOD musi zapewnić prowadzenie spraw w jednostce. 165. SEOD musi umożliwiać założenie sprawy na podstawie każdego dokumentu. 166. Numeracja spraw musi być automatyczna. 167. SEOD musi nadawać numer sprawie pochodzący ze spisu spraw dla wskazanej teczki JRWA. 168. SEOD musi umożliwiać zmianę przyporządkowania sprawy do teczki i co za tym idzie zmianę numeru w sprawie. 169. SEOD musi umożliwiać założenie sprawy na podstawie przesyłki przychodzącej, wychodzącej, dokumentu wewnętrznego, wiadomości e-mail, notatki, a także bez konieczności dołączania jakiegokolwiek dokumentu. 170. Na parametry sprawy składają się co najmniej: znak sprawy, opis, data wszczęcia, data zakończenia (narzucony termin i rzeczywista data zakończenia), stanowisko merytoryczne, współpracujący i zdefiniowane zakresy współpracy, status, przypisane zlecenia, akta sprawy. 171. SEOD musi umożliwiać wskazanie jako współprowadzący sprawę: osób, wydziałów. 172. SEOD musi zapewnić możliwość zdefiniowania współpracy (współprowadzenia) która musi dotyczyć: dodawania dokumentów do sprawy (pism przychodzących i wychodzących), interesantów, zmiany parametrów opis, status sprawy. 173. SEOD musi zapewnić możliwość prezentacji na dedykowanym ekranie kierownikowi wydziału wszystkich spraw w których jego wydział został wskazany jako współprowadzący. 174. SEOD musi zapewnić kierownikowi wydziału z dedykowanego ekranu przejść do opcji dekretacji sprawy na wybranego pracownika. Mechanizm musi być niezależny od mechanizmu dekretacji pism wpływających. 175. SEOD musi umożliwiać łączenie ze sprawą jednocześnie wielu dokumentów pochodzących z opisanych rejestrów. 176. SEOD musi również umożliwiać łączenie ze sprawą plików wskazanych ze stacji roboczej z automatycznym przepisaniem ich nazwy i prezentację w szczegółach sprawy na odrębnym widoku. 177. SEOD musi umożliwiać nadanie znaku sprawie tylko i wyłącznie w formie zgodnej z obowiązującą instrukcją kancelaryjną. SEOD musi posiadać również mechanizmy globalnego definiowania numeracji spraw, tj. być przygotowana na zmiany znakowania spraw, gdyby w przyszłości była taka potrzeba. 178. SEOD musi udostępniać mechanizmy ustalania punktów w strukturze organizacyjnej według których będą numerowane i gromadzone sprawy: punkty zbiorcze. 179. SEOD musi prezentować użytkownikowi spisy spraw z danej teczki. 180. SEOD musi zapewnić predefiniowany widok (domyślny) na rejestr spraw wraz z możliwością późniejszego samodzielnego zdefiniowania widoczności kolumn w rejestrze. 181. SEOD musi umożliwiać wydzielenie zbioru spraw podczas zakładania sprawy, czyli uznania że sprawa będzie zakładana w podteczce. 182. Mechanizm zakładania podteczek nie może się opierać na rozbudowie słownika Jednolitego Rzeczowego Wykazu Akt. 183. Mechanizm zakładania spraw musi pozwalać przy zakładaniu sprawy przez pracownika oznaczenie, że właśnie zakładana sprawa będzie stanowiła sprawę w podteczce 184. Mechanizm prezentowania spisów spraw danej teczki musi pozwalać na przejrzenie jednocześnie zawartości całego spisu spraw teczki razem z pozycjami spisu pod którymi zostały zarejestrowane podteczki. 185. Mechanizm prezentowania spisów spraw musi pozwalać na przeglądanie zawartości spisów spraw podteczek we wskazanej teczce bez potrzeby rozwijania zawartości każdej z podteczek. 186. Mechanizm prezentowania spisów spraw we wskazanej teczce musi umożliwiać przełączanie widoku spisu spraw teczki na widok: prezentujący spis spraw teczki, widok prezentujący spis spraw teczki wraz z prezentacją spisów spraw we wszystkich założonych podteczkach. Musi istnieć mechanizm umożliwiający sprawne przechodzenie między tymi widokami. Mechanizm nie może polegać na odrębnym otwieraniu zawartości poszczególnych podteczek. 187. Zamawiającemu szczególnie zależy aby pracownik przeglądając spisy prowadzonych spraw mógł w sprawny sposób przejść do tworzenia odpowiedzi w danej sprawie. Stąd wymogiem jest aby przejście do tworzenia odpowiedzi w danej sprawie było ograniczone do maksymalnie 2 kliknięć. 188. SEOD musi umożliwiać pracownikowi prowadzącemu sprawę dołączanie do niej różnych dokumentów i wiązanie relacjami z tą dokumentacją. 189. SEOD musi umożliwiać określenie osób i komórek pracujących nad sprawą, przez – prowadzącego sprawę. 190. SEOD musi automatycznie nadawać uprawnienia do dostępu do sprawy osobie zakładającej sprawę w systemie oraz umożliwiać zmianę zakresu dostępu dodatkowym osobom/komórkom upoważnionym do sprawy przez stanowisko merytoryczne. Osoby upoważnione do sprawy (stanowiska pomocnicze) muszą domyślnie uzyskiwać uprawnienia do dodawania dokumentów do sprawy. Stanowisko merytoryczne udostępniające do współprowadzenia sprawę innym stanowiskom pomocniczym musi mieć możliwość ustawienia zakresu dostępu do każdego dokumentu składającego się na akta sprawy oddzielnie, a także określenie czy zakres udostępnienia obejmuje:      1. odejmowanie dokumentów ze sprawy,      2. potwierdzanie komentarzy do sprawy,      3. zarządzanie listą interesariuszy sprawy      4. zawieszanie postępowania,      5. dodawanie i usuwanie zadań związanych ze sprawą,      6. uzupełnianie metadanych sprawy      7. zmianę parametrów sprawy. 191. SEOD musi umożliwiać stanowisku merytorycznemu przydzielanie sprawy innemu stanowisku w dowolnym momencie. SEOD musi umożliwiać przekazanie w całości sprawy do prowadzenia innemu pracownikowi wraz z automatycznie generowanym w systemie wydrukiem będącym zestawieniem dokumentów przekazywanych razem ze sprawą. 192. SEOD musi umożliwiać uprawnionym użytkownikom monitorowanie całości spraw prowadzonych przez inne stanowiska. 193. SEOD musi odrębnie prezentować sprawy: bieżące, , zamknięte, sprawy każdego z podwładnych , sprawy całej komórki. Widoki na sprawy muszą prezentować konkretne teczki 194. Po zamknięciu sprawy w systemie, co wiąże się z zakończeniem prac nad sprawą – możliwy ma być tylko:      1. podgląd,      2. ponowne otwarcie,      3. archiwizacja. 195. SEOD musi gromadzić akta spraw w teczki, grupować sprawy w zbiory (podteczki jeśli występują) oraz umożliwiać wydrukowanie spisów spraw zgodnie z obowiązującą Zamawiającego instrukcją kancelaryjną. Teczka sprawy musi przechowywać wszystkie wersje dokumentacji. 196. SEOD musi umożliwiać stanowisku posiadającemu dostęp do sprawy określenie statusu sprawy, który może być upubliczniany w dowolnym BIP. SEOD musi udostępniać mechanizmy integracji z dowolnym BIP. 197. SEOD musi umożliwiać wskazywanie wszystkich interesariuszy w odniesieniu do każdej sprawy z osobna. 198. SEOD musi pozwalać na jednoczesne zamknięcie wszystkich spraw w teczce rozumiane jako wybranie funkcji „zamknij” wszystkie widoczne bieżące sprawy. 199. SEOD musi zapewnić wsparcie dla użytkownika podczas tworzenia i wysyłki korespondencji na zewnątrz. 200. SEOD musi umożliwiać tworzenie pism wychodzących z poziomu pracowników prowadzących sprawy oraz bez powiązania ze sprawami. 201. SEOD musi prowadzić Rejestr Przesyłek Wychodzących. 202. SEOD musi zapewniać zasilenie rejestru z pliku CSV. 203. SEOD musi pozwalać na rejestrację pism wychodzących: w formie tradycyjnej, e-maili, dokumentów elektronicznych kierowanych na platformę ePUAP. 204. SEOD musi umożliwiać tworzenie odpowiedzi na pismo bezpośrednio z pisma które wpłynęło, bez rejestracji sprawy. 205. SEOD musi umożliwiać ewidencjonowanie różnego rodzaju pism i ich automatyczną numerację. 206. Pisma które zostały utworzone w sprawach mają mieć numer pochodzący ze sprawy. Pisma nie przydzielone do spraw mają mieć numery tymczasowe. 207. SEOD musi posiadać szereg słowników umożliwiających opisanie przesyłek, co najmniej: słownik rodzajów pism, słownik sposobów wysyłki, słownik operatorów pocztowych, cennik, słownik uwag na zwrotkach, klasyfikacja tematyczna. 208. SEOD musi posiadać możliwość wielostopniowej akceptacji pism wraz z możliwością składania podpisów kwalifikowanych podczas akceptacji lub wykorzystania Profilu Zaufanego. 209. SEOD musi pozwalać na dynamiczne budowanie list osób akceptujących, czyli umieszczać na liście zawsze bezpośredniego kierownika, z możliwością dodania lub usunięcia dowolnych pracowników z domyślnej listy akceptacyjnej. Pracownik kieruje do akceptacji pismo wskazując osobę z listy akceptacyjnej. Na czas akceptacji pracownik (twórca pisma) traci możliwość zmian w piśmie, uzyskuje je osoba akceptująca. 210. Osoba akceptująca może zwrócić pismo lub skierować dalej do akceptacji korzystając z możliwości wyboru z własnej listy osób akceptujących. 211. Osoba akceptująca musi mieć możliwość wykonywania zmian w treści załączonego pliku. 212. Osoba akceptująca musi mieć możliwość oznaczenia pisma jako nieakceptowalne i zwrotu do właściciela. 213. SEOD musi udostępniać możliwość kierowania pism do miejsca wysyłki, czyli dowolnej komórki zdefiniowanej przez administratora jako zajmującej się wysyłką. 214. SEOD musi umożliwiać odbiór osobisty u pracownika. 215. SEOD musi umożliwiać oznaczenie pisma jako odebrane osobiście przez interesanta, 216. SEOD musi prezentować pisma przeznaczone do odbioru osobistego na dedykowanym zestawieniu. 217. SEOD musi umożliwiać kierowanie w jednym kroku pisma na zewnątrz (do interesanta) i jednocześnie do osób ze struktury organizacyjnej jednostki (pismo wewnętrzne). 218. SEOD musi umożliwiać wzajemne wskazanie na siebie pism, tak żeby można było sprawdzić do jakich osób ze struktury organizacyjnej poszło pismo, oraz z jaką pozycją z rejestru przesyłek wychodzących jest powiązane pismo wewnętrzne. 219. SEOD musi pozwalać na grupowe zmiany statusów pismom, grupowe kierowane pism do kancelarii wysyłkowej, grupowe pospisywanie podpisem kwalifikowanym, grupowe zmiany sposobu wysłania pism. 220. SEOD musi zapewnić predefiniowany widok (domyślny) na rejestr przesyłek wychodzących wraz z możliwością późniejszego samodzielnego zdefiniowania widoczności kolumn w rejestrze. 221. SEOD musi zapewnić możliwość wysyłki odpowiedzi na ePUAP. 222. SEOD musi umożliwiać użytkownikowi kierującemu dokument do konta/skrytki platformy ePUAP na stworzenie treści odpowiedzi. 223. SEOD musi wspomagać doręczanie korespondencji w formie papierowej i elektronicznej (poprzez e-mail, platforma ePUAP). SEOD musi automatycznie kontrolować czy doręczenie może być zrealizowane poprzez platformę ePUAP, weryfikując czy wskazany adresat przesyłki ma informację o adresie skrytki. 224. SEOD musi umożliwiać szybkie rejestrowanie zwrotów i zwrotek z poziomu Rejestru Przesyłek Wychodzących po wskazaniu powiązanej przesyłki. Ponadto, musi być możliwość odszukania przesyłki na podstawie kodu graficznego umieszczonego na zwrotce a wskazującego przesyłkę. Zwrotki muszą automatycznie przypisywać się do pisma którego dotyczą, oraz zwrotnie każdy status mówiący o piśmie wysyłanym zmieniany przez obsługujących wysyłki w kancelarii musi automatycznie być przyporządkowany i widoczny na piśmie którego dotyczy, a w związku z tym również widoczny przez osobę która pismo kierowała do wysyłki . 225. SEOD musi rejestrować zwrotkę lub zwrot, jako załącznik do korespondencji, której dotyczy. SEOD musi umożliwiać skanowanie zwrotek oraz ich opisywanie za pomocą słownika dedykowanego zwrotkom. 226. Adresaci przesyłek wychodzących muszą być wskazywani z ewidencji interesantów. 227. Pisma muszą być kierowane do wysyłki na dwa sposoby:      1. Przez stanowiska merytoryczne z poziomu akt spraw – w tym wypadku procedura wysyłki musi ograniczać działania kancelarii do określenia fizycznej daty wysyłki przesyłki wychodzącej.      2. Przez pracowników kancelarii z pominięciem rejestrowania ich w aktach sprawy, z poziomu Rejestru Przesyłek Wychodzących. 228. W systemie musi być możliwe określenie komórek innych niż kancelaria które będą gromadziły korespondencję od pracowników i zarządzały wysyłką. 229. SEOD musi umożliwiać wysyłkę korespondencji za pośrednictwem kancelarii oraz oznaczanie jako odebrane osobiście z poziomu pracownika lub kancelarii. Pracownik musi mieć możliwość przejrzenia na oddzielnym zestawieniu pism które oczekują na odbiór osobisty na jego stanowisku. 230. SEOD musi umożliwiać obsługiwać doręczanie przesyłek wychodzących za pośrednictwem dowolnych operatorów pocztowych. SEOD musi mieć słownik operatorów pocztowych. SEOD musi umożliwiać definiowanie i zarządzanie cennikiem przesyłek, tj. dowolnym zestawem form wysyłki przesyłek wychodzących, ich przedziałów wagowych i gabarytów, od których uzależniony jest koszt przesyłki. Cennik przesyłek musi rozróżniać koszty przesyłki ze względu na formę wysyłki, wagę i gabaryt. 231. SEOD musi umożliwiać generację Pocztowej Książki Nadawczej zgodnej ze wzorem ustalanym przez Pocztę Polską SA, dla wskazanego rodzaju (np. zwykłe, polecone), komórki organizacyjnej, całościowo dla jednostki lub imiennie dla stanowiska. 232. SEOD musi umożliwiać sortowanie listy przesyłek wychodzących w centralnym rejestrze co najmniej wg kryteriów: numer przesyłki, numer nadawczy, forma doręczenia, data wysłania, adresata rozumianego jako jego nazwa, adresata rozumianego jako dane adresowe. 233. SEOD musi opatrywać przesyłki wychodzące poniższymi lub podobnymi statusami oraz zapamiętywać historię operacji na tych przesyłkach:      1. przyjęto do wysyłki w kancelarii, czyli została doniesiona przez pracownika merytorycznego koperta zawierająca korespondencję do wysyłki,      2. nie wysłano – przesyłki dla których jeszcze nie podjęto próby wysyłki i nie wskazano daty wysyłki;      3. wysłano – przesyłki wysłane;      4. odebrano – przesyłki wysłane i odebrane;      5. zwrócono – przesyłki wysłane i zwrócone jako nieodebrane. 234. SEOD musi zapewnić możliwość kierowania korespondencji również wewnątrz jednostki: w powiązaniu z jednocześnie tworzonym pismem wychodzącym na zewnątrz i bez takiego powiązania. Mechanizm tworzenia pisma tego rodzaju musi być taki analogiczny jak korespondencji kierowanej na zewnątrz. Obie czynności wymaga się aby były wykonane w jednym kroku (jednocześnie), z oznaczeniem na dedykowanym ekranie: osób ze struktury oraz interesantów z bazy interesantów dla tworzonego pisma. 235. Korespondencja kierowana wewnątrz jednostki, po oznaczeniu jako wysłana, musi automatycznie zostać zarejestrowana w Rejestrze Przesyłek Przychodzących dedykowanym dla takiej wewnętrznej korespondencji i dalej procesowana analogicznie jak pozostała korespondencja wpływająca. 236. Jeżeli korespondencja wewnętrzna zostanie zaadresowana na kilka komórek lub pracowników to dla każdego egzemplarza musi zostać nadany unikalny numer z Rejestru Przesyłek Przychodzących   **Wymagania warstwy workflow:**   1. SEOD ma być wyposażony w narzędzie do graficznego modelowania przepływów procesów „Workflow”, 2. Moduł Workflow ma zapewnić możliwość projektowania procesów przez Zamawiającego, 3. SEOD ma mieć możliwość pełnej konfiguracji w systemie wszystkich etapów procesu obiegu dokumentów i dopasowanie ich do zmieniających się procesów biznesowych, 4. SEOD ma mieć możliwość automatycznego przechowywania wszystkich oryginałów dokumentów będących wynikiem obiegu procesu, 5. SEOD musi umożliwiać śledzenie poszczególnych etapów procesu oraz stan ich realizacji przez uprawnionych użytkowników, 6. SEOD musi prezentować graficzną wizualizację przebiegu procesu wg ścieżki jego faktycznego wykonania, 7. SEOD musi umożliwiać przerwanie procesu i dalszego załatwiania sprawy poza schematem w nim opisanym, 8. SEOD musi umożliwiać określenia czasu realizacji procesu i każdego z jego etapów oraz nadzór nad terminowością realizacji, 9. SEOD musi umożliwiać automatyczne przydzielanie zleceń użytkownikom wynikających z realizacji procesu workflow, 10. SEOD musi umożliwiać nadawanie terminów realizacji zleceń w edytorze procesów, 11. SEOD musi umożliwiać równoległe wykonywanie niezależnych ścieżek w edytorze procesów, 12. SEOD musi umożliwiać dynamiczne określenie osoby przypisanej w edytorze procesów (na podstawie zmiennych z procesu), 13. Edytor procesów musi umożliwiać administratorowi zdefiniowanie ścieżki procesu, w tym co najmniej: określenia nazw przyjaznych dla użytkownika kroków procesu, 14. Musi być możliwe zdefiniowanie nazwy całego procesu oraz zdefiniowanie opisu całego procesu jak i jego poszczególnych kroków. Opisy poszczególnych kroków muszą być prezentowane użytkownikom realizującym dany krok, 15. Musi być możliwe zdefiniowanie czasu potrzebnego na wykonanie danego kroku procesu, 16. Edytor procesów musi umożliwiać tworzenie kolejnych wersji procesu na podstawie już istniejących wersji oraz aktywowania i dezaktywowania danej wersji procesu do użytkowania, 17. Edytor procesu musi opierać się o graficzny interfejs użytkownika, pozwalający zarządzać procesem oraz wizualizować proces (tj. jego kroki i przejścia między nimi) w formie grafu, 18. SEOD musi umożliwiać eksport i import definicji procesu, 19. Dokumentacja w aplikacji winna być przemieszczana między krokami procesu (stanowiskami i statusami) zgodnie ze ścieżką w wykorzystywanym procesie. W przypadku rozgałęzienia się ścieżki, użytkownik musi mieć wybór następnego kroku, 20. W wyniku każdorazowej decyzji użytkownika, SEOD musi przemieszczać dokumentację między krokami procesu lub przydzielać ją wybranemu stanowisku. Które stanowisko może wybrać użytkownik jako odbiorcę dokumentacji, musi wynikać z definicji procesu   **Wymagania warstwy administracji systemem SEOD**   1. Cały obszar uprawnień musi być realizowany tylko i wyłącznie wg jednego mechanizmu: przyznawania uprawnień albo odbierania uprawnień. Zakres uprawnień musi dotyczyć co najmniej: przeglądania pism, spraw określonych użytkowników. Zakres uprawnień musi umożliwiać określenie uprawnień do podglądu realizowanych całościowo, tj np. użytkownik x widzi całą korespondencję przychodzącą wpadającą na użytkownika y, bez potrzeby definiowania dodatkowych uprawnień. 2. SEOD musi pozwalać na zdefiniowanie ograniczonego dostępu do dokumentów, w zakresie co najmniej informacji o pismach przychodzących. 3. SEOD musi umożliwiać odzwierciedlenie struktury organizacyjnej Zamawiającego z uwzględnieniem podległości komórek organizacyjnych, w formie graficznej i drzewiastej z widocznością: podległości, nazw i skrótów komórek organizacyjnych, stanowisk i osób na stanowiskach i umożliwiać definiowanie co najmniej:    1. Nazwy i symbolu każdej komórki (wykorzystywane do generowania znaków spraw);    2. Nazwy, symbolu i rodzaju stanowiska, SEOD musi posiadać rozróżnienie graficzne co najmniej w zakresie stanowisk: kierownika komórki, zastępcy, pracownika;    3. Dane adresowe całego urzędu i każdej placówki urzędu z osobna.    4. Przypisania użytkowników w odniesieniu do każdego stanowiska z osobna;    5. Obsługiwać wielostanowiskowość. 4. Stanowisko w aplikacji musi być opisane co najmniej parametrami: typem, słownikowaną nazwą stanowiska, symbolem komórki (wykorzystywanym do znakowania spraw zakładanych przez to stanowisko), dostępnym obszarem poszukiwań. SEOD musi prezentować pełne lub ograniczone informacje dotyczące dokumentów w zakresie uprawnień jakie zostały nadane. 5. SEOD musi pozwalać na utworzenie grup użytkowników z uprawnieniami pełnego dostępu do wyszukanych dokumentów i grup użytkowników o ograniczonej informacji o dokumentach wyszukanych, np. grup nie mających możliwości podejrzenia skanu lub pliku dokumentu. 6. SEOD musi zawierać oddzielny od struktury organizacyjnej słownik użytkowników. Każdy użytkownik musi być parametryzowany co najmniej: nazwą (loginem), hasłem, symbolem (wykorzystywanym do znakowania spraw), imieniem, nazwiskiem, lokalizacją, datą aktywności konta, statusem, prezentacją daty ostatniego udanego i nieudanego logowania. 7. SEOD musi umożliwiać prezentację użytkowników z nieaktywnymi kontami. 8. Definiowanie użytkowników, stanowisk w relacji z również definiowalną strukturą organizacyjną. 9. Definiowanie struktury organizacyjnej w postaci drzewa. 10. Ustalanie uprawnień pracowników szeregowych jak i administratorów do funkcji, operacji i danych, a także definiowanie grup uprawnień, a następnie przydzielanie ich pracownikom. 11. Wymuszanie definiowania haseł przez użytkowników zgodnych ze wskazanym poziomem bezpieczeństwa, w tym określanie minimalnej liczby znaków, powtarzalności kolejnych haseł, maksymalnej liczby nieudanych prób logowania. 12. Generowania nowych haseł dla każdego użytkownika z osobna (np. po utracie poprzedniego hasła). Musi być możliwe nadanie hasła startowego i wymuszenie na użytkowniku jego zmiany przy pierwszym logowaniu, 13. SEOD musi umożliwiać samodzielne zrestartowanie hasła przez użytkownika i wysyłkę hasła tymczasowego na maila, 14. Definiowanie procesów, raportów, rejestrów, szablonów dokumentów, wydruków, słowników. 15. Kontrolę dziennika zdarzeń w aplikacji. 16. Moduł administrowania systemem musi pozwalać na zmianę jego parametrów wykonywaną przez administratora systemu bez interwencji Wykonawcy. 17. SEOD powinien pozwalać na zarządzanie strukturą organizacyjną jednostki 18. SEOD musi umożliwiać administratorowi dodawanie i modyfikowanie komórek organizacyjnych i stanowisk, w tym co najmniej: zmianę nazwy, symbolu, rodzaju i podległości komórek organizacyjnych oraz stanowisk odpowiednio a także zmianę danych adresowych placówek jak i samego urzędu. Ponadto, administrator musi mieć możliwość oznaczania komórek organizacyjnych i stanowisk jako nieaktywne. 19. SEOD musi umożliwiać administratorowi przyporządkowywanie grup uprawnień stanowiskom poprzez przydział do grupy uprawnień oraz ustalanie zakresów widoczności wraz z kopiowaniem pomiędzy stanowiskami uprawnień do widoczności. 20. Mechanizm kopiowania uprawnień musi zapewniać kopiowanie uprawnień (widoczności) wybranego użytkownika, oznaczenie zakresu kopiowanych uprawnień oraz wskazanie pracownika lub pracowników na których zostaną skopiowane uprawnienia. 21. SEOD musi umożliwiać przypisanie użytkownika do wielu stanowisk, przez co dany użytkownik może pełnić różne role w aplikacji, wynikające z uprawnień przypisanych stanowiskom. 22. W strukturze organizacyjnej, SEOD musi umożliwiać wyszukiwanie osób, co powoduje automatyczne oznaczanie ich na drzewku struktury organizacyjnej, zapewnić funkcjonalność jednoczesnego zwijania i rozwijania całej struktury drzewka za pomocą jednego kliknięcia, a ponadto odrębne rozwijanie i zwijanie poszczególnych rozgałęzień drzewa struktury. 23. SEOD musi umożliwiać administratorowi nałożenie i zdjęcie blokady logowania wskazanego użytkownika oraz usunięcie użytkownika jeżeli nie wystąpił jako dysponent dokumentów ani nie został zarejestrowany w historiach życia dokumentów, w przeciwnym wypadku może zostać deaktywowany. 24. SEOD musi umożliwiać administratorowi tworzenie czasowych kont użytkowników, które są możliwe do wykorzystania (zalogowania się na danego użytkownika) do wyznaczonej daty. 25. SEOD powinien pozwalać na zarządzanie słownikami systemu. 26. SEOD musi umożliwiać administratorowi lub upoważnionym osobom definiowanie i zarządzanie słownikami, które następnie można wykorzystywać w różnych obszarach systemu, co najmniej w odniesieniu do dokumentacji (pism, spraw, dokumentów) i interesantów. 27. Administrator musi mieć możliwość rozbudowy i edycji słownika danych adresowych w zakresie np. funkcji, rejestracji dowolnych danych dodatkowych, numerów identyfikacyjnych. 28. SEOD musi posiadać słownik jednolitego rzeczowego wykazu akt (JRWA), prezentowany w postaci struktury drzewiastej który co najmniej:     1. Zawiera już wprowadzone hasła tworzące aktualnie obowiązujący Zamawiającego słownik JRWA;     2. Umożliwia administratorowi definiowanie nowych i edycję już istniejących haseł JRWA wraz z datami obowiązywania każdego hasła,.     3. Umożliwia administratorowi rozwinięcie i zwinięcie całej struktury drzewiastej JRWA jednocześnie oraz wybiórczo poszczególnych jego rozgałęzień.. 29. Wpis w słowniku JRWA musi zawierać co najmniej: symbol JRWA, hasło JRWA, przypisaną kategorię archiwalną, przedział dat obowiązywania hasła, uwagi do hasła. Musi być możliwe wskazanie do każdej z pozycji JRWA czy sprawy w prowadzone w teczce są prowadzone w formie elektronicznej, czy papierowej, co ma skutkować wyróżnieniem graficznym teczki. Musi być możliwe oznaczenie czy pozycja JRWA jest pozycją wynikającą z przepisów prawa, oraz musi być możliwa deaktywacja pozycji JRWA. 30. Administrator musi mieć możliwość oznaczenia, czy dana pozycja JRWA ma się pokazywać użytkownikowi prowadzącemu sprawy, czy użytkowi prowadzącemu rejestry. 31. SEOD musi posiadać słowniki dedykowane dla modułu oraz słowniki współdzielone. Słownikiem współdzielonym ma być słownik JRWA, bazy interesantów, klasyfikacji tematycznej pism. 32. Przykładem słownika dedykowanego modułowi ma być np. słownik: operatorów pocztowych w Rejestrze Przesyłek Wychodzących   **Wymagania warstwy podstaw prawnych definiujących działanie SEOD**   1. Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. 2011 nr 14 poz. 67 z późn. zm.). 2. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. 1960 nr 30 poz. 168 z późn. zm.). 3. Rozporządzenie Ministra Finansów z dnia 5 marca 2012 r. w sprawie wzoru i sposobu prowadzenia metryki (Dz.U. 2012 poz. 246). 4. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 6 marca 2012 r. w sprawie wzoru i sposobu prowadzenia metryki sprawy (Dz.U. 2012 poz. 250). 5. Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. 1983 nr 38 poz. 173 z późn. zm.) wraz z odpowiednimi rozporządzeniami. 6. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz.U. 2006 nr 206 poz. 1517). 7. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz.U. 2006 nr 206 poz. 1518). 8. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 2 listopada 2006 r. w sprawie wymagań technicznych formatów zapisu i informatycznych nośników danych, na których utrwalono materiały archiwalne przekazywane do archiwów państwowych (Dz.U. 2006 nr 206 poz. 1519). 9. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000 z późn. zm.). 10. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004, Nr 100, poz. 1024). 11. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. 2001 nr 112 poz. 1198 z późn. zm.). 12. Ustawa z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64 poz. 565 z późn. zm.).   **Wymagania warstwy integracyjnej**  **Integracja Systemu SEOD z systemem ePUAP:**   1. SEOD musi mieć możliwość bezpośredniej integracji z ePUAP. Zakres integracji to co najmniej:    1. Pobieranie w sposób automatyczny przesyłek przychodzących z dowolnego konta/skrytki Zamawiającego na platformie ePUAP i ich automatyczna rejestracja w poczekalni systemu SEOD lub automatyczna rejestracja w Rejestrze Przesyłek Przychodzących w zależności od konfiguracji aplikacji.    2. Wysyłanie z aplikacji w sposób automatyczny przesyłek wychodzących do dowolnych kont/skrytek interesantów Zamawiającego na platformie ePUAP, zarówno w trybie przedłożenia jak i doręczenia. 2. Automatyczne pobieranie i wysyłanie przesyłek musi odbywać się regularnie, w ustalonych odstępach czasu. 3. Przedmiotem zamówienia jest uruchomienie integracji aplikacji z platformą ePUAP oraz weryfikacji Profilu Zaufanego ePUAP na żądanie użytkownika aplikacji. 4. Rejestracja przesyłek z ePUAP musi być możliwa w trybie automatycznym i ręcznym. Tryb ręczny musi polegać na prezentacji przesyłek w poczekalni dostępnej na żądanie i automatycznym przeniesieniu wskazanej w poczekalni przesyłki do rejestru przesyłek przychodzących. Tryb automatyczny musi polegać na automatycznej rejestracji w rejestrze przesyłek przychodzących . 5. Udostępniać uprawnionym pracownikom listę przesyłek przychodzących, które wpłynęły z platformy. Poszczególne przesyłki na tej liście muszą być opisane co najmniej następującymi parametrami:    1. danymi konta/skrytki nadawcy w platformie;    2. datą i czasem wpływu przesyłki do konta/skrytki ePUAP, na podstawie momentu generacji UPO;    3. unikalnym identyfikatorem przesyłki w aplikacji;    4. plikami oryginału przesyłki przychodzącej oraz skojarzonym z nią plikiem UPO. 6. Na żądanie użytkownika podczas przeglądania poczekalni weryfikować podpis elektroniczny. 7. Na żądanie użytkownika wyświetlać i udostępniać listę plików dołączonych do treści pliku przesyłki przychodzącej lub wychodzącej oraz umożliwiać lokalny zapis lub wyświetlenie w skojarzonej z typem pliku aplikacji na klienckiej stacji roboczej. 8. Umożliwiać w odniesieniu do każdej przesyłki przychodzącej z platformy ePUAP na liście co najmniej:    1. Rejestrację przesyłki przez uprawnionego użytkownika w Rejestrze Przesyłek Przychodzących. Rejestracja przesyłki musi wiązać się z wypełnieniem formularza rejestracji, przydzieleniem odpowiedniej komórki lub stanowiska merytorycznego będącego odbiorcą przesyłki.    2. Rezygnację z rejestracji przesyłki. Rezygnacja z rejestracji przesyłki musi wiązać się z usunięciem z listy oczekujących na rejestrację. 9. Automatycznie rejestrować UPO jakie wpływają z platformy do aplikacji. 10. Automatycznie i trwale kojarzyć ze sobą przesyłki przychodzące z platformy ePUAP albo wychodzące do platformy z dotyczącymi je UPO oraz udostępniać je razem na wszystkich listach aplikacji w sposób umożliwiający użytkownikowi łatwy dostęp do zarówno do przesyłki jak i UPO. 11. Przekazanie przesyłki przychodzącej komórce lub stanowisku merytorycznemu musi być jednoznaczne z przekazaniem dotyczącego jej UPO. 12. Poświadczenia odbioru przesyłki wychodzącej (UPD, UPP) przyporządkowane do przesyłki wychodzącej muszą być dostępne z poziomu widoku szczegółów pisma w sposób jasno przedstawiający przyporządkowanie do danej przesyłki wychodzącej/dokumentu. 13. Poszczególne przesyłki muszą być opisane co najmniej następującymi parametrami:     1. datą odbioru przesyłki wychodzącej;     2. datą wpływu poświadczenia do aplikacji;     3. danymi interesanta – adresata przesyłki wychodzącej;     4. numerem przesyłki wychodzącej w Rejestrze Przesyłek Wychodzących. 14. SEOD ma umożliwiać powiązanie przesyłki przychodzącej z platformy ePUAP z odpowiednim interesantem, utworzonym uprzednio albo tworzonym w momencie rejestracji przesyłki, na podstawie danych konta/skrytki nadawcy. 15. Umożliwiać pracownikom merytorycznym wysyłanie przesyłek wychodzących do kont/skrytek interesantów na platformie ePUAP.   **Integracja z platformą ePUAP z wykorzystaniem niezależnej aplikacji pośredniczącej (dalej Aplikacja)**   1. SEOD musi mieć możliwość integracji z ePUAP za pośrednictwem aplikacji pośredniczącej. 2. Aplikacja ma uczestniczyć w wymianie danych na styku: SEOD – ePUAP. 3. Aplikacja ma zapewnić możliwość zdefiniowania niezależnego od systemu SEOD konta administratora i użytkowników zarządzających wymianą za pośrednictwem aplikacji pośredniczącej. 4. Aplikacja ma być specjalistycznym, zaawansowanym narzędziem służącym do konfiguracji i uruchomienia dwukierunkowej wymiany danych pomiędzy systemem ePUAP, a systemem SEOD, w tym również jej blokowania. 5. Aplikacja ma umożliwiać prezentację pism jakie wpłynęły na konto ePUAP jednostki oraz pism, które zostały wysłane z SEOD do ePUAP. 6. Aplikacja ma zapewnić możliwość przechowywania dokumentów jakie zostały wymienione wraz z możliwością określenia czasu przechowywania. 7. Aplikacja ma umożliwiać zablokowanie przekazywania pism z ePUAP do Rejestru Przesyłek Przychodzących systemu SEOD oraz z Rejestru Przesyłek Wychodzących do ePUAP. 8. Aplikacja ma umożliwiać zarządzanie skrytkami służącymi do komunikacji. 9. Aplikacja ma umożliwiać wyświetlanie danych o dokumentach oraz np. zmianę ich statusu. 10. Aplikacja ma umożliwiać prezentację numerów dokumentów jakie zostały nadane w systemie SEOD Aplikacja ma umożliwiać informowanie osoby zalogowanej o ilościach pism, które wpłynęły z ePUAP oraz zostały wysłane na ePUAP za jej pośrednictwem. 11. Aplikacja ma zapewnić prezentację różnego rodzaju statystyk np. graficzne przedstawienie raportu tygodniowego wymiany z rozbiciem na poszczególne dni tygodnia, przedstawienie raportu rocznego. 12. Aplikacja ma zapewnić prezentację raportu graficznego wykorzystania poszczególnych skrytek wymiany w ujęciu tygodniowym oraz rocznym. 13. Aplikacja musi wykorzystywać certyfikat wydawany przez Ministra właściwego do spraw informatyzacji dla systemu teleinformatycznego służącemu zapewnieniu bezpieczeństwa wymiany informacji ePUAP, oraz zapewnić możliwość przypisania certyfikatu do skrytki oraz prezentację daty ważności certyfikatu z poziomu aplikacji. 14. Aplikacja ma zapewnić możliwość przejrzenia pism kierowanych na ePUAP i np. zmiany adresu skrytki jeżeli okazał się nieprawidłowy i wymiana się nie powiodła oraz powtórzenie wymiany. 15. Aplikacja musi zapewniać przyjmowanie e-maili i odseparowanie w związku z tym spamu wraz z możliwością zablokowania nadawcy spamu.   **Integracja Systemu SEOD z systemem Elektroniczny Nadawca Poczty Polskiej**   1. SEOD musi mieć możliwość integracji z systemem Elektroniczny Nadawca. Zakres integracji to co najmniej:    1. Wstępne oraz końcowe przekazywanie z SEOD do Elektronicznego Nadawcy przesyłek    2. Pobieranie z Elektronicznego Nadawcy identyfikatorów numerów nadawczych, właściwych dla przekazanych wstępnie przesyłek wychodzących. 2. Wstępne przekazywanie w sposób automatyczny przesyłek wychodzących do Elektronicznego Nadawcy musi odbywać się na żądanie. 3. Wycofywanie z Elektronicznego Nadawcy uprzednio wstępnie przekazanych pojedynczych przesyłek wychodzących, musi się odbywać na żądanie użytkownika, po wskazaniu przesyłki w rejestrze przesyłek wychodzących. 4. Hurtowe ostateczne przekazanie do Urzędu Pocztowego wszystkich wstępnie przekazanych do Elektronicznego Nadawcy przesyłek wychodzących.   **Integracja Systemu SEOD z systemem elektronicznego fakturowania PEF**   1. SEOD musi być zintegrowany z rządową platformą PEF umożliwiając automatyczne pobieranie faktur oraz innych dokumentów ustrukturyzowanych bez względu na Brokera PEF obsługującego Zamawiającego. 2. SEOD musi umożliwiać możliwość dokonanie wyboru pomiędzy dwoma oficjalnymi Brokerami. 3. SEOD nie może wymagać od użytkownika logowania do platformy PEF. 4. Pobieranie dokumentów w platformy PEF musi przebiegać automatycznie tj. bez angażowania pracowników Zamawiającego w proces importu dokumentów   **Integracja Systemu SEOD z dowolną zewnętrzną bazą zawierającą dane firm oraz bazą TERYT**   1. SEOD musi mieć możliwość automatycznego pobierania na żądanie danych podmiotów gospodarczych i instytucji publicznych na podstawie numeru NIP lub REGON 2. SEOD powinien umożliwiać pobieranie danych adresowych po wpisaniu poprawnego numeru NIP lub REGON. 3. SEOD nie może wymuszać logowania użytkownika Zamawiającego do jakiegokolwiek systemu zewnętrznego celem pobrania danych. 4. SEOD musi posiadać integrację z bazą TERYT: słownik danych adresowych zawierający powiązane ze sobą dane:    1. miejscowości, ulic – w oparciu o dane baz np. TERYT GUS;    2. kodów pocztowych – w oparciu o dane bazy np. Spis Pocztowych Numerów Adresowych udostępnianych przez Pocztę Polską SA.   **API systemu SEOD**   1. SEOD musi posiadać mechanizmy integracji z oprogramowaniem zewnętrznym w postaci udokumentowanych interfejsów programistycznych API. 2. Wykonawca dostarczy Interfejs komunikacyjny (dalej API) umożliwiający pobranie spraw z systemu SEOD do systemów zewnętrznych, co musi stanowić zespół narzędzi pozwalających na integrację. 3. API musi posiadać ustandaryzowane interfejsy zewnętrzne, obejmujące udostępnianie usług integracyjnych systemom zewnętrznym poprzez: Web Services, z wykorzystaniem protokołu SOAP. 4. API musi zapewniać udostępnianie na potrzeby integracji:    1. statusów spraw,    2. danych interesantów,    3. danych pism,    4. danych spraw,    5. danych użytkowników.   **Pozostałe szczegółowe wymagania warstwy funkcjonalnej Systemu SEOD**  **Obsługa jednostek organizacyjnych w Systemie SEOD :**   1. Zamawiający wymaga, aby dla każdej z wymienionych w dokumencie jednostek organizacyjnych została zapewniona odrębna instalacja systemu SEOD o pełnej funkcjonalności wskazanej jak dla systemu SEOD w jednostce głównej. 2. SEOD musi umożliwiać kierowanie korespondencji do jednostek. 3. Administrator jednostki centralnej musi mieć możliwość zdefiniowania połączenia pomiędzy jednostkami, a jednostka główną, komunikacja oparta na protokole SOAP. 4. Administrator jednostki centralnej musi mieć dedykowany centralny ekran zarządzania jednostkami, na którym będzie mógł wskazać adresy poszczególnych instalacji systemów dla jednostek podległych oraz będzie miał zestawienie jednostek skonfigurowanych: nazwa jednostki, adres instalacji, status aktywności jednostki oraz jej rozróżnienie pozwalające ustalić strukturę połączenia, czyli która jednostka jest wskazana jako centralna. 5. Musi istnieć możliwość zdefiniowania widoczności na komórki jednostki zintegrowanej w kontekście praw do kierowania korespondencji na tak wskazane komórki. 6. Odrębny SEOD udostępniony poszczególnym jednostkom organizacyjnym musi posiadać wszystkie funkcjonalności opisane jak dla SEOD.   **Obsługa rejestrów (Rejestry wewnętrzne RW) w Systemie SEOD:**   1. SEOD musi umożliwiać definiowanie i zarządzanie dowolną liczbą rejestrów urzędowych oraz rejestrowanie dokumentacji w tych rejestrach. 2. Rejestry muszą być prowadzone w oparciu o Jednolity Rzeczowy Układ Akt. 3. Rejestry muszą zawierać zbiory (ewidencje pomocnicze) dokumentów wewnętrznych prowadzone na potrzeby wewnętrzne jednostki, odrębnie od rejestrów związanych z przepływem i załatwianiem korespondencji z interesantami. 4. Administrator musi mieć dostęp do narzędzia służącego do definiowania i konfigurowania rejestrów, w tym zakresu danych w nich rejestrowanych, konfiguracji schematu numeracji pozycji w rejestrze, widoku zarejestrowanych pozycji. 5. Widok pozycji w rejestrze ustala się poprzez definiowanie kolumn rejestru, oraz ustalanie zakresu danych w niej prezentowanych wraz ze wskazaniem nazw kolumn w rejestrze. 6. Moduł obsługi rejestrów musi zapewniać tworzenie dodatkowych rejestrów prowadzonych w jednostce, zasilanie ich nowo tworzonymi z widoku rejestru dokumentami oraz zasilanie ich dokumentami pochodzącymi z Rejestru Przesyłek Przychodzących i Rejestru Przesyłek wychodzących. 7. SEOD musi umożliwiać uprawnionemu użytkownikowi na wyszukiwanie i filtrowanie zawartości rejestru. 8. SEOD musi umożliwiać przypisanie użytkownikowi widoku na rejestr. 9. Informacja o przypisaniu dokumentacji do rejestru muszą być dostępne z poziomu tej dokumentacji. 10. Administrator musi mieć możliwość definiowania w odniesieniu do rodzaju dokumentów:     1. przedział dat wpływu dokumentacji,     2. przedział dat wprowadzenia dokumentacji do systemu,     3. przedział dat akceptacji dokumentacji, 11. SEOD musi umożliwiać użytkownikowi generację raportów i zestawień ze zdefiniowanych rejestrów. 12. SEOD musi udostępniać słownik umożliwiający definiowanie rodzajów dokumentów rejestrowanych w rejestrach. 13. SEOD musi umożliwiać administratorowi zdefiniowanie:     1. nazwy rodzaju dokumentów i nazwy skróconej,     2. podpowiadanie pozycji JRWA dla danego rodzaju, podpowiadanie tematu i statusu jaki będzie miał dokument po rejestracji,     3. udostępnienie dla danego rodzaju mechanizmu akceptacji,     4. udostępnienie dla danego rodzaju pola dane adresowe, zasilanego danymi z ewidencji interesantów,     5. dostępność słownika zawierającego listę kategorii z możliwością zaznaczenia wielu pozycji,     6. dostępność pól wyboru z możliwością wskazania jednej pozycji,     7. definiowanie reguł walidacji pól liczbowych i widoczności pól tekstowych i liczbowych.   **Prowadzenie rejestrów wewnętrznych (RW), funkcje dodatkowe:**   1. SEOD musi zapewnić przechowywanie zawartości rejestrów w pozycjach JRWA. W każdej pozycji JRWA może występować wiele różnych rodzajów dokumentów. 2. Dokumenty mogą być prezentowane w widoku teczki JRWA, lub w widoku rodzaju dokumentu. 3. Każdemu dokumentowi musi być przypisany rodzaj i odpowiadający mu formularz. Administrator musi mieć możliwość definiowania nowych i zarządzania istniejącymi rodzajami dokumentów wraz z ich formularzami. Administrator musi mieć możliwość zdefiniowania dowolnego formularza dla danego rodzaju dokumentu, składającego się z pól i dostępnych funkcji, co najmniej: pola tekstowe, liczbowe, słownikowe, funkcje akceptacji, wskazania pozycji z ewidencji interesantów, 4. Administrator musi mieć możliwość definiowania słownika słów kluczowych, służących do oznaczania dokumentów w RW. Uprawniony użytkownik musi mieć możliwość opatrywania danego dokumentu w Rejestry Wewnętrzne dowolnym i w dowolnej liczbie słowem kluczowym. 5. Administrator musi mieć możliwość definiowania słownika relacji, służących do powiązywania ze sobą różnych dokumentów w RW. Każda relacja musi wskazywać stosunek między powiązanymi dokumentami. Uprawniony użytkownik musi mieć możliwość powiązywania wybraną relacją pary dowolnych dokumentów. Jeden dokument może być powiązany wieloma relacjami jednocześnie z jednym oraz wieloma innymi dokumentami. 6. Wiązanie relacjami musi być również dostępne dla spraw. 7. Administrator musi mieć możliwość nadawania uprawnień dostępu do poszczególnych pozycji JRWA (a przez to do zgromadzonych w nich dokumentów), w tym co najmniej w układach:    1. Pozycja JRWA: oznaczenie kto ma dostęp    2. Użytkownik: oznaczenie do jakich pozycji JRWA ma dostęp, 8. Administrator musi mieć możliwość definiowania widoków list dokumentów w RW, oddzielnie dla każdego rodzaju dokumentu (na podstawie pól formularza) w zakresie układu zawartości i nagłówków kolumn. 9. SEOD musi umożliwiać uprawnionemu użytkownikowi wprowadzanie dokumentacji (jej plików i parametrów) do RW, z uwzględnieniem praw dostępu danego użytkownika do przeglądania zawartości pozycji JRWA. 10. SEOD musi umożliwiać robienie zapisów w Rejestry Wewnętrzne na podstawie dokumentów wpływających i wychodzących, zasilanie danymi pochodzącymi z tych rejestrów. 11. SEOD musi umożliwiać uprawnionemu użytkownikowi wyszukiwanie dokumentów w RW. Musi istnieć możliwość ograniczenia obszaru poszukiwań do wskazanego JRWA, wskazanego rodzaju dokumentu, wyszukiwania w całym RW. Lista wyników musi być ograniczona do dokumentów zlokalizowanych w JRWA, do których dane stanowisko ma prawo dostępu. 12. Administrator musi mieć możliwość definiowania szablonów oznaczeń dokumentów w RW, w kontekście każdego rodzaju z osobna. Definiowanie szablonu oznaczenia może składać się z elementów statycznych oraz wartości pól formularza dokumentu, co najmniej z teczki JRWA. SEOD musi automatycznie generować oznaczenie dokumentu w Rejestry Wewnętrzne i proponować je użytkownikowi w momencie zapisu dokumentu w RW, a użytkownik musi mieć możliwość zmiany tego oznaczenia przed zapisem.   **Dokumenty własne jednostki i ich prezentacja w Systemie SEOD:**   1. SEOD musi być wyposażony w moduł który zapewni pracownikom dostęp do dokumentów wybranych z rejestrów wewnętrznych, o charakterze ogólnodostępnym i prezentację ich w odrębnym, łatwo dostępnym module, bez potrzeby szukania ich w pozycjach JRWA w których były gromadzone w rejestrach wewnętrznych. 2. Tak gromadzone dokumenty mogą być na przykład udostępniane jako kompendium podstawowej wiedzy na temat funkcjonowania jednostki osobom rozpoczynającym w niej pracę. 3. SEOD musi umożliwiać umieszczenie prezentowanych dokumentów w definiowalnych strukturach katalogów oraz ich czasową prezentację w katalogu. 4. SEOD musi umożliwiać uprawnionym pracownikom dowolne definiowanie struktury katalogów oraz umieszczanie w nich wytypowanych dokumentów o charakterze ogólnodostępnym. 5. Struktura katalogów w module musi być niezależna od struktury JRWA. 6. SEOD musi umożliwiać dołączenie dokumentu do katalogu oraz późniejsze jego odłączenie. 7. SEOD musi udostępniać informację kto umieścił dokument w katalogu. 8. SEOD musi zapewnić filtrowanie katalogów po: pracowniku który umieścił dokument w katalogu, przedziałach dat; 9. SEOD musi zapewnić również umieszczanie w katalogach wskazanych osób z bazy interesantów oraz ich prezentację na odrębnym ekranie, np. pozwolić na wprowadzenie danych wszystkich Radnych wraz z oznaczeniem jaką funkcję pełnią w jednostce.     **Obsługa skanerów:**   1. SEOD musi obsługiwać skanery obrazu w standardzie TWAIN bez konieczności uruchamiania natywnego oprogramowania producenta obsługującego skaner. 2. Administrator musi mieć możliwość przygotowania dla użytkowników szablonów skanowania, stanowiących ustalony zbiór pożądanych parametrów skanowania. W szczególności musi być możliwość zdefiniowania szablonów odpowiadających zestawowi parametrów skanowania przewidzianych w Instrukcji Kancelaryjnej dla odwzorowań cyfrowych. 3. SEOD musi umożliwiać automatyczne rozpoznawanie tekstu (OCR) zeskanowanych dokumentów, tj. posiadać mechanizm OCR, bez konieczności zakupu komercyjnych licencji. Wynik rozpoznania tekstu, może być powiązywany z dokumentem wraz z oryginalnym obrazem. 4. SEOD musi umożliwiać w momencie tworzenia OCR przypisanie zawartości do określonych pól w formatce rejestracji pisma wpływającego. 5. SEOD musi umożliwiać utworzenie odwzorowań cyfrowych dokumentacji w formie tradycyjnej w formatach, rozdzielczościach, paletach i głębiach kolorów, kompresjach obrazu wymaganych instrukcją kancelaryjną obowiązującą Zamawiającego a także z wykorzystaniem funkcji duplex skanerów, pomijania pustych stron, ręcznego sortowania, porządkowania, usuwania oraz korekcji orientacji stron.   **Obsługa zastępstw w Systemie SEOD :**   1. SEOD musi umożliwiać uprawnionemu użytkownikowi ustawianie zastępstw podczas nieobecności. Ustawianie zastępstw musi być ograniczone do grupy wyboru spośród listy zdefiniowanej przez administratora. SEOD musi umożliwiać określenie osoby zastępującej, oraz okresu, w jakim będzie realizowane zastępstwo z dokładnością do godziny i minuty. 2. Domyślnie każdy z przełożonych musi mieć możliwość ustawienia zastępstwa za nieobecnego pracownika, jeżeli ten nie zdążył wykonać samodzielnie tej czynności. 3. SEOD musi zapamiętywać i udostępniać informacje o rzeczywistym wykonawcy operacji i prezentować je w powiązaniu do dokumentacji jakiej dotyczy w postaci historii. 4. SEOD musi umożliwiać ewidencjonowanie zastępstw. Musi być możliwość zarządzania zastępstwami przez pracownika. 5. SEOD musi pozwalać uprawnionym użytkownikom definiowanie stałych zastępstw, tj. takich na nieokreślony okres. Osoba zastępująca i zastępowana mogą w każdym momencie, również jednocześnie pracować na zastępowanym stanowisku.   **Wyszukiwanie dokumentacji w Systemie SEOD :**   1. SEOD musi umożliwiać wyszukiwanie zgromadzonej dokumentacji. 2. SEOD musi umożliwiać w zależności od uprawnień globalne poszukiwanie dokumentacji lub przeszukiwanie dokumentacji w zakresie udzielonych uprawnień. 3. SEOD musi umożliwiać poszukiwanie dokumentacji w obrębie modułu z którą jest powiązana, dzięki udostępnieniu wyszukiwarki dedykowanej dla danej listy/modułu. Każda lista dotycząca dokumentacji (pism przychodzących i wychodzących, spraw, rejestrów), a także interesantów musi mieć dedykowaną wyszukiwarkę, której kryteria są dostosowane do rodzaju i statusu dokumentacji na niej zgromadzonej. 4. Każda wyszukiwarka musi umożliwiać wyszukiwanie dokumentacji za pomocą wielu różnych kryteriów. Kryteria mogą być ze sobą łączone wg uznania użytkownika, co ma powodować zawężanie listy wyników do zbioru wspólnego wyznaczonego wybranymi kryteriami (iloczyn logiczny). Musi istnieć możliwość prezentowania wyniku jednego wyszukiwania z wynikiem drugiego wyszukiwania. 5. Wyniki wyszukiwania musza uwzględniać posiadane przez dane stanowisko uprawnienia oraz zakresy dostępu do dokumentacji. 6. SEOD musi umożliwiać każdemu użytkownikowi, w kontekście każdej dostępnej mu wyszukiwarki z osobna, definiowanie i zarządzanie wielu szablonów wyszukiwania oraz domyślnych kryteriów wyszukiwania. W momencie uruchomienia danej wyszukiwarki, SEOD musi automatycznie ustawić domyślne kryteria wyszukiwania, zgodnie z definicją danego użytkownika. Użytkownik musi mieć możliwość wyboru innych niż domyślne kryteriów wyszukiwania, m.in. poprzez wybranie uprzednio zdefiniowanego szablonu. Po wybraniu szablonu, SEOD musi automatycznie ustawić kryteria wyszukiwania zgodne z definicją danego szablonu. 7. SEOD wśród kryteriów wyszukiwania musi udostępniać wszystkie atrybuty opisujące dokumentację, w tym również zesłownikowane klasyfikatory. 8. SEOD musi umożliwiać wykorzystanie jako wartości kryteriów symbolu wieloznacznego (jednego znaku dostępnego na klawiaturze), zastępującego dowolny ciąg znaków. 9. SEOD musi umożliwiać wyszukiwanie pełnotekstowe na podstawie zawartości dołączonych do dokumentacji plików tekstowych oraz wyszukiwanie po komentarzach do dokumentacji. Wyszukiwanie pełnotekstowe musi uwzględniać polską fleksję. 10. SEOD musi umożliwiać wyszukanie dokumentacji z wykorzystaniem przypisanego doń unikalnego identyfikatora zapisanego w formie kodu graficznego.   **Systemowy dziennik zdarzeń, powiadamianie użytkowników:**   1. SEOD musi automatycznie monitorować dostęp do zasobów i zapisywać w Systemowym Dzienniku Zdarzeń czynności wykonywane przez użytkowników w odniesieniu do poszczególnych użytkowników. 2. SEOD musi odnotowywać i rejestrować w dzienniku: błędy, logowania, szczegóły z tym związane . 3. Wszystkie odnotowywane w Systemowym Dzienniku Zdarzeń operacje muszą być skategoryzowane. Administrator musi mieć możliwość wskazania kategorii, których operacje są prezentowane na ekranie. 4. W Systemowym Dzienniku Zdarzeń administrator musi mieć możliwość:    1. eksportu do pliku każdego wpisu z SDZ, zaznaczenia jednorazowo wszystkich wpisów i eksportu do pliku,    2. filtrowanie wpisów wg co najmniej: daty, pracownika wykonującego operację, rodzaju operacji, 5. SEOD musi pozwalać użytkownikowi będącemu pracownikiem na jak najszybsze powzięcie informacji o tym co powinien zrobić i o przekroczeniu terminów przeznaczonych na realizację. 6. W związku z powyższym SEOD musi być wyposażony w szereg narzędzi opisanych w dokumencie, umożliwiających zawiadomienie użytkownika, zwrócenie jego uwagi. 7. Stąd między innymi SEOD w części przeznaczonej dla użytkowników musi zawierać funkcjonalność alertów wysyłanych automatycznie z aplikacji. 8. SEOD musi automatycznie powiadamiać użytkownika o zdarzeniach w systemie w formie alertów (zgodnie z konfiguracją danego użytkownika), wyskakujących na pierwszy plan okien zawierających wykaz powiadomień, niezależnie od aktualnie użytkowanego obszaru aplikacji. 9. Użytkownicy muszą mieć możliwość samodzielnej konfiguracji listy i częstotliwości pojawiania się otrzymywanych alertów. 10. Alerty muszą dotyczyć co najmniej:     1. Wpis w kalendarz,     2. Zastępstwa przydzielone,     3. Sprawy do których użytkownik został upoważniony,     4. Pismo wychodzące do akceptacji,     5. Wysyłka pisma wychodzącego,     6. Dokumenty i sprawy otrzymane od innych pracowników,     7. Otrzymane zlecenia do realizacji, do akceptacji,     8. Pisma do załatwienia przez pracownika,     9. Nowe dokumenty wewnętrzne w Twojej komórce,     10. Dołączenie przez kancelarię skanu zwrotki do pisma skierowanego do wysyłki przez pracownika, 11. Oprócz powiadomień generowanych w formie alertów, definiowanych przez użytkownika, musi istnieć w systemie również zdefiniowana na stałe w systemie tablica komunikatów pojawiająca się na stronie startowej, od razu po zalogowani się użytkownika. 12. Tablica tych komunikatów musi zawierać zbiorcze informacje pozwalające uzyskać wiedzę nt.:     1. grup obiektów wśród których są elementy ulegające przeterminowaniu w ciągu: 1 dnia,     2. grup obiektów wśród których są elementy ulegające przeterminowaniu w ciągu: 1 tygodnia. 13. Tablica musi zawierać podsumowania ilościowe w obrębie grup obiektów dot. następujących zdarzeń:     1. Pism skierowanych do realizacji na pracownika,     2. Pism skierowanych do dekretacji u kierownika, pism zwróconych,     3. Pism niedołączonych jeszcze do spraw,     4. Pism wychodzących skierowanych do akceptacji,     5. Przygotowywanych pism wychodzących,     6. Ilości spraw bieżących, załatwionych,     7. Dokumentów oznaczonych komentarzem,     8. Zleceń w podziale na: w przygotowaniu, otrzymane do wykonania, zwrócone po wykonaniu do akceptacji. 14. SEOD musi być wyposażony w funkcje umożliwiające użytkownikowi spersonalizowanie preferencji co do wyglądu aplikacji. 15. Personalizacja musi dotyczyć co najmniej:     1. konfiguracji działania systemu alertów (w zakresie opisanym wyżej);     2. wskazania domyślnego stanowiska użytkownika (spośród jemu przypisanych);     3. ustawienia rozmiaru czcionek używanych w aplikacji;     4. ustawienia domyślnej skórki.   **Archiwum zakładowe**   1. SEOD musi umożliwiać prowadzenie Archiwum Zakładowego (AZ) zgodnie z Rozporządzeniem MSWIA w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz.U. 2006 nr 206 poz. 1518): 2. SEOD musi umożliwiać ewidencjonowanie, przechowywanie, zabezpieczanie i udostępnianie dokumentacji archiwalnych. 3. SEOD musi zapewniać przejęcie spraw prowadzonych w systemie do archiwum zakładowego. 4. SEOD musi zapewniać wprowadzenie spraw nie prowadzonych w systemie SEOD do archiwum zakładowego. 5. SEOD musi zapewniać integralność treści i parametrów opisujących dokumentację, limitując ich edycję osobom nieuprawnionym lub poza ustalonymi procedurami. W szczególności nie może zezwalać na zmiany zawartości akt przekazanych do AZ. 6. SEOD musi umożliwiać gromadzenie i odczyt metadanych wymaganych przepisami. 7. SEOD musi umożliwiać uprawnionemu użytkownikowi pobranie i odczyt dokumentu w postaci takiej jakiej został on dołączony do akt sprawy w trakcie jej procedowania. 8. SEOD musi zapewniać uprawnionemu użytkownikowi dostęp do danych pozwalających na odtworzenie pełnego przebiegu obsługi dokumentacji. 9. SEOD musi wspomagać proces przekazywania dokumentacji do AZ przez wskazywanie dokumentacji nadającej się do przekazania, generację spisów zdawczo-odbiorczych, ustalania przez stanowisko przekazujące i archiwisty zawartości porcji dokumentacji przekazywanej do AZ. 10. SEOD musi wspomagać procesy:     1. brakowania dokumentacji – przez ustalanie porcji dokumentacji przeznaczonej do brakowania, generację spisu dokumentacji niearchiwalnej przeznaczonej do brakowania;     2. zmiany kategorii archiwalnej – przez ustalenie porcji dokumentacji przeznaczonej do ekspertyzy, generację spisu dokumentacji przeznaczonej do ekspertyzy;     3. przekazania dokumentacji do Archiwum Państwowego – przez ustalenie porcji dokumentacji archiwalnej, generację spisu zdawczo-odbiorczego.     **Ewidencja urlopów pracowników oraz obsługa wniosków urlopowych:**   1. SEOD musi rejestrować i odnotowywać w odniesieniu do każdego użytkownika z osobna ilość urlopu do wykorzystania, datę od kiedy był zatrudniony, wymiar urlopu w skali roku, podział na: urlop wykorzystany, niewykorzystany, ilość dni do wykorzystania. 2. SEOD musi umożliwiać złożenie nowego wniosku wraz z możliwością określenia czy składany wniosek dotyczy urlopu, nadgodzin, wyjścia, itd. 3. Formularz wniosku dostępny w systemie musi pozwalać na określenie rodzaju urlopu: np. na żądanie, wypoczynkowy. 4. Formularz musi umożliwiać określenie przedziału dat jakiego dotyczy wniosek oraz odnotowanie opisu. 5. SEOD musi zapewnić możliwość obsługi akceptacji wniosku oraz jego wydruk. 6. Formularz wniosku musi umożliwiać wprowadzenie osoby zastępującej. 7. SEOD musi umożliwiać zdefiniowanie automatycznego utworzenia zastępstwa po zaakceptowaniu wniosku urlopowego. 8. SEOD musi umożliwiać przeglądanie użytkownikowi rejestru wniosków z możliwością jego filtrowania.   **Ewidencjonowanie zleceń:**   1. SEOD musi posiadać możliwość kierowania do pracowników zleceń. 2. SEOD musi umożliwiać rejestrację zleceń w kontekście prowadzonych spraw, procesów workflow oraz niezależnie od nich. 3. SEOD musi mieć możliwość definiowania zleceń przez uprawnione osoby oraz przekazywanie ich do wykonania podległym pracownikom. 4. SEOD musi umożliwiać osobie tworzącej oraz dekretującej zlecenie określanie stopnia ważności, czasu realizacji oraz uwag dotyczących sposobu realizacji zlecenia. 5. SEOD musi udostępniać użytkownikowi ewidencję zleceń zawierającą zlecenia utworzone w kontekstach wymienionych w punkcie powyższym. 6. SEOD musi sygnalizować o przekroczeniu terminu realizacji zleceń. 7. Użytkownik musi mieć możliwość utworzenia zlecenia: bez powiązania ze sprawą, w powiązaniu ze sprawą. 8. Zlecenia muszą być możliwe do zarejestrowania i w kolejnym kroku oddalonym w czasie uruchomione do realizacji (wykonania). 9. Do zlecenia użytkownik musi mieć możliwość podłączenia: dowolnego dokumentu zarejestrowanego wcześniej w aplikacji, dowolnego pliku ze stacji roboczej. 10. Zlecenia muszą być możliwe do kierowania do wykonania dla pracowników (możliwość wskazania wielu), pracowników + komórek (wielu), utworzonych wcześniej grup nie powiązanych ze strukturą. 11. Zlecenia muszą być wyposażone w mechanizmy przepływu: pracownik zlecający kieruje do realizacji, wyznacza czas, opisuje zlecenie, dołącza dokumenty – realizator zwraca zlecenie, opisuje jak zostało zrealizowane, dołącza dokumenty wynikowe, odsyła - zlecający potwierdza prawidłowość realizacji zlecenia lub odmawia akceptacji co powoduje ponowne uruchomienie ścieżki. 12. SEOD musi umożliwiać wprowadzenie treści zlecenia oraz formatowanie tej treści bezpośrednio w formularzu służącym do rejestracji zlecenia. Formatowanie treści musi umożliwiać: zmianę czcionki, zmianę rozmiaru czcionki, pogrubienie czcionki, podkreślenie czcionki, wyjustowanie we wbudowanym wewnętrznym edytorze systemu. 13. SEOD musi zawierać słownik zleceń w którym można tworzyć koszyki zleceń. 14. Koszyk zleceń musi umożliwiać tworzenie grup zleceń w celu ich późniejszego wykorzystania przy prowadzeniu spraw. Koszyk zleceń musi posiadać swoje oznaczenie w systemie (nazwę). 15. SEOD musi umożliwiać łączenie ze sprawą wielu różnych koszyków zleceń, wielokrotne ponowne dodawanie koszyka zleceń. W każdym przypadku zlecenia należące do koszyka muszą być przypisywane do sprawy i prezentowane w sprawie. 16. SEOD musi umożliwiać pracownikowi prowadzącemu sprawę: wskazanie koszyka jaki chce dołączyć do sprawy. Wskazanie koszyka musi spowodować przypisanie zleceń jakie zawierał do konkretnej sprawy z możliwością ich późniejszego skierowania lub nie do realizacji. 17. SEOD nie może uzależniać możliwości zamknięcia sprawy od uruchomienie do wykonania zleceń do niej przypisanych, to pracownik prowadzący sprawę decyduje czy daje do realizacji zlecenie, czy pomija ten krok. 18. SEOD musi umożliwiać sprawdzenie listy zleceń do wykonania, przydzielonych określonemu pracownikowi (informacja dotycząca ilości wykonywanych zleceń itp.).   **Kierowanie do pracowników komunikatów.**   1. SEOD musi być wyposażony w mechanizm publikowania na tablicach widocznych dla użytkownika po zalogowaniu (ekran startowy), komunikatów, np. ogłoszeń o planowanej niedostępności systemu, ogłoszeń o zmianie wersji, itd. 2. SEOD musi udostępniać uprawnionemu użytkownikowi tworzenie i publikowanie komunikatów. 3. SEOD musi umożliwiać wprowadzenie podczas tworzenia daty i godziny wygaśnięcia komunikatu. 4. SEOD musi umożliwiać wprowadzenie treści komunikatu we wbudowanym edytorze treści oraz formatowanie tej treści bezpośrednio w formularzu służącym do rejestracji. 5. Formatowanie treści musi umożliwiać: zmianę czcionki, zmianę rozmiaru czcionki, koloru, pogrubienie czcionki, podkreślenie czcionki, wyjustowanie. 6. SEOD musi automatycznie ewidencjonować utworzony komunikat w rejestrze. 7. Komunikaty muszą być możliwe do zarejestrowania i w kolejnym kroku oddalonym w czasie opublikowane. 8. Do komunikatu użytkownik musi mieć możliwość podłączenia: dowolnego dokumentu zarejestrowanego wcześniej w aplikacji, dowolnego pliku ze stacji roboczej. 9. Dokumenty podłączone do komunikatu muszą być dostępne dla użytkownika na żądanie. 10. Komunikaty muszą być możliwe do opublikowania i wskazania widoczności dla: pracowników i komórek. 11. Każdy z użytkowników który uzyskał widoczność na komunikat musi mieć możliwość wprowadzenia komentarza. 12. Każdy z użytkowników musi mieć możliwość wyboru jaką ilość komunikatów chce widzieć bez potrzeby przewijania okna.   **Udostępnianie kalendarza oraz funkcjonalność rezerwacji:**   1. SEOD musi być wyposażony w funkcjonalność umożliwiającą prezentację w kalendarzu użytkownika wpisów własnych oraz dokonywanych przez pracowników (terminów). 2. SEOD musi umożliwiać użytkownikom wprowadzanie terminów, opisywanie oraz dołączanie dokumentów już zarejestrowanych w aplikacji. 3. SEOD musi umożliwiać określenie ram czasowych terminu. 4. SEOD musi umożliwiać określenie cykliczności z jaką terminy mają się pojawić w kalendarzu. 5. SEOD musi umożliwiać wpisywanie terminów w kalendarze tych pracowników którzy zostali udostępnieni przez administratora. 6. SEOD musi umożliwiać zbiorcze oznaczenie wpisu dla wszystkich udostępnionych kalendarzy pracowników. 7. SEOD musi umożliwiać rezerwacje zasobów materialnych jednostki: np. samochody służbowe, sale oraz umożliwiać zarządzanie tymi zasobami. 8. SEOD musi pozwalać na gromadzenie zasobów i ich prezentację w zbiorach struktur drzewiastych. 9. SEOD musi pozwalać na ustalenie osób mogących rezerwować zasób. 10. SEOD musi przed umożliwieniem zarezerwowania zasobu informować o tym czy w żądanym przedziale czasowym zasób jest dostępny.   **Ocena okresowa pracownika:**   1. SEOD musi umożliwiać w ramach funkcji administratora ma umożliwiać dodawanie pracownika do konkretnej jednostki ze wskazaniem następujących atrybutów:    1. Imię i nazwisko,    2. Adres e-mail,    3. Nazwa użytkownika,    4. Numer ewidencyjny,    5. Nr telefonu,    6. Nr pokoju,    7. Data zatrudnienia,    8. Data zakończenia pracy 2. SEOD musi umożliwiać w ramach funkcji administratora na dodawanie pracownika do konkretnej zdefiniowanej grupy uprawnień. 3. SEOD musi umożliwiać w ramach uprawnień Administratora na dodawanie i aktualizację struktury jednostki z wyszczególnieniem poszczególnych wydziałów 4. SEOD musi umożliwiać w ramach zmienianie statusu danej jednostki. 5. SEOD musi umożliwiać na przypisanie do struktury organizacyjnej stanowisk w obrębie danej jednostki. 6. SEOD musi umożliwiać w ramach uprawnień Administratora na zarządzanie stanowiskami pracownika. 7. SEOD musi zawierać teczki osobowe pracowników przedstawiające wszystkie oceny pracownika, listę szkoleń w których uczestniczył oraz jego zestawienie kompetencji. 8. SEOD musi umożliwiać na zdefiniowanie aktywnych użytkowników, którzy będą brali w ocenie pracownika oraz badaniach. 9. SEOD musi umożliwiać na definiowanie stanowisk przypisanych do działów w strukturze organizacyjnej oraz definiowania ich domyślnych kompetencji. 10. SEOD musi umożliwiać definiowanie słownika stanowisk. 11. SEOD musi umożliwiać osobom z uprawnieniami Administratora na monitorowanie zalogowanych użytkowników. 12. SEOD musi umożliwiać użytkownikom na wyświetlanie wszystkich ankiet, badań, oceń pracowniczych, do których został przypisany. 13. SEOD musi umożliwiać osobom z Działu Kadr i Płac na tworzenie nowej rekrutacji przydzielonej do konkretnego stanowiska pracy, za pomocą formularza do generowania oferty pracy. 14. Formularz do generowania oferty pracy ma umożliwiać:     1. wypełnienia listy obowiązków na danych stanowisku,     2. wypełnienia listy głównych kompetencji przypisanych do danego stanowiska,     3. wypełnienia listy dodatkowych kompetencji przypisanych do danego stanowiska,     4. ustalenia poziomów kompetencji głównych i dodatkowych,     5. wypełnienia podstawowych informacji o rekrutacji, 15. SEOD musi umożliwiać definiowanie listy prowadzonych rekrutacji ze wskazaniem:     1. stanowiska, którego dotyczy,     2. daty rozpoczęcia rekrutacji,     3. daty zakończenia rekrutacji,     4. statusu rekrutacji,     5. osoby tworzącej dane ogłoszenie. 16. SEOD musi umożliwiać generowanie PDF z ofertą pracy po uzupełnieniu wszystkich formularzy rekrutacji. 17. SEOD musi umożliwiać na dodawanie nowego kandydata do toczącej się rekrutacji wraz z zapisaniem do bazy danych, z której Zamawiający będzie mógł skorzystać podczas przyszłych rekrutacji. 18. SEOD musi umożliwiać podczas dodawania kandydata do toczącej się rekrutacji na określenie jego poziomu kompetencji wskazanych podczas rekrutacji. 19. SEOD musi umożliwiać podczas prowadzenia rekrutacji na wyszukanie aplikanta w istniejącej bazie danych, system musi wyświetlić listę aplikantów pasujących profilem do danej rekrutacji. 20. SEOD musi umożliwiać podczas prowadzenia rekrutacji na dopasowanie listy pracowników pasujących do profilu kandydata na dane stanowisko. 21. SEOD musi zawierać formularz dodawania, usuwania, edycji danego szkolenia. 22. W ramach formularza dodawania szkolenia użytkownik zarządzający tym szkoleniem, ma mieć możliwość umieszczenia informacji ogólnych o szkoleniu, wykazu kompetencji, których dotyczy to szkolenie, zadeklarowania listy dostępnych miejsc do szkolenia, wskazania daty rozpoczęcia i daty zakończenia szkolenia. 23. SEOD musi umożliwiać wyświetlanie listy wszystkich szkoleń, do których dany użytkownik został zapisany. 24. SEOD musi umożliwiać, definiowanie przy danym szkoleniu opisu kompetencji, których to szkolenie będzie dotyczyło. 25. SEOD musi umożliwiać zapisywanie się poszczególnych użytkowników do zaplanowanego szkolenia wraz ze wskazaniem liczby miejsc dostępnych. 26. SEOD musi umożliwiać zarządzającym danym szkoleniem na akceptowanie bądź odrzucenie zapisu danego użytkownika do szkolenia wraz z dodaniem odgórnie danego pracownika z listy pracowników lub dodaniem uczestnika na podstawie listy rankingowej posiadanych kompetencji. 27. SEOD musi umożliwiać na ocenę danego szkolenia wraz z przygotowaniem raportu na podstawie opinii uczestników. Ocena ma obejmować ocenę wszystkich kompetencji, których dotyczyło dane szkolenie. 28. SEOD musi umożliwiać na ocenę kompetencji oraz zachowań pracowników na danych stanowisku. 29. SEOD musi umożliwiać na definiowanie szablonów oceny konkretnych grup pracowników. Raz zdefiniowany szablon może być wykorzystany wielokrotnie do kolejnych ocen 30. SEOD musi umożliwiać na przeprowadzanie cyklicznych ocen pracowników. 31. Proces rozpoczęcia oceny pracownika powinien zakładać możliwość konfigurowania bazy kompetencji przez kierowników wydziałów, dział kadrowo-płacowy oraz administratorów systemu. Baza kompetencji musi zakładać podział na kompetencje zawodowe, miękkie, menedżerskie, osobiste, społeczne. 32. Ocena każdej kompetencji powinna zakładać skonfigurowanie zachowań według, których dana kompetencja pracownika będzie oceniania. SEOD musi umożliwiać konfigurowanie bazy zachowań pracowników podlegających ocenie ze wskazaniem pytań pomocnych dla pracownika i osoby oceniającej. 33. Użytkownicy na stanowiskach Kierownicy Wydziałów, Dział Kadr i Płac, Administratorzy muszą mieć możliwość konfigurowania formularza oceny pracownika, formularza celów pracownika na konkretnych stanowisku. W ramach każdego formularza powinna być oceniana konkretna pula kompetencji wybranych ze wcześniej zdefiniowanego słownika kompetencji. Do każdego stanowiska osoba przygotowująca ocenę musi podać poziom oczekiwanej oceny uprzednio wybranych kompetencji do stanowiska. 34. Moduł formularzy oceny okresowej pracownika i formularza celów rocznych pracownika musi umożliwiać dodawanie kolejnych szablonów na podstawie już istniejących. 35. Użytkownicy na stanowiskach Kierowników Wydziałów, Dział Kadr i Płac, Administratorzy muszą mieć możliwość konfigurowania szablonu badania oceny okresowej pracownika oraz szablonu celów rocznych pracownika. W ramach tego formularza musi być możliwość wyboru typu oceny z wyszczególnieniem:     1. 90 stopni – ocena prowadzona jest tylko w ramach arkusza oceny przełożonego. Przełożony wypełnia arkusz oceny i wystawia pracownikowi ocenę ogólną.     2. 180 stopni - ocena prowadzona jest w ramach arkusza samooceny pracownika oraz arkusza oceny przełożonego. Przełożony wypełnia arkusz oceny finalnej na podstawie danych z obu źródeł i wystawia pracownikowi ocenę ogólną.     3. 270 stopni – ocena prowadzona jest w ramach arkusza samooceny pracownika, arkusza oceny przełożonego oraz arkusza oceny współpracownika. Przełożony wypełnia arkusz oceny finalnej na podstawie samooceny pracownika i średniej z pozostałych dwóch źródeł, a następnie wystawia pracownikowi ocenę ogólną.     4. 270 stopni dla Kierowników Wydziałów – ocena prowadzona jest w ramach arkusza samooceny pracownika, arkusza oceny przełożonego oraz arkusza ocen podwładnych. Przełożony wypełnia arkusz oceny finalnej na podstawie samooceny pracownika i średniej z pozostałych 2 źródeł, a następnie wystawia pracownikowi ocenę ogólną.     5. 360 stopni – ocena prowadzona jest w ramach arkusza samooceny pracownika, arkusza oceny przełożonego, arkusza oceny współpracownika, arkusza oceny konsultanta zewnętrznego. Przełożony wypełnia arkusz oceny finalnej na podstawie samooceny pracownika i średniej z pozostałych 3 źródeł, a następnie wystawia pracownikowi ocenę ogólną. 36. Do każdej oceny okresowej pracownika musi być możliwość dodania pracowników z określonego działu lub przypisanych do konkretnego stanowiska pracy. 37. Podczas tworzenia formularza oceny okresowej pracownika musi zostać zwizualizowany przełożony lub współpracownik, który będzie wypełniał arkusz oceny. Również musi nastąpić wizualizacja kompetencji weryfikowanych podczas tej oceny dla każdego pracownika. 38. Ocena okresowa pracownika powinna być automatycznie uruchomiona po zdefiniowaniu daty rozpoczęcia. Powinna trwać maksymalnie do wskazanej przy konfiguracji formularza daty zakończenia. 39. Osoby na stanowiskach kierowniczych muszą widzieć wszystkie teczki osobowe swoich podwładnych oraz ich oceny pracownicze. 40. Osoby na stanowiskach kierowniczych w ramach widoku swoich podwładnych muszą widzieć oceny pracowników w toku. W kolejnym kroku muszą widzieć ankiety uzupełnione przez podwładnych, w których mogą już dokonać oceny finalnej.   **Funkcjonalności pozostałe:**   1. SEOD musi umożliwiać filtrowanie słownika JRWA na potrzeby oznaczania spraw i prowadzenia rejestrów. Filtrowanie musi być możliwe co najmniej wg kryteriów:    1. tylko hasła wykorzystywane przez pracownika,    2. tylko hasła wykorzystywane przez całą jednostkę,    3. brak filtrowania – pełna lista haseł. 2. SEOD musi zawierać moduł umożliwiający rejestrację pism kierowanych do pracowników, komórek. 3. Rejestracja musi odbywać się analogicznie do rejestracji korespondencji wychodzącej do interesanta. 4. SEOD musi zapewnić możliwość wyboru osoby i komórki ze struktury organizacyjnej będącej odbiorcą takiej korespondencji. Struktura organizacyjna musi być prezentowana analogicznie jak w module dedykowanym administratorowi, czyli w strukturze drzewa. 5. Korespondencja wewnętrzna po rejestracji i wysyłce z poziomu pracownika komórki musi trafiać do rejestrów dokumentów wpływających do urzędu. SEOD musi zapewnić rejestrację ich w odrębnym dzienniku. SEOD musi zapewnić wzajemne wskazanie zapisów: pismo wewnętrzne u nadawcy wskazuje na pismo wewnętrzne u odbiorcy. Mechanizm tworzenia korespondencji wewnętrznej musi być wykorzystywany w komunikacji z jednostkami organizacyjnymi. 6. SEOD musi umożliwiać generację korespondencji seryjnej na podstawie dostępnych szablonów. Korespondencja seryjna musi generować wszystkie pisma dla poszczególnych adresatów w jednym pliku. Elementami zmiennymi w szablonie korespondencji seryjnej muszą być dane adresatów. Procedura generacji korespondencji seryjnej nie może blokować możliwości edycji wygenerowanej treści do momentu ostatecznej akceptacji. 7. SEOD musi umożliwiać generację korespondencji wychodzącej na podstawie dostępnych szablonów. Musi być możliwe utworzenie jednorodnych odpowiedzi do wielu adresatów z wykorzystaniem szablonów (wzorców) jednocześnie, bez tworzenia odrębnych pism dla każdego z adresatów i zapisanie automatyczne utworzonych odrębnych plików odpowiedzi w metadanych pisma. Elementami zmiennymi w szablonie korespondencji seryjnej muszą być dane adresatów. Procedura generacji korespondencji seryjnej nie może blokować możliwości edycji wygenerowanej treści do momentu ostatecznej akceptacji. 8. SEOD musi umożliwiać stanowiskom posiadającym dostęp do dokumentacji opatrywanie jej komentarzami. Komentarze mogą być prywatne, bądź publiczne i musi istnieć możliwość wskazania, że treść danego komentarza publicznego ma się znaleźć w metryce sprawy. Komentarze prywatne musza być widoczne tylko dla ich autorów. Komentarze publiczne mają być widoczne dla wszystkich stanowisk posiadających dostęp do dokumentacji. 9. SEOD musi umożliwiać uprawnionemu użytkownikowi zasilenie listy interesariuszy dokumentacji listą pochodzącą z innej dokumentacji poprzez jej skopiowanie. 10. SEOD musi umożliwiać wskazanie adresatów dokumentacji (która będzie podstawą powstania przesyłek wychodzących) poprzez jednokrotne przydzielenie wszystkich interesariuszy dokumentacji. Ponadto użytkownik musi mieć możliwość usuwania po jednym adresatów przydzielonych w ten sposób. 11. SEOD musi pozwalać na tworzenie grup adresatów w celu ich łatwiejszego wskazania. 12. Uprawniony użytkownik musi mieć możliwość zarejestrowania sprawy której rozpatrywanie rozpoczęło się przed wdrożeniem aplikacji, w tym podanie jej numeru, celem kontynuowania postępowania i możliwości dołączania nowej dokumentacji do tak utworzonej sprawy. 13. SEOD musi rejestrować i prezentować uprawnionym użytkownikom na żądanie:     1. Zmiany w strukturze organizacyjnej.     2. Historię obiegu dokumentacji, w tym informację o wszystkich zmianach statusów, czynnościach wykonanych na danym etapie przez użytkowników, o punktach zatrzymania oraz datach i czasach wykonania poszczególnych czynności.     3. Historię zmian danych w formularzu dokumentacji z oznaczeniem kto i kiedy wykonał zmiany.     4. Historię zmian danych interesanta z oznaczeniem kto i kiedy wykonał zmiany. 14. SEOD powinien umożliwić dodawanie przez użytkownika notatek opisujących poszczególne sprawy, rejestrowanie ich treści za pomocą wewnętrznego edytora tekstowego oraz umieszczanie ich w dokumentach związanych ze sprawą. 15. SEOD powinien zapewnić prowadzenie odrębnej ewidencji notatek. 16. SEOD powinien umożliwiać tworzenie notatek w sprawach lub niezwiązanych ze sprawami. 17. SEOD musi pozwolić na uruchamianie formularza rejestracji notatki z kilku obszarów funkcjonalnych, bez konieczności przerywania pracy i powrotu do ewidencji notatek. |

## Aplikacja mobilna – Gmina

|  |
| --- |
| 1. Aplikacja mobilna powinna być dostępna w wersjach na popularne systemy operacyjne stosowane dla urządzeń mobilnych (Android, iOS) 2. Aplikacja powinna być podzielona na strefę ogólnodostępną oraz strefę użytkownika zalogowanego. 3. Konto użytkownika zalogowanego powinno być wspólne z kontem na platformie ePłatności. Aplikacja zapewni bezpieczne logowanie przez autoryzację z wykorzystaniem powszechnie dostępnego profilu zaufanego (<https://pz.gov.pl>) za pośrednictwem krajowego węzła identyfikacji elektronicznej z wykorzystaniem portalu ePłatnosci. 4. Pierwsza rejestracja konta użytkownika logowanego oraz jego konfiguracja dokonywana będzie na platformie ePłatnosci. Z poziomu aplikacji mobilnej dla zalogowanego użytkownika dostępne będzie dezaktywacja konta. 5. Zalogowany użytkownik posiada dostęp do danych z systemów dziedzinowych w zakresie wymaganym dla portalu ePłatności z możliwością dokonywania zapłat. Wizualizacja danych w swoim zakresie i sposobie prezentowania powinna być w miarę możliwości technicznych jednolita z portalem ePłatności. 6. Aplikacja musi umożliwić prezentację załączników (dokumentów z systemów dziedzinowych) z wykorzystaniem formatu PDF. 7. Ekran powitalny („O nas”) wizualizować ma dane pobierane z serwera a administrator powinien mieć możliwość aktualizowania i konfigurowania tych danych. 8. Aplikacja powinna mieć obsługę „Aktualności” dynamicznie pobieranych z list aktualności zarządzanych przez administratora. Obsługa aktualności z poziomu administratora musi umożliwiać zamieszczanie w niej plików graficznych oraz prosty edytor treści. Administrator może dodawać i usuwać wpisy do listy oraz określać typy „Aktualności” a użytkownik może je potem sortować i wybierać według zadanego kryterium. 9. Aplikacja powinna mieć obsługę „Miejsc” dynamicznie pobieranych z listy zarządzanej przez administratora. Obsługa „Miejsc” z poziomu administratora musi umożliwiać zamieszczanie w niej plików graficznych, prosty edytor treści, oraz określenie położenia na mapie – np. google maps. Administrator może dodawać i usuwać wpisy do listy oraz określać typy „Miejsc” a użytkownik może je potem sortować i wybierać według zadanego kryterium. 10. Aplikacja powinna zawierać obsługę i wizualizację „Galerii” z podziałem na kategorie. Galeria jest dostępna dla użytkowników niezalogowanych. 11. Aplikacja mobilna musi otrzymywać powiadomienia z systemów dziedzinowych zgodnie z ustawieniami w module ePłatności i kontem zalogowanego użytkownika. 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. 12. Aplikacja umożliwi automatyczne wysłanie e-maili do gminy. System umożliwi wybranie tematu wiadomości i automatycznie skieruje ją do osoby odpowiedzialnej za dane zadanie. 13. Aplikacje mobilne powinny być udostępnione na powszechnie dostępnych serwisach do ich pobierania. |

## Przełączniki sieciowe - szt. 2 – wymagania minimalne

|  |
| --- |
| Urządzenia sieciowe i osprzęt sieciowy pozwalający na przyłączenie do szerokopasmowego Internetu. Przełącznik wielowarstwowy L2/L3, zarządzany  Typ i liczba portów:  Min. 24 porty 10/100/1000BaseT RJ-45, min. uplink 4x10G SFP+  Porty SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:   * Gigabit Ethernet 1000Base-SX * Gigabit Ethernet 1000Base-LX/LH * 10Gigabit Ethernet 10GBase-SR * 10Gigabit Ethernet 10GBase-LR * 10Gigabit Ethernet typu twinax   Port konsoli USB Type-B/RJ45  Porty dostępowe przełącznika musza być zgodne ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)  Parametry wydajnościowe:   * Przepustowość przełącznika (switching bandwidth) min. 125 Gb/s * Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów min. 95 Mpps * Pamięć DRAM – min. 512 MB * Pamięć flash – min. 256 MB * Wielkość bufora pakietów – min. 1,5 MB * Min. 255 grup IGMP * Min. 4 grupy połączeń zagregowanych typu „port channel” LACP * Min. 8 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP * Min. 512 wpisów w listach kontroli dostępu ACL * Min. 8 kolejek sprzętowych   Obsługa:   * Min. 255 aktywnych sieci VLAN * Min. 8 000 adresów MAC * Min. 32 statyczne trasy IPv4 * Min. 16 interfejsów L3 * ramek Ethernet Jumbo 9 000 B   Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:   * IEEE 802.1w Rapid Spanning Tree * Per-VLAN Rapid Spanning Tree (PVRST+) * IEEE 802.1s Multi-Instance Spanning Tree * Obsługa 126 instancji protokołu STP   Przełącznik musi wspierać:   * obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego. * protokół rejestracji GARP VLAN (GVRP)   Przełącznik musi wspierać mechanizmy związane z bezpieczeństwem sieci:   * Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level) * Autoryzacja użytkowników w oparciu o IEEE 802.1X * Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X * Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, * Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+, * Obsługa HTTPS, SSH, SSL, * Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP)   Przełącznik musi wspierać mechanizmy związane z zapewnieniem jakości usług w sieci:  • Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi  • Implementacja algorytmu Weighted Round Robin dla obsługi kolejek  • Możliwość obsługi jednej z kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)  • Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP  • Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi,  • Kontrola sztormów dla ruchu broadcast/multicast/unicast  • Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP  Przełącznik musi wspierać obsługiwać standardy komunikacyjne:  IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3ae 10 Gbit/s Ethernet over fiber for LAN, IEEE 802.3an 10GBase-T 10 Gbit/s Ethernet over copper twisted pair cable, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w Rapid STP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.3af, IEEE 802.3at, IEEE 802.1AB Link Layer Discovery Protocol, IEEE 802.3az Energy Efficient Ethernet  Obsługa protokołu NTP  Funkcje DHCP server, DHCP relay  Obsługa IGMPv1/2/3 i MLDv1/2 Snooping, DHCP snooping  Blokowanie Head of Line (HOL)  Zabezpieczenie przed wejściem w pętlę Unidirectional Link Detection (UDLD)  Zapobieganie atakom DoS  Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6  Zarządzanie   * Port konsoli * Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją * Obsługa protokołów SNMPv3, SSHv2, https, syslog * Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia * Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki * Obsługa protokołu LLDP i LLDP-MED * Obsługa funkcji Plug & Play * Przycisk reset   Inne   * Zasilanie 230V AC * Wysokość maksymalnie 1U, montowany w szafie typu RAC 19’’ * Wraz z przełącznikami należy dostarczyć 8 szt. kabli DAC o przepustowości 10G SFP+ |

## Firewall - szt. 1 – wymagania minimalne

|  |
| --- |
| Wymagania Ogólne  Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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 musi wspierać 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 – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.   Interfejsy, Dysk, Zasilanie:   1. System realizujący funkcję Firewall musi dysponować minimum:  * 10 portami Gigabit Ethernet RJ-45.  1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System realizujący funkcję Firewall musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 128 GB. 4. System musi być wyposażony w zasilanie AC.   Parametry wydajnościowe:   1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. 5. 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 1.4 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.   Funkcje Systemu Bezpieczeństwa:  W ramach dostarczonego systemu ochrony muszą być 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 – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 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. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone 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. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system   Polityki, Firewall   1. ~~.~~ Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać 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 musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 3. Element systemu realizujący funkcję Firewall musi integrować 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 * Google Cloud Platform (GCP). * OpenStack. * VMware NSX.   Połączenia VPN   1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  * Wsparcie dla IKE v1 oraz v2. * Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19 i 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. * 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. * Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.  1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:  * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać 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 musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.   Routing i obsługa łączy WAN   1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:  * Routingu statycznego. * Policy Based Routingu. * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.   Funkcje SD-WAN   1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.   Zarządzanie pasmem   1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.   Ochrona przed malware   1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.   Ochrona przed atakami   1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać 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) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.   Kontrola aplikacji   1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.   Kontrola WWW   1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.   Uwierzytelnianie użytkowników w ramach sesji   1. System Firewall musi umożliwiać 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. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 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 powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępni dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.   Logowanie   1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.   Certyfikaty  Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:   * ICSA lub EAL4 dla funkcji Firewall.   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 producenta, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |

## Usługi wdrożenia i konfiguracji oprogramowania

|  |
| --- |
| Usługa w zakresie wdrożenia i konfiguracji oprogramowania tj. aplikacji opisanych w pkt. 5.6 - 5.10 SOPZ.  W ramach pozycji:   1. Zostanie zainstalowane środowisko bazodanowe (robocze i testowe) z wykorzystaniem dostarczonych licencji. 2. Zostanie zainstalowane dostarczone oprogramowanie wraz z niezbędnymi modułami, w lokalizacjach wskazanych przez Wnioskodawcę na nowej platformie sprzętowej. 3. Zostanie wykonane wdrożenie i konfiguracja integracji dostarczonych modułów celem stworzenia jednolitego systemu informatycznego z obecnie posiadanymi rozwiązaniami dziedzinowymi. 4. Zostanie skonfigurowane dostarczone oprogramowanie z uwzględnieniem wyników analizy procesów biznesowych zachodzących u Wnioskodawcy. 5. Zostaną wygenerowane konta użytkowników wraz z prawami dostępu do aplikacji i modułów oraz zintegrowane z rozwiązaniami funkcjonującymi u Zamawiającego. 6. Zostaną przeprowadzone testy użytkownika na bazie roboczej i produkcyjnej celem weryfikacji prawidłowości działania. 7. Zostaną uruchomione e-usługi. 8. Zostanie wykonana integracja z systemami dziedzinowymi posiadanymi przez Zamawiającego – systemy firmy BUK Softres. 9. Zostanie wykonana i dostarczona dokumentacja powykonawcza.   Dokumentacja Powykonawcza  Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową, techniczną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej w formacie edytowalnym oraz w co najmniej jednym egzemplarzu papierowym.  W szczególności dokumentacja ta powinna zawierać następujące elementy:   1. Opis sposobu licencjonowania elementów aplikacji i środowiska. 2. Opis wykonanej konfiguracji wdrożonego systemu oraz urządzeń. 3. Opis architektury logicznej systemu. 4. Opis zainstalowanej bazy danych. 5. Instrukcje obsługi i instrukcje użytkowania dla wersji dostarczonego oprogramowania z podziałem na poszczególne moduły. 6. Opis sposobu przetwarzania danych oraz wykaz zbiorów danych osobowych. |

## Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania

|  |  |  |
| --- | --- | --- |
| Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania. | | |
|  | **Usługi** | Celem prac jest przygotowanie środowiska teleinformatycznego, na potrzeby realizacji e-usług publicznych, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie.  Część sprzętowa powinna zostać oparta na systemie wirtualizacji zasobów IT.  Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. 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.  **W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową**.  Zamawiający wymaga następującego zakresu usług realizowanego w porozumieniu z Zamawiającym:   * 1. Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia.   2. Sporządzenia Dokumentacji Systemu według której nastąpi realizacja. Dokumentacja Systemu musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia. W szczególności:      1. koncepcję techniczną projektu, która powinna zawierać opis mechanizmów działania systemu z wykorzystaniem dostarczonych i rozbudowywanych elementów sprzętowych.      2. schematy połączeń      3. mechanizmy działania głównych elementów sprzętowych: * sieć LAN * klaster wirtualizacyjny * system backupu i archiwizacji danych * system serwerowy * system macierzowy * Firewall/UTM   + 1. testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności     2. sposób odbioru uzgodniony z Zamawiającym     3. listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu     4. opis przypadków, w których projekt dopuszcza niedziałanie systemu     5. realizacja wdrożenia nastąpi według Planu Wdrożenia po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą   Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Planem Wdrożenia. |
|  | **Montaż i fizyczne uruchomienie systemu** | **Zamawiający wymaga, aby Wykonawca zainstalował całośćdostarczonego 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 np.: laptopy, 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 dostarczonego oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji. 2. Instalacja i konfiguracja dostarczonego oprogramowania do systemu wykonywania backupu i archiwizacji danych. 3. Instalacja dostarczonego 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 dostarczonych systemów operacyjnych dla serwerów wirtualnych. |
|  | **Konfiguracja przełączników sieci LAN:** | Zamawiający wymaga stworzenia połączeń sieciowych pomiędzy wszystkimi lokalizacjami występującymi w projekcie według topologii gwiazdy. Centralnym punktem będzie serwerownia zlokalizowana w Urzędzie.  Przełączniki będą stanowiły centralny punkt wymiany danych sieciowych z punktu widzenia warstwy drugiej modelu ISO/OSI – L2 (warstwa łącza danych) oraz zapewnią wsparcie dla protokołu STP (protokół drzewa rozpinającego).  Konfiguracja dostarczanych przełączników w zakresie:   * 1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.   2. Stworzenia odpowiednich konfiguracji STACK z wykorzystaniem dedykowanych modułów.   3. Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym).   4. Konfiguracja połączeń pomiędzy przełącznikami sieci LAN.      1. Rozpięcie połączeń przełączników IDF na centralne przełączniki CORE z zachowaniem nadmiarowości z wykorzystaniem wszystkich dostępnych portów uplink.      2. Z wykorzystaniem połączeń światłowodowych oraz miedzianych.      3. Agregacja połączeń celem uzyskania pasma nx10Gbps w obu kierunkach ruchu.      4. Należy wykorzystać wkładki o najwyższej możliwej przepustowości dla danego połączenia np.: dla portu o możliwej przepustowości 1/10Gbs (wkładka: SFP/SFP+), należy wykorzystać wkładki SFP+ o przepustowości 10Gbps.   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. Ustawienie serwera czasu dla urządzeń sieci LAN – przełączników sieciowych - na klaster firewall.   9. Zamawiający wymaga instalacji i konfiguracji serwera logów dla urządzeń sieci LAN (maszyna wirtualna) – przełączników sieciowych, z graficznym interfejsem przeszukiwania. Zamawiający dopuszcza rozwiązania Open Source.   10. Zamawiający wymaga instalacji i konfiguracji dedykowanego serwera monitorowania pracy urządzeń sieciowych z graficznym interfejsem przeszukiwania (maszyna wirtualna): przełączniki sieciowe, drukarki, UTM. Zamawiający dopuszcza rozwiązania Open Source.   11. Wykonawcza skonfiguruje urządzenia aby raportowały, przesyłały dane do zainstalowanego serwera logów i monitorowania sieci.   12. Testowanie obsługi ruchu sieciowego.   13. Testowanie skuteczności zabezpieczeń. |
|  | **Konfiguracja elementów bezpieczeństwa sieciowego.** | Urządzenie firewall/modernizacja konfiguracji urządzenia UTM 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. Przygotowanie projektu włączenia urządzenia do sieci LAN urzędu. 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 (np.: RCIM). 14. Konfiguracja logowania i raportowania. |
|  | **Serwery pod wirtualizację** | Zamawiający wymaga instalacji i konfiguracji dostarczonych serwerów celem stworzenia bazy sprzętowej dla klastra niezawodnościowego i wydajnościowego stworzonego na bazie dostarczonych serwerów i oprogramowania do wirtualizacji. |
|  | **Macierz**  **dyskowa** | Macierz musi być wykorzystywana do gromadzenia i przechowywania „danych produkcyjnych” – wykorzystywanych przez oprogramowanie dziedzinowe. Musi zostać podłączona do środowiska wirtualizacyjnego (klaster serwerów) |
|  | **Serwera NAS - Backup** | Urządzenie NAS należy dołączyć do infrastruktury Zamawiającego celem stworzenia miejsca na przechowywanie danych backupu. |
|  | **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.  Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej min. w pełnym zakresie danych i rejestrów systemów dziedzinowych. |
|  | **Serwer SMTP** | Zamawiający wymaga zainstalowania oraz uruchomienia i skonfigurowania dedykowanego serwera SMTP. Serwer SMTP powinien być uruchomiony na dedykowanym wirtualnym serwerze pracującym pod kontrolą systemu Linux.  Serwer SMTP będzie wykorzystywany na potrzeby wysyłania powiadomień systemowych między innymi z:   * Urządzeń sieciowych * Serwerów * Macierzy dyskowej * Systemu zarządzania kopiami zapasowymi * Systemu wirtualizacji serwerów * Aplikacji   Zamawiający wymaga zabezpieczenia serwera w taki sposób, aby uniemożliwić przesyłanie wiadomości z nieautoryzowanych źródeł. Zamawiający wymaga, aby wysyłane powiadomienia były poprawnie dostarczane na zewnętrzne konta email. |
|  | **Uruchomienie środowiska wirtualizacyjnego.** | Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w zakresie:   1. Aktywacja licencji oprogramowania wirtualizacyjnego na stronie producenta. 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 dostarczonych serwerach. 5. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów. 6. Konfiguracja i podłączenie serwerów wirtualizacyjnych 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. 7. Konfiguracja i podłączenie serwerów wirtualizacyjnych 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. 8. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q. 9. Przygotowanie koncepcji wirtualizacji fizycznych maszyn. 10. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym. 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). |
|  | **System backupu** | 1. Instalacja oprogramowania zarządzającego wykonywaniem kopii zapasowych. 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 NAS.     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 przywrócony.   System musi zostać podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na serwerze NAS oraz replikowanych na taśmy streamera HP Ultrium 1760 SAS LTO-4. |
|  | **Usługa katalogowa.** | **Instalacja usługi katalogowej wraz z dodatkowymi komponentami w taki sposób, aby spełnione były poniższe wymagania celem świadczenia e-usług publicznych:** |
|  | **Zaplanowanie liczby serwerów na potrzeby usługi katalogowej oraz serwerów plików** | Taka liczba serwerów, aby w przypadku awarii pojedynczego serwera był zapewniony ciągły dostęp do usługi katalogowej, a w szczególności mechanizmy uwierzytelniania oraz rozwiązywania nazw oraz serwera plików. Zamawiający dopuszcza wykorzystanie serwerów wirtualnych uruchomionych na dostarczonym środowisku wirtualizacyjnym. |
|  | **Wersja systemu operacyjnego serwerów** | Zastosowany system operacyjny musi zapewniać, co najmniej:   1. możliwość uruchomienia usługi katalogowej w trybie usługi 2. możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń 3. możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem (w tym przynależność do grup zabezpieczeń) 4. możliwość zarządzania usługą katalogową poprzez interfejs graficzny oraz CLI 5. możliwość zainstalowania lokalnego Centrum Certyfikacji zapewniającego wydawanie niekwalifikowanych certyfikatów X.509 umożliwiających uwierzytelnianie na stacjach roboczych i serwerach z wykorzystaniem kart kryptograficznych, szyfrowanie danych |
|  | **Instalacja systemu operacyjnego serwerów** | Instalacja systemu operacyjnego serwerów w taki sposób, aby w łatwy sposób możliwe było włączenie funkcji szyfrowania partycji systemowej za pomocą wbudowanych w system operacyjny mechanizmów. Po instalacji systemy operacyjne muszą zostać prawidłowo aktywowane. Następnie należy zainstalować niezbędne aktualizacje oraz poprawki związane z bezpieczeństwem udostępnione przez producenta systemu operacyjnego. |
|  | **Uruchomienie usługi katalogowej oraz niezbędnych komponentów, migracja danych do/z obecnej usługi katalogowej** | Uruchomienie usługi katalogowej, komponentów odpowiedzialnych za rozwiązywanie nazw. Usługa katalogowa musi być uruchomiona na wszystkich serwerach przewidzianych do rozbudowy. Na wszystkich serwerach muszą być uruchomione także komponenty odpowiedzialne za rozwiązywanie nazw. Należy szczególną uwagę zwrócić na poprawne funkcjonowanie mechanizmów replikacji. Usługę katalogową należy skonfigurować w taki sposób, aby możliwe było wykorzystanie możliwie wszystkich funkcjonalności oferowanych przez zastosowane systemy operacyjne, a w szczególności możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń, możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem.  Utworzenie struktury jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego.  Zamawiający wymaga skonfigurowania delegacji uprawnień do zadanych jednostek organizacyjnych dla administratorów niższego poziomu. Administratorzy niższego poziomu powinni mieć uprawnienia do:   1. Resetowania haseł użytkowników 2. Odblokowywania kont użytkowników 3. Zmiany atrybutów „Display Name” oraz „Last name”   Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi:   1. Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości 2. Śledzenie zmian dotyczących tworzenia, usuwania obiektów   Zamawiający wymaga skonfigurowania dwóch stacji zarządzających. Zarządzanie środowiskiem będzie się odbywać z poziomu stacji zarządzających (usługa katalogowa, wszystkie możliwe do zarządzania z poziomu stacji zarządzającej komponenty serwerów). |
|  | **Konfiguracja polityki haseł oraz polityki blokowania kont** | Konfiguracja globalnej polityki haseł dla domeny:   1. Hasło musi zawierać minimum 8 znaków 2. Maksymalny czas ważności hasła: do ustalenia z Zamawiającym 3. Minimalny czas, po którym możliwa jest zmiana hasła: do ustalenia z Zamawiającym 4. Hasło musi spełniać zasady złożoności   Konfiguracja polityki haseł dla kadry zarządzającej:   1. Hasło musi zawierać minimum 10 znaków 2. Maksymalny czas ważności hasła: 30 dni 3. Minimalny czas, po którym możliwa jest zmiana hasła: 240 dni 4. Hasło musi spełniać zasady złożoności   Po 3 nieudanych próbach uwierzytelniania konto powinno być blokowane na 30 minut. Automatyczne anulowanie blokady ma następować po 480 minutach.  Szczegółowe dane zostaną przekazane na etapie konfiguracji. |
|  | **Stworzenie skryptów służących do tworzenia struktury usługi katalogowej** | Po oddaniu wdrożonego systemu do eksploatacji konieczne będzie tworzenie nowych kont użytkowników, grup zabezpieczeń oraz jednostek organizacyjnych. Zamawiający oczekuje stworzenia przez Wykonawcę skryptów ułatwiających te zadania.  **Założenia skryptu tworzącego nowe jednostki organizacyjne oraz grupy:**   1. Możliwość skonfigurowania za pomocą zmiennych w skrypcie, co najmniej:    1. ścieżki i nazwy pliku wejściowego    2. ścieżki i nazwy pliku logującego    3. ścieżki i nazwy pliku wyjściowego (właściwego skryptu)    4. nazwy FQDN domeny    5. nazwy NetBIOS domeny    6. nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty    7. ścieżek do udziałów dyskowych SHARE1 oraz SHARE2 2. Skrypt ma pobierać z pliku wejściowego listę jednostek organizacyjnych 3. Skrypt tworzy nowe jednostki organizacyjne w jednostce organizacyjnej nadrzędnej zdefiniowanej w części konfiguracyjnej skryptu 4. Skrypt tworzy nowe grupy zabezpieczeń o nazwie G\_Nazwa\_Jednoski\_Organizacyjnej 5. Skrypt tworzy foldery:    1. \\DOMENA\Public\SHARE1    2. \\DOMENA\Public\SHARE2   Foldery muszą posiadać tak ustawione parametry zabezpieczeń, aby użytkownicy nie mogli samodzielnie tworzyć nowych katalogów ani plików w lokalizacjach \\DOMENA\SHARE1 oraz \\DOMENA\SHARE2.   1. Skrypt tworzy podkatalogi: [\\DOMENA\Public\SHARE1\Nazwa\_Jednostki\_Organizacyjnej](file://DOMENA/Public/SHARE1/Nazwa_Jednostki_Organizacyjnej) oraz [\\DOMENA\Public\SHARE2\Nazwa\_Jednostki\_Organizacyjnej](file://DOMENA/Public/SHARE2/Nazwa_Jednostki_Organizacyjnej) 2. Skrypt nadaje uprawnienia do utworzonych podkatalogów według założeń:    1. [\\DOMENA\Public\SHARE1\Nazwa\_Jednostki\_Organizacyjnej](file://DOMENA/Public/SHARE1/Nazwa_Jednostki_Organizacyjnej):       1. Administratorzy Domeny – Pełna kontrola       2. Grupa G\_Nazwa\_Jednostki\_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa\_Jednostki\_Organizacyjnej       3. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu       4. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze    2. [\\DOMENA\Public\Share2\Nazwa\_Jednostki\_Organizacyjnej](file://DOMENA/Public/Share2/Nazwa_Jednostki_Organizacyjnej):       1. Administratorzy Domeny – Pełna kontrola       2. Grupa G\_Nazwa\_Jednostki\_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa\_Jednostki\_Organizacyjnej       3. Użytkownicy Uwierzytelnieni - Odczyt       4. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu       5. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze 3. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina) 4. Działanie skryptu właściwego musi być w całości logowane do pliku tekstowego, opatrzonego bieżącą datą i godziną w celu umożliwienia każdorazowego zweryfikowania poprawności działania   **Założenia skryptu tworzącego nowe konta użytkowników:**   1. Możliwość skonfigurowania za pomocą zmiennych w skrypcie co najmniej:    1. ścieżki i nazwy pliku wejściowego    2. ścieżki i nazwy pliku logującego    3. ścieżki i nazwy pliku wyjściowego (właściwego skryptu)    4. nazwy FQDN domeny    5. nazwy NetBIOS domeny    6. nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty    7. ścieżki do udziału sieciowego HOME    8. litery dysku katalogu domowego 2. Skrypt ma pobierać z pliku wejściowego listę kont użytkowników w formacie:   Nazwa Uzytkownika;  Imie;Nazwisko:  Haslo;Dzial;NumerTelefonu   1. Skrypt tworzy nowe konta użytkowników w jednostce organizacyjnej nadrzędnej zdefiniowanej w części konfiguracyjnej skryptu pobierając wszystkie niezbędne dane z pliku wejściowego 2. Nowo utworzone konta użytkowników muszą mieć jednorazowo ustawione hasła – użytkownik musi zmienić hasło podczas pierwszego logowania 3. Skrypt tworzy katalog [\\DOMENA\HOME\NazwaUzytkownika](file://DOMENA/HOME/NazwaUzytkownika) 4. Skrypt nadaje uprawnienia do utworzonych katalogów użytkowników według założeń:    1. Administratorzy Domeny – Pełna kontrola    2. Użytkownik – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu NazwaUzytkownika    3. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu    4. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze 5. Skrypt ma ustawić dla każdego konta użytkownika literę dysku domowego oraz poprawną ścieżkę sieciową 6. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina) 7. Działanie skryptu właściwego musi być w całości logowane do pliku tekstowego, opatrzonego bieżącą datą i godziną w celu umożliwienia każdorazowego zweryfikowania poprawności działania 8. Skrypt ma wygenerować dla każdego zakładanego konta osobny plik tekstowy zawierający między innymi: Nazwę użytkownika, Imię, Nazwisko, Hasło do pierwszego zalogowania. Tak utworzone pliki mogą zostać wydrukowane i przekazane użytkownikom.   Powyżej opisane skrypty muszą posiadać w treści kodu stosowne komentarze opisujące działanie skryptów. Skrypty zostanę przekazane Zamawiającemu w wieczyste użytkowanie bez dodatkowych opłat wraz ze stosowną dokumentacją użytkownika oraz szczegółową instrukcja obsługi.  Zamawiający wymaga wygenerowania kont użytkowników, katalogów domowych użytkowników, jednostek organizacyjnych, grup zabezpieczeń za pomocą opracowanych skryptów. |
|  | **Skonfigurowanie mapowania zasobów sieciowych** | Skonfigurowanie mechanizmów mapowania dysków sieciowych dla systemów klienckich Windows.  Mapowane mają być między innymi zasoby:  \\DOMENA\Public\SHARE1  \\DOMENA\Public\SHARE2  Oraz określone przez Zamawiającego drukarki sieciowe.  Zamawiający wymaga skonfigurowanie mapowania dysków sieciowych za pomocą zasad grup na dwa sposoby:   1. Z wykorzystaniem skryptów logowania 2. Z wykorzystaniem mechanizmów zaimplementowanych w systemach Microsoft Windows Vista i nowszych (Wymagane jest także skonfigurowanie automatycznej instalacji niezbędnych składników na stacjach klienckich. Zamawiający nie dopuszcza instalacji wymaganych składników ręcznie). |
|  | **Uruchomienie i skonfigurowanie serwera plików oraz wydruków** | Zamawiający wymaga uruchomienie oraz skonfigurowanie serwerów plików oraz serwerów wydruków tak, aby były spełnione poniższe założenia:  Serwery plików muszą być skonfigurowane z wykorzystaniem dostępnych w zaoferowanych systemach operacyjnych serwerów mechanizmów zwiększających dostępność danych poprzez zastosowanie technologii replikacji systemu plików. Konieczność taka podyktowana jest zapewnieniem ciągłości dostępu do krytycznych danych Wnioskodawcy w przypadku awarii jednego z serwera plików. Zastosowane mechanizmy replikacji systemu plików muszą zapewniać:   * Replikację multi-master z rozwiązywaniem konfliktów * Wykorzystanie algorytmów kompresji danych wykrywających zmiany na poziomie bloków danych w obrębie plików – replikacji podlegają tylko zmienione bloki danych, a nie całe pliki.   Serwery plików muszą być skonfigurowane w taki sposób, aby ograniczać ekspozycję danych dla użytkowników oraz grup, które nie mają do nich dostępu.  Na serwerach plików muszą być skonfigurowana przydziały dyskowe dla użytkowników i grup. Zamawiający wymaga także skonfigurowania przydziałów dyskowych dla wskazanych folderów.  Zamawiający wymaga włączenia i skonfigurowania mechanizmów uniemożliwiających przechowywanie niedozwolonych typów plików. Konieczne jest także skonfigurowanie mechanizmów raportujących.  Zamawiający wymaga skonfigurowania mechanizmów przekierowania lokalnych folderów „Moje Dokumenty” oraz „Pulpit” ze stacji roboczych na serwery plików. Funkcjonalność ta musi poprawnie działać dla systemów klienckich Zamawiającego.  Zamawiający wymaga stworzenie domyślnego, obowiązującego profilu wędrującego dla klienckich systemów operacyjnych. Domyślny profil ma uwzględniać opracowanie i wykonanie grafiki na pulpit komputera klienta. Grafika będzie akceptowana przez Zamawiającego. Zamawiający wymaga stworzenia i przypisania odpowiednich polityk globalnych dla wymuszenia stosowania obowiązkowych (niemodyfikowalnych) profili mobilnych.  Zamawiający wymaga opracowania koszyka dozwolonych aplikacji wraz z implementacją polityk globalnych ograniczających dostęp do aplikacji z wykorzystaniem np.: dedykowanych ustawień związanych z polityką kontroli uruchomienia aplikacji.  Zamawiający wymaga skonfigurowania parametrów audytu dla serwerów plików umożliwiających między innymi:   1. Określenie daty, czasu, nazwy użytkownika, który usunął / próbował usunąć plik/folder 2. Określenie daty, czasu, nazwy użytkownika, który zapisał / próbował zapisać plik/folder 3. Określenia daty, czasu, nazwy użytkownika, który próbował uzyskać nieuprawniony dostęp do zasobów, do których nie ma uprawnień.   Zamawiający wymaga uruchomienia serwera wydruków oraz podłączenia i skonfigurowania drukarek sieciowych. Zamawiający wymaga opracowania i skonfigurowania odpowiednich polityk globalnych mapujących odpowiednie drukarki użytkownikom. Niedopuszczalne jest przyłączenie wszystkim użytkownikom wszystkich dostępnych drukarek. Użytkownicy powinni mieć przyłączone drukarki znajdujące się najbliżej jego komputera. |
|  | **Serwery uwierzytelniające** | Zamawiający wymaga uruchomienia serwerów uwierzytelniających współpracujących z infrastrukturą AD, realizujących funkcję uwierzytelniania na dostarczanych przełącznikach sieciowych.  Zamawiający wymaga uruchomienia co najmniej dwóch instancji serwera uwierzytelniania w celu zachowania redundancji na dwóch niezależnych serwerach.  Instancja serwera może być uruchomiona na serwerach domenowych z zastrzeżeniem, że będzie ona kompatybilna z usługami uruchomionymi na tych serwerach i nie będzie wpływać negatywnie na ich pracę.  Zamawiający wymaga skonfigurowania odpowiednich polityk bezpieczeństwa na zainstalowanych serwerach uwierzytelniających bazujących na utworzonych w strukturze usługi katalogowej Zamawiającego grupach.  Jeżeli jest potrzebna, Zamawiający wymaga dostarczenia licencji na instalowane serwery uwierzytelniające oraz ujęcia ich ceny w ofercie. |
|  | **Dołączenie stacji roboczych do domeny** | Zamawiający wymaga dołączenia wszystkich stacji roboczych do domeny. W procesie dołączania stacji roboczych do domeny konieczne jest przeprowadzenie migracji profili użytkowników mająca na celu zachowanie specyficznych ustawień lokalnych kont użytkowników (miedzy innymi zachowanie ustawień aplikacji oraz poczty elektronicznej). Po zalogowaniu się użytkownika na konto domenowe użytkownik nie powinien zauważyć znaczących różnic w wyglądzie profilu (zachowane tapety oraz ustawienia pulpitu, dotychczas działające aplikacje powinny działać jak dotychczas bez potrzeby ponownej konfiguracji). |
|  | **Uruchomienie usług umożliwiającą instalację i zarządzanie aktualizacjami stacji roboczych Windows** | Zamawiający wymaga uruchomienia i skonfigurowania usług dostępnych w dostarczonych systemach operacyjnych serwerów umożliwiających zarządzanie aktualizacjami stacji roboczych i serwerów Windows według założeń:   1. Aktualizacje i poprawki mają być pobierane na serwer instalacyjny za pośrednictwem sieci Internet 2. Administrator zatwierdza aktualizacje do instalacji 3. Stacje robocze i serwery pobierają i automatycznie instalują zatwierdzone przez Administratora aktualizacje według określonego harmonogramu   Zamawiający wymaga skonfigurowania co najmniej następujących parametrów:   1. Systemów operacyjnych, aplikacji oraz wersji językowych, dla których będą pobierane aktualizacje 2. Kategorii aktualizacji 3. Grup komputerów (KOMPUTERY, SERWERY, KOMPUTERY-TEST, SERWERY-TEST) 4. Polityk globalnych przypisujących komputery znajdujące się w określonych jednostkach organizacyjnych do odpowiednich grup komputerów 5. Zasad automatycznego zatwierdzania nowych aktualizacji. 6. Mechanizmów raportowania (email) |
|  | **Przygotowanie infrastruktury PKI** | Zamawiający wymaga przygotowania i uruchomienia wewnętrznej infrastruktury PKI. Zamawiający posiada stacje robocze pracujące w oparciu o następujące systemy operacyjne: Windows 10.  Wymagana przez Zamawiającego konfiguracja zawiera co najmniej:   1. Zaplanowanie i uruchomienie wewnętrznej struktury CA 2. Konfiguracja szablonów certyfikatów 3. Wydanie certyfikatów dla serwerów oraz stacji roboczych 4. Zastosowanie mechanizmów bezpieczeństwa poprzez możliwość backupu archiwizacji kluczy prywatnych wydawanych certyfikatów. 5. Wskazanie wszystkich możliwych dróg publikacji list CRL 6. Instalacji i konfiguracji stacji (komputer PC) do wydania kart – stacja do personalizacji. |
|  | **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 |
|  | **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 szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu.   1. Wszelkie zmiany w stosunku do Dokumentacji systemu z podaniem ich powodów. 2. Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację). 3. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały. 4. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały. 5. Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów. |

## Diagnoza cyberbezpieczeństwa

|  |
| --- |
| Pozycja dotyczy przeprowadzenia diagnozy bezpieczeństwa zgodnie z wymaganiami konkursu programu "Cyfrowa Gmina", opisanymi na stronie <https://www.gov.pl/web/cppc/cyfrowa-gmina>  Wykonawca musi wykonać usługę zgodnie z zakresem oraz z formularzem stanowiącym załącznik do dokumentacji konkursowej. załączniku nr  Załącznik\_nr\_8\_-\_Formularz\_informacji\_związanych\_z\_przeprowadzeniem\_diagnozy\_cyberbezpieczeństwa  Diagnoza musi zostać przeprowadzona przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. |