Załącznik nr 5

Wyciąg ze specyfikacji technicznej

(parametry minimalne)

1. Zestawienie ilościowe

Lp.	nazwa	ilość
	sprzęt	
1	Przełącznik sieci LAN	4
2	Firewall z analizatorem ruchu sieciowego	1
3	Serwer aplikacyjny	3
4	Przełącznik FC	1
5	rozbudowa macierzy	1
6	Serwer telekomunikacyjny	1
7	Rejestrator rozmów	1
8	Zestaw komputer z monitorem	20
9	notebook	15
10	UPS	1
11	Szafa 42U	1
12	Szafa 12U	4
	oprogramowanie	
13	System e-urząd	1
14	System elektronicznego obiegu dokumentów	1
15	Portal płatności i komunikacji społecznej	1
	pozostałe	
16	Sieć strukturalna LAN	180

POWIAT EŁCKI
ul. Piłsudskiego 4
19-300 EŁK

tępca Przewodniczącego
ZARZĄDU POWIATU
Anna Iwaszko

PRZEWODNICZĄCY
ZARZĄDU POWIATU
Marek Chojnowski

2. Główne parametry techniczne sprzętu

2.1. Przełącznik sieci LAN

charakterystyka	• urządzenie o stałej konfiguracji fizycznej min. 48 portów dostępowych 10/100/100 RJ-45 oraz 4 interfejsów definiowalnych wkładkami SFP+ mogących pracować z prędkością 1G • porty dostępowe o styku fizycznym RJ-45 wspierające funkcjonalność Power-over-Ethernet+ 802.3at do 30 Watt/port, • urządzenie musi umożliwiać łączenie min. 8 urządzeń w stos, • min. 256MB pamięci SDRAM oraz min. 128MB pamięci Flash • obsługa min. 16000 adresów MAC, • matryca przełączająca min 104 Gb/s • wydajność przełączania urządzenia co najmniej 76 Mpps, • automatyczne wykrywanie przeplotu (AutoMDIX) na portach miedzianych • wbudowane narzędzia do diagnozy okablowania na portach miedzianych (np. time domain reflector) • obsługa co najmniej 4000 sieci VLAN i 4000 VLAN ID, • obsługa co najmniej 1000 list kontroli dostępu (ACL) • obsługa mechanizmów dystrybucji informacji o sieciach VLAN pomiędzy przełącznikami • funkcjonalność port-fast lub równoważna •
obsługa protokołów sieciowych zgodnie ze standardami:	• IEEE 802.1x • IEEE 802.1s • IEEE 802.1w • IEEE 802.3x full duplex dla 10BASE-T i 100BASE-TX • IEEE 802.3ad • IEEE 802.1D • IEEE 802.1p • IEEE 802.1Q • IEEE 802.3 10BASE-T • IEEE 802.3u 100BASE-TX

	• IEEE 802.3z 1000BASE-X • IEEE 802.3ab 100BASE-T
Wsparcie routingu	• IPv4 i IPv6: routing statyczny, • Wsparcie dla minimum 8 interfejsów IPv4 i IPv6
Wsparcie dla mechanizmów multicast	• IGMPv1, v2, v3 snooping, • Multicast Listener Discovery snooping, • Minimum 1000 grup multicastowych, • IP Multicast VLAN
mechanizmy związane z zapewnieniem jakości usług w sieci	• obsługa co najmniej ośmiu kolejek sprzętowych, wyjściowych dla różnego rodzaju ruchu. • mechanizm automatycznej konfiguracji portów do obsługi VoIP, • flow-based QoS z wejściową i wyjściową zmianą parametrów (tzw. remarking), • zarządzanie kolejkowaniem: Stricte Priority (SPQ), Weighted Round Robin (WRR), Deficit Round Robin (DRR), • mechanizm zapobiegania powstawaniu zatorów w sieci E2E-HOL Blocking Protection
mechanizmy związane z zapewnieniem bezpieczeństwa sieci	• dostęp do urządzenia przez konsolę szeregową, SSHv2 i SNMPv3, HTTPS/SSL • wsparcie dla standardu 802.1x port-based, multiple-client, MAC authentication • obsługa mechanizmu typu Guest VLAN, MAC address lockdown, • możliwość aplikowania list kontroli dostępu (ACL) per port, MAC SA/DA, IP SA/DA, TCP/UDP port, • funkcjonalność typu STP Root Guard, STP BPDU guard lub równoważna • możliwość autoryzacji prób logowania do urządzenia za pomocą serwerów TACACS+, RADIUS i LDAP, • wsparcie dla profili sieciowych użytkowników, • możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu z pozostawieniem możliwości komunikacji z portem nadrzednym lub funkcjonalność private VLAN • monitorowanie zapytań i odpowiedzi DHCP (tzw. DHCP Snooping), DHCP Option 82, DHCP IP Spoof protection • możliwość tworzenia portów monitorujących, pozwalających na kopiowanie na port monitorujący ruchu z innego dowolnie wskazanego portu • ochrona przed rekonfiguracją struktury topologii Spanning Tree spowodowana przez niepowołane i nieautoryzowane urządzenie sieciowe,

	• gradacja poziomów uprawnień na podstawie definicji typów profili, • współpraca z systemami kontroli dostępu do sieci typu NAC lub NAP lub podobne,
inne	• obsługa grupowania portów w jeden kanał logiczny zgodnie z LACP 802.3ad • plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nie ulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian • przechowywanie co najmniej 2 obrazów systemu operacyjnego • możliwość zarządzania przy pomocy bezpłatnej aplikacji graficznej zainstalowanej na urządzeniu, dostarczanej przez producenta • możliwość zarządzania przy pomocy dedykowanej aplikacji do zarządzania infrastrukturą sieciową producenta urządzenia • możliwość montażu w szafie 19

2.2. Firewall z analizatorem ruchu sieciowego

Firewall

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System bezpieczeństwa zapewni poniższe funkcje i parametry pracy:

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
5. System realizujący funkcję Firewall powinien dysponować minimum 16 portami Ethernet 10/100/1000 Base-TX oraz 2 gniazdami SFP 1Gbps.

6. System powinien umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
7. W zakresie Firewall'a obsługa nie mniej niż 3 miliony jednoczesnych połączeń oraz 70 tys. nowych połączeń na sekundę
8. Przepustowość Firewall'a: nie mniej niż 3 Gbps dla pakietów 512 B
9. Wydajność szyfrowania VPN IPSec: nie mniej niż 1,2 Gbps
10. System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 60 GB. System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
11. System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń.
12. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:
    - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    - Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
    - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN
    - Ochrona przed atakami - Intrusion Prevention System
    - Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
    - Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP
    - Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma
    - Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów)
    - Możliwość analizy ruchu szyfrowanego protokołem SSL
    - Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
13. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 1,7 Gbps
14. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 300 Mbps

15. W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż:
    - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    - Praca w topologii Hub and Spoke oraz Mesh
    - Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
16. W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
17. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
18. Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a.
19. Translacja adresów NAT adresu źródłowego i docelowego.
20. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.
21. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
22. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR.
23. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
24. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
25. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.
26. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
27. System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż:
    - 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
- Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory

28. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
    - ICSA lub EAL4 dla funkcji Firewall
    - ICSA lub NSS Labs dla funkcji IPS
    - ICSA dla funkcji: SSL VPN, IPSec VPN
29. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

Analizator ruchu - Centralne logowanie i korelacja

Elementy systemu bezpieczeństwa odpowiedzialne za zarządzanie i monitoring mają umożliwiać centralizację procesów zarządzania wszystkimi funkcjonalnościami elementów realizujących funkcje bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

W ramach systemu logowania i raportowania dostawca powinien dostarczyć spójny system monitorujący, gromadzący logi, korelujący zdarzenia i generujący raporty na podstawie danych ze wszystkich elementów systemu bezpieczeństwa.

Platforma powinna dysponować predefiniowanym zestawem przykładów raportów, dla których administrator systemu będzie mógł modyfikować parametry prezentowania wyników.

System centralnego logowania i raportowania powinien być dostarczony w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

W ramach centralnego systemu logowania, raportowania i korelacji powinny być realizowane przynajmniej poniższe funkcjonalności:

1. Konfigurowalne opcje powiadamiania o zdarzeniach jak. email, SNMP
2. Podgląd logowanych zdarzeń w czasie rzeczywistym.
3. Możliwość generowania raportów w zakresie wszystkich funkcjonalności bezpieczeństwa realizowanych przez system - na żądanie oraz w trybie cyklicznym, w postaci popularnych formatów min: PDF, HTML. Raporty powinny obejmować zagadnienie dotyczące całej sfery bezpieczeństwa.

4. Zastosowane systemy logowania powinny umożliwiać cykliczny eksport zgromadzonych logów do zewnętrznych systemów przechowywania danych w celu ich długo czasowego składowania.
5. Na podstawie analizy przeprowadzonych testów w zakresie ilości logów w ciągu sekundy, zastosowany system centralnego logowania powinien umożliwiać zapis oraz analizę co najmniej 120 nowych logów/sekundę.
6. System powinien dysponować co najmniej 4 interfejsami Ethernet 10/100/1000 oraz powierzchnią dyskową min. 1 TB

2.3. serwer aplikacyjny

obudowa	Umożliwiająca przystosowana do montaży w szafie rack 19"
płyta główna	• dedykowana do zastosowań serwerowych • 2 gniazda procesorów • 24 gniazda pamięci DDR4 DIMM • 4 karty 1G lub 2 karty 10G • 1 port RJ45 • RAID 0/1 6GBit/s • Kontroler SAS / SATA • Redundantne wentylatory hot-plug • Redundantne zasilacze 450W hot-plug
wyposażenie	• 2 x procesor 8-rdzeniowy taktowany zegarem 2,2 GHz • RAM: 16 x 16GB DDR4 2600 MHz ECC • 1 x port FC 8G • 3 x HDD SAS 12G 1.2TB 10K 512n hot-plug 2.5" • 1 x SSD SATA 6G 120GB hot-plug 2.5" • 4 x port 1G • kontroler FC 8Gb/s 2 kanały
System operacyjny	• 64 bit, dedykowany do rozwiązań serwerowych, zawierający narzędzia do wirtualizacji

2.4. Przełącznik FC

wyposażenie	• 24 porty FC • obsadzone 8 SFP (8 GB/s)

2.5. rozbudowa macierzy

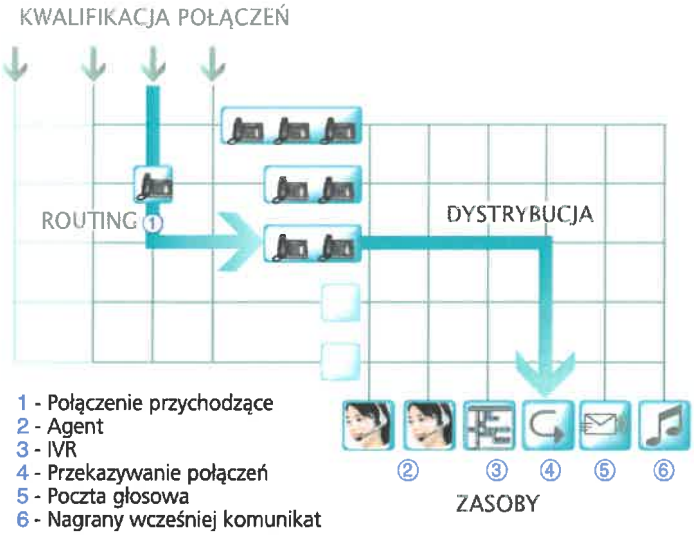
HDD	SAS 4 TB, 7200 rpm.3,5" – 4 szt.
kontroler	2 x FC 8G – 1 szt.

2.6. serwer telekomunikacyjny

System telekomunikacyjny oferował będzie zaawansowaną komunikację głosową, multimedialną zarówno na miejscu, jak i poza budynkiem Starostwa. Możliwość uruchomienia dodatkowej usługi - funkcjonalności contact center pozwoli na uruchomienie centralnego punktu obsługi (kontaktu) z mieszkańcami powiatu. Pracownicy, którzy głównie pracują na terenie Starostwa i na szeroką skalę wykorzystują komunikację głosową, skorzystają z zaawansowanej komunikacji głosowej dostępnej z poziomu telefonu stacjonarnego, telefonów przenośnych DECT lub WLAN i aplikacji na komputerach PC, tabletach i smartfonach.
System telekomunikacyjny oparty o serwer telekomunikacyjny zastąpi obecnie funkcjonującą centralę telefoniczną oraz pozwoli na stopniowe wdrażanie telefonii IP.

Sercem systemu jest serwer komunikacyjny przetwarzający połączenia multimedialne pomiędzy telefonami oraz aplikacjami komunikacyjnymi, realizowanymi w technologiach TDM, IP oraz SIP. Urządzenie umożliwi wdrożenie w Starostwie zaawansowanej komunikacji głosowej klasy korporacyjnej oraz zaoferuje możliwość wyboru scentralizowanych lub zdecentralizowanych rozwiązań opartych o protokół IP. Serwer, uzupełniony o moduły funkcjonalne, stanowił będzie trzon planowanego do wdrożenia systemu contact center opartego na protokole IP, obejmującego najnowsze technologie Linux, XML, SIP, VXML oraz standardy otwarte, takie jak QSIG, H.323, CSTA oraz SIP. Moduł Contact Center to system do automatycznej dystrybucji połączeń, oparty na macierzy zarządzania ruchem i zasobami oraz zaawansowanych algorytmach routingu.

Schemat działania contact center



Schemat działania contact center

Serwer telekomunikacyjny

Sprzęt	• Port Ethernet we wszystkich kartach procesorów • budowa modularna • Komutacja TDM lub IP • Wszystkie moduły (główny i wyniesione) mają możliwość zamontowania w szafach rack 19' • Sloty w obudowach są uniwersalne i zapewniają dowolność rozmieszczenia kart. • Procesory sterujące są oparte o zewnętrzne serwery sprzętowe dedykowane do pracy z serwerem telekomunikacyjnym. • Budowa modułów umożliwia podłączenia elementów okablowania RJ45 bezpośrednio do interfejsów kart serwera. • Moduł główny serwera może posiadać zasilanie zapasowe na minimum 4h pracy autonomicznej. Elementy zasilania zapasowego głównego modułu są montowane w szafach rack 19".
Wymagania funkcjonalne	• Będzie realizował usługi telekomunikacyjne w technologii TDM i IP • Do komunikacji pomiędzy budynkami zostanie wykorzystana sieć LAN klienta • Ma budowę modułową z możliwością modyfikacji i rozszerzenia. • Będzie mógł obsługiwać sieć publiczną za pomocą traktów ISDN PRA, BRA, SIP Trunk, bram VoIP oraz bramek GSM – wymagania ilościowe odnośnie interfejsów zostały przedstawione w opisie przedmiotu zamówienia.

- Będzie mógł obsługiwać abonentów wewnętrznych za pomocą aparatów analogowych, systemowych, aparatów IP, aplikacji softphone, DECT, VoWLAN, IP DECT
- Na wszystkich aparatach (analogowych i IP) będzie prezentowana identyfikacja numeru dzwoniącego (CLIP, CLIR)
- Posiada funkcję automatycznego wyboru najtańszej trasy połączenia (funkcja Least Cost Routing).
- Umożliwia nagrywanie i odtwarzanie komunikatów głosowych i zapowiedzi.
- Posiada możliwość integracji poprzez CTI tak, aby w momencie realizacji połączenia przychodzącego umożliwić pop up na ekranie z informacją o identyfikacji osoby dzwoniącej.
- Posiada możliwość integracji poprzez CTI tak aby za pomocą myszki komputera można było wybrać numer z kontaktów klienta pocztowego
- Posiada możliwość integracji poprzez CTI tak aby można było za pomocą myszki wstawić numer do aplikacji CTI i wykonać połączenia z terminala IP, systemowego czy analogowego
- Posiada możliwość integracji poprzez API Open pack (CSTA, TAPI) z wybranymi aplikacjami
- Umożliwia tworzenie grup abonenckich i definiowanie ścieżki połączeń dla różnych abonentów w grupie (dzwonienie jednoczesne, kolejne, przechwytywanie połączeń w grupie, przekazywanie połączenia na inny numer przy określonej sytuacji np. po określonej liczbie sygnałów lub zajętości).
- Umożliwia nadawanie uprawnień jak i ograniczeń w zakresie realizowania połączeń i korzystania z funkcjonalności dla poszczególnych grup i poszczególnych abonentów wewnętrznych serwera.
- Będzie miał możliwość stworzenie skrzynek poczty głosowej dla każdego z użytkowników – niezależnie od rodzaju obsługującego go portu i posiadanego aparatu (analogowy, IP, softphone)
- Umożliwia utworzenie centralnej i indywidualnej dla każdego abonenta książki telefonicznej.
- Umożliwia wybieranie, z poziomu aparatu, numeru użytkownika (wewnętrznego i zewnętrznego) po nazwie pobieranej z centralnej książki telefonicznej.
- Zapewnia różnicowanie pracy w zależności od pory dnia.
- Zapewnia funkcjonalność DISA
- Daje możliwość nagrywania własnych zapowiedzi słownych.

	• Daje możliwość zawieszania połączenia, zaprogramowania bezwzględnego przekierowania wywołania na określony numer, przekierowania wywołania w przypadku nie zgłoszenia abonenta, przekierowania w przypadku zajętości numeru, sygnalizacja rozmowy oczekującej. • Daje możliwość stworzenia jednorodnego planu numeracji o następującej charakterystyce: o Dopasowany do zewnętrznej numeracji telefonicznej o Dopuszczający różną długość planu numeracji od 3 do minimum 8 cyfr • Posiada mechanizm zarządzania jakością usług (QoS) w sieci IP/WAN i Ethernet/LAN: • Znakowanie/etykietowanie zgodnie ze standardami: 802.1Q, DSCP/DiffServ, • Wykrywanie ciszy/głosu [Silence/Voice Activity Detection]. • Daje możliwość tworzenia sześciostronnych telekonferencji dla abonentów wewnętrznych i zewnętrznych. • Daje możliwość zablokowania/odblokowania telefonu osobistym kodem. • Umożliwia nadanie użytkownikowi wewnętrznemu uprawnień do włączenia się w trwającą między innymi wewnętrznymi abonentami rozmowy. • Posiada funkcję przewodnika w języku polskim Posiada możliwość utworzenie drzewa aktywnego wyboru od 1 do 5-ciu drzew
Zintegrowane oprogramowanie Contact Center	Serwer jest wyposażony w zintegrowane z serwerem oprogramowanie typu Contact Center i uruchamiany przez wykupienie licencji
Oprogramowanie do administracji i zarządzania dostępne poprzez sieć LAN/WAN.	• ma możliwość konfiguracji z wykorzystaniem dedykowanej aplikacji dostarczanej wraz z serwerem lub z dedykowanego oprogramowania do zarządzania serwerem jak przełącznikami dostępowymi jako opcja. • umożliwia autentykację użytkowników i możliwość przypisania ich do odpowiednich grup o ściśle określonych uprawnieniach (pełny dostęp / do odczytu). • umożliwia zarządzanie centralną książką telefoniczną. • umożliwia administrowanie wszystkimi typami użytkowników (analogowi, systemowymi, IP, SIP, DECT) • obsługuje protokół SNMP w celu monitorowania stanu poszczególnych serwerów serwera telekomunikacyjnego. • posiada możliwość dostępu do rejestru zdarzeń serwera telekomunikacyjnego. • Pozwala na taryfikację połączń

2.7. Rejestrator rozmów

Rozwiązanie sprzętowo-programowe do rejestrowania połączeń telefonicznych. Nagrywanie rozmów odbywało się będzie w czasie rzeczywistym, na wielu kanałach jednocześnie. Zarejestrowane rozmowy przechowywane będą na dysku twardym komputera w formie zaszyfrowanej. Oprogramowanie administracyjne pozwoli administratorom na konfigurowanie systemu, przeszukiwanie nagrań, odsłuchiwanie oraz ich kopiowanie.

Rejestrator rozmów

Jakość nagrań	Standardowo nagrania rozmów przechowywane są w formacie MP3 pozwalającym na zachowanie dobrej jakości nagrania przy małej objętości plików. Jeżeli wymagane są nagrania bez utraty jakości spowodowanej kompresją można skonfigurować rejestrator do zapisu plików w formacie WAV.
Rejestracja rozmów na różnych typach linii	• analogowych • ISDN BRI (2B+D) • ISDN PRA (E1) • cyfrowe wewnętrzne
Specyfikacja systemu	• Kompresja nagrań do formatu MP3 • Definiowanie kryteriów nagrywania dla poszczególnych linii (przychodzące, wychodzące) • Definiowanie numerów telefonu, których nie należy nagrywać (indywidualnie dla każdej linii) • Rejestrowanie numeru rozmówcy (jeżeli jest udostępniany przez centralę) • Rejestrowanie kierunku rozmowy (przychodząca, wychodząca) • Baza klientów, przeglądanie historii nagranych rozmów wybranego klienta • Brak limitu czasu nagrania (uzależnione jedynie od pojemności dysku zainstalowanego w komputerze) • Szyfrowanie nagrań • Wyszukiwanie nagrań wg różnych kryteriów • Definiowanie grup linii do wyszukiwania nagrań • Definiowanie użytkowników o różnych uprawnieniach (np. odsłuchiwania wybranych linii, kopiowaniu nagrań) • Ograniczenie dostępu do odsłuchiwania i kopiowania nagrań zależnie od

	uprawnień zalogowanego użytkownika • Możliwość zapisywania komentarzy do nagrań • Logi z użytkowania systemu (logowania, odtwarzania nagrań, kopiowania) • Przechowywanie danych w bazie SQL

2.8. Zestaw komputer z monitorem

komputer	• Stacjonarny, all-in-one • Płyta główna dedykowana do zastosowań desktop • procesor 2 rdzeniowy, taktowany zegarem 2,5 GHz • pamięć RAM: 8 GB z możliwością rozbudowy do 32 GB • HDD 500 GB • 2 x USB 3.0
monitor	• 21", LCD • podświetlenie LED • 16:9
Wyposażenie dodatkowe	• klawiatura • mysz USB • preinstalowany system operacyjny dedykowany do zastosowań desktop • pakiet oprogramowania biurowego (edytor, arkusz, poczta) • program antywirusowy

2.9. Laptop

komputer	• przenośny • procesor 2 rdzeniowy, taktowany zegarem 2,2 GHz • pamięć RAM: 8 GB • HDD 500 GB • 2 x USB 3.0 • czas pracy na baterii: 4 h • waga 2,3 kg
ekran	• 15" LCD

	• podświetlenie LED • 16:9
Wyposażenie dodatkowe	• preinstalowany system operacyjny dedykowany do zastosowań desktop • pakiet oprogramowania biurowego (edytor, arkusz, poczta) • program antywirusowy

2.10. UPS

Ilość faz WE : WY	3:3
moc	80 kVA
Napięcie WE/WY	380 / 400 / 415 VAC
Sprawność w trybie On-Line	96%
wyposażenie	• Bypass typu static switch, przełączenie bezprzerwowe. • Bypass ręczny
komunikacja	2 x Smart Slot, 1 x RS232 & USB (dla serwisu), SNMP,
inne	• Prostownik IGBT • Budowa modułowa • Złącze zdalnego wyłącznika P. Poż. • Wyłącznik P .Poż.

2.11. Szafa 42U

Standardowo wyposażona przez producenta w drzwi przednie oszklone z możliwością zmiany strony mocowania, zdejmowane osłony boczne, możliwość wyprowadzenia kabli przez podłogę sufit oraz tył szafy. Profile montażowe regulowane.

wysokość	42U
Szerokość x głębokość	800 x 800
Wyposażenie szafy	• panel wentylacyjny, • panele krosowe modularne kat.6, • panele z prowadnicami kabla, • listwy zasilające,

2.12. Szafa 12 U

Szafa wisząca, standardowo wyposażona przez producenta w drzwi przednie oszklone z możliwością zmiany strony mocowania, zdejmowane osłony boczne, możliwość wyprowadzenia kabli przez podłogę oraz sufit. Profile montażowe regulowane.

wysokość	12U
Szerokość x głębokość	600 x 450
Wyposażenie szafy	• panel wentylacyjny, • panele krosowe modularne kat.6, • panele z prowadnicami kabla, • listwa zasilająca,

3. Główne wymagania funkcjonalne dla oprogramowania

3.1. System e-Urząd

W ramach projektu Wnioskodawca przewiduje wdrożenie systemu umożlwiającego elektronizację procesu informacji i obsługi mieszkańca, obsługi podatkowej i niepodatkowej. Wdrażany System zapewni:

- dostęp do danych z Rejestrów Publicznych (podatki/opłaty/inne),
- Bezpieczne zalogowanie się na opracowaną platformę poprzez przeglądarkę z wykorzystaniem:
    - SSO Single Sign-On (Jednokrotne Logowanie) platformy ePUAP (protokół SAML); Dzięki temu osoba posiadająca konto w ePUAP nie musi zakładać konta w systemie, żeby mieć dostęp do zastrzeżonych danych , czyli podatnik loguje się systemu za pomocą swojego konta na ePUAP.
    - zewnętrznego mechanizmu autoryzacji serwisu Cyfrowy Urząd Województwa Warmińsko-Mazurskiego (http://cu.warmia.mazury.pl),
    - wewnętrznego mechanizmu autoryzacji (system indywidualnych kont użytkownika).
- Uzyskanie danych o aktualnych zobowiązaniach zalogowanego klienta w stosunku do Wnioskodawcy (w tym: odsetki i inne koszty na bieżącą datę logowania),
- Wybranie dowolnych pozycji do opłacenia;
- Przekierowanie do systemu płatności elektronicznych i zapłacenie jedną transakcją za wszystkie wybrane pozycje.
- Pobieranie informacji o wpłatach.
- Platforma będzie korzystała z jednego z dostępnych na polskim rynku, systemu płatności elektronicznych.
- Platforma umożliwi generowanie pliku z elektronicznymi przelewami w formacie XML dla potrzeb przeksięgowań transakcji pomiędzy rachunkiem technicznym, a rachunkami docelowymi związanymi z wybranymi przez Wnioskodawcę zobowiązaniami. Ten proces będzie obsługiwany przez uprawnionych

pracowników Urzędu. Platforma zapewni możliwość dostosowania struktury pliku XML do potrzeb banku obsługującego konto Wnioskodawcy.

- Platforma będzie wykorzystywała SSO (Single Sign-On - przekazywanie tożsamości) udostępnione przez mechanizm integracyjny platformy ePUAP zgodnie z wytycznymi na stronach portalu ePUAP oraz udostępnionymi w dokumencie „Wykorzystanie SAML 2.0 w systemie ePUAP".
- Platforma Informacyjno-Płatnicza jest systemem typu „front-office" i zbudowana jest w oparciu o „lekkie" technologie wykorzystując:
    - serwer www Apache,
    - środowisko PHP,
    - baza danych MySQL.

3.2. System elektronicznego obiegu dokumentów

System obsługi spraw i dokumentów, pracującym w środowisku sieciowym, którego zadaniem jest wspomaganie procesu wymiany dokumentów pomiędzy poszczególnymi komórkami, zarządzanie realizacją spraw, a także usprawnienie komunikacji z klientem.
System posiada wbudowane narzędzie umożliwiające implementację norm i procedur obowiązujących w urzędzie, w tym także norm ISO 9001:2000.

System ma za zadanie usprawnić obsługę spraw i dokumentów w organizacji:

- zapewnia sprawny przepływ informacji,
- wspomaga proces wymiany dokumentów pomiędzy poszczególnymi komórkami,
- nadzoruje proces zarządzania realizacją spraw,
- usprawnia komunikację z klientem.

SEOD stanowić będzie kompleksowy system realizujący elektroniczny obieg dokumentów oraz system obsługi i zarządzania procesami, zawierający:

- elektroniczne repozytorium dokumentów
- mechanizmy skanowania i przetwarzania danych,
- bazę kontaktów,
- pocztową książkę nadawczą,
- moduł obsługi dokumentów,
- moduł obsługi spraw,
- szablony dokumentów,
- moduł archiwum elektronicznego,
- moduł wsparcia procesów biznesowych (WorkFlow).

Ponadto system umożliwi:

- elektroniczną rejestrację dokumentów posiadających formę:
  - zeskanowanych dokumentów papierowych,
  - faksów,
  - wiadomości poczty elektronicznej,
  - formularzy udostępnionych na stronie WWW organizacji itp.,
- składanie pism i wypełnianie formularzy poprzez Internet z wykorzystaniem podpisu elektronicznego,
- tworzenie i korzystanie z przygotowanych szablonów dokumentów,
- prowadzenie osobistego terminarza, w którym użytkownik może planować swoje spotkania, zgłaszać nieobecności itp. – dzięki zintegrowaniu kalendarza z resztą systemu, przy dekretacji sprawy/dokumentu do osoby nieobecnej wysyłana jest informacja zwrotna,
- pełną obsługę poczty elektronicznej – wysyłanie i odbieranie wiadomości wraz z załącznikami bezpośrednio z systemu i bez udziału innej aplikacji,
- wersjonowanie dokumentów – system rejestruje wszystkie zmiany wprowadzane w dokumencie oraz dane użytkowników dokonujących modyfikacji,
- przesyłanie dokumentów/spraw, dla których z góry przewidziany jest pewien schemat prac do kolejnych etapów dekretacji według zdefiniowanych dla nich węzłów dekretacji – Workflow (obieg dokumentów),
- dokładne monitorowanie postępu prac nad daną sprawą lub dokumentem.

System oparty będzie o rozwiązanie sieciowe i wymagał będzie jedynie posiadania przeglądarki internetowej po stronie użytkownika końcowego.

Jako relacyjny system zarządzania bazą danych zastosowane zostanie rozwiązanie, które jest wiodącym motorem bazy danych spełniającym wszystkie wymagania stawiane systemom przetwarzania transakcji, magazynom danych, aplikacjom klient-serwer, aplikacjom WEB i rozproszonym bazom danych.
Rozwiązania będzie pracowało zarówno z wykorzystaniem technologii klient-serwer, jak i technologii webowej.

Wymagania funkcjonalne dotyczące Systemu Elektronicznego Obiegu Dokumentów

przygotowany do pracy jako – system podstawowy, określony w instrukcji kancelaryjnej (pełna obsługa dokumentów elektronicznych i papierowych zarówno przychodzących i wychodzących)
przygotowany do pracy grupowej z możliwością nadawania uprawnień do konkretnych dokumentów
zintegrowany z poczta elektroniczną
zintegrowany z platformą ePUAP oraz CU Warmii i Mazur
obsługa skrzynki podawczej urzędu
możliwość rejestracji pism przychodzących w jednym rejestrze korespondencji przychodzącej

System musi mieć zaimplementowany mechanizm wysyłki sms do klientów załatwiających sprawę (stan ostatecznego załatwienia sprawy).

System musi wystawiać UPO (Urzędowe Potwierdzenie odbioru) - wiarygodne i jednoznacznie potwierdzające odbiór.

System musi mieć mechanizm, który pozwala na łatwą zmianę przepływu dokumentów, ustawianie dowolnych poziomów akceptacji

System ma mieć zaimplementowane narzędzie do projektowania, modyfikacji i zarządzania workflow i obiegami dokumentów

System musi mieć możliwość tworzenia/modyfikowania JRWA wraz z oznaczeniem typu prowadzonych spraw (sprawy elektroniczne, sprawy prowadzone tradycyjnie)

System musi dawać możliwość podpisywania dokumentów profilem zaufanym

System musi dawać możliwość wielostopniowego podpisywania\weryfikowania dokumentów bezpiecznym podpisem kwalifikowanym (podpis elektroniczny)

System musi obsługiwać \ weryfikować dokumenty „zagraniczne" podpisane podpisem elektronicznym zgodnymi z założeniami EIDAS

System ma mieć panel informujący o statystykach przyjmowanych dokumentów, prowadzonych sprawach przez pracowników

System ma mieć moduł-wyszukiwarkę, w której będzie można przeglądać historię pism, które złożył klient wraz z podglądem skanu, listę spraw interesanta, kto prowadzi/stan załatwienia /wydruk

System ma mieć możliwość wydawania poleceń przez kierownictwo naczelne podczas przeglądania pism\spraw\innych dokumentów

System musi mieć funkcjonalność generowania statystyk dziennych rocznych kwartalnych co do liczby korespondencji przychodzącej, prowadzonych spraw, liczbie korespondencji wychodzącej z podziałem na kategorie.

System ma mieć funkcjonalność do obsługi składów chronologicznych

System musi obsługiwać formularze XML (e-usługi)

System ma mieć zaimplementowaną obsługę urządzeń: skanerów TWAIN, czytników kodów kreskowych, drukarki kodów kreskowych.

System ma mieć zaimplementowany silnik OCR

System ma mieć możliwość tworzenia formularzy dla pism przychodzących w zależności od rodzaju pism

System musi obsługiwać korespondencję wychodzącą (pisma wychodzące papierowe, mail, fax, ePUAP) oraz powrót zwrotki (skanowanie zwrotek, dodanie do składów chronologicznych)

System musi być przygotowany na eksportowanie spraw do archiwum zakładowego

System musi być przygotowany na eksportowanie spraw do archiwum Państwowego a eksportowane sprawy \ dokumenty muszą być przygotowane zgodnie z wytycznymi Archiwum Państwowym

System ma dawać możliwość eksportu stanu załatwienia sprawy do Biuletynu Informacji Publicznej.

System musi mieć możliwość tworzenia i prowadzenia rejestrów

System musi dawać możliwość exportu i aktualizowania danych prowadzonych rejestrów publicznych do Biuletynu Informacji Publicznej i prezentowania tych danych w logiczny sposób czytelny dla interesanta.

System musi dawać możliwość ustawiania zastępstw dla pracowników nieobecnych (funkcja ta musi być realizowana wg uprawnień zarówno dla administrator\a\ów, kierownik, pracowników)

System musi mieć możliwość tworzenia dowolnych szablonów dokumentów wychodzących

System musi mieć możliwość integracji z AD/LDAP

System musi być otwarty na integrację z systemami dziedzinowymi (np. systemem finansowo-księgowym)

System musi działać w oparciu o przeglądarkę internetową w bezpiecznym kanale komunikacji.

Wymagania pozafunkcjonalne dotyczące Systemu Elektronicznego Obiegu Dokumentów

System Elektronicznego Obiegu Dokumentów musi pełnić funkcję i spełniać wszystkie warunki określone dla systemu EZD w Rozporządzeniu Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.

System Elektronicznego Obiegu Dokumentów musi umożliwiać prowadzenie obsługi kancelaryjnej zarówno w systemie tradycyjnym, jak i w systemie EZD, w zależności od decyzji kierownika jednostki.

System Elektronicznego Obiegu Dokumentów musi umożliwiać przejście z systemu tradycyjnego do systemu EZD bez utraty danych przechowywanych w SEOD.

SEOD musi być zgodny z obowiązującymi oraz ogłoszonymi przepisami prawa na dzień składania oferty. SEOD musi być zgodny w szczególności z następującymi przepisami prawa:

- USTAWY:
    - Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2005 r. Nr 64, poz. 565 z późn. zm.).
    - Ustawa z dnia 14 czerwca 1960 Kodeks Postępowania Administracyjnego (Dz.U. z 2000 r. Nr 98, poz. 1071 z późn. zm.).
    - Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. z 2001 r. Nr 130, poz.

1450 z późn. zm.).

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r. Nr 182 poz. 1228).
- Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U. z 2001 r. Nr 128 poz. 1402 z późn. zm.
- Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2011 r. Nr 123 poz. 698).
- Ustawa o dostępie do informacji publicznej (Dz. U. z 2001 r. Nr 112 Poz. 1198 z późn. zm.).

- ROZPORZĄDZENIA:
  - Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 6 marca 2012 r. w sprawie wzoru i sposobu prowadzenia metryki sprawy (Dz.U. z 2012 r. poz. 250).
  - Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. z 2011 r. Nr 14, poz. 67 z późn. zm.).
  - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 kwietnia 2011 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji użytkowników (Dz.U. z 2011 r. Nr 93, poz. 545).
  - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2011 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (Dz.U. z 2011 r. Nr 93, poz. 546).
  - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2011 r. w sprawie zasad potwierdzania, przedłużania ważności, wykorzystania i unieważniania profilu zaufanego elektronicznej platformy usług administracji publicznej (Dz.U. z 2011 r. Nr 93, poz. 547).
  - Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz.U. z 2011 r. Nr 206, poz. 1216).

- 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 r. Nr 100, poz.1024).

- Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego.(Dz.U. z 2002 r. Nr 128, poz.1094).

- 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. z 2006 r. Nr 206, poz. 1519).

- Rozporządzenie Rady Ministrów dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków (Dz.U. z 2002 r. Nr 5, poz. 46).

- Rozporządzenie Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (Dz.U. z 2005 r. Nr 205 poz. 1692).

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz.U. z 2006 r. Nr 206 poz. 1518).

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz.U.
  z 2006 r. Nr 206 poz. 1517).

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz.U. z 2007 r. Nr 10 poz. 68).

- Rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania (Dz.U. z 2005 r. Nr 217 poz. 1836).

- Rozporządzenie Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz.U. z 2002 r. Nr

167 poz. 1375).

- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz /minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z dnia 16 maja 2012 r. poz. 526).

SEOD musi posiadać architekturę trójwarstwową. SEOD musi składać się z następujących warstw:

a) warstwa bazodanowa, oparta o motor bazy danych zgodny ze standardem SQL;

b) warstwa aplikacyjna, oparta o serwer aplikacji, realizująca logikę biznesową systemu;

c) warstwa prezentacji, udostępniająca interfejs użytkownika przez przeglądarkę internetową.

SEOD musi być systemem interoperacyjnym co najmniej w zakresie prezentacji danych: umożliwi uruchomienie systemu przez użytkownika końcowego z poziomu przeglądarki internetowej, co najmniej Internet Explorer w wersji 8 i od wersji 10, Firefox od wersji 20, Firefox ESR, Google Chrome od wersji 24, Opera od wersji 12, Safari w najnowszych wersjach. System musi być w pełni dostępny dla użytkownika pracującego na systemach operacyjnych z rodziny Windows (XP SP3/Vista/7/8/10), Linux (Ubuntu od wersji 12.04, Debian od wersji 6.0.5, a także co najmniej jeden z następujących: Fedora od wersji 16 lub OpenSUSE od wersji 12.1, Red Hat Enterprise Linux oraz CentOS i Scientific Linux od wersji 6), MacOS. System będzie działał w środowisku 32- i 64-bitowym.

Wymaga się dostosowania rozwiązania do rozdzielczości ekranu danego typu urządzenia. Wymaga się pełnej dostępności interfejsu SEOD dla urządzeń o rozdzielczości 800x600 i wyższej.

System musi być w pełni transakcyjny i musi zabezpieczać dane przed zniszczeniem lub przypadkowym nadpisaniem w przypadku równoczesnego korzystania z tych danych przez wielu użytkowników.

System od strony technicznej musi zapewnić skalowalność (na poziomie warstwy bazodanowej i aplikacyjnej) w zakresie wydajności i pojemności oraz dołączania dodatkowych użytkowników, elementów infrastruktury sprzętowej.

System będzie pozwalał na uruchomienie zarówno warstwy bazodanowej, jak i aplikacyjnej, w środowiskach systemowych bazujących na technologii Microsoft oraz w środowiskach opartych na systemie Linux.

Interfejs użytkownika

Interfejs użytkownika SEOD musi być interfejsem graficznym (GUI), w szczególności wykorzystywać menu, listy, formularze, przyciski. Musi istnieć także możliwość przechodzenia miedzy polami formularzy z wykorzystaniem klawisza TAB.

Interfejs użytkownika SEOD musi posiadać widok indywidualny, w ramach którego prezentowane będą tylko te składniki zawartości informacyjnej Systemu (w tym zakres menu), które potrzebne są w danym węźle struktury organizacyjnej, do którego przypisany jest dany użytkownik.

Dostępne funkcje oraz interfejs użytkownika SEOD dla poszczególnych rodzajów węzłów organizacyjnych powinny być dostosowane do danego rodzaju węzła. Rodzaje węzłów powinny być co najmniej następujące: kierownik komórki, referent, archiwista, kancelaria.

System powinien umożliwiać tworzenie nowych rodzajów węzłów na podstawie jednego z istniejących i dostosowanie do niego wyglądu menu.

Wymaga się, aby w widoku użytkownika wyróżnione były wszystkie zadania realizowane przez pracowników danego węzła struktury organizacyjnej, dla których to zadań:

1) termin zakończenia realizacji zadania już minął,
2) termin zakończenia realizacji zadania mija za określoną w konfiguracji systemowej liczbę dni kalendarzowych.

System powinien wyróżniać elementy (np. zadania, korespondencję) nowe, tzn. takie, które na danym stanowisku nie były jeszcze otwarte ani przetwarzane.

System nie zaburza pracy użytkownika nad rozpoczętym formularzem i nie przeładowuje go w wyniku innych zdarzeń na jego koncie (np. nadejście nowej korespondencji).

Wymaga się, aby interfejs użytkownika zawierał informację o węźle struktury organizacyjnej, w którym aktualnie pracuje użytkownik.

Wymaga się, aby była możliwość podglądu zestawień dokumentów i spraw innych osób, do których dany użytkownik jest uprawniony.

Wymaga się, aby była możliwość wykorzystania mechanizmu wielokryteriowego wyszukiwania różnych elementów w systemie wg konfigurowalnych warunków, w tym: wg dokładnej treści/wartości pola, wg zakresu liczb, dat, numeracji, wg jednej lub kilku liter rozpoczynających tekst w danym polu lub w nim występujących.

Interfejsy integracyjne

System musi posiadać interfejsy zewnętrzne, obejmujące udostępnianie usług integracyjnych (m.in. wymiany danych) Systemu Elektronicznego Obiegu Dokumentów poprzez usługi Web Services (w oparciu o standardy SOAP 1.2, WSDL co najmniej 1.1). System musi umożliwiać dodawanie nowych interfejsów integracyjnych opartych na XML oraz włączanie tych usług i pozyskanych w ten sposób danych w ścieżki przetwarzania spraw.

SEOD musi umożliwiać administratorowi skonfigurowanie automatycznej weryfikacji i transformacji (poprzez pliki XSD i XSL załadowane do systemu przez administratora) danych w formacie XML pozyskiwanych z określonego źródła zewnętrznego oraz automatycznego przesyłania tak przekształconych danych jako jednego lub wielu dokumentów do użytkownika lub użytkowników SEOD wg określonych w konfiguracji kryteriów.

Bezpieczeństwo, skalowalność i wydajność

System musi posiadać mechanizm kontroli dostępu do usług pozwalający na dostęp do danej usługi ze względu na użytkownika oraz funkcję.

System musi rejestrować wszystkie czynności dostępu do usług i zasobów w systemie, w zakresie dostępu przez użytkowników oraz aplikacje współpracujące z SEOD.

Oszacowanie wydajności musi uwzględniać okresowe (w określonych dniach roku) spiętrzenia prac skutkujące trzykrotnym wzrostem obciążenia w stosunku do obciążenia przeciętnego.

Odpowiednia pojemność systemu oznacza możliwość przechowywania w systemie takiej ilości danych, jaka średnio gromadzona jest w urzędzie o danej wielkości w okresie pięciu lat oraz dodatkowo 20% tej wielkości (zapas). Należy uwzględnić, że w systemie będą przechowywane pliki zawierające zeskanowane pisma wchodzące w postaci papierowej.

Jeżeli System dostarczony przez Wykonawcę nie będzie spełniał ww. wymagań lub przestanie je spełniać do 5 lat po dokonania odbioru końcowego, Wykonawca obowiązany jest odpowiednio uzupełnić sprzęt i oprogramowanie (np. poprzez zwiększenie pojemności dysków, mocy obliczeniowej, dostarczenie dodatkowych maszyn, licencji) bez dodatkowych kosztów po stronie Zamawiającego.

Zarządzalność systemu

SEOD musi być wyposażony w pulpit administratora, umożliwiający wykonywanie czynności administracyjnych, w szczególności zarządzanie użytkownikami, uprawnieniami, konfiguracją, w tym konfiguracją przepływu pracy, strukturą organizacyjną jednostki, formularzami SEOD, interfejsami integracyjnymi, a także umożliwiający podgląd procesów przepływu pracy, raportowanie, wykrywanie i rozwiązywanie typowych problemów z systemem SEOD.

SEOD musi umożliwiać udzielanie uprawnień według pełnionych funkcji (np. pracownik kancelarii podawczej, archiwista, administrator), w zakresie odpowiednich komórek organizacyjnych oraz z dokładnością do rodzaju pojedynczych operacji (np. odczyt, zapis, akceptacja dokumentów). Udzielanie uprawnień opiera się na wskazaniu roli i komórki z możliwością korekty wartości pojedynczych uprawnień dla danego użytkownika.

Inne wymagania

System musi umożliwić obsługę plików (dokumentów) w dowolnym formacie, w szczególności zgodnym z obowiązującymi przepisami prawa (pliki te są otwierane i modyfikowane przez użytkowników w odrębnych aplikacjach, jednak mogą być przedmiotem obiegu w SEOD).

System musi posiadać wbudowany mechanizm zdalnej asysty technicznej pozwalający na wsparcie użytkowników systemu przez uprawnionych do tego administratorów.

3.3. Portal płatności i komunikacji społecznej

Realizacja projektu przewiduje stworzenie portalu internetowego, który zapewni:

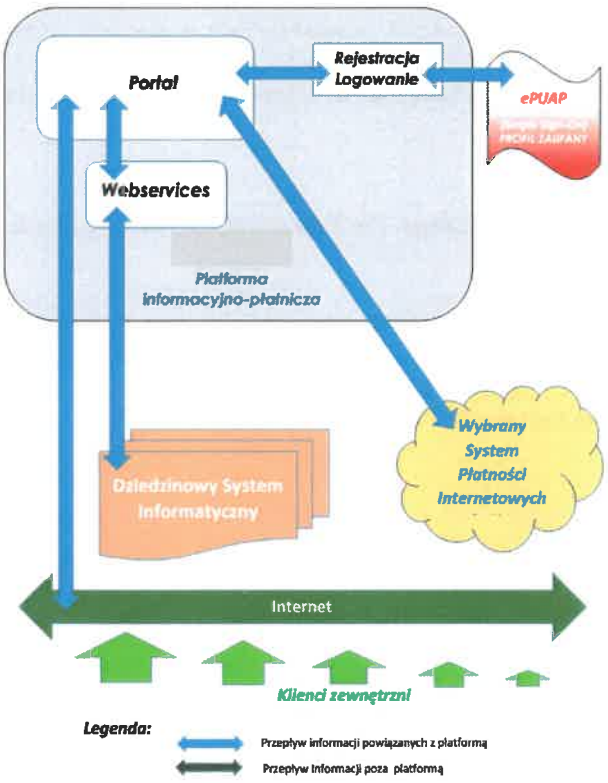
1. udostępnianie informacji publicznych z danych strukturalnych w zakresie informacji budżetowych takich jak dochody budżetu wg klasyfikacji plan i wykonanie oraz wydatki budżetu wg klasyfikacji plan i wykonanie;
2. możliwość prostego dodawania zestawień danych z innych obszarów;
3. możliwość pobierania danych z różnych baz danych;
4. możliwość prezentacji danych w postaci kontrolek (tabela, wykres kołowy itd.) na konfigurowalnych pulpitach analiz;
5. po uwierzytelnieniu, dostęp do e-usług i płatności
6. Sterowanie portalem w części publicznej:
   - edycja i sterowanie widocznością poszczególnych pozycji menu
   - funkcja publikacji menu pozwalająca na przygotowanie zmian off-line
   - obsługa różnych szablonów stron podpinanych do pozycji menu
   - obsługa kontrolek w szablonach: HTML, odsyłacz zewnętrzny, odsyłacz do pulpitu analiz
   - możliwość obsługi kontrolek dedykowanych
   - wersjonowanie zawartości kontrolek HTML – możliwość cofania zmian
   - funkcja publikacji strony pozwalająca na przygotowanie zmian off-line
   - funkcje administracyjne dostępne jedynie wewnątrz urzędu
   - funkcje exportu i importu treści serwisu
7. Zarządzanie użytkownikami:
   - obsługa własnych kont użytkowników systemu,
   - możliwość wykorzystania kont użytkowników z platformy ePUAP do logowania do systemu (integracja z ePUAP w zakresie „Single Sign-on"),
   - możliwość wykorzystania kont użytkowników z platformy CU Warmii i Mazur
   - obsługa mechanizmu upoważnień,
   - aplikacja wewnętrzna do zarządzania użytkownikami serwisu oraz weryfikacji dostępnych dla nich danych

Portal oparty będzie o system zarządzania treścią CMS, który pozwoli na dowolne profilowanie przekazywanych treści. Formatowanie publikowanych treści ma następować w oparciu o zdefiniowane szablony, zapewniające spójną prezentację informacji w całym Portalu

Portal będzie zgodny z rekomendacjami wypracowanymi przez W3C i opisanymi na stronie http://www.w3.org/WAI/guid-tech.html w dokumencie WCAG 2.0. Portal będzie spełniał wymagania WCAG 2.0 na poziomie podstawowym (wersja graficzna strony o wysokim kontraście pozbawiona animacji - zgodnie ze standardem WCAG 2.0 wskazanym w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych).

Portal będzie wykonany w sposób, który gwarantuje automatyczne dostosowanie go do wielkości ekranu, na którym jest wyświetlany.

Portal będzie prawidłowo obsługiwać urządzenia mobilne najpopularniejszych platform (iOS, Android, Windows Phone).



Portal, poza dostępem do e-usług, udostępni, w ramach podportalu, funkcjonalność komunikacji społecznej. Wymagania i funkcjonalności dla modułu przedstawia poniższa tabela.

1	Zapewnić bezpieczeństwo wprowadzania i przesyłania danych za pomocą szyfrowanego kanału transmisji.
2	Pozwoli na wyświetlanie informacji w wersji dla osób niedowidzących.

3	Pozwoli na importowanie dokumentu XML z edytorów aktów prawnych.
4	Umożliwi automatyczną konwersję pliku XML umożliwiającą nanoszenie komentarzy do poszczególnych sekcji.
5	Pozwoli na wyświetlanie zaimportowanego pliku XML (uchwały) w sposób umożliwiający intuicyjne dodawanie komentarzy poprzez zaznaczenie obszaru (paragrafu, akapitu, punktu etc.): a. wizualne odznaczenie na akcie prawnym punktów (oraz paragrafów, akapitów) posiadających komentarze za pomocą ustalonego indeksu b. lista wyświetlająca wszystkie dodane komentarze: • wyświetlona pod przeglądanym aktem prawnym, • filtrowanie komentarzy ze względu na autora - wyświetl wszystkie lub wyświetl „moje", • wyświetlanie dodanych komentarzy w zgrupowany sposób, umożliwiający łatwą interpretację (komentarze dotyczące zagnieżdżonych punktów będą wyświetlane jako podpunkty w ramach sekcji), • tworzenie oraz edycja komentarzy do aktów prawnych (użytkownik), • podgląd dodanych komentarzy (własnych oraz obcych) do aktów prawnych (użytkownik), • moderowanie wprowadzonych komentarzy (administrator), • generowanie raportów zbiorczych wszystkich dodanych komentarzy przez użytkowników (administrator).
6	Udostępni dedykowany formularz pozwalający na głosowanie nad budżetem obywatelskim.
7	Będzie posiadać moderowane forum na potrzeby konsultacji z obywatelami - platforma dialogu społecznego.
8	Musi poprawnie wyświetla informacje w przeglądarkach w wersji co najmniej Internet Explorer, Opera, Firefox, Chrome, Safari
9	Musi współpracować z relacyjną bazą danych w wersji komercyjnej oraz darmowej.

API Portalu

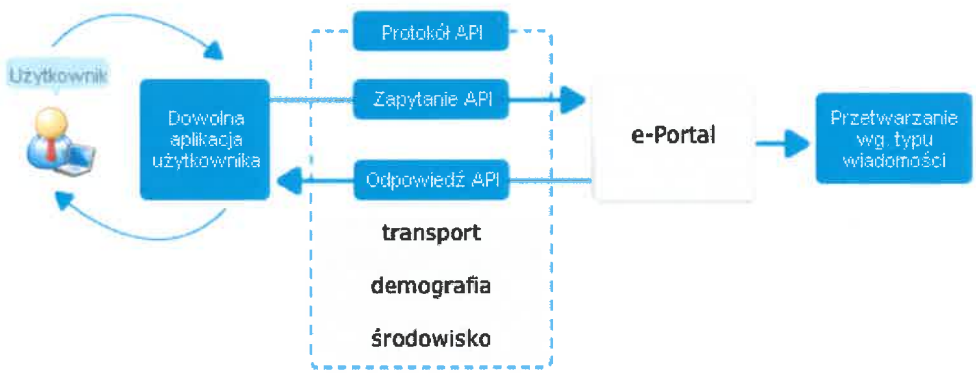
Zbiór danych składał się będzie ze wskazanych zasobów (transport, demografia, środowisko) oraz metadanych je opisujących.

Dane dostępne będą, w formacie XML, na portalu oraz przekazywane na serwer Wnioskodawcy, na którym wczytywane będą do bazy SQL.

API portalu udostępni dane w formatach:

- XML
- JSON

Formaty te są najbardziej popularne wśród programistów tworzących aplikacje internetowe. Umożliwiają łatwe i szybkie wykorzystanie danych tekstowych w aplikacjach zewnętrznych.



W danych udostępnionych poprzez API portalu widoczne będą pola:

- **start** - indeks, od którego prezentowane są dane
- **stop** - indeks, do którego prezentowane są dane
- **size** - liczba elementów zwróconych w wyniku
- **total_size** - maksymalna liczba elementów jakie może zwrócić strona

API portalu umożliwia łatwą integrację i dostęp do wszystkich metadanych zasobów danych oraz grupujących je zbiorów. Niektóre z tabelarycznych zasobów udostępnionych w otwartych formatach umożliwiają także wybiórcze pobieranie treści zasobów.
Korzystając z dobrych praktyk serwisu Dane Publiczne (danepubliczne.gov.pl), który zbudowany jest na otwartym kodzie na popularnym rozwiązaniu CKAN, Wnioskodawca przewiduje wykorzystanie zasad tworzenia API opisanych w dokumentacji CKAN.

4. Sieć strukturalna LAN

Rozbudowa sieci logicznej i instalacji elektrycznej będzie obejmowała łącznie instalację 180 PEL. Szczegółowa lokalizacja PEL zostanie wskazana na etapie opracowania projektu wykonawczego.

Przez punkt elektryczno-logiczny (PEL), należy rozumieć zintegrowany punkt przyłączeniowy, który składa się z 2 gniazd RJ45 (montowanych w kanałach instalacyjnych natynkowych) kategorii 5e lub wyższej oraz dwóch gniazd elektrycznych 230V (montowanych w korycie), z blokadą uniemożliwiającą podłączenie nieuprawnionych odbiorników, gniazda RJ45 i zasilanie jako jeden element.

W ramach instalacji okablowania strukturalnego przewidziano następujące prace:

- budowę nowych tras kablowych,
- układanie kabli w nowych i istniejących trasach,
- instalacja punktów PEL - (punkt elektryczno-logiczny),
- montaż paneli krosowych 48xRJ45 w szafach w punktach dystrybucyjnych,
- dostarczenie i montaż do szafy telekomunikacyjnej patchpaneli krosowych RJ45 kat. 6, Ilość paneli należy dostosować do liczby instalowanych gniazd z zapewnieniem 50% nadmiarowości
- terminowanie kabli w osprzęcie przyłączeniowym,
- pomiary tras kablowych, wykonanie dokumentacji powykonawczej

System okablowania strukturalnego musi posiadać następujące parametry funkcjonalno-użytkowe:

- system okablowania strukturalnego co najmniej kategorii 6 musi zapewnić możliwość transmisji głosu, danych, sygnałów wideo,

- w okablowaniu muszą być zastosowane 4-parowe kable symetryczne UTP które charakteryzują się parametrami i jakością niezbędną do prawidłowej pracy systemu zarówno w chwili obecnej, jak i w przyszłości,
- budowane trasy mają być prowadzone w kanale instalacyjnym natynkowym (korytka PCV),
- izolacja zewnętrzna okablowania miedzianego musi być wykonana z PVC lub z materiału LSZH nie wydzielającego toksycznych oparów podczas spalania (nie zawiera halogenu),
- w okablowaniu wszystkie komponenty (w tym parametry transmisyjne) muszą charakteryzować się pełną zgodnością ze specyfikacją dla kategorii 6,
- moduły RJ45 powinny być zarabiane narzędziowo,
- gniazda naścienne i na panelu krosowym muszą być oznaczone tj. posiadać czytelną numerację na obydwu końcach toru,
- wymiar panelu krosowego musi być następujący - szerokość 19", max wysokość 2 U,
- panel musi umożliwić zamontowanie min. 24 modułów RJ45,
- okablowanie musi bazować na jednorodnym rozwiązaniu systemu okablowania strukturalnego, którego wszystkie elementy toru transmisyjnego pochodzą od tego samego producenta.

Wymagania dotyczące dedykowanej instalacji elektrycznej:

- rozbudowy instalacji elektrycznej gniazd wtykowych zasilania dedykowanego – dwa gniazda na PEL,
- rozbudowy istniejących rozdzielnic lub ich wymiany (w przypadku braku możliwości rozbudowy),
- wykonania dedykowanej instalacji zasilającej w układzie TN-S,
- wszystkie gniazda elektrycznej sieci zasilającej, powinny posiadać zabezpieczenie w postaci klucza typu DATA, aby uniemożliwić podłączenia dowolnych urządzeń elektrycznych i tym samym wprowadzić podniesienie bezpieczeństwa użytkowania. Wymagane jest dostarczenie kluczy w ilości odpowiadającej zainstalowanym gniazdom,
- do budowy toru zasilającego koniecznym jest użycie przewodów izolowanych YDY – 750V, 3x2,5 mm2 lub innych o porównywalnych parametrach izolacyjno-eksploatacyjnych,
- obwody elektryczne w obrębie pomieszczeń mają być prowadzone łącznie z instalacją logiczną w kanale instalacyjnym natynkowym (korytka PCV) - rozdzielone przegrodą lub w odrębnych kanałach,
- należy zaprojektować max. 5 urządzeń na jeden obwód zabezpieczający.
- Każdy obwód elektryczny musi zostać zabezpieczony wyłącznikiem przepięciowym i różnicowoprądowym,

Instalację należy zasilić z dedykowanej rozdzielni umieszczonej w pomieszczeniach serwerowni. Od istniejących tablic rozdzielczych zostanie wykonane zasilanie YDYżo 5x10mm². Dla poprawienia wartości uziomu, który nie powinien przekraczać wartości 10Ω, jeżeli zajdzie taka potrzeba, zostanie wbity pręty pomiedziowane typu galmar, w okolicy istniejącego złącza kablowego na zewnątrz budynku aby zapewnić prawidłowe funkcjonowanie ochrony TN-S w całym obiekcie.

W istniejących tablicach elektrycznych zostaną umieszczone zabezpieczenia gniazd zasilania komputerowego. W przypadku gdy istniejące tablice okażą się za małe, zostaną wymienione na nowe.

Instalacja gniazd wtyczkowych zostanie wykonana przewodami miedzianymi typu YDYżo 3x750V o przekroju 2,5 mm² z osobną żyłą „N" i PE. Wszystkie gniazda wtyczkowe będą posiadać bolec ochronny.

Obwód gniazd komputerowych 230V, w tablicach elektrycznych zostanie zabezpieczony wyłącznikiem różnicowo-prądowym 16A, ΔI=0,03A, o charakterystyce typu „A".

Jako dodatkową ochronę od porażeń prądem elektrycznym po stronie nn-0,4kV zastosowane zostaną „samoczynne wyłączanie zasilania" w układzie TN-C-S (dla sieci zasilającej układ TN-C, dla odbiorczej TN-S). W celu zapewnienia ochrony przepięciowej, w istniejącej rozdzielnicy głównej zastosowane zostaną odgromniki 4xDEHNbloc i ochronniki przepięciowe 4xDEHNquard. Dla prawidłowego funkcjonowania ochrony przepięciowej zastosowany zostanie dławiki typu DEHNbridge.

Wstępny schemat sieci pokazano na rysunkach poniżej.

5. Lokalizacja urządzeń

Lp.	nazwa	ilość	miejsce instalacji
1	Przełącznik sieci LAN	4	Parter, I piętro, II piętro, serwerownia
2	Firewall z analizatorem ruchu sieciowego	1	serwerownia
3	Serwer aplikacyjny	3	serwerownia
4	Przełącznik FC	1	serwerownia
5	rozbudowa macierzy		serwerownia
6	Serwer telekomunikacyjny	1	serwerownia
7	Rejestrator rozmów	1	serwerownia
8	Zestaw komputerowy	20	pomieszczenia oznaczone na rysunkach
9	notebook	15	pomieszczenia oznaczone na rysunkach
10	ups	1	serwerownia
11	Szafa 42U	1	serwerownia
12	Szafa 12U	4	Parter, I piętro, II piętro

Ostateczna lokalizacja urządzeń zostanie wskazana na etapie realizacji projektu.