RAG.271.1.2026 Załącznik nr 1 do SWZ

Opis przedmiotu zamówienia

Obszar techniczny

1. Zapora sieciowa klasy UTM TYP 1 - 1 sztuka

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

- 4 portami Gigabit Ethernet RJ-45.

2. System Firewall posiada wbudowany port konsoli szeregowej.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 580 tys. jednoczesnych połączeń oraz 28 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 4 Gbps dla pakietów 512 B.
3. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 3 Gbps.
4. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 750 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.

12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

- Translację jeden do jeden oraz jeden do wielu.
- Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

- Amazon Web Services (AWS).
- Microsoft Azure.
- Cisco ACI.
- Google Cloud Platform (GCP).
- OpenStack.
- VMware NSX.
- Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

- Wsparcie dla IKE v1 oraz v2.

- Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
- Obsługa protokołu Diffie-Hellman grup 19, 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
- Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
- Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 20000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 6000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 260 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:

- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
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 mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.

2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres do 30.06.2026 r.

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres min. 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

Wymagania w zakresie instalacji i wdrożenia urządzenia klasy UTM:
Zamawiający wymaga:

1. Instalacji urządzenia klasy UTM we wskazanym punkcie dystrybucji okablowania.
2. Wdrożenia urządzenia klasy UTM do ochrony styku z Internetem we wskazanych przez Zamawiającego segmentach sieci, w tym:
    a. Konfiguracji interfejsów urządzenia (w tym LACP, VLAN),
    b. Konfiguracji routingu IP,
    c. Konfiguracji mechanizmów zarządzania,
    d. Konfiguracji reguł firewalla,
    e. Konfiguracji modułów funkcyjnych (min. IPS, AntiVirus).

2. Zakup oraz konfiguracja 2 fizycznych serwerów oraz konfiguracja zasilania awaryjnego tych serwerów, zakup oraz konfiguracja oprogramowania systemowego.

Serwer fizyczny – 2 sztuki

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U • 8 slotów na dyski 2.5” • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. • Obsługa procesorów 144 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinny znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do 4TB pamięci RAM.
Procesor	• Zainstalowany jeden procesor min. 16-rdzeniowy, min. 3.2GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 197 w teście SPECspeed®2017_fp_base, dostępnym na stronie www.spec.org dla konfiguracji jednoprocesorowej oferowanego serwera.
RAM	• 32GB DDR5 RDIMM 6400MT/s,
Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający o Min. 8GB nieulotnej pamięci cache, o Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. o Wsparcie dla dysków samoszyfrujących o Obsługa dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS
Dyski twarde	• Zainstalowane: o 6x dysk SSD SATA MU o pojemności min. 960GB, Hot-Plug

	• Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Gniazda PCI	• Dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	• 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)

Wbudowane porty	• 4 porty USB w tym min:
	  ○ 1 port USB 2.0 Type-C
	  ○ 2 porty USB 3.1
	  ○ 1 port USB 3.0 wewnątrz obudowy
	• Port VGA z tyłu obudowy

Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	• Redundantne, Hot-Plug min. 800W klasy Titanium
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
System operacyjny/dodatkowe oprogramowanie	• Windows Server 2025 Standard – licencja dobrana tak, aby umożliwić uruchomienie 2 maszyn wirtualnych • 18x Windows Server 2025/2022 User CALs
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0

	• Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego spełnienie powyższych zaleceń.
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej o szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika o możliwość podmontowania zdalnych wirtualnych napędów o wirtualną konsolę z dostępem do myszy, klawiatury o wsparcie dla IPv6 o wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer o integracja z Active Directory o możliwość obsługi przez sześciu administratorów jednocześnie o Wsparcie dla automatycznej rejestracji DNS o wsparcie dla LLDP o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej

	○ możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. ○ Monitorowanie zużycia dysków SSD ○ Automatyczne zgłaszanie alertów do centrum serwisowego producenta ○ Automatyczne update firmware dla wszystkich komponentów serwera ○ Możliwość przywrócenia poprzednich wersji firmware ○ Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON ○ Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych ○ Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. ○ Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera ○ kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania ○ możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień ○ możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera ○ możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer ○ możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe możliwość rozszerzenia funkcjonalności o: ○ możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch ○ możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej ○ Automatyczne odświeżanie certyfikatów SSL

	○ monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB

	○ Przesyłanie alertów „as-is" do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. ○ Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin:

	▪ wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów ▪ wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityka konfiguracji ▪ z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny) ▪ inwentaryzacja komponentów w serwerze i ich mikrokodów ▪ historia poboru mocy i temperatury serwera ▪ zbieranie danych diagnostycznych serwera do paczki serwisowej
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: o ilość podłączonych oraz rozłączonych systemów o stan podłączonych urządzeń o informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów o Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia o informacje o statusie gwarancji dla poszczególnych urządzeń o informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń o informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. o Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych o Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących.

	Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. o Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. o Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. o Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. o Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. o Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów

	○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO,

	○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu

	aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver, dla kraju, w którym produkt będzie użytkowany, według normy wprowadzonej w 2019 roku - **Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie powyższych wymogów.** • 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.
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.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii minimum na okres 3 lat.

	• Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. • Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: o Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. o Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. o Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji

	przypisanym do urządzenia, które posiada wykupioną usługę serwisową. ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

Zasilacz awaryjny do serwera – 2 szt.

Parametr	**Wymagania minimalne**
Technologia	online, VFI-SS-111,
Moc wyjściowa	3kVA/3kW; PF=1
Obudowa	Rack/Tower Zestaw do montażu w szafie rack na wyposażeniu
Napięcie wejściowe	110 ÷ 300 V AC ± 2 %
Napięcie znamionowe (wartość skuteczna)	230V AC
Prąd znamionowy (wejście)	15,6A
Częstotliwość napięcia wejściowego (zakres oraz tolerancja)	45 ÷ 55 / 55 ÷ 65 Hz ± 1 Hz

Częstotliwość znamionowa napięcia wejściowego	50Hz / 60Hz
Zniekształcenia prądu wejściowego THDi	< 5%
Zakres napięcia wyjściowego	200/208/220/230/240V AC konfigurowalne z poziomu oprogramowania oraz z menu zasilacza na wyświetlaczu LCD (domyślnie 230V AC)
Zniekształcenia napięcia wyjściowego THDu	< 1% dla Pmax (liniowe) < 5% (nieliniowe wg PN EN 62040-3)
Gniazda wyjściowe	4x IEC320 C13 (10A) sterowalne + 4x IEC320 C13 (10A) + 1x IEC320 C19 (16A)
Akumulatory wewnętrzne UPS	Minimum 6szt akumulatorów 12V9Ah
Moduły bateryjne	Opcja – możliwość podpięcia do 4szt modułów (każdy z minimum 12szt akumulatorów 12V9Ah)
Czas podtrzymania UPS dla obciążenia 3kW/2kW/1,5kW	3 / 6 / 9 min
Przeciążalność	105-125% - 5min / 125-150% - 30s / >150% - 500ms
EPO	Wymagane – standard NC
Sygnalizacja	akustyczno-diodowa, wyświetlacz LCD oraz diody sygnalizujące usterkę, pracę bateryjną, pracę w trybie online, obejście bypass
Język oprogramowania	polski i angielski do wyboru z poziomu interfejsu użytkownika

Konfiguracja minimalnego poziomu naładowania baterii po powrocie zasilania sieciowego (po rozładowaniu baterii przed ponownym samoczynnym załączeniem zasilania na wyjściu)	Wymagane, konfigurowalne z poziomu oprogramowania (przez USB)
Wymagane certyfikaty	CE, ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu; (załączyć dokument potwierdzający do oferty)
Komunikacja z urządzeniem	RS232, USB HID, styki bezpotencjałowe 1-wejście; 1-wyjście; SNMP – karta w zestawie
Wymiary UPS i MODUŁY (rack) (wys x szer x gł)	Nie więcej niż 89 x 439 x 610 mm
Oprogramowanie do monitorowania pracy zasilacza UPS	a) Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na min. 75 stanowiskach komputerowych w sieci; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux. b) Możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów: Powyższe wymagania potwierdzone oświadczeniem producenta oprogramowania dołączonym do oferty.
Oprogramowanie - funkcjonalność	możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPS'ów w oprogramowaniu
Oprogramowanie - funkcjonalność	Konfiguracja minimalnego poziomu naładowania baterii. UPS po rozładowaniu baterii przed samoczynnym załączeniem zasilania wyjść (po powrocie zasilania sieciowego) będzie musiał naładować baterie do tego poziomu. Parametr ten ma zastosowanie w przypadku, gdy załączenie zasilania wyjść może nastąpić tylko wtedy, gdy UPS zgromadzi niezbędny zapasa energii na wypadek kolejnego zaniku.
Oprogramowanie - funkcjonalność	Uruchom poprzez Bypass - Aktywacja tej funkcji powoduje, że UPS zawsze przed załączeniem zasilania wyjść na kilka sekund załączy zasilanie poprzez Bypass i po chwili przełączy się w zasilanie wyjść poprzez falownik (normalny tryb pracy). Funkcja ta umożliwia załączenie urządzeń o zwiększonym prądzie rozruchowym bez przeciążania falownika UPS.

Serwis producenta	wymagany, zlokalizowany na terenie Polski, autoryzacja serwisowa lub oświadczenie producenta - załączyć do oferty
Gwarancja	Minimum 24 miesiące elektronika, 24 miesiące akumulatory, serwis door to door, czas naprawy 5 dni roboczych
Dokumentacja	Instrukcja w języku polskim

Wymagania w zakresie instalacji i wdrożenia serwera wraz z zasilaniem awaryjnym:

Zamawiający wymaga:

1 Instalacji sprzętu we wskazanej serwerowni i szafie rack.
2 Instalacji i konfiguracji – dostarczonego wraz odpowiednimi urządzeniami – systemu operacyjnego Microsoft Windows Server na serwerze, podłączenie serwera do wskazanego przez Zamawiającego segmentu sieci.

3. Zakup oraz konfiguracja macierzy dyskowej wraz z oprogramowaniem w celu tworzenia automatycznych kopii zapasowych danych z serwerów aplikacyjnych, serwerów baz danych oraz danych z komputerów użytkowników zgodnie z harmonogramem tworzenia kopii zapasowych (1 szt.) oraz powielenia kopii w innej lokalizacji UGK (2 szt.)

Typ	Sieciowy serwer plików NAS
Obudowa	Rack
Procesor	4-rdzeniowy 64-bitowt procesor o taktowaniu min. 1.7 GHz
Pamięć RAM	4 GB UDIMM DDR4 z możliwością rozszerzenia do 16GB RAM
Wewnętrzna pamięć masowa	Możliwość instalacji 8 dysków 3,5-calowe SATA 6 Gb/s, 3 Gb/s Zamawiający wymaga dostarczenia zestawu z 4 dyskami o pojemności 8 TB każdy
Kompatybilność dysków	3,5-calowewnęki: 3,5-calowe dyski twarde SATA 2,5-calowe dyski twarde SATA, 2,5-calowe dyski SSD SATA
Interfejsy sieciowe	Min. 2 x 2,5 Gigabit Ethernet (2,5G/1G/100M/10M), 2 x 10GbE SFP+
Złącza dodatkowe	Min. 2 porty typu A USB 3.2,
Gniazdo M.2	Opcjonalne, poprzez kartę PCIe
Szyfrowanie	AES 256bit
Zasilacz	250 W PSU, 100–240 V
Gwarancja	Minimum 24 miesiące gwarancji producenta

Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim, w formie elektronicznej.

4. **<u>Zakup, konfiguracja oraz wdrożenie systemu zintegrowanego zarządzania infrastrukturą oraz bezpieczeństwem IT wraz z opieką na 24 mc</u>**

Oprogramowanie powinno posiadać poniższe funkcjonalności (moduły):

1. **MONITOROWANIE INFRASTRUKTURY**

- obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

- wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
- wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją OU)
- wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
- wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
- wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach w dowolnym rozmiarze i kolorze
- wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
- wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny
- zablokowania mapy urządzeń przed przypadkową edycją
- serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów
- serwerów pocztowych:

- program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty
- program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem)
- program ma możliwość wykonywania operacji testowych
- program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa

- monitorowania serwerów WWW i adresów URL
- cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
- obsługi szyfrowania SSL/TLS w powiadomieniach e-mail

- obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID
- obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
- monitoringu routerów i przełączników wg:

- zmian stanu interfejsów sieciowych
- ruchu sieciowego
- podłączonych stacji roboczych – graficzna prezentacja panelu switcha
- ruchu generowanego przez podłączone do portów stacje robocze

- serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
- wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
- monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano
- zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny
- wydajności systemów Windows:

- obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

2. INWENTARYZACJA

- gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

1. Prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
2. Możliwość odczytu parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.
3. Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
4. Informacje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
5. Informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
6. Możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
7. Odczytanie numeru seryjnego (klucze licencyjne).
8. Automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
9. Możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
10. Możliwość utworzenia listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI), znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).

11. Możliwość wymiany plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.

Możliwość prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:

- przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
- przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów,
- tworzenia powiązań między zasobami a urządzeniami,
- tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
- tworzenia relacji pomiędzy zasobami,
- wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
- definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości:

- dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,

- określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
- określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
- masową edycję atrybutów zasobów,
- definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
- importu danych z zewnętrznego źródła (.CSV),
- przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury
- zakupu, gwarancji, dowolnego dokumentu itp.,
- tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
- oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
- ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie,
- konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
- generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
- przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
- konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
- konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
- archiwizacji i porównywania audytów zasobów,

- tworzenia kodów kreskowych dla zasobów,
- drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
- inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów,
- dodawanie czynności serwisowych, drukowanie etykiet,
- możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
- inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
- definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data" z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja").

Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
2. Informacje o aplikacjach używanych w organizacji.
3. Tworzenie własnych wzorców aplikacji.
4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
5. Informacje o komputerach, na których aplikacja została wykryta.
6. Zarządzanie posiadanymi licencjami.
7. Wskazywanie osób odpowiedzialnych za licencję.
8. Wskazanie użytkowników licencji.
9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
10. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
12. Zarządzanie posiadanymi licencjami: raport zgodności licencji.
13. Możliwość przypisania do programów numerów seryjnych, wartości itp.

3. **OCHRONA DANYCH PRZED WYCIEKIEM** poprzez blokowanie urządzeń.

1. Blokowanie urządzeń i nośników danych.
- możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.

4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
9. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.
10. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
11. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.
12. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Zarządzanie prawami dostępu do urządzeń:
1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.
3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:
1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
2. Podłączenie/odłączenie urządzenia przenośnego.

Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.

Definiowanie reguł monitorowanych folderów w postaci list.

Ochrona przed usunięciem
- program musi być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.

Zabezpieczenia
Instalator programu musi być zabezpieczony podpisem cyfrowym wystawionym i zweryfikowanym przez zaufany globalny urząd certyfikacji (CA).

Program musi być dostępny w języku polskim, wraz z Podręcznikiem Użytkownika w formie strony internetowej.

Wsparcie techniczne świadczone telefonicznie lub mailowo w języku polskim lub angielskim.

Doradztwo i utrzymanie dokumentacji w zakresie ustawy o KSC

Zamawiający wymaga świadczenia usług doradczych, organizacyjnych i operacyjnych w zakresie realizacji obowiązków wynikających z ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa, w tym outsourcing funkcji Koordynatora ds. KSC dla Zamawiającego.

Doradztwo w zakresie KSC:

- interpretacja przepisów ustawy o KSC w kontekście funkcjonowania Urzędu Gminy,
- wsparcie Zamawiającego w dostosowaniu organizacji do wymagań KSC,
- bieżące konsultacje w trakcie realizacji zamówienia,
- rekomendacje działań organizacyjnych i technicznych.

Pełnienie funkcji Koordynatora ds. KSC (outsourcing w trakcie realizacji zamówienia):

- koordynowanie działań związanych z cyberbezpieczeństwem w Urzędzie Gminy,
- wsparcie w obsłudze incydentów bezpieczeństwa,
- rekomendacje działań naprawczych.

Utrzymanie dokumentacji KSC:

- analiza dokumentacji w zakresie KSC, w szczególności:
  - procedur zarządzania incydentami,
  - polityk bezpieczeństwa informacji,
  - analiz ryzyka,
  - planów ciągłości działania (jeżeli dotyczy),
- dostosowywanie dokumentacji do wymagań KSC,
- raport stanu zgodności z KSC.

Termin związania umową: 30 dni od dnia podpisania umowy.

5. Zakup oraz konfiguracja zarządzalnych przełączników sieciowych.

5.1 Zakup i konfiguracja zarządzalnych przełączników sieciowych – 2 sztuki

Dane techniczne

Typ przełącznika: Zarządzany

Warstwa przełącznika: L3

Zarządzanie przez stronę www: Tak

Porty i interfejsy

Podstawowe przełączanie RJ-45, Liczba portów Ethernet: 24

Podstawowe przełączania Ethernet RJ-45 porty typ: 10G Ethernet (100/1000/10000)

Ilość portów SFP28: 2

Ilość slotów Modułu SFP: 12

Sieć

Obsługa 10G: Tak

Prędkość transferu danych przez Ethernet LAN: 10,1000,2500,5000,10000 Mbit/s

Funkcjonalności warstw 2 i 3:

DHCP Server (Local Networks)

DHCP Relay

Inter-VLAN Routing (Local Networks)

Static Routing (Local Networks)

LACP Port Aggregation

STP & RSTP

QoS (DSCP)

Pro AV Profiles (Play, Dante, Q-SYS, NDI, SDVoE, Shure, AES67, Crestron)

Advanced IGMP Configuration (Querier, Fast Leave, Router Port)

IGMP Snooping

802.1X Control

MAC-Based ACLs & Device Isolation

DHCP Snooping & Guarding

Egress Rate Limit

Flow Control

Storm Control

Multicast & Broadcast Rate Limiting

MAC Address Blocking

IP-Based ACLs & Network Isolation

MAC-Based Port Restriction

Port Isolation

Port Mirroring

Jumbo Frames

LLDP-MED

Voice VLAN

Loop Protection

Virtual Network Override

Przesyłanie danych

Wydajność: 290 Gbit/s

Prędkość przekazywania: 431,52 Mpps

Przepustowość rutowania/przełączania: 580 Gbit/s

Zasilanie

Obsługa zasilania zapasowego (RPS): Tak

Maksymalne zużycie mocy: 100 W

Napięcie wejściowe AC: 100 - 240 V

Napięcie wejściowe DC: 11.5 V

Certyfikaty zgodności CE

Gwarancja: minimum 12 miesięcy

5.2 Zarządzalne przełączniki sieciowe TYP 2 – 1 sztuka

Cechy zarządzania

Typ przełącznika: Zarządzany

Warstwa przełącznika: L2

Ochrona

Typ uwierzytelniania: radius

Zasilanie przez sieć Ethernet (PoE)

Obsługa PoE: Tak

Power over Ethernet Plus (PoE +) ilość portów: 32

Zasilanie przez Ethernet (PoE) zasilanie na port: 32 W

Całkowita Power over Ethernet (PoE) budżetu: 195 W

Porty i interfejsy

Podstawowe przełączanie RJ-45 Liczba portów Ethernet: 48

Podstawowe przełączania Ethernet RJ-45 porty typ: Gigabit Ethernet (10/100/1000)

Ilość slotów Modułu SFP: 4

Sieć

Standardy komunikacyjne: IEEE 802.1x, IEEE 802.3af, IEEE 802.3at

Podpora kontroli przepływu: Tak

Dublowanie portów: Tak

Automatyczne wykrywanie: Tak

Obsługa sieci VLAN: Tak

Agregator połączenia: Tak

Automatyczne MDI/MDI-X: Tak

Protokół drzewa rozpinającego: Tak

Produkt stackowalny

Funkcjonalność warstwy 2:

LACP Port Aggregation

STP & RSTP

Advanced IGMP Configuration (Querier, Fast Leave, Router Port)

IGMP Snooping

802.1X Control

MAC-Based ACLs & Device Isolation

DHCP Snooping & Guarding

Egress Rate Limit

Flow Control

Storm Control

Multicast & Broadcast Rate Limiting

MAC Address Blocking

IP-Based ACLs & Network Isolation

MAC-Based Port Restriction

Port Isolation

Port Mirroring

Jumbo Frames

LLDP-MED

Voice VLAN

Loop Protection

Virtual Network Override

Przesyłanie danych

Wydajność: 52 Gbit/s

Prędkość przekazywania: 77,38 Mpps

Przepustowość rutowania/przełączania: 104 Gbit/s

Zgodny z Jumbo Frames: Tak

Moc

Maksymalne zużycie mocy: 45 W (240 W z PoE)

Napięcie wejściowe AC: 100 - 240 V

Zasilacz dołączony: Tak

Certyfikaty zgodności CE

Gwarancja: minimum 12 miesięcy

5.3 Zarządzalne przełączniki sieciowe TYP 3 – 1 sztuka

Nazwa	**Parametr**
Procesor	4-rdzeniowy 1.7 GHz
Pamięć systemowa	4 GB DDR4
Pamięć wbudowana	16 GB eMMC Zintegrowany dysk 128 GB SSD
Przepustowość IDS/IPS	3.5 Gb/s (mierzona w iPerf3)
Maks. pobór mocy (nie licząc wyjścia PoE)	50W
Sposób zasilania	1x Uniwersalne wejście AC, 100-240VAC, 4.4A Maks, 50/60 Hz 1x USP-RPS wejście DC, 52VDC, 3.94A
Zasilanie	AC/DC, wewnętrzne, 240W
Obsługiwany zakres napięcia	100 do 240VAC
Interfejs zarządzania	Ethernet Bluetooth
Interfejs sieciowy	1x port WAN: 2.5 Gigabit Ethernet RJ45 8x portów LAN: 10/100/1000 Mb/s RJ45
Interfejs SFP+	1x WAN: 10G SFP+ 1x LAN: 10G SFP+
PoE	2x porty PoE+ IEEE 802.3at (pair A 1, 2+; 3, 6-) 6x portów PoE IEEE 802.3af (pair A 1, 2+; 3, 6-)
Maks. PoE na port 802.3af	15.4W
Maks. PoE na port 802.3at	30W

Zakres napięcia dla PoE 802.3af	44 do 57V
Zakres napięcia dla PoE 802.3at	50 do 57V
Zabezpieczenie ESD/EMP	Powietrze: ± 15 kV, kontakt: ± 8 kV
Wyświetlacz LCM	1x dotykowy ekran 1.3" Animacja rozruchu: trwa rozruch Ikona aktualizacji oprogramowania: aktualizacja oprogramowania
Przyciski	Reset
Temp. pracy	-10 do 40° C (14 to 104° F)
Wilgotność pracy	5 - 95% niekondensująca
Waga	Max. 4.95 kg (10.91 lb)
Uchwyt	stal SGCC, uszy do montażu w szafie rack
Gwarancja	Minimum 12 miesięcy

6. Bezprzewodowa sieć komputerowa dla pracowników oraz gości urzędu – 2 sztuki

Rodzaj produktu: Access Point WLAN
Obsługa pasm: 2,4 GHz lub 5 GHz
Częstotliwość Wifi: 2.4 GHz, 5 GHz
Szybkość transmisji WLAN: 2,4 GHz, 574 MBit/s
Szybkość transmisji WLAN 5 GHz: 4800 MBit/s
Szybkość transmisji WLAN: 4800 MBit/s
Szyfrowanie: WPA, WPA-Enterprise, WPA-PSK, WPA2, WPA3
Ilość portów LAN: 1 x
Standard WLAN: IEEE802.11b, IEEE802.11a, IEEE802.11g, IEEE802.11n, IEEE802.11ac, IEEE802.11ax
Interfejs: LAN (10/100/1000 MBit/s)
Szybkość transmisji LAN: 10 / 100 / 1000 MBit/s
Anteny: 4 dBi, 6 dBi
Zasilanie: poprzez sieć (PoE)
Gwarancja: minimum 12 miesięcy

Obszar kompetencyjny

1. Szkolenie z zakresu cyberbezpieczeństwa dla kadry kierowniczej

Zakres szkolenia winien obejmować w szczególności:

- rolę kierownictwa w zapewnieniu cyberbezpieczeństwa w jednostce samorządu terytorialnego,
- podstawowe obowiązki Zamawiającego wynikające z przepisów prawa, w tym ustawy o Krajowym Systemie Cyberbezpieczeństwa,
- zarządzanie ryzykiem w obszarze cyberbezpieczeństwa,
- reagowanie na incydenty bezpieczeństwa z perspektywy kadry kierowniczej,
- odpowiedzialność organizacyjna i decyzyjna kadry kierowniczej.

- Forma szkolenia: online
- Czas trwania jednego szkolenia: jeden dzień roboczy w wymiarze min. 6 godzin
- Miejsce szkolenia: siedziba Zamawiającego lub inny budynek wskazany przez Zamawiającego zlokalizowany na jego terenie. Zamawiający zapewni salę szkoleniową wyposażoną w sprzęt niezbędny do odbycia szkolenia, w tym projektor multimedialny i notebook.
- Wymagania dotyczące wykonawcy:
- - 2 letnie doświadczenie w szkoleniach z cyberbezpieczeństwa

2. Szkolenie z zakresu cyberbezpieczeństwa dla pracowników

Zakres szkolenia winien obejmować w szczególności:

- podstawowe zagrożenia cyberbezpieczeństwa (phishing, złośliwe oprogramowanie, ataki socjotechniczne),
- zasady bezpiecznego korzystania z poczty elektronicznej i Internetu,
- bezpieczne hasła i ochrona danych,
- postępowanie w przypadku podejrzenia incydentu bezpieczeństwa,
- dobre praktyki cyberbezpieczeństwa w codziennej pracy.

- Forma szkolenia: online
- Czas trwania jednego szkolenia: jeden dzień roboczy w wymiarze min. 6 godzin
- Miejsce szkolenia: siedziba Zamawiającego lub inny budynek wskazany przez Zamawiającego zlokalizowany na jego terenie. Zamawiający zapewni salę szkoleniową wyposażoną w sprzęt niezbędny do odbycia szkolenia, w tym projektor multimedialny i notebook.
- Wymagania dotyczące wykonawcy:

- - 2 letnie doświadczenie w szkoleniach z cyberbezpieczeństwa

3. Akademia cyberbezpieczeństwa – cykl szkoleń online cykl 9 szkoleń online mających na celu utrwalenie oraz podniesienie poziomu wiedzy w obszarze cyberbezpieczeństwa

Zamawiający wymaga dostarczenia platformy szkoleniowej przeznaczonej dla 35 użytkowników, spełniającej poniższe warunki:

1. Platforma szkoleniowa w formacie *security awareness* dostarczająca narzędzia i zasoby niezbędne do zapewnienia pracownikom wartościowej wiedzy i umiejętności w zakresie ochrony przed cyberzagrożeniami.
2. Użytkownicy otrzymują dostęp do materiałów szkoleniowych oraz testów wiedzy. Menedżerowie grup oraz administratorzy zyskują wgląd w postęp nauki i poziom wiedzy w całej organizacji i dla poszczególnych grup.
3. Dedykowany kurs: „Bezpieczna praca w Internecie" – co najmniej 9 modułów, 60 lekcji i 15 testów sprawdzających nabytą przez kursantów wiedzę. Każdy moduł składa się z 4-9 lekcji w formie video oraz testu. Oprócz testów wewnątrz modułu, kurs zawiera również testy obejmujące swoim zakresem tematycznym przekrojowo więcej niż 1 moduł szkoleniowy. Szkolenia powinny być przygotowane i odpowiednio ułożone przez ekspertów w dziedzinie cyberbezpieczeństwa. Informacje zawarte w szkoleniach muszą być aktualne, istotne i odnoszące się do realnych zagrożeń, na które użytkownik może natknąć się podczas codziennego korzystania z komputera w pracy i nie tylko**.**
4. **Zakres tematyczny kursu „Bezpieczna praca w Internecie":**

- Socjotechniki wykorzystywane w ruchu sieciowym
- Bezpieczeństwo haseł
- Bezpieczeństwo poczty e-mail i ochrona przed SCAM-em
- Obrona przed phishingiem
- Bezpieczeństwo stron WWW i przeglądarek
- Ataki socjotechniczne z wykorzystaniem urządzeń
- Ataki za pośrednictwem telefonu
- Zagrożenia związane w urządzeniami mobilnymi
- Zagrożenia związane z sieciami Wi-Fi
- Zagrożenia w mediach społecznościowych
- Dobre praktyki bezpieczeństwa
- Prywatność, poufność i anonimowość w Internecie

Cechy szkolenia:

- Umożliwia szczegółowe monitorowanie postępu użytkownika
- Statusy lekcji: nierozpoczęta, w toku, ukończona
- Statusy modułu: nierozpoczęty, w toku, ukończony
- Statusy testu: nierozpoczęty, rozpoczęty, niezaliczony, zaliczony
- Brak ustalonej kolejności kursu, użytkownik może od razu przejść do zaliczenia testu lub zapoznawać się z lekcjami video według uznania lub według narzuconego w organizacji harmonogramu

- Każdy moduł zawiera krótkie streszczenie zawartości
- Każda lekcja zawiera notatki w formie tekstowej
- Po ukończeniu materiału użytkownik wciąż ma do niego nieograniczony dostęp w ramach trwającej subskrypcji, przypisanej do organizacji
- Postęp w lekcji jest zapisywany, użytkownik po powrocie do danej lekcji zaczyna od momentu, w którym zakończył oglądanie materiału video
- Kurs umożliwia filtrowanie dostępnych modułów kursu (wszystkie moduły, nowe, rozpoczęte, ukończone)
- Kurs pozwala użytkownikowi na ukrywanie ukończonych lekcji
- Po ukończeniu każdego modułu kursu użytkownik otrzymuje certyfikat (do wydruku)
- Po ukończeniu kursu użytkownik otrzymuje certyfikat (do wydruku)
- Administrator platformy ma możliwość konfigurowania minimalnego postępu w kursie (tempa postępów) osiąganego przez użytkowników
- Szkolenie dostępne również w wersji mobilnej z poziomu przeglądarki, bez konieczności instalacji dodatkowego oprogramowania

Test:

- Składa się z pytań i odpowiedzi jednokrotnego wyboru
- Do testu można podejść przed ukończeniem lekcji video (dowolna kolejność wykonywania działań w obrębie kursu)
- Administrator platformy ma możliwość konfigurowania progu punktowego wymaganego do
- zaliczenia testu
- Administrator platformy ma możliwość konfigurowania czasu, który musi upłynąć zanim użytkownik po raz kolejny może podejść do testu
- Test zapamiętuje odpowiedzi użytkownika (na wypadek opuszczenia testu przed ukończeniem)
- Kolejność pytań i odpowiedzi jest losowana przed rozpoczęciem przez użytkownika testu
- Ukończenie/Zaliczenie testu wpływa na postęp ukończenia modułu
- Brak limitu czasowego na ukończenie testu
- Zmiana wymaganego w organizacji progu procentowego zaliczenia testu po ukończeniu przez użytkownika testu nie ma wpływu na status testu (zaliczony/niezaliczony)
- Kursy zawierają test końcowy sprawdzający wiedzę z całego kursu

ZARZĄDZANIE PLATFORMĄ
Zarządzanie użytkownikami:

- Podział na 3 role: właściciel konta - Administrator Główny - z uprawnieniami administratora, administrator, użytkownik

- Administrator Główny jest kontem zarządzającym platformą, zintegrowanym z zewnętrznym serwisem do zarządzania subskrypcją, który jest właścicielem subskrypcji.
- Konto Administratora Głównego nie wlicza się do limitu użytkowników subskrypcji, ma dostęp do wszystkich funkcji platformy. Konta Administratora Głównego nie można usunąć, dezaktywować lub obniżyć uprawnień. Edycja danych Administratora Głównego wymaga zalogowania się do zewnętrznego serwisu do zarządzania subskrypcją
- Administrator jest rolą nadawaną przez Administratora Głównego lub innego Administratora, ma dostęp do wszystkich funkcji platformy, można go usunąć, dezaktywować lub obniżyć uprawnienia
- Użytkownik - ma dostęp do swojego pulpitu oraz szkolenia w platformie, nie może zarządzać platformą. Konto użytkownika może zostać utworzone ręcznie przez dowolnego administratora lub zaimportowanie z pliku .CSV.

- Możliwość nadania funkcji menedżera grupy - wiąże się z rozszerzeniem widoczności użytkownika o członków grupy, którymi zarządza (wglądu do ich danych, postępów w nauce itd.) Platforma pozwala na śledzenie postępów użytkowników w kursie (tylko dla Administratorów oraz Menedżerów) Platforma wyświetla listę aktywności każdego użytkownika w organizacji wraz z informacją o dacie i rodzaju aktywności.
  - Administrator ma możliwość podglądu postępu nauki w danym materiale szkoleniowym (lekcja lub test) użytkowników w organizacji (dedykowany widok "Postęp nauki")
  - Administrator oraz Menedżer mogą pobierać uzyskane przez użytkowników w organizacji certyfikaty
  - Menedżer ma dostęp do dedykowanej zakładki "Lista treści", w której może zapoznać się z postępami w nauce użytkowników należących do grup, którymi zarządza.
  - Każdy materiał w AST zawiera dedykowany widok z tabelą użytkowników, w których znajdują się informacje o statusie nauki i dacie ukończenia (materiał video/materiał własny) lub status, wynik (w %) oraz data zaliczenia (test)

Właściwości użytkowników:

- Imię i nazwisko, e-mail oraz rola (administrator/użytkownik)
- Wymóg unikalnego adresu e-mail w obrębie organizacji
- Możliwość dodawania użytkowników do platformy z poziomu interfejsu (formularz)
- Możliwość masowego dodawania użytkowników oraz grup do platformy poprzez import pliku .json, wygenerowanego w programie Axence nVision
- Możliwość masowego dodawania użytkowników do platformy poprzez import pliku .csv
- Możliwość aktualizacji danych użytkownika (imię i nazwisko) za pomocą importu csv.

- Importowany plik może mieć do 5000 wierszy (limit użytkowników)
- Po dodaniu użytkownika do platformy, otrzymuje on wiadomość e-mail z zaproszeniem do organizacji i ustaleniem pierwszego hasła
- Administrator może dowolnie edytować dane wszystkich użytkowników (imię, nazwisko, adres e-mail, rola)
- Administrator może dowolnie aktywować oraz dezaktywować konta wszystkich użytkowników
- Administrator może dowolnie usuwać konta wszystkich użytkowników
- Administrator ma dostęp do wszystkich funkcji w platformie
- Administrator ma dostęp do wszystkich zakładek w platformie
- Użytkownik ma dostęp do zakładki „Pulpit" oraz „Mój kurs"
- Menedżer ma rozszerzony dostęp do grup i użytkowników, którymi zarządza

Zarządzanie grupami:

- Administrator może dowolnie tworzyć, edytować oraz usuwać grupy
- Każda grupa może mieć dokładnie 1 menedżera
- Menedżer nie może edytować grupy, którą zarządza
- Menedżer nie może dodawać lub usuwać użytkowników z grup, którymi zarządza
- Użytkownik może należeć do dowolnej liczby grup
- Menedżer nie musi być członkiem grupy, którą zarządza

Zarządzanie treścią:

- Platforma pozwala na globalne włączanie lub wyłączanie materiałów edukacyjnych
- Wyłączać/włączać można całe moduły, testy z zagadnień, testy końcowe oraz własne materiały
- Platforma pozwala na nieograniczone dodawanie własnych materiałów
- Materiały własne mogą być elementem udostępnionego przez Axence kursu lub znajdować się w osobnej przestrzeni "Materiały wewnętrzne"
- Materiały własne można przenosić pomiędzy kursami
- Materiały własne składają się z następujących elementów: o nazwa lekcji,
- szacunkowa długość materiału,
- miniaturka (widoczna na liście materiałów)
- osadzone nagranie video (jeden osadzony materiał w serwisie Vimeo lub Youtube),
- treść materiału – w formie tekstowej, możliwość formatowania treści, osadzenia linków oraz obrazków
- Platforma pozwala na zmianę kolejności na liście, edytowanie oraz usuwanie własnych materiałów
- Możliwość podejrzenia postępu nauki w konkretnym materiale edukacyjnym użytkowników w organizacji

Postępowanie pn.: „Cyberbezpieczny samorząd" w ramach zadania pn. „Cyberbezpieczny Samorząd realizowanego w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC). Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa, konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23.

Ustawienia organizacji:

- Ustawienia szkolenia Konfiguracja procentowego progu zdawalności testu
- Konfiguracja czasu przed kolejnym podejściem do testu
- Konfiguracja minimalnego wymaganego postępu w kursie (liczba ukończonych materiałów na tydzień)
-
- Ustawienia powiadomień Wysyłanie newslettera – trzy opcje: brak wysyłki, wysyłka tylko do Administratorów, wysyłka do Użytkowników i Administratorów
- Wysyłanie powiadomień przypominających o nauce - trzy opcje: brak wysyłki, wysyłka tylko do Użytkowników, wysyłka do Użytkowników i Administratorów
-
- Informacja o rodzaju subskrypcji (pełna/demo)
- Informacja o czasie pozostałym do wygaśnięcia subskrypcji
- Wykres limitu użytkowników (użytkownicy w organizacji/limit subskrypcji)

Inne:

- Platforma posiada dedykowaną i stale aktualizowaną Bazę Wiedzy, w której znajdują się artykuły objaśniające najważniejsze funkcje platformy
- Motyw ciemny/jasny
- Comiesięczny newsletter dla użytkowników organizacji (wysyłany na adres e-mail użytkowników)
- Platforma umożliwia Administratorom oraz Menedżerom eksport danych z tabel do pliku CSV oraz Excel

Wspierane przeglądarki:

- Google Chrome
- Firefox
- Microsoft Edge

Licencjonowanie:

- Platforma jest udostępniania w formie płatnego dostępu do usługi on-line w chmurze
- Platforma jest dostępna w modelu subskrypcyjnym.
- Licencjonowanie usługi obejmuje okres 12- miesięcy na określoną Liczbę dostępów (użytkownicy platformy) – 35 użytkowników.
- Po zakończeniu okresu świadczenia usługi Zamawiający będzie mógł zamówić dostęp na nowy okres (przedłużenie świadczenia usługi)
- Istnieje możliwość rozszerzenia subskrypcji w ciągu roku tj. dokupienia dodatkowych użytkowników w zależności od pozostałych miesięcy do końca ważności dostępu (subskrybcji)
- Usunięcie użytkownika skutkuje usunięciem jego danych i historii szkoleniowej

Konto demo:

W ramach bezpłatnej wersji demo Zamawiający wymaga:

- dostęp do 5 lekcji na 30 dni
- jeden dostęp administratora oraz 3 dodatkowych użytkowników

Wymagania ogólne:

1. Statystyki i raporty dla użytkowników, grup i menadżerów
2. Możliwość dodawania własnych materiałów
3. Platforma jest systemem chmurowym osadzonym w środowisku Microsoft Azure, który nie wymaga konserwacji przez nabywcę.

<u>Wymagania ogólne w zakresie instalacji, wdrożenia oraz konfiguracji sprzętu i oprogramowania:</u>

Zamawiający wymaga:

1. Zaktualizowania oprogramowania/sterowników/firmware dla wszystkich urządzeń/rozwiązań objętych instalacją i konfiguracją zgodnie z OPZ do najnowszej dostępnej w dniu wdrożenia i stabilnej wersji.
2. Realizacji prac wdrożeniowych, które będą skutkowały niedostępnością środowiska IT Zamawiającego, w godzinach 20:00 – 5:00 w dni od poniedziałku do piątku lub w sobotę i niedzielę przez cała dobę i planowane w uzgodnieniu z Zamawiającym z minimum trzydniowym wyprzedzeniem.