

Załącznik nr 1 do SWZ
Znak sprawy: GK.271.1.2026.MG

Szczegółowy opis przedmiotu zamówienia

dla zamówienia pn.:

„Zakup urządzeń i oprogramowania”

w ramach projektu "Podniesienie poziomu ochrony cybernetycznej w gminie Unisław,
poprzez realizację zaplanowanych działań w obszarach organizacyjnym,
kompetencyjnym oraz technicznym" realizowanego w ramach projektu Cyberbezpieczny Samorząd"
dofinansowanego w formie grantu
z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC)
Priorytet II: Zaawansowane usługi cyfrowe,
Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Opracował:

Mariusz Bartosik

Unisław, styczeń 2026 r.

Spis treści:

1. Wymagania ogólne dla urządzeń i oprogramowania sieciowego.
2. Wymagania gwarancyjne.
3. Miejsce instalacji sprzętu i oprogramowania/systemu.
4. Zestawienie zakresu dostaw i usług.
5. Szczegółowy opis pozycji:
 - 5.1. Firewall – next generation – **CZĘŚĆ PIERWSZA**
 - 5.1.1 Przedłużenie licencji posiadanego urządzenia Fortinet FortiGate FG-60F
 - 5.2. Oprogramowanie EDR-XDR plus serwer - **CZĘŚĆ DRUGA**
 - 5.3. Klaster niezawodności i ciągłości działania systemów informatycznych: - **CZĘŚĆ TRZECIA**
 - 5.3.1. System do backupu
 - 5.3.2. Serwer do wykonywania kopii
 - 5.3.3. Macierz dyskowa
 - 5.3.4. Dyski do macierzy
 - 5.3.5. UPS Stanowiskowy
 - 5.4. Usługa bezpiecznej poczty - 2 lata - **CZĘŚĆ CZWARTA**
 - 5.5. Oprogramowanie do zarządzania logami plus serwer - **CZĘŚĆ PIĄTA**
 - 5.6. Teleinformatyczny System Zarządzania Bezpieczeństwem Informacji - **CZĘŚĆ SZÓSTA**

1. Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

- Zamawiany sprzęt musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w styczniu 2025 r., dostarczony w oryginalnym opakowaniu. Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Nie dopuszcza się zastosowanie urządzeń tzw. „refurbished”.
- Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, w którym nie wskazano szczegółowych warunków gwarancji, musi być objęte minimum 36 miesięczną gwarancją jeśli w opisie parametrów nie wskazano inaczej.
- Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji danego elementu.
- Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
- Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
- Wszystkie urządzenia muszą posiadać oznakowanie CE.
- Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL).
- Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V \pm 10%, 50 Hz.
- Wymagane jest, aby infrastruktura sprzętowa była gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.
- Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).
- Do każdej zmiany w infrastrukturze jednostki należy dostarczyć dokumentację w języku polskim, w pliku pdf, zawierającą opis wprowadzonych zmian oraz jeśli to konieczne schematy.

Zamawiający wymaga, aby Wykonawca realizując opisane w przedmiocie zamówienia dostawę i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:

- posiadaną konfigurację sieci,
- posiadaną konfigurację baz danych i backupów,
- posiadaną konfigurację serwerów,
- posiadaną konfigurację stacji roboczych.

2. Wymagania gwarancyjne.

Sprzęt:

- Jeśli wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona gwarancja oparta na gwarancji producenta rozwiązanie; 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 i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu;
- W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

Oprogramowanie

- Oprogramowanie powinno posiadać gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba że zapisy szczegółowe stanowią inaczej);

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

3. Miejsce instalacji sprzętu i oprogramowania/systemu.

- Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części dokumentu, w budynkach urzędu lub budynkach jednostek podległych, w miejscach wskazanych przez Zamawiającego.

4. Zestawienie zakresu dostaw i usług.

Lp.	Nazwa	Wymagana minimalna długość gwarancji (m-ce)	Ilość	jed. miary	Uwagi	Numer części zamówienia
1.	Firewall – next generation	24	1	Szt.	Monitorowanie, wykrywanie i reakcja na zagrożenia.	1
2.	Przedłużenie licencji posiadanego urządzenia Fortinet FortiGate FG-60F	24	1	Szt.	Aktualizacje, wsparcie producenta i utrzymanie funkcji bezpieczeństwa.	1
3.	Oprogramowanie EDR-XDR plus serwer	36	1	Kpl.	Monitorowanie, wykrywanie i reakcja na zagrożenia w punktach końcowych.	2
4.	Klaster niezawodności i ciągłości działania systemów informatycznych:					

	System do backup	36	1	Szt.	Tworzenie kopii bezpieczeństwa danych z komputerów i serwerów urzędu.	3
	Serwer	36	1	Szt.	Pozycja dotyczy budowy klastra niezawodnościowego HA, chmury prywatnej z dwóch fizycznych serwerów. W ramach tej pozycji należy również dostarczyć oprogramowanie do wirtualizacji, system operacyjny. Należy stworzyć min. dwa środowiska wirtualne.	3
	Macierz dyskowa	36	1	Szt.	Pozycja dotyczy zakupu macierzy dyskowej w celu zapewnienia przestrzeni dyskowej dla klastra serwerów HA, który zostanie do niej podłączony.	3
	Dyski do macierzy	36	4	Szt.	Pozycja dotyczy zakupu dysków do macierzy. Dodatkowe dyski zwiększą dostępną przestrzeń magazynową, umożliwiając obsługę rosnących danych i wymagań aplikacji działających w klastrze HA oraz poprawią wydajność.	3
5.	Usługa bezpiecznej poczty - 2 lata	24	1	Szt.	Usługa bezpiecznej poczty z ochroną SPF, DMARC, DKIM, antyspam oraz ochroną antywirusową, interfejsem poczty spełnia wymagania dostępności WCAG 2.1	4
6.	Oprogramowanie do zarządzania logami plus serwer	24	1	Szt.	Przechowywanie danych backupowych (z szyfrowaniem, deduplikacją, ochroną przed ransomware).	5
7.	Teleinformatyczny System Zarządzania Bezpieczeństwem Informacji	24	1	Szt.	Teleinformatyczny System Zarządzania Bezpieczeństwem Informacji (TSZBI) służy do monitorowania, kontrolowania i ochrony informacji w organizacji przed nieautoryzowanym dostępem, utratą lub uszkodzeniem. Umożliwia	6

					również zarządzanie ryzykiem oraz zapewnia zgodność działań z obowiązującymi przepisami i standardami bezpieczeństwa.	
7.	UPS Stanowiskowy	24	10	Szt.	Zakup w celu zapewnienia ciągłości działania oraz ochrony danych na stanowiskach komputerowych.	3

5. Szczegółów opis pozycji

5.1. Firewall – next generation - szt.1 (część nr 1 zamówienia) – 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 1 oddzielnego (fizycznego lub logicznego) 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.

Wraz z urządzeniem należy dostarczyć 2 wkładki sfp+ SR kompatybilne do dostarczanych urządzeń.

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. W ramach postępowania system musi zostać dostarczony w postaci pojedynczego urządzenia.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. 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:
 - 8 portów Gigabit Ethernet RJ-45.
 - 2 gniazdami SFP+ 10 Gbps.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System mieć możliwość podłączenia 2 zasilaczy. Należy dostarczyć 2 zasilacze.

Parametry wydajnościowe:

W zakresie Firewall'a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz nie mniej niż 124 tys. nowych połączeń na sekundę.

4. Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B.
1. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.7 Gbps.
2. Wydajność szyfrowania IPSec VPN nie mniej niż 25 Gbps.
3. 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 4.5 Gbps.
4. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.2 Gbps.
5. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.2 Gbps.

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 - zaporą ogniową 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.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.

5. 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.
2. 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 1000 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 1000 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:
 - Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

- Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Hasel dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
 4. 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 udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall 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 na okres 12 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, 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 24/7.

Opisy do wymagań ogólnych

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. **Wybrany Wykonawca przed zawarciem umowy powinien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie oferowanych rozwiązań.**

5.1.1 Przedłużenie licencji posiadanego urządzenia Fortinet FortiGate FG-60F (część nr 1 zamówienia)

Przedmiotem zamówienia jest przedłużenie licencji urządzenia Fortinet FortiGate FG-60F, (numer seryjny dostępny dla Wykonawcy po podpisaniu umowy), na okres 24 miesięcy (gwarancja 24 miesiące).

Wymagany zakres licencji obejmuje utrzymanie pełnej funkcjonalności urządzenia w okresie obowiązywania gwarancji, w tym:

- aktualizacje systemu i oprogramowania urządzenia,
- aktualizacje podpisów antywirusowych i sygnatur IPS,
- utrzymanie ochrony przed zagrożeniami (DoS/DDoS, malware, intruzami, exploitami),
- wsparcie techniczne zgodne z zakresem licencji Fortinet UTM (UTP lub Security Bundle).

Wykonawca nie może ograniczać funkcjonalności urządzenia ani przerwać świadczenia aktualizacji i ochrony w okresie obowiązywania licencji.

W przypadku awarii lub problemów technicznych Wykonawca zobowiązany jest do ich usunięcia w terminach określonych w umowie, zapewniając ciągłość działania urządzenia.

5.2. Oprogramowanie EDR-XDR plus serwer (część nr 2 zamówienia) – wymagania minimalne:

Zamawiający wymaga dostawy 70 licencji ze wsparciem technicznym i gwarancją na okres 36 miesięcy. Oprogramowania klasy EDR-XDR. Zamawiający wymaga przeprowadzenia certyfikowanego przez producenta oprogramowania szkolenia dla administratora Urzędu, wdrożenia w siedzibie klienta, zainstalowania na wyznaczonych stacjach/serwerach/urządzeniach mobilnych oraz przeniesienia konfiguracji z obecnie stosowanego systemu. Operacja ma się odbywać po godzinach pracy urzędu ze względu na potencjalne utrudnienia dla pracowników.

W przypadku, gdy oferowane rozwiązanie jest tożsame z obecnie stosowanym u Zamawiającego, Wykonawca dokona aktualizacji, standaryzacji oraz optymalizacji konfiguracji

zgodnie z aktualnymi wytycznymi producenta, a także przeprowadzi inwentaryzację i weryfikację polityk bezpieczeństwa.

Oprogramowanie EDR/XDR powinno spełniać następujące wymagania minimalne:

Administracja zdalna

1. Konsola centralnego zarządzania musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS).
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiającą co najmniej:
 - Pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania,
 - Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta,
 - Buforowanie ruchu HTTPS.
6. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej. Uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android:
 - Google Authenticator,
 - Microsoft Authenticator,
 - Authy,
 - Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
8. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
9. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej:
 - adresy sieciowe IP,
 - aktywne zagrożenia,
 - stan funkcjonowania oraz ochrony,
 - wersja systemu operacyjnego,
 - podzespoły komputera.
10. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:
 - wyrażenie CRON,
 - codziennie,
 - co tygodniowo,
 - co miesiąc,
 - co rok,
 - po wystąpieniu nowego zdarzenia,
 - po automatycznym umieszczeniu hosta w grupie dynamicznej.
11. Konsola centralnego zarządzania musi być dostępna co najmniej w językach polskim oraz angielskim
 - 11.1. Język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania
12. Rozwiązanie musi mieć możliwość tagowania obiektów.
13. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.

13.1. Eksport danych musi być możliwy w co najmniej następujących formatach:

13.1.1. JSON,

13.1.2. LEEF,

13.1.3. CEF.

Ochrona stacji roboczych - Windows

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).

2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:

3.1. wirus,

3.2. trojan,

3.3. robak,

3.4. adware,

3.5. spyware,

3.6. dialer,

3.7. phishing,

3.8. backdoor.

4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.

6. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.

7. Rozwiązanie musi posiadać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.

7.1. Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.

7.2. Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service).

7.3. Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.

8. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

9. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

10. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:

10.1. całego dysku,

10.2. wybranych katalogów,

10.3. pojedynczych plików,

10.4. plików spakowanych oraz skompresowanych,

10.5. dysków sieciowych,

10.6. dysków przenośnych.

11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:

11.1. wybranych plików,

11.2. wybranych procesów,

11.3. wybranych lokalizacji,

11.4. wybranych rozszerzeń,

11.5. nazwy wykrycia,

11.6. sumy kontrolnej (SHA1).

12. Rozwiązanie musi integrować się z Intel Threat Detection Technology.

13. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:

13.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.

13.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

13.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

14. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego,

zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

15. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.

16. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

17.1. typ urządzenia:

17.1.1. pamięci masowe,

17.1.2. optyczne pamięci masowe,

17.1.3. pamięci masowe Firewire,

17.1.4. urządzenia do tworzenia obrazów,

17.1.5. drukarki USB,

17.1.6. urządzenia Bluetooth,

17.1.7. czytniki kart inteligentnych,

17.1.8. modemy,

17.1.9. porty LPT/COM,

17.1.10. urządzenia przenośne.

17.2. parametry urządzenia:

17.2.1. numer seryjny,

17.2.2. producent,

17.2.3. model.

17.3. typ dostępu:

17.3.1. brak możliwości zapisu,

17.3.2. pełen dostęp,

17.3.3. ostrzeżenie użytkownika,

17.3.4. brak dostępu.

18. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

18.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

18.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

18.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

18.4. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

18.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

19. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.

19.1. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

19.2. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.

19.3. Raport musi posiadać co najmniej:

19.3.1. Listę zainstalowanych aplikacji,

19.3.2. Listę usług systemowych,

19.3.3. Informacje o systemie operacyjnym i sprzęcie,

19.3.4. Listę aktywnych procesów i połączeń sieciowych,

19.3.5. Harmonogram systemu operacyjnego,

19.3.6. Szczegóły pliku hosts,

19.3.7. Informacje o sterownikach.

20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu

- 20.1. antywirus,
- 20.2. zaporą osobista
- 20.3. sandbox,
- 20.4. antyspyware,
- 20.5. metody heurystyczne.

21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.

22. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.

22.1. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.

22.2. Ochrona musi być realizowana w oparciu o co najmniej:

- 22.2.1. globalna czarna lista RBL,
- 22.2.2. czarna lista użytkownika,
- 22.2.3. biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.

23. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:

23.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:

- 23.1.1. Skanowanie portów TCP oraz UDP,
- 23.1.2. Wykrywanie duplikacji adresu IP,
- 23.1.3. Atak zatrutowania ARP,
- 23.1.4. Nieprawidłowa długość pakietu TCP oraz UDP.

23.2. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:

- 23.2.1. RDP,
- 23.2.2. SMB,
- 23.2.3. My SQL,
- 23.2.4. MS SQL.

23.3. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

24. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.

24.1. Zaporą osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.

24.2. Zaporą osobista musi posiadać co najmniej cztery tryby pracy:

- 24.2.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
- 24.2.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
- 24.2.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
- 24.2.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.

24.2.4.1. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

25. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.

25.1. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

25.2. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

25.3. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.

26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.

26.1. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.

26.2. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej:

26.2.1. Treść komunikatu,

26.2.2. Obraz.

Ochrona stacji roboczych – MacOS

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych.

2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:

3.1. wirus,

3.2. trojan,

3.3. robak,

3.4. adware,

3.5. spyware,

3.6. dialer,

3.7. phishing,

3.8. backdoor.

4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć ożliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

6. Rozwiązanie musi chronić pliki co najmniej za pomocą:

6.1. Sygnatur wirusów.

6.2. Reputacji chmurowej.

7. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:

8.1. Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.

8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:

9.1. całego dysku,

9.2. wybranych katalogów,

9.3. pojedynczych plików,

9.4. plików spakowanych oraz skompresowanych,

9.5. Dysków sieciowych,

9.6. dysków przenośnych.

10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:

10.1. wybranych plików,

10.2. wybranych procesów,

10.3. wybranych lokalizacji,

10.4. wybranych rozszerzeń,

10.5. nazwy wykrycia,

10.6. sumy kontrolnej (SHA1).

11. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.

11.1. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł, stworzonych przez producenta.

11.2. Zapora osobista musi posiadać co najmniej dwa tryby pracy:

11.2.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

11.2.2. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

Ochrona stacji roboczych – Linux

1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne:

1.1. Ubuntu Desktop,

1.2. Red Hat Enterprise Linux

1.3. Linux Mint.

2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu:

2.1. Cinnamon,

2.2. GNOME,

2.3. KDE,

2.4. MATE,

2.5. XFCE.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:

3.1. wirus,

3.2. trojan,

3.3. robak,

3.4. adware,

3.5. spyware,

3.6. dialer,

3.7. phishing,

3.8. backdoor.

4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

6. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:

6.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

6.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

7. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:

7.1. całego dysku,

7.2. wybranych katalogów,

7.3. pojedynczych plików,

7.4. plików spakowanych oraz skompresowanych,

7.5. dysków sieciowych,

7.6. dysków przenośnych.

8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:

8.1. wybranych plików,

8.2. wybranych procesów,

8.3. wybranych lokalizacji,

8.4. wybranych rozszerzeń,

9. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

9.1. typ urządzenia:

9.1.1. pamięci masowe,

9.1.2. optyczne pamięci masowe,

9.2. parametry urządzenia:

9.2.1. numer seryjny,

9.2.2. producent,

9.2.3. model.

9.3. typ dostępu:

9.3.1. brak możliwości zapisu,

9.3.2. pełen dostęp,

9.3.3. brak dostępu.

Ochrona serwera – Windows Server

1. Rozwiązanie musi wspierać systemy w tym co najmniej:

1.1. Microsoft Windows Server 2012 R2,

1.2. Microsoft Windows Server 2016,

1.3. Microsoft Windows Server 2019,

1.4. Microsoft Windows Server 2022,

1.5. Microsoft Windows Server 2025.

2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:

3.1. wirus,

3.2. trojan,

3.3. robak,

3.4. adware,

3.5. spyware,

3.6. dialer,

3.7. phishing,

3.8. backdoor.

4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.

5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. W rozwiązaniu musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:

8.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.

8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:

9.1. całego dysku,

9.2. wybranych katalogów,

9.3. pojedynczych plików,

9.4. plików spakowanych oraz skompresowanych,

9.5. dysków sieciowych,

9.6. dysków przenośnych.

10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:

10.1. wybranych plików,

10.2. wybranych procesów,

10.3. wybranych lokalizacji,

10.4. wybranych rozszerzeń,

10.5. nazwy wykrycia,

10.6. sumy kontrolnej (SHA1).

11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

12.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez

użytkownika,

12.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

12.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

12.4. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika.

Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

12.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.

13.1. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

13.2. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.

13.3. Raport musi posiadać co najmniej:

13.3.1. Listę zainstalowanych aplikacji,

13.3.2. Listę usług systemowych,

13.3.3. informacje o systemie operacyjnym i sprzęcie,

13.3.4. Listę aktywnych procesów i połączeń sieciowych,

13.3.5. harmonogram systemu operacyjnego,

13.3.6. Szczegóły pliku hosts,

13.3.7. Informacje o sterownikach.

14. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu

14.1. antywirus,

14.2. zapora osobista

14.3. sandbox,

14.4. antyspyware,

14.5. metody heurystyczne.

15. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.

16. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

17.1. typ urządzenia:

17.1.1. pamięci masowe,

17.1.2. optyczne pamięci masowe,

17.1.3. pamięci masowe Firewire,

17.1.4. urządzenia do tworzenia obrazów,

17.1.5. drukarki USB,

17.1.6. urządzenia Bluetooth,

17.1.7. czytniki kart inteligentnych,

17.1.8. modemy,

17.1.9. porty LPT/COM,

17.1.10. urządzenia przenośne.

17.2. parametry urządzenia:

17.2.1. numer seryjny,

17.2.2. producent,

17.2.3. model.

17.3. typ dostępu:

17.3.1. brak możliwości zapisu,

17.3.2. pełen dostęp,

17.3.3. ostrzeżenie użytkownika,

17.3.4. brak dostępu.

18. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:

18.1. MS SQL,

18.2. Active Directory,

18.3. IIS,

18.4. Sysvol,

18.5. DNS,

18.6. DHCP,

18.7. Hyper-V,

18.8. Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.

19. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:

19.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:

19.1.1. Skanowanie portów TCP oraz UDP,

19.1.2. Wykrywanie duplikacji adresu IP,

19.1.3. Atak zatrutowania ARP,

19.1.4. Nieprawidłowa długość pakietu TCP oraz UDP.

19.2. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:

19.2.1. RDP,

19.2.2. SMB,

19.2.3. My SQL,

19.2.4. MS SQL.

19.3. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

20. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.

21. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.

21.1. Zapora osobista musi posiadać co najmniej cztery tryby pracy:

21.1.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

21.1.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

21.1.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

21.1.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.

21.1.4.1. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

Ochrona serwera – Linux

1. Rozwiązanie musi wspierać systemy w tym co najmniej:

1.1. RedHat Enterprise Linux (RHEL),

1.2. Rocky Linux,

1.3. Ubuntu,

1.4. Debian,

1.5. SUSE Linux Enterprise Server (SLES),

1.6. Oracle Linux,

1.7. Amazon Linux.

2. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:

2.1. wirus,

2.2. trojan,

2.3. robak,

2.4. adware,

2.5. spyware,

2.6. dialer,

- 2.7. phishing,
 - 2.8. backdoor.
 - 3. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS.
 - 4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
 - 5. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
 - 6. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
 - 7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
 - 7.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 7.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
 - 8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
 - 8.1. całego dysku,
 - 8.2. wybranych katalogów,
 - 8.3. pojedynczych plików,
 - 8.4. plików spakowanych oraz skompresowanych,
 - 8.5. dysków sieciowych,
 - 8.6. dysków przenośnych.
 - 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
 - 9.1. wybranych plików,
 - 9.2. wybranych procesów,
 - 9.3. wybranych lokalizacji,
 - 9.4. wybranych rozszerzeń,
 - 10. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
 - 10.1. Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
 - 11. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
 - 12. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonych mikro-serwisów.
 - 13. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach:
 - 13.1. proces budowania obrazu kontenera,
 - 13.2. wdrażanie obrazu kontenera.
- Mobile Device Management
- 1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
 - 2. MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania.
 - 2.1. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami:
 - 2.1.1. Android,
 - 2.1.2. iOS,
 - 2.1.3. iPadOS.
 - 2.2. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:
 - 2.2.1. Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),
 - 2.2.2. Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
 - 2.2.3. VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),

2.2.4. Apple Business Manager (ABM),

2.2.5. Android Enterprise (co najmniej w zakresie Device Owner).

3. MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

- 3.1. usunięcie zawartości urządzenia,
- 3.2. przywrócenie urządzenia do ustawień fabrycznych,
- 3.3. zablokowanie urządzenia,
- 3.4. uruchomienie sygnału dźwiękowego,
- 3.5. lokalizację GPS,
- 3.6. Resetowanie hasła blokady ekranu.

4. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.

5. MDM musi umożliwiać co najmniej:

5.1. Dla systemów iOS oraz iPadOS

- 5.1.1. konfigurację kont e-mail,
- 5.1.2. konfigurację połączeń VPN,
- 5.1.3. Konfigurację połączeń Wi-Fi,
- 5.1.4. Konfigurację listy certyfikatów,
- 5.1.5. możliwość uruchomienia trybu jednej aplikacji.

5.2. Dla systemu Android:

- 5.2.1. blokadę wykonywania połączeń,
- 5.2.2. blokadę konfiguracji sieci Wi-Fi,
- 5.2.3. blokadę konfiguracji tuneli VPN,
- 5.2.4. zarządzanie aktualizacjami systemu operacyjnego,
- 5.2.5. blokadę zmiany tapety urządzenia.

Mobile Threat Defense (MTD) dla systemu Android

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych.

2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:

2.1. Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.

2.2. Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.

3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

4. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:

4.1. Złożoność kodu blokady ekranu:

- 4.1.1. Wzór,
- 4.1.2. PIN,
- 4.1.3. Hasło,

4.2. Przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu,

4.3. Zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.

5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:

- 5.1. nazwę aplikacji,
- 5.2. nazwę pakietu,
- 5.3. kategorię sklepu Google Play,
- 5.4. uprawnienia aplikacji,
- 5.5. pochodzenie aplikacji z nieznanego źródła.

6. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.

Sandbox w chmurze

1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.

2. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.

3. Rozwiązanie musi wspierać systemy w tym co najmniej:

- 3.1. Microsoft Windows 10 oraz 11,
- 3.2. Microsoft Windows Server,
- 3.3. macOS 11 (Big Sur) oraz nowszych
- 3.4. RedHat Enterprise Linux (RHEL),
- 3.5. Rocky Linux,
- 3.6. Ubuntu,

- 3.7. Debian,
 - 3.8. SUSE Linux Enterprise Server (SLES),
 - 3.9. Oracle Linux,
 - 3.10. Amazon Linux.
 4. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
 5. Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego.
 6. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:
 - 6.1. archiwa,
 - 6.2. skrypty,
 - 6.3. pliki wykonywalne,
 - 6.4. pliki rejestru systemowego (.reg),
 - 6.5. możliwy spam,
 - 6.6. dokumenty.
 7. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:
 - 7.1. natychmiast po ich przeanalizowaniu,
 - 7.2. po upływie 30 dni,
 - 7.3. nigdy.
 8. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
 9. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
 10. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia.
 11. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
 12. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.
 - 12.1. Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.
 13. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników:
 - 13.1. czysty,
 - 13.2. podejrzany,
 - 13.3. bardzo podejrzany,
 - 13.4. szkodliwy.
 14. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej:
 - 14.1. wstrzymania uruchamiania pobieranych plików z następujących źródeł:
 - 14.1.1. przeglądarki internetowe,
 - 14.1.2. programy poczty e-mail,
 - 14.1.3. nośniki wymienne,
 - 14.1.4. pliki wyodrębnione z archiwum.
 15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzenia oraz z poziomu klienta antywirusowego.
- Szyfrowanie
1. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
 2. Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker.
 3. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
 4. Rozwiązanie musi umożliwiać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego.
 5. Rozwiązanie musi posiadać autentykację typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
 - 5.1. Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia.
 - 5.2. Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność

może ustalić administrator konsoli centralnego zarządzania.

6. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania.

6.1. Hasło odzyskiwania po użyciu musi zostać zmodyfikowane.

6.2. Hasło odzyskiwania nie może być krótsze niż 8 znaków.

6.3. Hasło odzyskiwania nie może być dłuższe niż 20 znaków.

7. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

8. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.

9. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.

10. Rozwiązanie musi wspierać dyski wykorzystujące funkcji OPAL w wersji co najmniej 2.0.

11. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku.

Endpoint Detection and Response / eXtended Detection and Response

1. Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego.

2. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego.

3. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego:

3.1. tworzenie procesów,

3.2. uruchamianie, zatrzymanie i modyfikacja usług,

3.3. utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym,

3.4. usuwanie oraz zmiana nazw plików,

3.5. tworzenie i usuwanie kluczy rejestru systemowego,

3.6. ładowanie bibliotek DLL,

3.7. zalogowanie użytkowników,

3.8. elementy sieciowe, w tym co najmniej

3.8.1. pobranie plików wykonywalnych,

3.8.2. zestawienie połączeń TCP/IP,

3.8.3. zapytania HTTP,

3.8.4. zapytania DNS.

4. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa.

4.1. Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach:

4.1.1. blokowanie pliku wykonywalnego,

4.1.2. blokowanie pliku wykonywalnego i poddanie go kwarantannie,

4.1.3. blokowanie podejrzanej biblioteki DLL,

4.1.4. zakończenie procesu,

4.1.5. skanowanie komputera w poszukiwaniu zagrożeń,

4.1.6. wyłączenie komputera,

4.1.7. izolacja sieciowa hosta,

4.1.8. wylogowanie użytkownika.

4.2. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML.

5. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

5.1. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.

5.2. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej:

5.2.1. proces,

5.2.2. proces nadrzędny (proces rodzica),

5.2.3. nazwę procesu,

5.2.4. ścieżkę procesu,

5.2.5. wiersz polecenia,

5.2.6. wydawcę,

5.2.7. typ podpisu,

- 5.2.8. SHA-1,
- 5.2.9. SHA-2,
- 5.2.10. użytkownika.
- 5.3. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML.
- 6. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.
- 6.1. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.
- 6.2. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące):
 - 6.2.1. SHA-1,
 - 6.2.2. SHA-256.
- 7. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej:
 - 7.1. hash pliku SHA-1,
 - 7.2. hash pliku SHA-256,
 - 7.3. hash pliku MD5,
 - 7.4. typ sygnatury podpisu cyfrowego,
 - 7.5. wydawcę certyfikatu,
 - 7.6. wersję pliku,
 - 7.7. oryginalną nazwę pliku,
 - 7.8. rozmiar pliku,
 - 7.9. reputację i popularność pliku w oparciu o system reputacji producenta tego samego rozwiązania antywirusowego,
 - 7.10. pierwsze uruchomienie pliku w środowisku,
 - 7.11. ostatnie uruchomienie pliku w środowisku,
- 8. Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL:
 - 8.1. oznaczania ich jako bezpieczne lub niebezpieczne,
 - 8.2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
 - 8.3. zablokowania wykonywania i wykorzystania pliku,
 - 8.4. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
- 9. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń).
 - 9.1. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
 - 9.2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
 - 9.3. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
 - 9.4. administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
- 10. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera.
 - 10.1. Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli.
- 11. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów.
- 12. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików, w tym co najmniej VirusTotal.

Serwer – wymagania minimalne

Ogólne

- Serwer klasy rack 2U, przystosowany do pracy w trybie ciągłym (24/7).
- Serwer musi być nowy, pochodzić z oficjalnego kanału dystrybucyjnego producenta i posiadać min. 36 miesięcy gwarancji on-site NBD (Next Business Day) lub równoważnej.

- Producent serwera musi zapewniać wsparcie techniczne oraz części zamienne przez okres min. 5 lat od zakończenia produkcji.

Procesor

- Minimum **1 × procesor 8-rdzeniowy / 16-wątkowy** o taktowaniu bazowym co najmniej 2,0 GHz, obsługą pamięci ECC DDR4/DDR5, zintegrowanym kontrolerem pamięci, cache L3 minimum 16 MB, obsługą technologii wirtualizacji sprzętowej, zoptymalizowany do pracy w środowiskach wielowątkowych i serwerach klasy średniej/wyższej, wydajnością równoważną nowoczesnym procesorom serwerowym 8–16 rdzeniowym. Możliwość rozbudowy o drugi procesor.
- **Pamięć RAM**
- Minimum 64 GB DDR4 lub DDR5 ECC RDIMM.
- Możliwość rozbudowy do min. 256 GB RAM.
- Minimum 8 banków pamięci dostępnych w serwerze.

Pamięć masowa

1. Minimum **6 zatok dyskowych 3.5" lub 2.5" hot-plug**.
2. Konfiguracja dysków:
 - 2 × SSD min. 480 GB (RAID 1 – system),
 - 4 × HDD min. 2 TB 7.2k (RAID 10 – dane/logi).
3. Sprzętowy kontroler RAID z pamięcią cache i podtrzymaniem (bateria/supercap).
4. Obsługa RAID 0/1/5/6/10.

Sieć

- Minimum 2 × 1 GbE RJ-45.
- Minimum 2 × 10 GbE (SFP+ lub RJ-45).
- Obsługa VLAN, PXE.

Zasilanie

- Minimum 2 redundantne zasilacze hot-plug.
- Zasilacze o sprawności min. 80 PLUS Platinum.

Zarządzanie

1. Wbudowany kontroler zarządzania z dedykowanym portem (np. iDRAC / iLO / XClarity lub równoważny).
2. Funkcje zdalnego zarządzania:
 - pełne KVM over IP,
 - monitoring sprzętu,
 - powiadomienia e-mail/SNMP,
 - zdalna konfiguracja BIOS/UEFI,
 - zdalna instalacja systemu operacyjnego.

Certyfikaty

Serwer musi posiadać deklaracja CE.

Warunki gwarancji

36 miesięcy gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24/7/365 poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii dyski zostają u Użytkującego. **Wybrany Wykonawca przed zawarciem umowy w sprawie zamówienia przedłoży Zamawiającemu oświadczenie, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Użytkującego.**

Wybrany Wykonawca przed zawarciem umowy w sprawie zamówienia przedłoży Zamawiającemu oświadczenie Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.

Dokumentacja użytkownika

Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Dodatkowe wymagania

- Szyny montażowe rack w zestawie.
- Możliwość instalacji systemu operacyjnego Linux (np. Debian, Ubuntu, CentOS, Rocky) lub Windows Server.
- Serwer musi umożliwiać rozbudowę o dodatkowe dyski, pamięć i interfejsy sieciowe.

Do serwera musi być dostarczony serwerowy **system operacyjny** spełniający minimum następujące funkcjonalności:

- licencje muszą mieć możliwość instalacji minimum 2 maszyn na serwerach wirtualnych
- wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych
- zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe
- wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play)
- graficzny interfejs użytkownika
- obsługa systemów wieloprocesorowych
- obsługa platform sprzętowych x86, x64
- możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu
- Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. Potwierdzenie dołączyć do oferty
- możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowego programowania:
 - usługi sieciowe DNS i DHCP,
 - usługi katalogowe pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe),
 - zdalna dystrybucja oprogramowania na stacje robocze,
 - praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
 - możliwość rozłożenia obciążenia serwerów,
 - serwis udostępniania stron WWW, serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management),
 - wsparcie dla protokołu IP w wersji 6 (IPv6)
- Możliwość tworzenie serwerów wirtualnych, oprogramowanie wspierające tworzenie serwerów wirtualnych musi spełniać następujące wymagania funkcjonalne:
 - warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych
 - licencja musi umożliwiać zmianę wersji oprogramowania na niższą (downgrade)
 - rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze
 - możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-4 wirtualnych kart sieciowych.
 - możliwość przydzielania większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji
 - możliwość udostępniania maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy
 - konsola graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.
 - możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach
 - możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
 - możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi

- możliwość integracji z usługami katalogowymi Microsoft Active Directory w tym jako kontroler domeny Microsoft Active Directory.
- mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (np. wgrywania krytycznych poprawek) bez potrzeby wyłączania wirtualnych maszyn
- obsługa przełączania ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z kilku dostępnych ścieżek.
- możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi,
- mechanizm wysokiej dostępności HA, w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione na nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym
- 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 wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia w razie awarii karty sieciowej
- wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN)
- Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
- Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
- Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
- Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET

5.3. Klaster niezawodności i ciągłości działania systemów informatycznych (Część nr 3 zamówienia):

W ramach realizacji zamówienia Wykonawca dostarczy fabrycznie nowe, nieużywane urządzenia oraz licencjonowane oprogramowanie, obejmujące:

1. System do backupu,
2. Serwer do wykonywania kopii,
3. Macierz dyskową,
4. Dyski do macierzy.

Urządzenia muszą zostać dostarczone w oryginalnych opakowaniach, posiadać oznaczenie CE oraz pochodzić z autoryzowanego kanału dystrybucyjnego producenta.

Zakres realizacji obejmuje również wszelkie czynności niezbędne do zapewnienia pełnej funkcjonalności dostarczonego rozwiązania, w tym w szczególności:

- montaż i instalację sprzętu w wyznaczonych lokalizacjach,
- instalację i konfigurację dostarczonego oprogramowania,
- integrację z istniejącą infrastrukturą Zamawiającego (serwery, sieć, systemy backupu, i inne),
- wykonanie konfiguracji środowiska wysokiej dostępności (HA) zgodnie z wymaganiami Zamawiającego,

- utworzenie co najmniej dwóch środowisk wirtualnych,
- przygotowanie i przekazanie dokumentacji powykonawczej w języku polskim w formie elektronicznej (PDF).

Wszystkie powyższe czynności stanowią integralną część realizacji dostawy i są wymagane w celu prawidłowego uruchomienia i przekazania Zamawiającemu gotowego do pracy rozwiązania.

5.3.1. System do backup

System do tworzenia kopii bezpieczeństwa danych z komputerów i serwerów urzędu.

Wykonawca zobowiązany jest do uwzględnienia w konfiguracji systemu backupu wszystkich środowisk bazodanowych działających u Zamawiającego na dzień rozpoczęcia realizacji zamówienia, niezależnie od ich typu i platformy systemowej. W szczególności Wykonawca zobowiązany jest do przeprowadzenia inwentaryzacji istniejących systemów baz danych (w tym m.in. PostgreSQL, MySQL, MS SQL, SQLite oraz innych stosowanych) oraz ich pełnej integracji z nowym systemem backupu zgodnie z wymaganiami ciągłości działania. Każde środowisko bazodanowe objęte backupem musi mieć skonfigurowane automatyczne zadania backupowe oraz harmonogram zgodny z polityką bezpieczeństwa. Dla każdego z tych środowisk Wykonawca musi przeprowadzić testowe odtworzenie danych i potwierdzić jego skuteczność w dokumentacji powykonawczej.

Zamawiający wymaga dostawy oprogramowania do tworzenia kopii zapasowych serwerów i maszyn wirtualnych, spełniającego następujące warunki minimalne:

- Licencja wieczysta dla minimum 10 maszyn wirtualnych ze wsparciem i gwarancją na okres 24 miesięcy.
- Oprogramowanie musi zapewniać pełną obsługę środowisk wirtualizacyjnych VMware vSphere w wersjach 7.x oraz 8.x, a także Microsoft Hyper-V w wersjach 2016, 2019 oraz 2022, obejmując w szczególności wykonywanie kopii zapasowych maszyn wirtualnych, odzyskiwanie ich w całości oraz odzyskiwanie na poziomie plików.
- Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami
- Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.
- Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V
- Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej oraz nie posiadać ograniczeń licencyjnych co do ilości przechowywanych danych
- Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
- Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności
- Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w takiej puli
- Oprogramowanie musi pozwalać na rozszerzenie lokalnej
- przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi lub serwisami online. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych

- Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu
- Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
- Oprogramowanie musi zapewniać backup jednorzbiegowy - nawet w przypadku wymagania granularnego odtworzenia
- Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP.
- Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota (migawki).
- Oprogramowanie musi mieć wbudowane mechanizmy
- szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
- Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
- Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych
- Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
- Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
- Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
- Oprogramowanie musi wspierać natywnie kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
- Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server
- Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej
- Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
- Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
- Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza
- Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu.
- Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. - Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
- Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
- Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji
- Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V
- Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere
- Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
- Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2

- Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
 - Linux - ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
 - Mac - HFS, HFS+
 - Windows - NTFS, FAT, FAT32, ReFS
- Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces
- Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej
- Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL Server włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat. Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia
- Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
- Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
- Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender.
- System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper- V bez potrzeby korzystania z narzędzi firm trzecich
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.x – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2016, 2019 oraz 2022
- System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej
- System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
- System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
- System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych

Raportowanie

1. Proponowane rozwiązanie musi posiadać możliwość centralnego zarządzania, monitorowanie i raportowanie w odniesieniu do środowisk oprogramowania i urządzeń, w tym wielu środowisk backupowych
2. Proponowane rozwiązanie musi umożliwiać wysyłanie powiadomień o zadaniach za pomocą poczty elektronicznej lub SNMP

Pakiet godzin serwisowych w ilości 20 godzin do wykorzystania w okresie do 30.06.2026 r. Okres gwarancji min. 24 miesiące.

5.3.2. Serwer - wymagania minimalne

1. Obudowa typu RACK o wysokości maksymalnie 2U z możliwością instalacji min. 16 dysków 2.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych wraz z podłączonymi przewodami.
2. Płyta główna z możliwością zainstalowania dwóch procesorów.
3. Zainstalowane dwa procesory klasy x86 dedykowane do pracy z oferowanym serwerem, umożliwiające osiągnięcie przez serwer wyniku co najmniej 25 855 punktów w teście CPU

Benchmark Multithread Rating, według wyników publikowanych na stronie <https://www.cpubenchmark.net> na dzień ogłoszenia zamówienia Wykonawca (składający ofertę) zobowiązany jest do dołączenia do oferty wydruku z ww. strony internetowej potwierdzającego spełnienie wymogu.

4. Pamięć RAM: zainstalowane min. 256 GB w najnowszej technologii oferowanej przez producenta, płyta główna musi obsługiwać do min. 8 TB pamięci RAM DDR5, co najmniej 24 slotów na pamięć wolnych w oferowanej konfiguracji.
5. Zabezpieczenia pamięci RAM: Memory Rank Sparing i/lub Memory Mirror i/lub Single Device Data Correction i/lub Memory Lockstep i/lub Chipkill i/lub Extended ECC i/lub Advanced Memory Device Correction i/lub AMD Memory Guard i/lub ECC i/lub Demand Scrubbing i/lub Patrol Scrubbing i/lub Permanent Fault Detection (PFD).
6. Zintegrowana karta graficzna ze złączem VGA.
7. Interfejsy sieciowe: Wbudowane co najmniej 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, co najmniej 2 interfejsy w 10GbE w standardzie SFP+ z dedykowanymi wkładkami do każdego portu oraz co najmniej 2 interfejsy FC o prędkości transferu min. 16 Gb/s na port w celu podłączenia serwerów z macierzą dyskową SAN.
8. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 2 dyski twarde Hot-Plug SSD SATA o prędkości min. 6 Gb/s o pojemności co najmniej 480 GB każdy. W przypadku uszkodzenia dysku w okresie gwarancji Zamawiający wymaga by uszkodzony dysk pozostał jego własnością.
9. Kontroler RAID: Sprzętowy kontroler dyskowy umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60 z podtrzymaniem bateryjnym.
10. Możliwość zainstalowania napędu LTO-8.
11. Wbudowane porty: min. 3 porty USB, w tym co najmniej 1 port USB musi być dostępny z przodu obudowy. Ilość dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakiegokolwiek slot PCI Express serwera.
12. Wentylatory: typu Hot Plug.
13. Zasilacze: Redundantne typu Hot Plug o mocy nieprzekraczającej 900W każdy, o klasie niezawodności Titanium.
14. Karta/moduł zarządzania: Niezależny od zainstalowanego na serwerze systemu operacyjnego posiadający dedykowane złącze umożliwiający zdalne zarządzanie:
 - zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
 - zdalne monitorowanie i informowanie o statusie serwera,
 - szyfrowane połączenie oraz autentykację i autoryzację użytkownika,
 - możliwość podmontowania zdalnych wirtualnych napędów,
 - wirtualną konsolę z dostępem do myszy, klawiatury,
 - wsparcie dla IPv6,
 - wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,
 - integracja z Active Directory,
 - wsparcie dla dynamic DNS.
15. System bezpieczeństwa serwera realizowany poprzez następujące zabezpieczenia:
 - wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera;
 - blokada zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych;
 - moduł TPM 2.0.
16. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzanie serwerem klasy Microsoft Windows Server Standard 2025 wraz z 25 licencjami dostępowymi umożliwiającymi korzystanie przez 25 użytkowników z zasobów klastra serwerowego lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności. Oferowany system musi mieć możliwość zainstalowania co najmniej 1 wersji wstecz (tj. Windows Server 2022).
17. Warunki równoważności dla dostawy oprogramowania Microsoft Windows Server Standard 2025 wraz z 25 licencjami dostępowymi Microsoft Windows Server 2025 CAL User:

- Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji oraz dostępu do serwerowego systemu operacyjnego dla minimum 25 użytkowników.
 - Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
 - 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.
 - Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
 - Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
 - Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
 - Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
 - Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
 - Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
 - Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
 - Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
 - Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
 - Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
 - Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
 - Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
 - Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
 - Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
 - Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
 - Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
 - Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
18. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
19. Producent oferowanego serwera powinien posiadać certyfikowany system zarządzania jakością i środowiskiem (np. ISO 9001, ISO 14001 lub równoważny). Oferowany serwer musi posiadać deklarację zgodności CE i spełniać kryteria środowiskowe, w tym zgodność z dyrektywą RoHS.
20. Gwarancja: min. 36 miesięcy gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z gwarantowaną skuteczną naprawą do końca następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dysków Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej

konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji przez portal producenta serwera. Gwarancja powinna rozpocząć swój bieg od dnia podpisania końcowego protokołu odbioru całego zamówienia. Możliwość przedłużenia gwarancji do co najmniej 7 lat.

5.3.3. Macierz dyskowa SAN - wymagania minimalne

1. Obudowa typu RACK o wysokości maksymalnie 2U z możliwością instalacji do 24 dysków 2.5" Hot-Plug.
2. Macierz musi posiadać co najmniej 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe.
3. Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania baterijnego lub z zastosowaniem innej technologii.
4. Macierz musi mieć możliwość obsługi dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie macierzy dyskowej. Macierz musi obsługiwać dyski 2,5" i 3,5" (możliwe w ramach dołączonej półki). Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 160 dysków twardych.
5. Macierz musi posiadać co najmniej 4 porty FC 16 Gb/s (2 porty FC na kontroler). W zestawie niezbędne okablowanie do podłączenia macierzy z serwerami zapewniające możliwie najszybszy przesył danych oferowany przez porty wraz z wkładkami.
6. Zainstalowane min. 4 dyski Hot-Plug SAS o prędkości min. 12 Gb/s o pojemności co najmniej 1,2 TB każdy oraz 3 dyski twarde Hot-Plug SSD SAS o prędkości min. 12 Gb/s o pojemności co najmniej 1,9 TB każdy.
7. Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID3, RAID10/RAID1+0, RAID5, RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).
8. Macierz musi umożliwiać definiowanie globalnych dysków Hot-spare.
9. Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.
10. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
11. Macierz musi umożliwiać dokonywanie na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.
12. Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.
13. Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).
14. Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, VMWare.
15. Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery,

- zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
16. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje Wykonawca jest zobowiązany dostarczyć w ramach niniejszego postępowania.
 17. Producent oferowanej macierzy powinien posiadać certyfikowany system zarządzania jakością i środowiskiem (np. ISO 9001, ISO 14001 lub równoważny). Oferowana macierz musi posiadać deklarację zgodności CE i spełniać kryteria środowiskowe, w tym zgodność z dyrektywą RoHS. .
 18. Gwarancja: min. 36 miesięcy gwarancji producenta obejmująca wszystkie komponenty macierzy wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z gwarantowaną skuteczną naprawą do końca następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dyski Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej macierzy, w tym model i typ dysków twardej, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji przez portal producenta macierzy.

5.3.4. Dyski do macierzy - wymagania minimalne

- Typ: Dyski twarde SAS (Serial Attached SCSI)
- Ilość: 4 sztuk
- Interfejs: SAS 12 Gb/s
- Pojemność: minimum 1,2 TB każdy
- Format: 2,5 cala (Hot-Plug)
- Prędkość obrotowa: min. 10 000 RPM
- Obsługa przez kontrolery macierzy w trybie active-active
- Kompatybilność z oferowaną macierzą dyskową
- Dyski muszą być fabrycznie nowe i pochodzić z oficjalnej dystrybucji producenta
- Dyski muszą umożliwiać pracę w konfiguracjach RAID (RAID 1/5/6/10), z wykorzystaniem wszystkich dysków w macierzy
- Dyski muszą być zgodne z oferowaną macierzą SAN oraz wspierane przez jej kontrolery macierzowe, przeznaczone do pracy ciągłej w środowisku enterprise, objęte gwarancją producenta.
- Wszystkie elementy muszą być dostarczone z odpowiednimi ramkami montażowymi i oznaczone w sposób umożliwiający ich identyfikację.

Wymagania gwarancyjne:

- Gwarancja: minimum 36 miesięcy realizowana w miejscu instalacji,
- W przypadku awarii, uszkodzone dyski pozostają u Zamawiającego,
- Możliwość zgłoszenia awarii przez infolinię lub portal producenta,
- Możliwość weryfikacji konfiguracji i gwarancji dysków po numerze seryjnym na stronie producenta.

W ramach klastra niezawodności i ciągłości działania systemów informatycznych należy wykonać niezbędną instalację, konfigurację, wdrożenie – wymagania minimalne

Wszystkie poniższe czynności stanowią integralną część realizacji dostawy i są wymagane w celu prawidłowego uruchomienia i przekazania Zamawiającemu gotowego do pracy rozwiązania.

Celem prac jest przygotowanie środowiska teleinformatycznego, na potrzeby realizacji elementów cyberbezpieczeństwa, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie.

Część sprzętowa powinna zostać oparta na rozbudowie systemu 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.

Zamawiający wymaga następującego zakresu usług realizowanego w porozumieniu z Zamawiającym:

- a) Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązanie dla sytuacji kryzysowych wdrożenia.
- b) Sporządzenia Dokumentacji Systemu według której nastąpi realizacja. Dokumentacja Systemu musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia. W szczególności koncepcję techniczną projektu, która powinna zawierać opis mechanizmów działania systemu z wykorzystaniem dostarczonych i rozbudowywanych elementów sprzętowych.
 - schematy połączeń
 - mechanizmy działania głównych elementów sprzętowych:
 - sieć LAN - przełączniki sieciowe
 - klaster wirtualizacyjny
 - system backupu i archiwizacji danych
 - system serwerowy
 - system macierzowy
 - mechanizmy działania głównych elementów programowych:
 - system EDR-XDR
 - system zarządzania siecią
 - testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności
 - sposób odbioru uzgodniony z Zamawiającym
 - listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu
 - opis przypadków, w których projekt dopuszcza niedziałanie systemu
 - 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 całość dostarczonego rozwiązania w pomieszczeniu serwerowni, co najmniej w zakresie:

1. Wniesienie, ustawienie i fizyczny montaż oraz konfiguracja wszystkich dostarczonych urządzeń. Wykonawca zobowiązany jest do dostarczenia szafy rack niezbędnej do montażu wszystkich dostarczonych urządzeń. Przed dostawą szafy Wykonawca przeprowadzi wizję lokalną oraz weryfikację warunków technicznych pomieszczenia serwerowni, obejmującą w szczególności dostępność miejsca, wymiary, nośność podłoża, istniejącą infrastrukturę okablowania i zasilania. Szafa rack musi zostać dobrana i dostarczona po akceptacji przez Zamawiającego, tak aby była zgodna z wymaganiami instalacyjnymi dostarczanych urządzeń oraz możliwościami pomieszczenia.
2. Rozbudowa istniejących zasobów sprzętowych.

3. Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego.
4. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
5. Podłączenie całości rozwiązania do infrastruktury Zamawiającego.
6. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
7. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.
8. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
9. Wykonawca musi dostarczyć i zintegrować z oferowanym rozwiązaniem urządzenie do podtrzymania zasilania, które zapewni nieprzerwaną pracę wszystkich komponentów systemu przez minimum 5 godzin w przypadku braku zasilania sieciowego.
10. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).
11. Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ między innymi celem:
12. Stworzenia połączeń sieci LAN pomiędzy przełącznikami.
13. Podłączenia urządzeń serwerowo-macierzowych (serwery, macierze) do przełączników sieci LAN.
14. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej $n+1$.
15. Połączenia muszą 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 oprogramowania do systemu wykonywania backupu i archiwizacji danych działającego na serwerze backupu.
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.
5. Instalacja i konfiguracja oprogramowania EDR-XDR
6. Migracja istniejącego środowiska baz danych PostgreSQL z systemu Linux na nowy serwer w środowisku Windows, obejmująca przeniesienie danych, konfiguracji oraz zapewnienie pełnej funkcjonalności i ciągłości działania systemu. Po zakończeniu migracji Wykonawca zobowiązany jest do przeprowadzenia testów poprawności działania przeniesionych baz danych oraz dostarczenia dokumentacji powykonawczej obejmującej opis przebiegu migracji, zastosowane rozwiązania, napotkane problemy oraz wyniki testów. Nowe środowisko bazodanowe musi zostać objęte systemem wykonywania backupu, zgodnie z konfiguracją i procedurami obowiązującymi w nowym środowisku. W ramach odbioru Wykonawca zobowiązany jest do wykonania testowego odtworzenia kopii zapasowej bazy danych i potwierdzenia jej integralności.

Konfiguracja przełączników/sieci LAN w zakresie:

1. Przeprowadzenie audytu obecnej topologii oraz konfiguracji.
2. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.
3. Stworzenia odpowiednich konfiguracji STACK z wykorzystaniem dedykowanych modułów.

4. Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym).
5. Wymagane jest wydzielenie i skonfigurowanie co najmniej stref:
 - SERWERY
 - DRUKARKI I URZĄDZENIA WIELOFUNKCYJNE
 - KAMERY
 - UŻYTKOWNICY WEWNĘTRZNI
 - UŻYTKOWNICY ZEWNĘTRZNI
 - INNE
6. Jeśli jest to konieczne – Zamawiający oczekuje rekonfiguracji adresacji IP w danych strefach (readresacja urządzeń, serwerów, komputerów leży po stronie Wykonawcy).
7. Zamawiający wymaga skonfigurowania polityk ruchu pomiędzy strefami na urządzeniach firewall.
8. Konfiguracja połączeń pomiędzy przełącznikami sieci LAN.
9. Konfiguracja sieci VLAN na wszystkich przełącznikach – konfiguracja propagacji sieci VLAN.
10. Konfiguracja routingu pomiędzy sieciami VLAN na centralnym urządzeniu firewall - klaster;
11. Zamawiający wymaga aby wszystkie sieci VLAN (L2) zostały rozpięte na warstwie L2 na urządzeniu firewall – (połączenie TRUNK).
12. Zamawiający wymaga skonfigurowania mechanizmów bezpieczeństwa na dostarczonych przełącznikach LAN co najmniej w zakresie:
 - Konfiguracja mechanizmów DHCP Snooping
 - Konfiguracja mechanizmów Dynamic ARP Inspection
 - Konfiguracja mechanizmów Port Security na wskazanych portach przełączników
 - Konfiguracja mechanizmów 802.1x na wskazanych portach przełączników w oparciu o certyfikaty komputerów (konfiguracja Centrum Certyfikacji oraz polityk leży po stronie Wykonawcy) z wykorzystaniem dostarczonego oprogramowania NAC.
13. Ustawienie serwera czasu dla urządzeń sieci LAN – przełączników sieciowych - na klaster firewall.
14. Zamawiający wymaga instalacji i konfiguracji serwera logów dla urządzeń sieci LAN (maszyna wirtualna) – przełączników sieciowych, z graficznym interfejsem przeszukiwania. Zamawiający dopuszcza rozwiązania Open Source.
15. 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.
16. Wykonawca skonfiguruje urządzenia aby raportowały, przesyłały dane do zainstalowanego serwera logów i monitorowania sieci.
17. Testowanie obsługi ruchu sieciowego.
18. Testowanie skuteczności zabezpieczeń.

Konfiguracja elementów bezpieczeństwa sieciowego:

Konfiguracja/Modernizacja konfiguracji UTM dla nowych urządzeń w zakresie:

1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.
2. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta.
3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email)
4. Przygotowanie projektu włączenia urządzenia do sieci LAN urzędu.
5. Konfiguracja dostarczonych systemów Firewall:
 - Konfiguracja podstawowych parametrów
 - Konfiguracja translacji adresów NAT
 - Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, macierze, itp.
 - Konfiguracja inspekcji określonych protokołów sieciowych;
 - Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall;
 - Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;

- Testowanie działania bramy
- 6. Konfiguracja modułów należących do systemu wykrywania włamań IPS:
 - Konfiguracja podstawowych parametrów
 - Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań;
 - Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego;
 - Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;
 - Testowanie działania ochrony IPS
- 7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL.
 - Przypisanie adresu IP do zarządzania.
 - Konfiguracja inspekcji protokołów HTTP, HTTPS; SMTP, FTP,
 - POP3
 - Definicja reguł filtrowania/blokowania
 - 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:
 - kontrola dostępu - zaporę ogniową klasy Stateful Inspection
 - ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiającą skanowanie wszystkich rodzajów plików, w tym zip, rar
 - ochrona przed atakami - Intrusion Prevention System
 - [IPS/IDS]
 - kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
 - kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
 - kontrola pasma oraz ruchu [QoS, Traffic shaping]
 - Kontrola aplikacji oraz rozpoznawanie ruchu P2P
 - Ochrona przed wyciekiem poufnej informacji (DLP)
 - Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL)
 - Inspekcja ruchu SSL
 - Ochrony przez atakami na stacje klienckie
 - Kontrola pasma
- 13. Konfiguracja szyfrowanych tuneli VPN (IPSec) pomiędzy lokalizacjami zdalnymi.
- 14. Konfiguracja logowania i raportowania.

Serwery:

1. Zamawiający wymaga instalacji i konfiguracji dostarczonych serwerów celem stworzenia bazy sprzętowej dla klastra niezawodnościowego i wydajnościowego stworzonego na bazie dostarczonych serwerów i oprogramowania.
2. Zamawiający wymaga przeniesienia aktualnych baz produkcyjnych systemów dziedzicznych urzędu na nowy serwer.

Serwer backupu + NAS:

1. Na serwerze należy zainstalować oprogramowanie do wirtualizacji – zarządzane z jednego centralnego miejsca, tego samego jak dla serwerów wirtualizacyjnych. System musi zostać podłączony do macierzy produkcyjnej, musie posiadać lokalne repozytoria danych na przestrzeni dyskowej, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na połowie zasobu dyskowego. Natomiast druga część zasobu musi zostać wykorzystana do wykonywania replikacji on-line maszyn wirtualnych na lokalną platformę wirtualizacyjną – na serwerze backupu. Takie podejście ma gwarantować zabezpieczenie kluczowych węzłów sieciowych (serwerów wirtualnych) na dwa sposoby tj. plik offline maszyny wirtualnej oraz kopia on-line replikowania asynchronicznie według harmonogramu.
2. Wykonywanie backupu musi być powiązane z procedurą sprawdzania poprawności jego wykonania oraz automatycznym raportowaniem do jednostki administracyjnej.
3. Oprogramowanie backupu musi obsługiwać również bibliotekę taśmową i system NAS, gdzie będzie można skorzystać z replikacji danych – przesłania backupu dyskowego np.: na zasób taśmowy.
4. Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej min. w pełnym zakresie danych i rejestrów systemów dziedzinowych.

Wymagania dotyczące backupu na centralny NAS:

1. Wykonawca zobowiązany jest do wykonania backupu wszystkich fizycznych hostów/maszyn wskazanych przez Zamawiającego na centralny serwer NAS.
2. Backup powinien być wykonywany w trybie **przyrostowym** (incremental), aby zminimalizować obciążenie sieci oraz czas wykonywania kopii zapasowych.
3. Backup musi być realizowany zgodnie z harmonogramem określonym przez Zamawiającego, uwzględniającym częstotliwość wykonywania pełnych backupów oraz backupów przyrostowych (np. pełny backup raz w tygodniu, backupy przyrostowe codziennie).
4. Wykonawca ma obowiązek zainstalować i odpowiednio skonfigurować agenta backupu na wszystkich komputerach, serwerach i urządzeniach wskazanych przez Zamawiającego jako objęte backupem. Instalacja agentów musi być wykonana w sposób niezakłócający bieżącej pracy użytkowników.
5. Wykonawca zapewni monitorowanie oraz raportowanie realizacji backupów, w tym informacje o sukcesie, niepowodzeniu lub problemach podczas wykonywania kopii zapasowych.
6. Backup musi obejmować pełne dane systemowe i użytkowe maszyn fizycznych, z uwzględnieniem plików, aplikacji oraz konfiguracji.
7. Wykonawca zobowiązany jest do regularnej weryfikacji poprawności wykonanych backupów poprzez testy odtwarzania danych (restore) z backupu na wybrane, wskazane przez Zamawiającego maszyny testowe.
8. Testy odtwarzania powinny być przeprowadzane co najmniej raz w miesiącu lub częściej, zgodnie z ustaleniami harmonogramu.
9. Wykonawca przedstawi Zamawiającemu raporty z przeprowadzonych testów odtwarzania, potwierdzające integralność i kompletność danych zbackupowanych oraz możliwość ich skutecznego przywrócenia.
10. W przypadku wykrycia nieprawidłowości lub błędów podczas testów odtwarzania, wykonawca niezwłocznie podejmie działania naprawcze oraz poinformuje Zamawiającego o podjętych krokach.

Mechanizm podłączenia

1. Konfiguracja i podłączenie serwera backupu do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) $n-(n-1)$ ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy.
2. Konfiguracja i podłączenie serwera backupu do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej

taką liczbą portów, by w przypadku niedostępności (awarii) $n-(n-1)$ ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN.

3. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q.

Serwer SMTP:

1. 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:
 - o Urzędzeń sieciowych
 - o Serwerów
 - o Macierzy dyskowej
 - o Systemu zarządzania kopiami zapasowymi
 - o Systemu wirtualizacji serwerów
 - o Aplikacji
2. 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.

Instalacja i konfiguracja serwera kopii zapasowych konfiguracji urządzeń sieciowych:

1. Zamawiający wymaga, aby wraz z uruchomieniem dostarczanych urządzeń sieciowych uruchomić serwer – repozytorium konfiguracji z dostarczanych urządzeń np.; przełączników sieciowych oraz innych urządzeń wspierających wykonywanie kopii zapasowych konfiguracji na zasób sieciowy.
2. Serwer musi być uruchomiony na dedykowanej maszynie (dopuszcza się maszynę wirtualną uruchomioną na infrastrukturze wirtualizującej Zamawiającego).
3. Serwer może działać w oparciu o dowolny system operacyjny, Zamawiający powinien uwzględnić cenę licencji w ofercie i dostarczyć ją we własnym zakresie.
4. Serwer może działać w oparciu o dowolne oprogramowanie bądź rozwiązanie autorskie Wykonawcy. Jeżeli takowa jest potrzebna, Zamawiający wymaga dostarczenia licencji. Cena licencji powinna być wliczona w cenę oferty.

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:
 - o 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.
 - o Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn.
 - o 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.
15. Konfiguracja powiadomień o krytycznych zdarzeniach (email).

Rekonfiguracja systemu zarządzania kopiami zapasowymi:

1. Instalacja i rekonfiguracja oprogramowania zarządzającego wykonywaniem kopii zapasowych na dostarczonym serwerze.
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:
 - o kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące;
 - o kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy;
 - o kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu;
 - o kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową;
 - o musi istnieć możliwość odtworzenia:
 - całej wirtualnej maszyny;
 - dysku wirtualnej maszyny;
 - 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:
 - Nazwę zadania backupu
 - Status zakończenia zadania backupu: Powodzenie/niepowodzenie
 - Długość trwania zadania backupu
 - Ilość zapisanych na taśmie danych
7. Zdefiniowanie powiadomień na wskazany adres email o zdarzeniach:
 - Błąd urządzenia
 - Uszkodzenie wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi
 - Brak miejsca w wewnętrznej bazie danych systemu zarządzania kopiami zapasowymi
 - Konieczność przeprowadzenia oczyszczania wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi
 - Zdarzenia dotyczące licencji
 - Zapelnienia 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:

- serwer backupu.
- na etapie wdrożenia należy ustalić czasy RPO (okresu czasu przez jaki dane mogą być utracone w wyniku awarii) i RTO (okresu czasu w ciągu którego system, który uległ awarii powinien zostać przewrócony) z Zamawiającym

12. Do serwera backupu należy podłączyć istniejąca macierz, system NAS i inne urządzenia zgodnie ze wskazaniami Zamawiającego.

13. System musi zostać podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na serwerze backupu.

14. Po przeprowadzanej aktualizacji wymagane jest przeszkolenie administratora z całości systemu.

System EDR-XDR:

1. System należy skonfigurować według zaproponowanych wytycznych przez Wykonawcę z uwzględnieniem wymagań Urzędu. Zakres konfiguracji musi zostać zaakceptowany i ustalony z administratorem.
2. Po przeprowadzanej aktualizacji wymagane jest przeszkolenie administratora z całości systemu.

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.

Asysta stanowiskowe:

1. Asysta stanowiskowa ma obejmować 16 godzin szkoleniowych w ujęciu 8 godzin na jeden dzień. Całość powinna się zamknąć w okresie 2 dni i ma dotyczyć autorskiego rozwiązania zrealizowanego w ramach podmiotowego wdrożenia.
2. Asysta musi być warunkiem dopuszczający do przekazania rozwiązania technicznego do wykorzystania produkcyjnego.
3. Asysta stanowiskowa musi zostać odebrana i zatwierdzona protokołem odbioru sygnowanym przez obie strony projektu tj. wykonawcę oraz użytkownika końcowego.

Termin wykonania prac Instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.

1. 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.
2. **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.**
3. W tym czasie przedstawiciel Wykonawcy:
 - zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji.
 - dokona prezentacji działania systemu dla pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności:
 - o zastosowanej technologii serwerów
 - o zastosowanej technologii pamięci masowej



- o wirtualizacji
 - o systemu backup
 - o zastosowanych rozwiązań aplikacyjnych
4. Wykonawca zapewni również wsparcie techniczne 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:

1. 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.
 - Wszelkie zmiany w stosunku do Dokumentacji systemu z podaniem ich powodów.
 - Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację).
 - Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały.
 - Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały.
2. Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów.

Opieka serwisowa:

Zamawiający wymaga świadczenia opieki serwisowej przez okres 12 miesięcy z czasem reakcji na zaistniałe problemy wynoszącym 4 godziny. Czas reakcji jest rozumiany jako podjęcie działań mających na celu rozwiązanie zaistniałych problemów technicznych.

5.3.5 UPS Stanowiskowy – 10 sztuk

Lp.	Minimalne parametry	
1.	Pojemność energetyczna	Min. 800VA / 480W
2.	Sprawność w trybie LINE [%] (pełne obciążenie)	Min. 96.2
3.	Czas transferu (tryb AC / linia do trybu bateryjnego) [ms]	Min. 2-6 ms
4.	Zakres napięcia wejściowego	Min. 162-290 VAC
5.	Zakres częstotliwości	Min. 45 Hz – 65 Hz (samoczynna adaptacja do 50/60 Hz)
6.	Nominalne napięcie wyjściowe	230 VAC
7.	Kształt fali wyjściowej	Pełna fala sinusoidalna
8.	Złącze wejściowe	CEE 7/7
9.	Typ wyjścia	Typ E
10.	Typ E (CEE 7/5)	Min. 2
11.	Ochrona linii danych	Min. Port RJ-11, port RJ-45 (100 mbit)
12.	Sygnalizacja pracy	Wyświetlacz LCD
13.	Zabezpieczenia	Automatyczna regulacja Napięcia (AVR)
14.	Obudowa	Wolnostojąca
15.	Wyposażenie	Kabel zasilający Instrukcja obsługi Oprogramowanie
16.	Gwarancja	co najmniej 36 miesięcy bezpłatnej gwarancji, której termin liczony będzie od dnia podpisania końcowego protokołu odbioru.

5.4. Usługa bezpiecznej poczty (część nr 4 zamówienia) - wymagania minimalne

1. Parametry Usługi

- Usługa musi być realizowana z polskiego centrum danych, posiadającego co najmniej certyfikację ISO/IEC 27001 oraz spełniającego wymagania RODO.
- Dostępność usługi musi wynosić $\geq 99,9\%$ miesięcznie (SLA).
- Ilość kont e-mail: bez limitu.
- Aliasy pocztowe: bez limitu.

2. Pojemność Usługi

- Dostarczona usługa pocztowa musi zapewniać łączną pojemność dyskową minimum 2 TB dla kont pocztowych Zamawiającego.
- Wykonawca musi zapewnić możliwość zwiększenia pojemności usługi w trakcie obowiązywania umowy, bez konieczności migracji systemu pocztowego, bez przestojów oraz bez konieczności zmiany domeny, kont lub konfiguracji po stronie Zamawiającego.
- Rozszerzenie pojemności musi być możliwe w krokach nie większych niż 500 GB.
- Zamawiający nie może ponosić kosztów prac technicznych związanych z rozszerzeniem pojemności — opłata może dotyczyć wyłącznie dodatkowej przestrzeni dyskowej.
- Wykonawca zobowiązany jest zapewnić monitorowanie wykorzystania przestrzeni dyskowej oraz możliwość bieżącego wglądu do poziomu jej użycia przez administratora Zamawiającego.

3. Bezpieczeństwo

Usługa musi zapewniać:

- SSL/TLS dla IMAP/SMTP/POP,
- szyfrowanie danych w spoczynku (at-rest),
- ochronę DoS/DDoS,
- Web Application Firewall (WAF),
- Intrusion Prevention System (IPS).

4. Systemy ochrony domenowej:

- SPF,
- DKIM,
- DMARC z możliwością trybu „reject”.

5. Ochrona treści wiadomości:

- Antyspam z możliwością treningu/własnych whitelist/blacklist,
- Antywirus z aktualizacją sygnatur w trybie ciągłym.

6. Dostęp użytkowników:

- Obsługa protokołu IMAP,
- Uwierzytelnianie dwuskładnikowe (2FA),
- Możliwość logowania przez SSO / LDAP / AD (opcjonalnie, jeśli potrzebne).

7. Funkcjonalność skrzynek

- Autoresponder,
- Przekierowania,

- Funkcja Catch-All,
- Panel administracyjny umożliwiający nadzór przez Zamawiającego.

8. Kopie i retencja

- Wykonawca zapewnia systemową kopię zapasową poczty, z retencją min. 14 dni lub zgodnie z polityką Zamawiającego.
- Możliwość przywracania pojedynczych wiadomości, skrzynek lub całych domen.

9. Migracja poczty

- Wykonawca zobowiązany jest do przeprowadzenia kompletnej migracji danych pocztowych z obecnie używanego systemu pocztowego Zamawiającego do oferowanej usługi.
- Migracja musi obejmować:
 - przeniesienie zawartości ok. 70 skrzynek pocztowych, w tym wiadomości, folderów i struktury katalogów,
 - przeniesienie książek adresowych (jeżeli istnieją po stronie źródłowej),
 - przeniesienie aliasów, przekierowań, grup dystrybucyjnych (jeżeli istnieją),
 - zachowanie integralności danych oraz znaczników odczyt/nieodczyt,
 - przeniesienie konfiguracji domenowej (SPF, DKIM, DMARC).
- Migracja musi zostać wykonana w sposób zapewniający minimalny czas niedostępności dla użytkowników, ustalony w porozumieniu z Zamawiającym, w oknie serwisowym.
- Przed wykonaniem migracji Wykonawca zobowiązany jest do zrealizowania:
 - analizy środowiska źródłowego,
 - przygotowania planu migracji,
 - przeprowadzenia migracji testowej na minimum 1 skrzynce i jej weryfikacji wraz z Administratorem Zamawiającego.
- Po zakończeniu migracji Wykonawca zobowiązany jest dostarczyć:
 - protokół migracji,
 - listę przeniesionych kont wraz z potwierdzeniem poprawności działania,
 - dokumentację zawierającą sposób logowania, parametry serwerów, zasady resetowania hasła oraz procedurę zgłaszania incydentów.
- Wszelkie koszty związane z migracją (w tym narzędzia migracyjne, roboczogodziny, transfer danych itp.) ponosi Wykonawca. Zamawiający nie ponosi dodatkowych opłat za migrację.

5.5. Oprogramowanie do zarządzania logami plus serwer (część nr 5 zamówienia)

1. Wymagania ogólne

Zamawiający wymaga dostarczenia i wdrożenia systemu centralnego logowania, raportowania i korelacji zdarzeń, umożliwiającego centralizację procesu gromadzenia logów z:

- urządzeń bezpieczeństwa (NGFW),
- serwerów fizycznych i wirtualnych,
- stacji roboczych (~70 szt.),
- urządzeń sieciowych.

System ma umożliwiać analizę zdarzeń w zakresie bezpieczeństwa, systemowym i sieciowym oraz wspierać administratorów w wykrywaniu incydentów.

2. Parametry wydajnościowe i retencja

1. System musi obsługiwać gromadzenie logów w wolumenie minimum 25 GB dziennie.

2. System musi umożliwiać przechowywanie logów przez okres minimum 90 dni w bazie operacyjnej (dostęp do szybkiej analizy).
3. System musi umożliwiać eksport i archiwizację logów na zewnętrzny serwer w celu ich długoterminowego przechowywania przez okres co najmniej 12 miesięcy.
4. Rozwiązanie musi zapewniać obsługę logów z systemów bezpieczeństwa NGFW dostarczanych w ramach postępowania.

3. Funkcjonalność logowania

1. Podgląd zdarzeń w czasie rzeczywistym.
2. Przeglądanie logów historycznych z możliwością filtrowania i sortowania.
3. Dostosowanie widoków logów (dodawanie, usuwanie i zmiana kolejności kolumn).
4. Predefiniowane i konfigurowalne raporty obrazujące:
 - najczęściej wykrywane ataki,
 - najbardziej aktywnych użytkowników i źródła ruchu,
 - najczęściej wykorzystywane aplikacje,
 - najczęściej odwiedzane strony www,
 - kraje docelowe połączeń,
 - używane polityki firewall,
 - informacje o połączeniach IPSec i SSL VPN,
 - najczęstsze zdarzenia systemowe.
5. Możliwość przesyłania logów do innych systemów (Syslog, CEF) z funkcją filtrowania.
6. Obsługa komunikacji z urządzeniami poprzez porty UDP/514 i TCP/514.
7. Eksport logów do zewnętrznego systemu (SFTP/SCP), z możliwością harmonogramowania.
8. Informacja o wykorzystaniu przestrzeni dyskowej na logi.
9. Wsparcie dla szyfrowanej transmisji logów (np. Syslog/TLS).

4. Raportowanie

1. Generowanie raportów w formatach: HTML, PDF, CSV, XLSX.
2. Raporty predefiniowane z możliwością modyfikacji parametrów.
3. Możliwość definiowania własnych raportów.
4. Raporty dostępne w języku polskim.
5. Raporty generowane cyklicznie lub na żądanie, z możliwością:
 - wysyłki na adres e-mail,
 - eksportu na zewnętrzny serwer (FTP, SCP, HTTPS).
6. Filtrowanie danych w raportach (np. po urządzeniu, adresacji IP).
7. Automatyczne usuwanie raportów po określonym czasie.

5. Korelacja zdarzeń

1. Korelowanie logów dla wskazanych urządzeń i kategorii.
2. Możliwość tworzenia własnych reguł korelacyjnych.
3. Powiadomienia o zdarzeniach poprzez e-mail, SNMP, API HTTP.
4. W powiadomieniach możliwość przesyłania szczegółowych informacji (np. nazwa zagrożenia).
5. Kategorie zdarzeń obsługiwane przez korelację (minimum):
 - Malware/AV,
 - aplikacje sieciowe,
 - e-mail,
 - IPS,
 - Web Filter,
 - ruch sieciowy,

- zdarzenia systemowe (utrata połączenia VPN, awarie sieci, zdarzenia klastra, zmiany w SD-WAN).
6. Możliwość automatycznego powiadamiania NGFW o zdarzeniach korelacji.

6. Zarządzanie

1. Zarządzanie lokalne przez HTTPS i SSH lub poprzez dedykowaną konsolę producenta.
 2. Uwierzytelnianie administratorów: lokalna baza, RADIUS, LDAP, TACACS+, PKI.
 3. Obsługa minimum 8 kont administratorów z różnymi poziomami uprawnień.
 4. Podział na wirtualne systemy logowania i raportowania (konteksty/domeny), z możliwością:
 - przypisania administratorów do kontekstów,
 - niezależnego przydziału zasobów,
 - definiowania czasu retencji dla poszczególnych kontekstów.
 5. Rejestracja i audyt działań administratorów.
7. Wsparcie i gwarancja
1. System objęty wsparciem producenta przez minimum 36 miesięcy.
 2. Wsparcie 24x7 z dostępem do aktualizacji oprogramowania i pomocy technicznej.

Wykonawca, który dostarczy oprogramowanie do zarządzania logami, zobowiązany jest do jego instalacji i pełnej konfiguracji na dostarczonym serwerze. Oprogramowanie ma być uruchomione i gotowe do pracy w środowisku Zamawiającego.”

Serwer – wymagania minimalne

Parametr	Charakterystyka (wymagania minimalne)
Ogólne	<ol style="list-style-type: none"> 1. Serwer klasy rack 2U, przystosowany do pracy w trybie ciągłym (24/7). 2. Serwer musi być nowy, pochodzić z oficjalnego kanału dystrybucyjnego producenta i posiadać min. 36 miesięcy gwarancji on-site NBD (Next Business Day) lub równoważnej. 3. Producent serwera musi zapewniać wsparcie techniczne oraz części zamienne przez okres min. 5 lat od zakończenia produkcji.
Procesor	<ol style="list-style-type: none"> 1. Minimum 1 × procesor 8-rdzeniowy / 16-wątkowy „Minimum 1 × procesor serwerowy 8-rdzeniowy / 16-wątkowy, o taktowaniu bazowym co najmniej 2,0 GHz, obsługą pamięci ECC DDR4/DDR5, zintegrowanym kontrolerem pamięci, cache L3 minimum 16 MB, obsługą technologii wirtualizacji sprzętowej, zoptymalizowany do pracy w środowiskach wielowątkowych i serwerach klasy średniej/wyższej, wydajnością równoważną nowoczesnym procesorom serwerowym 8–16 rdzeniowym.” 2. Możliwość rozbudowy o drugi procesor.
Pamięć RAM	<ol style="list-style-type: none"> 1. Minimum 64 GB DDR4 lub DDR5 ECC RDIMM. 2. Możliwość rozbudowy do min. 256 GB RAM. 3. Minimum 8 banków pamięci dostępnych w serwerze.
Pamięć masowa	<ol style="list-style-type: none"> 5. Minimum 6 zatok dyskowych 3.5” lub 2.5” hot-plug. 6. Konfiguracja dysków: <ul style="list-style-type: none"> • 2 × SSD min. 480 GB (RAID 1 – system), • 4 × HDD min. 2 TB 7.2k (RAID 10 – dane/logi). 7. Sprzętowy kontroler RAID z pamięcią cache i podtrzymaniem (bateria/supercap). 8. Obsługa RAID 0/1/5/6/10.
Sieć	<ol style="list-style-type: none"> 1. Minimum 2 × 1 GbE RJ-45. 2. Minimum 2 × 10 GbE (SFP+ lub RJ-45). 3. Obsługa VLAN, PXE.

Zasilanie	<ol style="list-style-type: none"> 1. Minimum 2 redundantne zasilacze hot-plug. 2. Zasilacze o sprawności min. 80 PLUS Platinum.
Zarządzanie	<ol style="list-style-type: none"> 3. 1. Wbudowany kontroler zarządzania z dedykowanym portem (np. iDRAC / iLO / XClarity lub równoważny). 4. Funkcje zdalnego zarządzania: <ul style="list-style-type: none"> • pełne KVM over IP, • monitoring sprzętu, • powiadomienia e-mail/SNMP, • zdalna konfiguracja BIOS/UEFI, • zdalna instalacja systemu operacyjnego.
Certyfikaty	Serwer musi posiadać deklaracja CE.
Warunki gwarancji	<p>36 miesięcy gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.</p> <p>W przypadku awarii dyski zostają u Użytkującego.</p> <p>Wybrany Wykonawca przed zawarciem umowy w sprawie zamówienia przedłoży Zamawiającemu:</p> <ol style="list-style-type: none"> 1) oświadczenie producenta sprzętu lub podmiotu realizującego serwis że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Użytkującego; 2) oświadczenia producenta sprzętu potwierdzając, że serwis urządzeń będzie realizowany bezpośrednio przez producenta lub we współpracy z autoryzowanym partnerem serwisowym producenta. <p>Możliwość rozszerzenia gwarancji przez producenta do 7 lat.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w</p>
Dokumentacja użytkownika	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>

Dodatkowe wymagania

1. Szyny montażowe rack w zestawie.
2. Możliwość instalacji systemu operacyjnego Linux (np. Debian, Ubuntu, CentOS, Rocky) lub Windows Server.
3. Serwer musi umożliwiać rozbudowę o dodatkowe dyski, pamięć i interfejsy sieciowe.
4. Do serwera musi być dostarczony serwerowy system operacyjny spełniający minimum następujące funkcjonalności:
 - licencje muszą mieć możliwość instalacji minimum 2 maszyn na serwerach wirtualnych
 - wbudowana zaporą internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych
 - zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe
 - wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play)
 - graficzny interfejs użytkownika
 - obsługa systemów wieloprocesorowych
 - obsługa platform sprzętowych x86, x64
 - możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu

Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. Potwierdzenie dołączyć do oferty

możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowego programowania:

 - usługi sieciowe DNS i DHCP,
 - usługi katalogowe pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe),
 - zdalna dystrybucja oprogramowania na stacje robocze,
 - praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
 - możliwość rozłożenia obciążenia serwerów,
 - serwis udostępniania stron WWW, serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management),
 - wsparcie dla protokołu IP w wersji 6 (IPv6)
 - Możliwość tworzenia serwerów wirtualnych, oprogramowanie wspierające tworzenie serwerów wirtualnych musi spełniać następujące wymagania funkcjonalne:
 - warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych
 - licencja musi umożliwiać zmianę wersji oprogramowania na niższą (downgrade)
 - rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze
 - możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-4 wirtualnych kart sieciowych.
 - możliwość przydzielania większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji
 - możliwość udostępniania maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy
 - konsola graficzna do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.
 - możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach
 - możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
 - możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi
 - możliwość integracji z usługami katalogowymi Microsoft Active Directory w tym jako kontroler domeny Microsoft Active Directory.
 - mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (np. wgrywania krytycznych poprawek) bez potrzeby wyłączania wirtualnych maszyn
 - obsługa przełączania ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z kilku dostępnych ścieżek.
 - możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi,
 - mechanizm wysokiej dostępności HA, w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione na nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym
 - 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 wirtualny przełącznik musi posiadać możliwość przyłączenia do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia w razie awarii karty sieciowej
 - wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN)
 - Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
 - Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
 - Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
 - Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
 - Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
 - Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET

5.6. Teleinformatyczny System Zarządzania Bezpieczeństwem Informacji (część nr 6 zamówienia)

DEFINICJE

Administrator systemu – osoba odpowiedzialna za merytoryczne funkcjonowanie wdrażanych rozwiązań z ramienia Zamawiającego.

Aplikacja mobilna - Aplikacja mobilna dostępna na urządzenia mobilne, dająca dostęp do części funkcjonalności Systemu.

Aktualizacja Systemu – uaktualnienia, wersje zmodyfikowane lub rozszerzone, dodatki.

API – Application Programming Interface, interfejs programowania aplikacji – jest to sposób rozumiany jako ściśle określony zestaw reguł i ich opisów, w jaki programy komunikują się między sobą. API definiuje się na poziomie kodu źródłowego dla takich składników oprogramowania jak np. aplikacje, biblioteki czy system operacyjny. Zadaniem API jest dostarczenie odpowiednich specyfikacji podprogramów, struktur danych, klas obiektów i wymaganych protokołów komunikacyjnych. Elementem API jest dokumentacja techniczna umożliwiająca jego wykorzystanie przez zewnętrzne systemy.

BIP – strona podmiotowa Biuletynu Informacji Publicznej.

CRWDE – Centralne Repozytorium Wzorów Dokumentów Elektronicznych.

CMS – system zarządzania treścią – oprogramowanie pozwalające na łatwe tworzenie i prowadzenie serwisu WWW, również przez redakcyjny personel nietechniczny.

Dane Osobowe – informacje dotyczące osoby w rozumieniu ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tj.. Dz.U. 2019 poz. 1781) oraz norm prawnych wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r., Nr 119, poz. 1).

Dokument Elektroniczny – Dokument Elektroniczny w rozumieniu przepisów Art. 3 ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj.. Dz.U. z 2024 poz. 307)

ePUAP – Elektroniczna Platforma Usług Administracji Publicznej <https://epuap.gov.pl>.

ESP – Elektroniczna Skrzynka Podawcza.

EZD – Elektroniczne Zarządzanie Dokumentacją, oprogramowanie umożliwiające wykonywanie czynności kancelaryjnych w podmiocie oraz postępowanie z dokumentacją począwszy od wpływu lub powstania dokumentacji wewnątrz podmiotu, poprzez dokumentowanie przebiegu załatwiania i rozstrzygania spraw, aż do momentu uznania dokumentacji za część dokumentacji w archiwum zakładowym i jej obsługi w ramach archiwum zakładowego zgodnie z wymaganiami Rozporządzenia 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. 2011 nr 14 poz. 67).

Formularz Elektroniczny – Graficzny interfejs użytkownika wystawiany przez oprogramowanie służący do przygotowania wygenerowania dokumentu elektronicznego zgodnego z odpowiadającym mu wzorem dokumentu elektronicznego w rozumieniu przepisów rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 roku w sprawie sporządzania pism w postaci dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz.U. z 2018, poz. 180, tj..).

Konto Firmowe (KF) – Konto podmiotu niebędącego osobą fizyczną - sp. z o.o., S.A., sp. komandytowa, fundacja, stowarzyszenie oraz inne.

Krajowy Węzeł Tożsamości (KWT) – rozwiązanie umożliwiające uwierzytelnianie użytkownika systemu teleinformatycznego, korzystającego z usługi online, z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła bezpośrednio albo za pośrednictwem węzła transgranicznego.

Instrukcja obsługi – dokument zawierający zasady działania i obsługi Systemu.

Kopia bezpieczeństwa systemu (BACKUP) – dane i pliki, które mają służyć do odtworzenia oryginalnych danych w przypadku ich utraty lub uszkodzenia.

Korzystanie – uzyskiwanie dostępu i używanie funkcjonalności Systemu.

Licencja – uprawnienie udzielane przez Wykonawcę Zamawiającemu uprawniające do Korzystania z

Systemu.

Naprawa – oznacza przywrócenie funkcjonowania Systemu poprzez usunięcie Błędu (błędu krytycznego, błędu, usterki) i doprowadzenie Systemu do działania zgodnego ze sposobem funkcjonowania opisanym w instrukcji obsługi Systemu.

Obejście – oznacza przywrócenie funkcjonowania Systemu poprzez zminimalizowanie uciążliwości Błędu (błędu krytycznego, błędu, usterki). Obejście nie stanowi naprawy, jednak pozwala korzystać nieprzerwanie z wszystkich funkcjonalności Systemu e-Urząd.

Portal – System dostępny za pośrednictwem przeglądarki internetowej.

Profil Zaufany (PZ) – zestaw informacji identyfikujących i opisujących podmiot lub osobę będącą użytkownikiem konta na ePUAP, który został w wiarygodny sposób potwierdzony przez organ podmiotu określonego w art. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj.. Dz.U. 2024 poz. 307).

Podpis Zaufany – podpis elektroniczny, którego autentyczność i integralność są zapewniane przy użyciu pieczęci elektronicznej ministra właściwego do spraw informatyzacji. Podpis Zaufany zawiera dane identyfikujące osobę (imię, nazwisko oraz numer PESEL), ustalone na podstawie środka identyfikacji elektronicznej wydanego w systemie, o którym mowa w art. 20aa pkt 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, identyfikator środka identyfikacji elektronicznej, przy użyciu którego został złożony oraz czas jego złożenia.

Protokół Odbioru – dokument potwierdzający wykonanie i zakończenie wdrożenia przedmiotu Umowy.

PUSH – powiadomienie wyświetlane na urządzeniu mobilnym.

Specyfikacja techniczno-funkcjonalna – dokument ustalający wymagania techniczne oraz funkcjonalne, które powinien spełniać System.

System – pojęcie obejmujące Elektroniczne Biuro Obsługi Interesanta, Systemy Dziedziny oraz BIP.

System e-Urząd – rozwiązanie informatyczno-funkcjonalne dostępne za pośrednictwem przeglądarki internetowej lub aplikacji mobilnej, za pomocą którego Użytkownik otrzymuje między innymi dostęp do swoich danych podatkowych i księgowych zgromadzonych w systemach informatycznych danego urzędu, możliwość wysłania dokumentów elektronicznych skierowanych do urzędu, opłacenia zobowiązania, umówienia wizyty w urzędzie oraz za pomocą którego ma możliwość otrzymania powiadomień o najważniejszych wydarzeniach lokalnych.

System Dziedziny (SD) – zintegrowany system informatyczny dedykowany do obsługi działalności Urzędu do realizacji zadań związanych z prowadzeniem rejestru mieszkańców, prowadzenia rejestru wyborców, pobierania danych z SRP, naliczania podatków rolnego, leśnego i od nieruchomości, naliczania podatku od środków transportowych, windykacji wszystkich naliczonych podatków i opłat, gospodarowania odpadami komunalnymi, fakturowania, rejestracji wpłat gotówkowych i bezgotówkowych, prowadzenia rejestru umów, zaangażowania i zobowiązań, prowadzenia kadr i płac oraz udostępniania niezbędnych danych pracownikom a także centralnego nadawania uprawnień oraz kontroli poprawności oraz wymiany danych pomiędzy poszczególnymi modułami, z którego m. in. są wizualizowane dane Użytkowników.

System Transakcyjny – Usługa dostępna w Internecie umożliwiająca wykonanie płatności.

UKF – Upoważnienie do Konta Firmowego.

UPD – Urzędowe Poświadczenie Dostarczenia.

UPO – Urzędowe Poświadczenie Odbioru.

UPP – Urzędowe Poświadczenie Przedłożenia.

Użytkownik – osoba fizyczna lub osoba prawna, którym Urząd udostępnia System celem Korzystania w zakresie określonym przez Wykonawcę i Użytkownika końcowego Systemu; Użytkownik końcowy Systemu nie posiada sublicencji do Systemu i nie jest uprawniony do dalszego udostępniania Systemu.

VPN- Virtual Private Network, wirtualna sieć prywatna – tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy stronami za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów.

Wdrożenie – świadczenia Wykonawcy mające na celu wykonanie Systemu.

Wsparcie – gwarantowana przez Wykonawcę i udzielana Zamawiającemu pomoc w eksploatacji (w tym prawo korzystania przez każdego z pracowników Zamawiającego z zdalnej pomocy helpdesk/telefon), prawo do otrzymywania Aktualizacji oraz usuwanie ewentualnych usterek Systemu na warunkach określonych w rozdziale pt. „Ogólne warunki gwarancji”, wsparcie merytoryczne opisane w rozdziale „Audyt postępowania z dokumentacją, szkolenie z przepisów prawa, konsultacje merytoryczne”.

Wzór dokumentu elektronicznego – Wzór pisma w formie Dokumentu Elektronicznego w rozumieniu Art.19 b) ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2020 r., poz. 346 tj..) oraz §18 rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 roku w sprawie sporządzania pism w postaci dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz. U. z 2019r., poz. 700).

XML – Format XML jest to obecnie powszechnie uznany standard publiczny, umożliwiający wymianę danych między różnymi systemami.

KSeF - Krajowy System e-Faktur.

PEF - Platforma Elektronicznego Fakturowania.

SZBI – Teleinformatyczny System Zarządzania Bezpieczeństwem Informacji modułu Kontroli Zarządczej w ramach posiadanego systemu elektroniczne zarządzanie dokumentacją.

KZ - modułu Kontroli Zarządczej w ramach posiadanego systemu elektroniczne zarządzanie dokumentacją.

PODSTAWY PRAWNE

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
2. Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 z późn. zm.).
3. Rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2011 nr 159, poz. 948 z późn. zm.).
4. Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz. U. z 2022 r., poz. 2509).
5. Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (tj.. Dz. U 2024 poz. 307)
6. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj.. Dz. U. z 2017 r., poz. 2247 z późn. zm.)
7. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2021 poz. 1797 z późn. zm.) (tj.. Dz. U. 2024 poz. 422)
8. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tj.. Dz. U. z 2020 r. poz. 344 z późn. zm.)
9. Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (tj.. Dz. U. 2023 r. poz. 285 z późn. zm.).
10. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz. U. 2006 r. Nr 206 poz. 1517 z późn. zm.).
11. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (tj.. Dz.U. 2024 poz. 422)
12. Ustawa z dnia 14 lipca 1983 roku o narodowym zasobie archiwalnym i archiwach (tj.. Dz. U. 2020 poz. 164).
13. 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. 2011 nr 14 poz. 67 oraz Dz. U. 2011 nr 27 poz. 140).
14. Ustawa z dnia 14 czerwca Kodeks Postępowania Administracyjnego (tj.. Dz.U. 2024 poz. 572)
15. Ustawa z dnia 29 sierpnia 1997 r. ordynacja (tj.. Dz.U. 2023 poz. 2383 z późn. zm.)
16. Ustawa z dnia 30 października 2002 r. o podatku leśnym (tj.. Dz. U. z 2019 poz. 888)
17. Ustawa z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (tj.. Dz. U. z 2023 poz. 70)
18. Ustawa z dnia 15 listopada 1984 . o podatku rolnym (tj.. Dz. U. z 2020 poz. 333 z późn. zm.)
19. Ustawa z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (tj.. Dz.U. 2024 poz. 399)
20. Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (tj.. Dz.U. 2024 poz. 609)
21. Ustawa z 27 kwietnia 2001 r. Prawo ochrony środowiska (tj.. Dz.U. 2024 poz. 54).

22. Ustawa z 27 marca 2003 r. o planowaniu i zagospodarowaniu (tj.. Dz.U. 2023 poz. 977 z późn. zm.).
23. Ustawa z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko (tj.. Dz.U. 2023 poz. 1094 z późn. zm.).
24. Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i wolontariacie (tj.. Dz.U. 2023 poz. 571).
25. Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług (tj.. Dz.U. 2024 poz. 361).
26. Rozporządzenie Ministra Finansów z dnia 18 czerwca 2019 r. w sprawie sposobu przysyłania informacji o nieruchomościach i obiektach budowlanych oraz deklaracji na podatek od nieruchomości za pomocą środków komunikacji elektronicznej (Dz.U. 2019 poz. 1185 z późn. zm.).
27. Rozporządzenie Ministra Finansów z dnia 30 maja 2019 r. w sprawie wzorów informacji o nieruchomościach i obiektach budowlanych oraz deklaracji na podatek od nieruchomości (Dz.U. 2019 poz. 1104 z późn. zm.).
28. Rozporządzenie Ministra Finansów z dnia 6 czerwca 2019 r. w sprawie sposobu przysyłania informacji o gruntach oraz deklaracji na podatek rolny za pomocą środków komunikacji elektronicznej (Dz.U. 2019 poz. 1153 z późn. zm.).
29. Rozporządzenie Ministra Finansów z dnia 30 maja 2019 r. w sprawie wzorów informacji o gruntach i deklaracji na podatek rolny (Dz.U. 2019 poz. 1105 z późn. zm.).
30. Rozporządzenie Ministra Finansów z dnia 3 czerwca 2019 r. w sprawie wzorów informacji o lasach i deklaracji na podatek leśny (Dz.U. 2019 poz. 1126 z późn. zm.).
31. Rozporządzenie Ministra Finansów z dnia 6 czerwca 2019 r. w sprawie sposobu przysyłania informacji o lasach oraz deklaracji na podatek leśny za pomocą środków komunikacji elektronicznej (Dz.U. 2019 poz. 1154 z późn. zm.).
32. Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (tj.. Dz.U. 2023 poz. 1440).
33. Ustawa z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (tj. Dz.U. z 2022 poz. 2240 z późn. zm.).
34. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (tj.. Dz.U. z 2022 r. poz. 902).
35. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz.U. 2007 nr 10 poz. 68).
36. Ustawa z dnia 24 września 2010 r. o ewidencji ludności (tj.. Dz.U. 2024 poz. 736).
37. Ustawa z dnia 5 stycznia 2011 r. – Kodeks wyborczy (tj.. Dz.U. 2023 poz. 2408).

INFORMACJE OGÓLNE

Przedmiotem zamówienia jest wdrożenie kompleksowego Teleinformatycznego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z normą ISO/IEC 27001 lub równoważną poprzez rozbudowę, modernizację i aktualizację modułu Kontrola Zarządcza, który jest częścią posiadanego przez Zamawiającego systemu EZD e-Instytucja.pl.

1. Cel Zamówienia:

Celem niniejszego zamówienia jest wdrożenie kompleksowego Teleinformatycznego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z normą ISO/IEC 27001 lub równoważną. System ma zapewniać najwyższy poziom ochrony danych, minimalizować ryzyko oraz gwarantować zgodność z przepisami prawnymi dotyczącymi ochrony danych osobowych i bezpieczeństwa informacji. Wdrożenie Teleinformatycznego Systemu Zarządzania Bezpieczeństwem Informacji będzie rozbudową modułu Kontroli Zarządczej w ramach posiadanego przez Zamawiającego systemu e-Kancelaria <http://gsko.unislaw.pl/>.

2. Zakres Przedmiotu Zamówienia:

2.1 Analiza Stanu Obecnego:

System powinien umożliwiać przeprowadzenie szczegółowej analizy aktualnego stanu bezpieczeństwa informacji w organizacji, obejmującej ocenę ryzyk, audyt bezpieczeństwa oraz identyfikację luk i słabych punktów.

2.2 Projektowanie SZBI:

System powinien umożliwiać opracowanie i przedstawienie projektu SZBI, w tym polityk, procedur oraz planów awaryjnych zgodnie z normą ISO/IEC 27001 lub równoważną. Moduł powinien wspierać definiowanie celów, strategii i wytycznych dotyczących bezpieczeństwa informacji.

2.3 Wdrożenie SZBI:

System powinien umożliwiać implementację zaprojektowanego systemu, obejmującą instalację niezbędnych narzędzi informatycznych, szkolenie personelu oraz uruchomienie procedur zarządzania bezpieczeństwem informacji. System powinien wspierać konfigurację i dostosowanie narzędzi do specyficznych potrzeb organizacji.

2.4 Monitorowanie i Audyt:

System powinien umożliwiać ustanowienie mechanizmów monitorowania zgodności systemu z przyjętymi politykami oraz przeprowadzanie regularnych audytów wewnętrznych i zewnętrznych. System powinien wspierać powiadomienia o niezgodnościach i generowanie raportów z audytów.

2.5 Ciągłe Doskonalenie:

System powinien umożliwiać zapewnienie mechanizmów ciągłego doskonalenia systemu, w tym analiza incydentów, regularne aktualizacje procedur oraz prowadzenie szkoleń doskonalących dla pracowników. System powinien wspierać raportowanie o postępach i wprowadzanych zmianach.

3. Wymagania Organizacyjne:

3.1 Polityki Bezpieczeństwa:

System powinien umożliwiać opracowanie i wdrożenie kompleksowych polityk bezpieczeństwa informacji, w tym polityki ochrony danych osobowych, polityki klasyfikacji informacji oraz polityki zarządzania ryzykiem. System powinien wspierać cykliczną rewizję i aktualizację polityk.

4. Szkolenia i Świadomość:

4.1 System powinien umożliwiać przeprowadzenie szkoleń dla pracowników na wszystkich poziomach organizacji w zakresie bezpieczeństwa informacji oraz podnoszenie świadomości zagrożeń związanych z cyberbezpieczeństwem. System powinien wspierać zarządzanie harmonogramem szkoleń i śledzenie ich realizacji.

4.2 Zarządzanie Incydentami:

System powinien umożliwiać opracowanie procedur zarządzania incydentami bezpieczeństwa, w tym procedur reakcji na incydenty, analizę przyczyn źródłowych oraz planów naprawczych. System powinien wspierać rejestrację i śledzenie incydentów oraz generowanie raportów z podjętych działań.

4.3 Zgodność z Przepisami:

System powinien umożliwiać zapewnienie zgodności z obowiązującymi przepisami prawnymi i regulacjami dotyczącymi ochrony danych osobowych oraz bezpieczeństwa informacji, w tym RODO oraz ustawą o ochronie danych osobowych. System powinien wspierać automatyczne aktualizacje zgodnie ze zmianami prawnymi.

5. Wymagania Dotyczące Dokumentacji:

5.1 Dokumentacja Polityk i Procedur:

System powinien umożliwiać opracowanie i dostarczenie dokumentacji polityk, procedur oraz instrukcji operacyjnych związanych z zarządzaniem bezpieczeństwem informacji. System powinien wspierać zarządzanie wersjami dokumentów.

5.2 Raporty z Audytów:

System powinien umożliwiać przedstawianie regularnych raportów z przeprowadzonych audytów bezpieczeństwa oraz ocen zgodności systemu z normą ISO/IEC 27001 lub równoważną. System powinien wspierać generowanie i archiwizację raportów.

Realizacja powyższych wytycznych powinna odbywać się poprzez następujące moduły: MODUŁ ZARZĄDZANIA RYZYKIEM

1. Moduł zarządzania ryzykiem pomaga kontrolować cały proces związany z zarządzaniem ryzykiem, już od chwili identyfikacji ryzyka poprzez jego obsługę w rejestrze, aż do momentu wygenerowania mapy ryzyka.
2. Moduł zarządzania ryzykiem w szczególności obejmuje:
 - Definiowanie rejestru ryzyk przez jednostkę;
 - Modyfikowanie rejestru ryzyk poprzez dopisywanie nowych pozycji ukrywanie widoczności nieaktualnych;
 - Możliwość zgłaszania ryzyka przez każdego pracownika;
 - Możliwość dodawania zgłoszonego ryzyka do rejestru;
3. Dzięki wykorzystaniu modułu zarządzania ryzykiem jednostka będzie mogła:
 - Zarządzać ryzykiem w sposób systemowy i tym samym realizować ustawowy obowiązek;
 - Przekazać kierownictwu jednostki rzetelną informację o ryzyku i na jej podstawie sformułować wstępne decyzje o charakterze zarządczym;
 - Wygenerować mapę ryzyka, która jest graficzną prezentacją

ryzyka w momencie pierwotnym i po zastosowaniu mechanizmów redukujących ryzyko; Moduł zarządzania ryzykiem umożliwia sprawozdawczość dającą pełną kontrolę nad ryzykiem mogącym wystąpić w jednostce.

MODUŁ LIST PYTAŃ KONTROLNYCH

1. System umożliwia prowadzenie bieżącego testu zgodności z przepisami prawa i innymi regulacjami.
2. Użytkownik ma możliwość tworzenia własnych list pytań kontrolnych lub skorzystania z gotowych list przygotowanych przez ekspertów z danej dziedziny (tj. zamówień publicznych, cyberbezpieczeństwa, norm ISO), w tym także przy użyciu wagowania istotności odpowiedzi.
3. Listy pytań kontrolnych są powiązane z jednostką redakcyjną podstawy prawnej lub orzeczenia, do której odwołują się poszczególne pytania w listach.
4. Listy pytań kontrolnych mogą być na bieżąco aktualizowane przez producenta - dopasowywane do zmieniających się przepisów; użytkownicy otrzymują informacje w systemie o zaktualizowanej liście pytań.
5. System w przejrzysty sposób prezentuje wyniki z wykonanych badań zgodności, wyszczególniając wszystkie zidentyfikowane niezgodności.

MODUŁ ZADAŃ

1. Proces przeprowadzania badania zgodności w szczególności obejmuje:
 - Możliwość zdalnego wydawania przez wskazane w organizacji osoby poleceń wykonania analizy, badania, raportu, sprawozdania;
 - Możliwość kierowania dowolnych zadań do pracowników na każdym poziomie organizacji, w tym zadań cyklicznych;
 - Możliwość kierowania zadań w formie checklist do pracowników na każdym poziomie odpowiedzialności, aby określić stopień zgodności w wykonywanych zadaniach;
 - możliwość dołączania do zadań delegowanych plików z wewnętrznymi procedurami placówki;
 - Możliwość automatycznego powiadamiania określonych w poleceniu użytkowników o konieczności przygotowania sprawozdania, wypełnienia listy kontrolnej, nowych wiadomościach i ogłoszeniach;
 - Możliwość generowania sprawozdań z wykonywanych zadań, w których parametrem będzie poziom zgodności z konkretną regulacją;
2. Dzięki zastosowanym mechanizmom zadaniowania i listom pytań kontrolnych Jednostka będzie mogła:
 - Sprawdzić zgodność działania jednostki/komórki organizacyjnej z obowiązującym prawem lub regulacjami określonymi w części prezentującej zawartość kontentu merytorycznego;
 - Weryfikować pojawiające się niezgodności w procesach i stopień zgodności w wykonywanych zadaniach;
 - Reagować na ryzyko niezgodności poprzez delegowanie pracownikom, za pomocą systemu, konkretnych zadań redukujących niezgodność i śledzących skuteczność i czas ich wykonania;
 - Na bieżąco monitorować działania pracowników w zakresie zadań przydzielonych w systemie;
3. W ramach modułu zadań system umożliwia raportowanie z realizowanych zadań i projektów we wszystkich obszarach i obowiązkach, wynikających z funkcjonowania jednostki samorządu terytorialnego. System prezentuje dwa rodzaje raportów - raporty statystyczne i przeglądowe. Moduł Raporty pozwala na:
 - Ustalenie, co zostało wykonane w systemie np. w ramach danego zadania;
 - Monitorowanie co i w jakich zakresach, zostało wykonane, jak duże są ewentualne zaległości oraz którzy pracownicy wykazują się największą aktywnością;
 - Możliwość automatycznego tworzenia raportów w czasie rzeczywistym.

MODUŁ ANKIET

Modułem wspierającym bieżące utrzymywanie zgodności jest moduł ankiet, który umożliwia:

- Tworzenie ankiet zawierających pytania jednokrotnego, wielokrotnego wyboru, z listy rozwijanej oraz

- pytania otwarte;
- Po utworzeniu ankiety wysłanie informacji o dostępności ankiety w systemie poprzez wewnętrzny komunikator;
 - Wykorzystanie kreatora ankiet i analizatora ankiet ułatwiającego przygotowanie narzędzi do analizy i oceny;
Korzystanie z kalendarza pozwalającego na bezkolizyjne ustalenie terminów wykonania określonych działań;
 - Włączenie opcji anonimowej ankiety podczas jej opracowania, co powinno być sygnalizowane w systemie przy jej wypełnianiu;
 - Określanie terminu dostępności ankiety i jej automatyczne zamykanie po wygaśnięciu terminu wypełnienia;
 - Dostęp do archiwum ankiet, raportów, sprawozdań;
 - Segregowanie ankiet, sprawozdań, raportów według dowolnych kategorii;
 - Włączanie filtrów podczas opracowania statystyk ankiet, np. poszczególnych pytań z wybranej ankiety.

MODUŁ ZARZĄDZANIA NIEZGODNOŚCIAMI (ZDARZENIAMI ORGANIZACYJNYMI)

1. Moduł zarządzania zdarzeniami organizacyjnymi umożliwia zgłaszanie zdarzeń organizacyjnych (administracyjnych, bhp, IT itp.) przez każdego pracownika placówki, ich rejestrowanie oraz monitorowanie.
2. Moduł zarządzania zdarzeniami w szczególności obejmuje:
 - Definiowanie indywidualnych słowników zdarzeń i incydentów;
 - Przypisywanie właścicieli kategorii i podkategorii zdarzeń i incydentów
 - Możliwość zgłaszania zdarzeń przez użytkowników zalogowanych oraz anonimowo;
 - Możliwość dodawania zgłoszonego naruszenia do rejestru;
 - Komentowanie zdarzeń w rejestrze;
 - Wysyłanie zadania z poziomu zgłoszonego naruszenia przez właściciela danej kategorii zgłoszenia;
 - Śledzenie historii zmian zdarzeń organizacyjnych oraz dokonanych w ramach zgłoszeń działań, zgłoszonych i w rejestrze;
3. Wykorzystanie modułu zarządzania zdarzeniami będzie wsparciem dla kierownictwa w zakresie:
 - Uzyskiwania rzetelnej informacji o obszarach zgłaszanych naruszeń i zdarzeń organizacyjnych;
 - Generowania raportów, analiz i statystyk oraz formułowania na ich podstawie decyzji o charakterze zarządczym;
 - Wsparcia funkcji osoby odpowiedzialnej za monitorowanie wszystkich zdarzeń organizacyjnych i ewentualnego określania ryzyk dla placówki.

MODUŁ KOMUNIKATÓW

1. System zawiera elektroniczną tablicę ogłoszeń - ogłoszenia są automatycznie dezaktualizowane (o dacie decyduje osoba o przyznanach odpowiednich uprawnieniach). Każdy użytkownik systemu jest informowany o nowych ogłoszeniach;
2. System umożliwia wysłanie wiadomości do konkretnego pracownika, grupy pracowników czy też zespołów zadaniowych z potwierdzeniem odbioru takiej wiadomości;

Wymagania niefunkcjonalne:

1. EZD musi posiadać architekturę trójwarstwową:
 - 1) warstwa prezentacji, obejmująca interfejsy użytkownika klienta WWW,
 - 2) warstwa aplikacji, obejmującą serwer Systemu,
 - 3) warstwa danych, zawierającą serwer bazy danych.
2. Interfejs użytkownika systemu musi być w całości polskojęzyczny. W języku polskim muszą być również wyświetlane wszystkie komunikaty przekazywane przez System, włącznie z komunikatami o błędach.
3. EZD musi informować użytkownika w momencie zaciągania plików, że plik przekroczył dopuszczalny rozmiar.
4. EZD musi przechowywać wszystkie dane w bazie danych zgodnej ze standardem SQL oraz zapewniającej transakcyjność operacji. Dopuszcza się przechowywanie poza bazą danych plików, w postaci repozytorium dyskowego – ich integralność z systemem musi być

- zapewniona przez metadane opisujące poszczególne pliki. Metadane muszą być przechowywane w bazie danych.
5. EZD musi działać w środowiskach systemowych bazujących na technologii Microsoft Windows oraz w środowiskach opartych na systemie Linux.
 6. EZD musi umożliwiać dostęp do systemu przez użytkownika końcowego z poziomu przeglądarki internetowej, co najmniej Firefox, Google Chrome, MS Edge, Safari w najnowszych wersjach.
 7. EZD musi cechować się interfejsem użytkownika opartym na nowoczesnych rozwiązaniach: wykorzystywać menu, listy, formularze, przyciski, referencje (linki), itp.
 8. Wymaga się, aby interfejs użytkownika EZD stosował oznaczanie pól wymaganych na formularzu ekranowym w sposób wyróżniający te pola, a w przypadku ich błędnego wypełnienia jednoznacznie wskazywał na pola błędnie wypełnione oraz informował o przyczynie błędu.
 9. EZD musi cechować dużą elastyczność, rozumiana jako możliwość dostosowania systemu do zmieniających się wymagań funkcjonalnych wynikających ze zmieniającego się stanu prawnego i zmieniających się warunków praktycznych i przepisów prawnych.
 10. EZD musi zabezpieczać dane przed przypadkowym nadpisaniem w przypadku równoczesnego korzystania z tych danych przez wielu użytkowników.
 11. EZD musi posiadać widok indywidualny, prezentujący tylko te składniki systemu, do których uprawniony jest dany użytkownik.
 12. System musi umożliwiać integrację z Active Directory w trybie SSO (Single Sign On). Logowanie do systemu odbywa się automatycznie za pomocą danych z konta AD. Użytkownik po zalogowaniu do AD nie musi logować się drugi raz do systemu EZD (Jednokrotne logowanie).
 13. EZD musi zapewniać możliwość:
 - 1) narzucenia minimalnej długości hasła oraz obowiązku wykorzystania różnych rodzajów znaków w hasle (np. liter, cyfr i znaków specjalnych);
 - 2) ustalenia czasu obowiązywania hasła;
 - 3) automatycznego odrzucania prób ustalenia przez użytkownika trywialnego hasła (np. imienia lub nazwiska użytkownika).
 14. EZD musi być wyposażony w filtry umożliwiające wyszukanie odpowiednich dokumentów (i innych obiektów) oraz interesantów według predefiniowanych atrybutów (kryteriów wyszukiwania).
 15. System EZD musi pozwalać na odbieranie i wysyłanie dowolnych dokumentów z i do zewnętrznych systemów za pośrednictwem skrytki ePUAP.
 16. Środowisko EZD powinno umożliwiać udostępnianie usług Webservice.
 17. EZD musi zapewniać możliwość integracji z systemem ePUAP, automatyczną rejestrację i wysyłanie dokumentów, weryfikację podpisów i paczek ePUAP oraz wizualizacji dokumentów pobranych z ePUAP oraz UPO, UPD i UPP.
 18. EZD musi zapewnić podpisywanie pojedynczych i wielu pism i załączników podpisem elektronicznym kwalifikowanym z poziomu aplikacji, weryfikację podpisu.
 19. EZD musi zapewniać możliwość podpisywania pism za pomocą Podpisu Zaufanego (PZ).
 20. EZD musi zapewniać możliwość podpisywania pism i załączników za pomocą kwalifikowanej pieczęci elektronicznej.
 21. EZD musi zapewniać współpracę z urządzeniami wspomagającymi rejestrację dokumentów, a w szczególności: skanerami; czytnikami kodów kreskowych; drukarkami etykiet adresowych i kodów kreskowych, tabletem do podpisu
 22. EZD musi umożliwiać definiowanie uprawnień każdego ze stanowisk w zakresie: dostępu do odpowiednich modułów, w tym dokumentów i spraw oraz uprawnień do aktualizacji i przeglądania ich zawartości.
 23. EZD musi umożliwiać wymuszanie zmiany hasła po upływie czasu, określonego przez Administratora.
 24. EZD musi cechować się rozbudowanym modułem bezpieczeństwa zarządzającym dostępem użytkowników do funkcji systemu. Musi zapewnić dostęp do wybranych funkcji administracyjnych dla uprawnionych pracowników.
 25. Panel administracyjny EZD musi umożliwiać uprawnionym Użytkownikom zdefiniowanie i prowadzenie rejestrów wszystkich typów dokumentów z zakresu działalności Zamawiającego zgodnie z wymaganiami prawnymi dotyczącymi tych dokumentów (np. ewidencja decyzji, zaświadczeń itd.).

26. EZD musi zapewnić: odwzorowanie struktury organizacyjnej urzędu (komórek, pracowników, stanowisk) z możliwością modyfikacji, przydzielanie zdefiniowanym grupom użytkowników uprawnień do wykonywania określonych funkcji.
27. Panel administracyjny EZD musi umożliwiać przeglądanie historii logowania użytkowników.
28. EZD musi umożliwiać zarządzanie słownikiem Jednolitego Rzeczowego Wykazu Akt i nadawanie uprawnień dla poszczególnych klas.
29. Panel administracyjny EZD musi umożliwiać zarządzanie kontami, w minimalnym zakresie:
 - 1) edycji uprawnień,
 - 2) musi umożliwiać zarządzanie i określanie przez Administratora wymaganej złożoności hasła,
 - 3) określanie co najmniej: maksymalnej i minimalnej długości hasła, czasu ważności hasła,
 - 4) ustawienia praw dostępu dla stanowiska.
30. EZD musi zapewniać funkcjonalność zarządzania dostępem do aplikacji:
 - 1) Administrator systemu musi mieć możliwość tworzenia, modyfikacji oraz dezaktywacji kont użytkowników,
 - 2) Administrator systemu, użytkownik może nadawać uprawnienia innym użytkownikom,
 - 3) Administrator systemu może przypisywać użytkowników do grup,
31. System musi pozwalać na wygenerowanie linka do zmiany hasła dla użytkownika.

Wymagania funkcjonalne

1. System musi umożliwiać pracę w trzech trybach:
 - 1) w trybie wspierającym obieg dokumentów papierowych,
 - 2) w trybie EZD,
 - 3) w trybie mieszanym.
2. EZD musi obsługiwać rejestrację przesyłek przychodzących, w formie papierowej i elektronicznej (przekazywanych za pośrednictwem Elektronicznej Skrzynki Podawczej na ePUAP, portalu e-usług lub innych skrzynek podawczych oraz poczty elektronicznej).
3. System EZD musi być zintegrowany z usługą e-Doręczeń elektronicznych umożliwiając:
 - 1) odbieranie, jak i wysyłanie dokumentów poprzez e-Doręczenia elektroniczne,
 - 2) obsługę wszystkich formatów dokumentów wymagane przez platformę e-Doręczeń
 - 3) Śledzenie statusów doręczeń (np. dostarczone, odebrane, odrzucone) i informowanie użytkowników o zmianach statusów za pomocą powiadomień systemowych,
4. System EZD musi obsługiwać procesy wysyłania i odbierania dokumentów metodą hybrydową (PUH), które obejmują formę tradycyjną (papierową) a w szczególności:
 - 1) Umożliwiać automatyczne przekształcanie dokumentów elektronicznych do formatu umożliwiającego prawidłowe wysłanie dokumentu,
 - 2) Umożliwiać śledzenie statusów doręczeń hybrydowych w sposób ciągły, z aktualizacją informacji o doręczeniach papierowych (np. potwierdzenia odbioru zwracane do systemu).
5. System EZD musi być zintegrowany z Platformą Elektronicznego Fakturowania (PEF) w celu odbierania, wysyłania i przetwarzania faktur elektronicznych oraz musi obsługiwać formaty dokumentów zgodne z europejskim standardem e-fakturowania.
6. System EZD musi być zintegrowany z Krajowym Systemem e-Faktur (KSeF) w celu wymiany faktur elektronicznych zgodnie z wymogami ustawowymi oraz wspierać procesy wysyłania, odbierania i archiwizacji e-faktur zgodnie z wymogami KSeF.
7. System EZD musi umożliwiać doręczenia korespondencji metodą gońcową wraz z wykorzystaniem do obsługi gońców aplikacji mobilnej a w szczególności:
 - 1) Umożliwiać tworzenie rejonów dostawczych i przypisywanie konkretnych gońców do obsługi poszczególnych rejonów,
 - 2) Pozwalać na przydzielanie zadań doręczeniowych do konkretnych gońców, z możliwością śledzenia realizacji tych zadań,
 - 3) Umożliwiać rejestrowanie potwierdzeń doręczeń za pomocą urządzeń mobilnych, w tym zbierania podpisów odbiorców na ekranach urządzeń mobilnych z funkcją zapisywania danych geolokalizacyjnych,
 - 4) Aplikacja mobilna musi umożliwiać gońcom zarządzanie zadaniami doręczeniowymi, rejestrowanie doręczeń oraz komunikację z centralnym systemem EZD,
 - 5) Umożliwiać gońcom synchronizację danych pomiędzy aplikacją mobilną a centralnym systemem EZD, w tym aktualizację statusów doręczeń i raportowanie postępów realizacji zadań,
 - 6) Umożliwiać generowanie raportów dotyczących działalności gońców, obejmujących m.in. liczbę doręczonych przesyłek oraz skuteczność doręczeń.
8. System EZD musi wspierać obsługę wysyłek z wykorzystaniem systemu E-nadawca Poczty

- Polskiej - wysyłka przesyłek krajowych i zagranicznych, obsługa EPO
9. Podczas procesu rejestracji przesyłek przychodzących w formie papierowej, EZD musi umożliwiać skanowanie z wykorzystaniem skanera zgodnego z TWAIN (z poziomu interfejsu aplikacji) poszczególnych dokumentów, wchodzących w skład przesyłki. Interfejs do skanowania musi posiadać co najmniej narzędzia do edycji obrazu ze skanera poprzez: obrót o dowolny kąt, zmianę kolejności stron, zapis do PNG i PDF, zmiany kontrastu.
 10. Podczas rejestracji przesyłek przychodzących w formie papierowej, EZD musi umożliwiać skanowanie wsadowe.
 11. System musi wspierać integrację z programami ABC Pro – Legislator oraz Anon
 12. EZD musi umożliwiać odebranie poczty elektronicznej za pomocą wbudowanego klienta pocztowego IMAP oraz SMTP i umożliwić rejestrację w rejestrze przesyłek wpływających lub bezpośrednio dołączenie wiadomości z załącznikami do akt sprawy.
 13. EZD musi umożliwiać opatrywanie przesyłek przychodzących metadanymi zgodnie z instrukcją kancelaryjną.
 14. System musi umożliwiać generowanie potwierdzenia przyjęcia przesyłki wpływającej przez punkt kancelaryjny, opatrzonego kodem kreskowym odpowiadającym kodowi kreskowemu przesyłki. Potwierdzenie przyjęcia wygenerowane przez EZD musi umożliwiać zamieszczenie co najmniej daty wpływu, oznaczenia graficznego jednostki, nazwy jednostki.
 15. EZD musi umożliwiać rejestrację zwrotów przesyłek oraz pocztowych potwierdzeń odbioru (zwrotek).
 16. System EZD musi wspierać funkcjonalność składania podpisu elektronicznego na urządzeniach mobilnych, takich jak tablety, podczas odbioru dokumentów w urzędzie.
 17. System EZD musi umożliwiać tworzenie tzw. kancelarii wydziałowych składających się z grup pracowników odpowiedzialnych za rejestrację dokumentów przychodzących w obrębie danego wydziału lub komórki organizacyjnej.
 18. Administrator EZD musi mieć możliwość elastycznego definiowania struktur kancelarii wydziałowych, dostosowując je do specyficznych potrzeb urzędu i poszczególnych komórek organizacyjnych.
 19. EZD musi umożliwiać zarządzanie zakresem zawartości słowników systemowych. Minimalna lista słowników to: JRWA, Gońcy, Rejony, Kody pocztowe, Rodzaje dokumentów, Sposoby dostarczania korespondencji, Sposoby wysyłania korespondencji, Statusy spraw, Sposoby płatności, rodzaje interesantów.
 20. EZD musi umożliwiać użytkownikom dekretnym wskazanie jednej lub kilku komórek lub stanowisk merytorycznych odpowiedzialnych za prowadzenie i zakończenie sprawy. W przypadku wyboru kilku osób, możliwe jest wskazanie osoby odpowiedzialnej za ostateczne załatwienie sprawy.
 21. EZD musi umożliwiać przekazywanie dokumentów na pojedyncze stanowiska i na wiele stanowisk.
 22. System musi pozwalać na wprowadzenie polecenia kierowanego do wszystkich adresatów dekretnacji i indywidualnego polecenia dla każdego adresata.
 23. EZD musi umożliwiać dekretację dokumentu ze wskazaniem komórki wiodącej, współpracującej oraz do wiadomości.
 24. EZD musi umożliwiać tworzenie kopii dokumentu na podstawie oryginału, kopii i do wiadomości.
 25. Utworzona kopia powinna mieć właściwości maksymalnie takie jak dokument, w oparciu o który powstała (np. z dokumentu do wiadomości nie może powstać kopia).
 26. System musi pilnować, by dokument w trakcie kolejnych dekretacji był zadekretowany maksymalnie z ustawieniem takimi, jak został zadekretowany krok wcześniej (np. w przypadku pierwszej dekretacji kopii dokumentu, kolejna dekretacja nie może się odbyć na oryginale na stanowisku, które otrzymało kopię).
 27. EZD powinno pozwalać administratorom na zdefiniowanie domyślnej grupy osób, do których dekretowany będzie dokument.
 28. EZD musi umożliwić odróżnienie oraz jednoznaczną identyfikację i odrębne przetwarzanie poszczególnych dokumentów, przechowywanych w postaci odwzorowań cyfrowych wchodzących w skład przesyłki, przy zachowaniu ich powiązania z przesyłką.
 29. EZD musi umożliwić dodawanie przez użytkownika informacji opisujących poszczególne dokumenty, przesyłki lub sprawy w postaci notatek, zgodnie z instrukcją kancelaryjną.
 30. EZD musi umożliwiać dwustronną komunikację z systemem ePUAP (odbieranie – wysyłanie dokumentów).
 31. EZD musi automatycznie przypisywać UPP i UPD do wysyłanych dokumentów przez ESP.

32. EZD musi posiadać wbudowany edytor tworzenia szablonów dokumentów służący do tworzenia dokumentów wewnątrz systemu, bez konieczności używania zewnętrznych aplikacji.
33. EZD musi obsługiwać szablony dokumentów co najmniej w zakresie:
 - 1) możliwości zdefiniowania szablonu dokumentu oraz przypisania do niego uprawnień dla stanowisk lub komórek organizacyjnych,
 - 2) możliwość tworzenia szablonów w zależności od typu dokumentu: korespondencja wychodząca, dokument wpływający, dokument wewnętrzny,
 - 3) prowadzenia repozytorium szablonów, które umożliwia zarządzanie szablonami,
 - 4) możliwości wstawiania znaczników do szablonu. Minimalny zakres znaczników:
 - a) dane nadawcy,
 - b) dane adresata (min. imię, nazwisko, adres, nazwa instytucji),
 - c) kod kreskowy,
 - d) pełne dane pracownika prowadzącego sprawę,
 - e) znak pisma/sprawy,
 - f) adresaci pisma,
 - g) data pisma,
 - h) lista stron sprawy,
 - i) elementy pozwalające na sterowanie zawartością dokumentu np. znacznik nowej strony,
 - 5) możliwości wykorzystania zdefiniowanego szablonu przy tworzeniu pism wychodzących z autouzupełnianiem zawartości w/w znaczników,
 - 6) możliwości generowania korespondencji seryjnej.
34. Każdy dokument opiera się o indywidualny szablon dokumentu, który jest definiowany w systemie.
35. Każdy szablon może posiadać dowolną liczbę kontrolek.
36. W przypadku rejestracji dokumentu XML (zgodnego z CRD) system musi automatycznie kopiować dane z poszczególnych węzłów dokumentu XML do odpowiednich kontrolek.
37. System musi umożliwić eksport dokumentu systemowego do następujących formatów: XML (zgodnego z CRD), PDF, DOCX, ODT.
38. EZD musi umożliwiać integrację z pakietem MS Office, OpenOffice i LibreOffice co najmniej w zakresie możliwości edycji dokumentów wychodzących (pisma, arkusze) dołączanych przez użytkowników do spraw bezpośrednio w pakiecie MS Office, OpenOffice i LibreOffice, EZD musi umożliwiać import tekstu przygotowanego w zewnętrznym procesorze tekstu.
39. EZD musi umożliwić generowanie i drukowanie nalepek z kodami kreskowymi na dokumenty papierowe oraz nośniki i odnajdywanie na podstawie zeskanowanej nalepki odwzorowania cyfrowego bądź metryki danego dokumentu.
40. EZD musi umożliwiać generowanie kopert/naklejek dla korespondencji wychodzącej wraz z kodem kreskowym zawierającym unikatowy identyfikator wysyłki.
41. System musi pozwalać na łączenie wielu przesyłek wychodzących w jedną kopertę, w przypadku, gdy użytkownik stwierdzi, iż dotyczą one tego samego adresata.
42. EZD musi być zintegrowane z programem obsługującym pocztę tradycyjną w zakresie automatycznego przesyłania listy przesyłek oraz odbioru z tejże aplikacji, informacji o numerze nadanym przesyłce, doręczeniu, ZPO lub zwrocie przesyłki. System musi umożliwiać wydruk książki nadawczej oraz dziennika korespondencji.
43. System musi umożliwiać tworzenie własnych cenników przesyłek uwzględniających formę wysyłki, wagę i gabaryt.
44. EZD musi prezentować informacje na temat statusu przeczytania zadekretowanego/przekazanego dokumentu i na tej podstawie umożliwiać cofnięcie wykonanej czynności.
45. EZD musi umożliwić rejestrację historii pisma (czynność wykonana, data i czas, użytkownik) dokumentów papierowych (dla których istnieje odwzorowanie cyfrowe oraz dla których nie zostało ono wykonane) oraz nośników.
46. EZD musi umożliwić wszczynanie, prowadzenie i załatwianie spraw, przechowywanie akt sprawy i prowadzenie spisów spraw zgodnie z obowiązującymi przepisami. System automatycznie musi nadawać znak sprawy i zapewnia jego zgodność z wymogami instrukcji kancelaryjnej.
47. EZD musi umożliwić prowadzenie rejestrów kancelaryjnych, w tym rejestru przesyłek wpływających, wychodzących oraz pism wewnętrznych.
48. EZD musi umożliwić numerację i klasyfikację spraw w oparciu o JRWA zgodnie z instrukcją

kancelaryjną.

49. EZD musi umożliwiać określenie terminu realizacji spraw w oparciu o dane JRWA.
50. EZD musi umożliwiać oddzielną rejestrację dokumentów nietworzących akt sprawy, w szczególności:
 - 1) rejestru faktur – wyposażonego w opcję wieloetapowego zatwierdzania faktury i potwierdzania płatności faktury przez uprawnionych użytkowników wraz z mechanizmem wizualnego oznaczania faktur przeterminowanych,
 - 2) definiowania z poziomu administratora systemu dowolnego rejestru poprzez:
 - 3) definicję pól i typów pól dokumentów wchodzących w skład rejestru,
 - 4) możliwość definiowania masek w polach rejestru,
 - 5) definiowanie uprawnień (podglądu, edycji),
 - 6) możliwość udostępnienia zawartości rejestru na BIP.
51. EZD musi umożliwiać wielostopniowy proces akceptacji dokumentów (zgodnie z instrukcją kancelaryjną podmiotu), z możliwością parametryzacji wymagalności akceptacji dla dokumentu przed jego wysłaniem do interesanta. System musi mieć możliwość wymuszenia przez użytkownika dokonania akceptacji dokumentu z podpisem (podpisem zaufanym, podpisem kwalifikowanym, pieczęcią elektroniczną).
52. EZD musi zapewniać możliwość podpisywania pism i załączników za pomocą kwalifikowanej pieczęci elektronicznej w postaci dostępu zdalnego (chmurowego). Pieczęć jest przetrzymywana na przeznaczonym do tego celu bezpiecznym urządzeniu HSM znajdującym się w infrastrukturze Kwalifikowanego Dostawcy Usług Zaufania. Dostęp do pieczęci musi być odpowiednio szyfrowany i wymagać odpowiedniej autoryzacji przed rozpoczęciem. Za pomocą usługi dostarczonej w takim modelu jest możliwość automatyzacji procesu sygnowania dokumentów. W ramach tej usługi wykonawca dostarczy niezbędne oprogramowanie do podpisywania pieczęcią kwalifikowaną oraz zapewni minimum 5 000 użyć pieczęci przez okres 1 roku
53. Użytkownik powinien mieć możliwość swobodnego definiowania ścieżek akceptacji (wskazania konkretnych osób oraz liczby pozytywnych zatwierdzeń dla każdego etapu akceptacji).
54. EZD musi umożliwić zapis projektów pism przekazywanych pomiędzy użytkownikami lub komórkami w trakcie załatwiania sprawy, a także zamieszczanie komentarzy odnoszących się do projektów pism.
55. EZD musi zapewnić prowadzenie, podgląd oraz wydruk metryki sprawy zgodnie z obowiązującymi przepisami.
56. EZD musi umożliwić opisywanie spraw i akt sprawy metadanymi zgodnie z obowiązującymi przepisami.
57. EZD musi umożliwić odnotowanie wysyłki przesyłek wychodzących w rejestrze i opatrzenie ich metadanymi zgodnie z przepisami.
58. EZD musi zapewnić przydzielanie spraw i korespondencji, przekazanych na dane stanowisko, konkretnym użytkownikom pracującym na tym stanowisku.
59. EZD musi umożliwić podgląd historii sprawy, ścieżki obiegu sprawy w taki sposób by możliwe było odwzorowanie pełnego przebiegu sprawy.
60. EZD musi umożliwiać grupowanie dynamiczne spraw w projekty, określenie członków grupy projektowej oraz praw dostępu do projektu.
61. EZD musi posiadać funkcjonalność obsługi kalendarzy. Każdy z użytkowników powinien posiadać dostęp do własnego kalendarza z możliwością dodawania do niego dowolnych zdarzeń. Użytkownik powinien mieć możliwość określenia typu zdarzenia oraz jego opisu. Użytkownik powinien mieć również możliwość definiowania zdarzeń całoniedziowych i dłuższych oraz cyklicznych. System ma umożliwiać przeglądanie kalendarzy podwładnych. Kalendarz musi umożliwiać dodawanie i edycję wpisów za pomocą mechanizmu „przeciągnij i upuść”.
62. EZD musi posiadać funkcjonalność planowania i raportowania spotkań, co najmniej w zakresie:
 - 1) opracowywanie agendy spotkania,
 - 2) zapraszanie uczestników,
 - 3) wyszukiwanie spotkań,
 - 4) pisanie raportów ze spotkań na podstawie agendy (również przy jej braku),
 - 5) zakładanie kolejnych spraw na podstawie protokołu za spotkania.

63. EZD musi umożliwiać zarządzanie zasobami poprzez ustalanie rezerwacji zasobów. System musi umożliwić definiowanie dowolnych zasobów. Każdy zasób musi być powiązany ze „swoim” terminarzem, do którego uprawnieni użytkownicy mają wgląd. Ponadto tylko uprawnieni użytkownicy mogą rezerwować zasoby, a fakt rezerwacji jest odnotowywany w terminarzu zasobu. Musi również istnieć możliwość grupowania zasobów (np. grupa „pojazdy” zawierająca pojazdy, którymi dysponuje Urząd).
64. EZD musi posiadać funkcjonalność pozwalającą na zbiorcze podejrzenie dostępności rezerwowanych zasobów i innych użytkowników. Każdy terminarz musi być możliwy do przeglądania w trybie dziennym, tygodniowym, miesięcznym.
65. EZD musi być wyposażony w funkcjonalność komunikatora tekstowego. Komunikator musi być integralnym elementem EZD. Komunikator musi umożliwić prowadzenie rozmów pomiędzy dwoma użytkownikami lub prowadzenie rozmów grupowych.
66. EZD musi umożliwić użytkownikowi podgląd przypisanych do niego spraw i korespondencji, z możliwością sortowania, filtrowania i przeszukiwania.
67. EZD musi mieć umożliwić wprowadzanie zmian kadrowych, urlopów i zastępstw. Umożliwia przekazanie osobie zastępującej części lub całości uprawnień osoby zastępowanej. Uprawnienia muszą być przekazane na określony czas dat lub bezterminowo.
68. EZD musi posiadać moduł urlopów umożliwiający co najmniej:
- 1) obsługę wniosków urlopowych umożliwiającą złożenie wniosku przez pracownika oraz późniejszą akceptację przez kierownika oraz ostateczne zatwierdzenie przez kadrową,
 - 2) wyznaczanie zastępstw na podstawie udzielonych urlopów,
 - 3) integrację funkcjonalności urlopów z kalendarzem systemowym co najmniej w zakresie widoku planowanych urlopów, uzależnionego od posiadanych uprawnień tj., pracownik widzi swoje urlopy, kierownik widzi urlopy swoje jak i pracowników podległych, kadrowa widzi urlopy wszystkich pracowników,
 - 4) informowanie w momencie dekretacji o nieobecności pracownika, na którego dekretowany jest dokument.
69. EZD musi umożliwiać definiowanie zastępstw na czas nieobecności, polegających na udzieleniu pełnomocnictwa innemu użytkownikowi do wykonywania czynności w imieniu użytkownika nieobecnego. Pełnomocnictwo powinno być definiowane w określonym przedziale czasu. Dostęp do danych nieobecnego użytkownika powinien być kontrolowany przez System i odbierany wraz z upłynięciem daty końcowej. W trakcie trwania zastępstwa w systemie jest prezentowana informacja o zastępowaniu jednej osoby przez drugą. Wszystkie operacje wykonywane w zastępstwie powinny być zapisane w sposób umożliwiający jednoznaczne określenie, kto wykonał daną operację.
70. EZD musi posiadać moduł obsługi delegacji umożliwiający obsługę wniosków o delegację krajową i zagraniczną oraz późniejszą akceptację przez kierownika.
71. EZD musi umożliwiać przekazywanie spraw na inne stanowisko lub do innej komórki organizacyjnej.
72. EZD musi umożliwić prowadzenie książki teleadresowej interesantów.
73. EZD musi posiadać wewnętrzny edytor, służący do sporządzania komentarzy załączanych do akt sprawy.
74. System musi udostępniać zestaw raportów niezbędnych do pracy urzędu. Użytkownik musi mieć możliwość określenia podstawowych parametrów raportów (okres za jaki raport będzie generowany, sposób sortowania). System musi umożliwiać wygenerowanie co najmniej następujących raportów:
- 1) Statystyki dla spraw;
 - 2) Statystyki dla pism;
 - 3) Raport pism przychodzących;
 - 4) Raport pism przekazanych na stanowisko;
 - 5) Raport pism wychodzących;
 - 6) Raport z książki doręczeń;
 - 7) Raport dekretacji;
 - 8) Raport zwrotów;
 - 9) Raport dokumentów interesanta;
 - 10) Raport udostępnień danych osobowych;
 - 11) Koszty wysyłek dokumentu;
 - 12) Raport terminowości pracowników.

75. Raporty muszą być zwizualizowane w postaci tabeli oraz wykresu.
76. Raporty można wygenerować dla całego urzędu, referatu, biura lub konkretnego pracownika.
77. EZD musi posiadać interfejsy komunikacyjne z Platformą usług informatycznych ePUAP – w zakresie dwukierunkowej integracji z usługą Elektronicznej Skrzynki Podawczej dostępną na ePUAP.
78. EZD ma mieć możliwość importu skrytek podawczych podmiotów z platformy ePUAP.
79. EZD musi posiadać moduł (funkcjonalność) zapewniający obsługę składów chronologicznych dla dokumentów papierowych, -archiwum zakładowe umożliwiające: przekazywania dokumentacji przez komórki organizacyjne do archiwum zakładowego, wypożyczania dokumentów, brakowania, wycofywania dokumentacji itd.
80. EZD musi umożliwić dokumentowanie wyjęcia dokumentacji ze składu chronologicznego lub ze składu informatycznych nośników danych oraz wydrukowanie karty zastępczej dla wypożyczanego nośnika. Procedura obsługi składów powinna być realizowana w następujący sposób: pracownik sprawdza dostępność nośnika, a następnie składa wniosek o wypożyczenie, osoba obsługująca skład akceptuje wniosek i wypożycza nośnik, zwrot nośnika również jest potwierdzany przez osobę obsługującą skład.
81. EZD musi zapewnić przejmowanie dokumentacji przez archiwum zakładowe po upływie okresu przewidzianego w instrukcji kancelaryjnej lub ustalonego w podmiocie. Przejęcie dokumentacji musi polegać na przekazaniu archiwizście uprawnień do tej dokumentacji w systemie EZD oraz ograniczeniu uprawnień komórki merytorycznej, zgodnie z instrukcją kancelaryjną.
82. EZD musi posiadać dedykowane funkcje do udostępniania i wycofywania dokumentacji elektronicznej z archiwum zakładowego.
83. EZD musi umożliwiać wypożyczanie spraw z archiwum, podgląd informacji o sprawie oraz zmianę kategorii archiwalnej sprawy przechowywanej w archiwum.
84. EZD musi posiadać funkcje wspierające proces porządkowania dokumentacji w archiwum zakładowym (wskazanie dokumentacji wymagającej uzupełnienia).
85. EZD musi realizować brakowanie akt elektronicznych oraz przekazanie akt do Archiwum Państwowego oraz sporządzenie i przechowywanie odpowiedniej dokumentacji.
86. EZD musi wspierać pracę archiwisty poprzez automatyczne typowanie dokumentacji do brakowania lub przekazania do archiwum państwowego (po upływie terminów związanych z danymi kategoriami archiwalnymi).
87. EZD musi wspomagać użytkownika w przygotowywaniu paczki archiwalnej dla Archiwum Państwowego poprzez przygotowywanie automatycznych spisów zdawczo-odbiorczych, wykazu akt, oraz zapisanie spraw w strukturze wymaganej przez Archiwum Państwowe.
88. EZD musi wspomagać użytkownika w przygotowywaniu paczki administracyjnej do przekazania między instytucjami administracji publicznej lub wewnątrz jednostki administracyjnej w formie elektronicznej, zawierającej wszystkie niezbędne dokumenty i metadane wymagane do kompletnej i zgodnej z przepisami wymiany informacji.
89. EZD musi wspomagać użytkownika w przygotowywaniu paczki sądowej do przekazania do sądu w formie elektronicznej, zgodnie z wymogami postępowania sądowego zawierającej wszystkie niezbędne dokumenty, załączniki oraz metadane wymagane przez sąd.
90. EZD musi umożliwiać sporządzenie pocztowej książki nadawczej dostosowanej do zróżnicowanych wymagań występujących w różnych urzędach pocztowych.
91. EZD musi posiadać wbudowany mechanizm powiadomień, informujący o istotnych zdarzeniach związanych z jego aktywnością w systemie. Minimalny zbiór powiadomień powinien obejmować informowanie o: zadekretowaniu dokumentu na pracownika, przekazaniu dokumentu do akceptacji, akceptacji dokumentu, udostępnieniu dokumentu pracownikowi.
92. EZD musi posiadać mechanizm parafowania dokumentów oraz podpisywania ich kwalifikowanym podpisem elektronicznym. W przypadku dokumentów podpisanych – istnieje możliwość weryfikacji złożonego podpisu oraz wydrukowania raportu z podpisu.
93. Klient ESP musi mieć możliwość obsługi wielu skrytek jednocześnie.
94. Klient ESP musi mieć możliwość wyświetlania dowolnego dokumentu XML. Jeśli dokument XML nie posiada wskazania na XSL lub wskazane XSL nie jest dostępne, klient ESP musi rozpoznać taką sytuację i wyświetlić wszystkie węzły tego dokumentu XML.
95. Klient ESP musi prawidłowo wyświetlać każdy dokument zgodnie z CRD.
96. Klient ESP musi automatycznie wyciągać następujące dane z dokumentu XML (zgodnego z CRD): załączniki, dane nadawcy i odbiorcy z węzła Dane Dokumentu oraz informacje o osobie, która podpisała dokument podpisem kwalifikowanym lub Profilem Zaufanym.
97. Klient ESP musi umożliwić automatyczne weryfikowanie podpisu złożonego za pomocą Podpisu

Zaufanego.

Administracja systemem i warunki techniczne

1. EZD musi umożliwić modelowanie wielopoziomowej struktury organizacyjnej instytucji, która umożliwi przypisanie pracowników do odpowiednich stanowisk, a także wprowadzanie modyfikacji w strukturze w ramach zmian organizacyjnych za pomocą dezaktywacji i aktywacji stanowisk i komórek organizacyjnych.
2. EZD musi umożliwić definiowanie uprawnień do poszczególnych funkcji systemu oraz grupowanie uprawnień w role w celu ułatwienia administracji systemem.
3. Uprawnienia i role przypisywane są do stanowiska, a nie do użytkownika systemowego.
4. Użytkownik logując się do systemu, ma dostęp do określonych obszarów systemu na podstawie uprawnień, które posiada stanowisko, do którego jest przypisany użytkownik.
5. EZD musi umożliwiać delegowanie części lub całości posiadanych uprawnień.
6. System musi posiadać wyodrębniony moduł administracyjny. Dostęp do tego modułu mogą uzyskać jedynie użytkownicy z odpowiednimi uprawnieniami.
7. EZD musi posiadać rozbudowany rejestr zdarzeń rejestrujący akcje użytkowników na obiektach systemowych, udane i nieudane próby logowania oraz typowe błędy aplikacji.
8. EZD umożliwi zarządzanie uprawnieniami w oparciu o grupy uprawnień i grupy zasobów, jakich dotyczą. System uprawnień musi być zdolny do odzwierciedlenia uprawnień i odpowiedzialności poszczególnych pracowników wynikający z instrukcji kancelaryjnych oraz struktury stanowisk.
9. Hasła w EZD muszą być przechowywane w systemie w formie zaszyfrowanej - nie może być możliwości ich odtworzenia, lecz jedynie zresetowania. Po zresetowaniu hasła użytkownika przez administratora system musi wymagać od użytkownika zdefiniowania nowego hasła przy pierwszym logowaniu.
10. EZD musi umożliwiać swobodne definiowanie polityki uwierzytelniania i blokowania kont w oparciu o następujące parametry:
 - 1) Minimalna długość nazwy użytkownika i hasła
 - 2) Ilość dużych liter, cyfr, znaków specjalnych w hasle,
 - 3) Długość cyklu wymuszania zmiany hasła (w miesiącach),
 - 4) Ilość nieudanych prób logowania, po których następuje blokada konta,
 - 5) Czas blokady konta po przekroczeniu liczby nieudanych prób logowania.
11. Zakres wartości w słownikach prowadzonych przez system powinien być konfigurowalny przez administratora lub pochodzić z rejestrów centralnych (np. TERYT).
12. System w przypadku rejestrów centralnych powinien umożliwiać wyłączenie walidacji pól, które wykorzystują dany rejestr (np. TERYT i pola adresowe), tak by użytkownik mógł dane wprowadzić samodzielnie.
13. EZD musi rejestrować wszystkie czynności dostępu do usług i zasobów w systemie, w tym informacje o:
 - 1) operacjach na dokumentach,
 - 2) operacjach na danych osobowych,
 - 3) zmianach haseł,
 - 4) zdarzeniach uwierzytelniania (udane logowanie, wylogowanie, nieudane logowanie);
 - 5) zdarzeniach autoryzacji (nieudane/udane operacje);
 - 6) zdarzeniach administracyjnych.
14. Zapisywanie danych identyfikujących musi obejmować:
 - 1) adres IP i nazwę maszyny, z której wykonano daną czynność;
 - 2) identyfikator/nazwa użytkownika, który wykonał daną czynność;
 - 3) czas wystąpienia.
 - 4) EZD musi posiadać mechanizm informujący użytkownika o wprowadzonych zmianach w aplikacji.

Integracja Systemu z Systemami Dziedzinowymi

1. Rozwiązanie musi umożliwiać jednoczesną integrację z dowolną liczbą wdrażanych w ramach niniejszego postępowania Systemów Dziedzinowych (SD).
2. Integracja musi umożliwiać zarówno pobieranie danych z EZD przez SD jak i wysyłanie danych do EZD przez SD.
3. W ramach weryfikacji przez EZD praw SD do wymiany danych, każdorazowe uruchomienie usług przez system kliencki musi wymuszać autoryzację i autentykację SD.
4. W przypadku jednoczesnego serwowania usług dla kilku SD, dane wymieniane z jednym SD nie mogą się mieszać, kolidować i być wspólne z danymi wymienianymi z innymi SD.

5. Dane szczegółowe obiektów udostępnianych przez aplikację w ramach integracji muszą być zawsze dostępne, niezależnie od tego, czy kiedykolwiek wcześniej zostały pobrane, tak aby można je było pobrać dowolną liczbę razy.
 6. Zakres wymienianych danych między EZD a SD musi obejmować co najmniej:
 - 1) dokumenty, sprawy i pliki składające się na dokumenty,
 - 2) odbieranie i kierowanie dokumentów do wysyłki.
 7. Musi istnieć możliwość odmiennej konfiguracji usługi dla kilku różnych SD jednocześnie zintegrowanych z EZD, a zakres tej konfiguracji musi umożliwiać udostępnienie usługi w pełnym lub częściowym zakresie, tj. konfiguracja ma dotyczyć co najmniej:
 - 1) typów wymienianych dokumentów i spraw,
 - 2) przyjmowania informacji o danych typach dokumentów,
 - 3) udzielania informacji o danych typach dokumentów,
 - 4) przyjmowania zleceń i realizowania wysyłki dokumentów (przesyłek wychodzących).
 - 5) Aplikacja w ramach usługi musi na każde żądanie SD udostępniać informacje o bieżącej konfiguracji usługi i zakresie wymienianych informacji.
 - 6) Udostępniana przez aplikację usługa musi umożliwiać realizację wymiany informacji co najmniej zgodnie i w zakresie przedstawionym w poniższych wariantach:
- Wariant 1:
- a) Dokument wpływa do urzędu i jest rejestrowany jako przesyłka przychodząca w EZD, otrzymując numer wpływu.
 - b) W EZD użytkownik wszczyna sprawę na podstawie dokumentu, nadając jej znak.
 - c) SD pobiera informacje o dokumencie i sprawie zarejestrowanych w EZD.
 - d) SD generuje dokument odpowiedzi.
 - e) SD przekazuje do EZD dokument odpowiedzi (wraz ze składającymi się nań plikami) i dołącza go do sprawy w Systemie EZD.
- Wariant 2
- a) SD wszczyna postępowanie „z urzędu”.
 - b) SD wprowadza do EZD sprawę wszczętą „z urzędu”.
 - c) SD generuje masowo dokumenty.
 - d) SD przekazuje do EZD wygenerowane dokumenty i dołącza je do uprzednio wprowadzonej sprawy w EZD.
 - e) SD wysyła za pośrednictwem Systemu EZD dokumenty do wskazanych adresatów.
- Wariant 3
- a) Pismo wpływa do urzędu i jest rejestrowane jako przesyłka przychodząca w EZD, otrzymując numer wpływu.
 - b) SD pobiera informacje o piśmie zarejestrowanym w EZD.
 - c) SD w EZD dołącza pismo do sprawy już istniejącej w EZD.
 - d) SD przekazuje do EZD dokument odpowiedzi i dołącza go do sprawy w EZD.
8. Ponadto, integracja musi umożliwiać realizację innych scenariuszy, w których będą występować różne kombinacje zdarzeń opisanych w w/w wariantach.

INSTRUKTAŻ PRACOWNIKÓW SZBI

1. Użytkownikami systemu będą wszyscy pracownicy Zamawiającego, stąd należy przyjąć, że instruktaże muszą objąć 24 osoby z podziałem na instruktaż dla kancelarii, administratorów i pracowników merytorycznych. Jeżeli ze względu na funkcjonalności systemu konieczne jest wydzielenie dodatkowych grup (np. kierownicy itp.) musi to zostać uwzględnione w ofercie przez Wykonawcę.
2. Zamawiający oczekuje realizacji instruktażu w godzinach pracy jednostki z podziałem pozwalającym na zachowanie ciągłości pracy, co oznacza, że instruktaż dla pracowników merytorycznych winien odbyć się z podziałem minimum na dwie grupy, w różnych terminach.
3. Wymiar czasowy instruktaży musi być adekwatny do zakresu zadań realizowanych we wdrażanych rozwiązaniach przez każdego pracownika i powinien zostać oszacowany przez Wykonawcę w taki sposób, aby każdy pracownik mógł po wdrożeniu sprawnie korzystać z Systemu. Ponieważ zakres obowiązków użytkowników poszczególnych modułów oprogramowania jest zbliżony w różnych urzędach samorządu szczebla gminnego, oszacowanie wymiaru czasowego instruktaży jest obowiązkiem Wykonawcy, posiadającego w tym zakresie stosowne doświadczenie.

4. Instruktaż należy zaplanować w dwóch turach obejmujących wszystkich pracowników Zamawiającego w każdej turze. Pierwsza i druga tura ma być zrealizowana w trybie stacjonarnym, na podstawie ustalonego z Zamawiającym harmonogramu.
5. Niezależnie od instruktażu Wykonawca zapewni asystę uruchomieniową realizowaną przy stanowiskach pracy wszystkich użytkowników systemu w miarę ich potrzeb. Maksymalny wymiar asysty uruchomieniowej to 2h dla każdego pracownika, przy czym Zamawiający ma prawo zróżnicować czas asysty dla poszczególnych pracowników wg własnych potrzeb (łącznie czas asysty wynosi 48h).
6. Niezależnie od instruktażu oraz asysty uruchomieniowej Wykonawca zapewni możliwość skorzystania z nielimitowanego wsparcia w trybie zdalnym (helpdesk/telefon) w całym okresie objętym wsparciem.

AUDYT POSTĘPOWANIA Z DOKUMENTACJĄ, SZKOLENIE Z PRZEPISÓW PRAWA, WSPARCIE MERYTORYCZNE

1. Wykonawca w ramach wdrożenia przeprowadzi audyt postępowania z dokumentacją.
2. Zakres audytu obejmie zarządzenia i procedury wewnętrzne, związane z wykonywaniem przez Zamawiającego czynności kancelaryjnych na różnych etapach pracy z dokumentacją oraz próbki dokumentów wytwarzanych i gromadzonych przez Zamawiającego.
3. Zamawiający przekaże Wykonawcy zarządzenia, instrukcje, procedury oraz skany zanonimizowanych dokumentów. Ilość i zakres przekazanych materiałów do audytu zostanie ustalony z Wykonawcą.
4. Po przekazaniu Zamawiającemu wyników audytu, Wykonawca przeprowadzi dla pracowników Zamawiającego szkolenie online dotyczące przygotowania urzędu do wdrożenia systemu
5. Szkolenie będzie trwało minimum 6 godzin (z przerwami ustalonymi z Zamawiającym) w godzinach pracy jednostki. Będzie omówieniem zasad postępowania z dokumentacją zgodnie z obowiązującymi u Zamawiającego: regulaminem organizacyjnym, instrukcją kancelaryjną, jednolitym rzeczowym wykazem akt, wybranymi zagadnieniami Kodeksu postępowania administracyjnego oraz z uwzględnieniem tematów, które po przeprowadzonym audycie będą wymagały szczególnej uwagi. Szkolenie, oprócz zagadnień formalnych, będzie zawierało tematy praktyczne i organizacyjne, związane z wdrożeniem systemu EZD i będzie okazją do rozmowy i odpowiedzi na pytania pracowników Zamawiającego. Szkolenie będzie nagrywane i wraz z materiałami szkoleniowymi udostępnione Zamawiającemu do późniejszego wykorzystania.
6. Audyt i szkolenie Wykonawca powinien zrealizować przed instruktażami pracowników z obsługi funkcjonalności systemu. Zamawiający wymaga takiej kolejności działań, ponieważ oczekuje, że audyt i szkolenie przyczynią się do sprawdzenia i powtórzenia podstawowych zasad postępowania z dokumentacją oraz umożliwią Zamawiającemu podjęcie różnych decyzji organizacyjnych, zanim pracownicy przejdą instruktaż z obsługi systemu.
7. Wykonawca zapewni pracownikom Zamawiającego wsparcie merytoryczne w zakresie konsultacji stosowania przepisów prawa, dotyczących postępowania z dokumentacją. Wsparcie będzie realizowane przez okres 24 miesięcy, liczony od dnia następnego po podpisaniu przez obie strony protokołu odbioru końcowego w wymiarze 48 godzin miesięcznie. Konsultacje będą realizowane telefonicznie, online oraz poprzez korespondencję e-mail na zasadach ustalonych z Wykonawcą.

OGÓLNE WARUNKI GWARANCJI

1. Świadczenie usługi gwarancji w okresie 24 miesięcy (wg oferty) rozpocznie swój bieg:
 - 1) w dniu następnym, licząc od daty potwierdzenia usunięcia wad lub usterek stwierdzonych przy odbiorze końcowym przedmiotu umowy,
 - 2) w dniu następnym, licząc od dnia podpisania przez obie strony protokołu odbioru końcowego, w przypadku gdy nie stwierdzono wad lub usterek,
2. W przypadku, jeżeli Wykonawca dokona modernizacji istniejącego systemu informatycznego, zmodernizowany system informatyczny musi zostać objęty gwarancją na warunkach określonych w niniejszym rozdziale. Świadczenie usługi gwarancji ma na celu zapewnienie ciągłości sprawnego działania systemu poprzez realizację działań naprawczych wynikających z analizy ujawnionych problemów, wykrytych błędów i wad systemów, niewłaściwego działania systemu, spadku wydajności oraz zmian prawnych uniemożliwiających zgodne z prawem funkcjonowanie systemu
3. W ramach gwarancji Wykonawca zobowiązany jest do nieodpłatnego:
 - 1) aktualizacji systemu do najnowszych wersji,
 - 2) usuwania błędów, awarii, wady z przyczyn zawinionych przez Wykonawcę będących

- konsekwencją wystąpienia: błędu w systemie, błędu lub wady fizycznej pakietu aktualizacyjnego lub instalacyjnego, błędu w dokumentacji administratora lub w dokumentacji użytkownika, błędu w wykonaniu usług przez Wykonawcę;
- 3) usuwania błędów, awarii, wady związanych z realizacją usługi wdrożenia oprogramowania;
 - 4) usuwania błędów lub awarii spowodowanych aktualizacjami oprogramowania.
 4. Zgłaszający, w przypadku wystąpienia błędu, awarii, wady przesyła do Wykonawcy przy pomocy środków komunikacji formularz zgłoszenia wystąpienia błędu/awarii/wad
 5. Zgłoszenia będą klasyfikowane na awarie, błędy i wady:
 - 1) Awaria - krytycznie wadliwa praca systemu lub jego części, niezgodna z przekazaną dokumentacją lub warunkami Umowy, polegająca na zatrzymaniu lub zakłóceniu pracy systemu lub jego części w takim zakresie, że nie istnieje możliwość realizacji przez Zamawiającego istotnych dla jego organizacji procesów (na przykład: niedostępne są usługi dla mieszkańców będące celem zamówienia, czy też niemożliwe jest terminowe wypełnienia przez Zamawiającego obowiązków wynikających z przepisów wewnętrznych lub zewnętrznych) lub też nieprawidłowość pracy części systemu w takim zakresie, że kontynuowanie jego działania doprowadziłoby do utraty danych lub naruszenia ich spójności, w przypadku Awarii nie jest możliwe prawidłowe użytkowanie systemu z powodu w szczególności uszkodzenia lub utraty spójności danych, struktur danych lub błędnego funkcjonowania platformy systemowo-sprzętowej;
 - 2) Błąd - wadliwa praca Systemu lub jego części, niezgodna z przekazaną dokumentacją lub warunkami Umowy, polegająca na zakłóceniu pracy Systemu lub jego części innym niż Awaria.;
 - 3) Wada - wadliwa praca Systemu lub jego części polegające na nienależytym działaniu jego części, nieograniczająca działania Systemu, nie mająca istotnego wpływu na zastosowanie Systemu.
 6. Wykonawca zobowiązany jest do usunięcia awarii/błędów/wad występujących w oprogramowaniu aplikacyjnym lub infrastrukturze kluczowej w następujących terminach:
 - 1) Awarie w terminie nie dłuższym niż 8h roboczych od przyjęcia zgłoszenia przez Wykonawcę.
 - 2) Błędy w terminie nie dłuższym niż 3 dni roboczych od przyjęcia zgłoszenia przez Wykonawcę,
 - 3) Wady w terminie nie dłuższym niż 10 dni roboczych od przyjęcia zgłoszenia przez Wykonawcę.
 7. W przypadku niemożności usunięcia awarii, błędu lub wady w terminie, o którym mowa w ust. 6 Wykonawca jest zobowiązany pisemnie uzasadnić zwłokę i wskazać termin usunięcia danej awarii, błędu lub wady. W takim przypadku Zamawiający zastrzega sobie prawo w uzasadnionych przypadkach do pisemnej odmowy akceptacji terminu podanego przez Wykonawcę i skorzystania z uprawnień zawartych w ust. 8.
 8. W przypadku niespełnienia zobowiązań określonych w ust. 6 i 7 względnie odmowy akceptacji podanego terminu usunięcia danej awarii, błędu lub wady zgodnie z ust. 7, Zamawiający może zlecić wykonanie napraw osobie trzeciej na koszt Wykonawcy – bez konieczności wyznaczania dodatkowego terminu i upoważnienia sądu.
 9. Wykonawca ponosi wobec Zamawiającego odpowiedzialność za wyrządzone szkody, będące normalnym następstwem nienależytego wykonania czynności objętych umową, ocenianego w granicach przewidzianych przez Kodeks cywilny.
 10. Wszystkie reklamacje dotyczące niepełnego, nienależytego lub nieterminowego wykonania przedmiotu umowy, Zamawiający będzie przekazywał niezwłocznie Wykonawcy w formie pisemnej.
 11. Usługobiorca wyznacza osoby odpowiedzialne za merytoryczną obsługę EKD (administratorów technicznych).
 12. Administrator lub inna osoba do tego upoważniona zgłasza problem dotyczący działania systemu do Usługodawcy. Każde zgłoszenie otrzyma unikalny numer, na podstawie którego będzie prowadzona dalsza komunikacja w sprawie zgłoszenia.

System umożliwia integrację z dostawcą systemu dziedzinowego Sigid w zakresie wymiany danych. Okres gwarancji 24 miesiące (wsparcie i aktualizacja).

Wykonawca zobowiązany jest do wykonania pełnej instalacji, konfiguracji oraz uruchomienia Teleinformatycznego Systemu Zarządzania Bezpieczeństwem Informacji, obejmującej wdrożenie wszystkich modułów systemu, dostosowanie ich parametrów do środowiska Zamawiającego oraz integrację z istniejącą infrastrukturą teleinformatyczną. Wykonawca zapewni również przeprowadzenie szkolenia dla administratorów i użytkowników systemu.