

.....
[nazwa zamawiającego, adres]

WYKONAWCY

ubiegający się o zamówienie

Dotyczy: postępowania o udzielenie zamówienia publicznego:

Nazwa zamówienia: Dostawa licencji systemu monitorowania sieci komputerowej, urządzeń do sieci komputerowych oraz serwerów dla Gminy Brześć Kujawski i jednostek podległych w ramach Konkursu Grantowego "Cyberbezpieczny Samorząd".

Numer referencyjny: BI.II.271.26.2025.NŻ

WYJAŚNIENIA TREŚCI SWZ

Zamawiający, **Gmina Brześć Kujawski**, działając na podstawie art. 284 ust. 6 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320 z późn. zm.), udostępnia poniżej treść zapytań do Specyfikacji Warunków Zamówienia (zwanej dalej "SWZ") wraz z wyjaśnieniami:

Pytanie nr 1

Zamawiający wymaga dostawy licencji do monitorowania w ilości 15szt. dla jednej z jednostek. Znani na rynku producenci takich systemów oferują minimalny próg zamówienia na poziomie 20 licencji, stąd wnosimy o zmianę wymagań w tym zakresie.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający dopuszcza złożenie oferty i zakup licencji do monitorowania sieci w liczbie 20 stanowisk komputerowych.

Pytanie nr 2

Czy usługi wdrożenia wymagane w części 2 mogą zostać wykonane w formie zdalnej? Pozwoli to na zaproponowanie niższych cen, nie rezygnując z ich jakości.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający dopuszcza konfigurację zakupionego sprzętu sieciowego w formie zdalnej.

Pytanie nr 3

Zamawiający w załączniku nr 9 - Wzór umowy dla części 2 paragraf 6 pkt 8 wymaga przedłużenia gwarancji o czas naprawy. Żaden z liczących się rynkowo producentów nie oferuje gwarancji w taki sposób. W związku z powyższym prosimy o usunięcie paragraf 6 pkt 8 projektu umowy.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający usunie z umów dla części drugiej i trzeciej zamówienia z paragrafu 6 pkt 8, zapis „Okres gwarancji zostanie wydłużony o czas przebywania sprzętu w naprawie.”

Pytanie nr 4

Zamawiający dla części 2 we wzorze umowy (paragraf 6 pkt 13) wymaga przeglądów okresowych. Przeglądy okresowe są to dodatkowe usługi, które znacznie podniosą wartość zamówienia, a nie są wymagane dla podtrzymania gwarancji takich systemów. W związku z powyższym prosimy o usunięcie paragraf 6 pkt 13, celem ograniczenia zbędnych kosztów.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający oświadcza, że rezygnuje z przeglądów okresowych dla dostarczonego sprzętu. Paragraf 6 pkt 13 zostanie usunięty z umów dla części drugiej i trzeciej zamówienia.

Pytanie nr 5

Zamawiający z załączniku nr 7 - Opis przedmiotu zamówienia dla części 2 zamieścił bliźniacze wymagania dla różnych typów przełączników. Prosimy o wyjaśnienie.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający informuje, że w załączniku nr 7 do SWZ wkradł się błąd dotyczący liczby portów i wydajności w związku z powyższym punkt 5 pn. „Zakup urządzenia sieciowego zarządzalnego w warstwie L2 L3 8p” otrzymuje brzmienie jak niżej:

Zamawiający wymaga dostarczenia 8 urządzeń, każde zgodne z poniższą specyfikacją:

Przełącznik sieciowy

W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 10 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 8 porty GE RJ-45.

b) 2 porty GE, SFP.

Zarządzanie

- Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).

- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 20 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 30 Mpps.
- Tablica adresów MAC o pojemności co najmniej 8k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 5 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania/

NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

- Centralne zarządzanie konfiguracją urządzenia
- Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
- Centralne zarządzanie sieciami VLAN.
- Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
- Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
- Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
- Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
- Automatyczna detekcja i rekomendacje konfiguracji.
- Przesyłanie logów na zewnętrzny serwer syslog.
- Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
- Obsługa białych i czarnych list adresów MAC.
- Wykrywanie aplikacji komunikujących się w sieci.

2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.

3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 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 24x7.
2. Wykonawca musi świadczyć pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest zatrudnianie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania oraz ISO 9001, ISO 27001 i ISO 22301 w zakresie serwisowania urządzeń i oprogramowania informatycznego. Wszystkie certyfikaty należy dołączyć do oferty.

Pytanie nr 6

Zamawiający zgodnie z SIWZ wymaga, aby dokumenty były przedstawione w języku polskim. Jednocześnie wraz z ofertą należy załączyć karty katalogowe oferowanych urządzeń. Żaden producent nie prowadzi dokumentacji technicznej w wielu językach, gdyż takie produkty się zmieniają wraz z kolejnymi aktualizacjami. Co więcej przyjmuje się, że język angielski jest językiem technicznym międzynarodowym. W związku z powyższym prosimy o możliwość złożenia kart katalogowych w języku angielskim.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający dopuszcza wersje anglojęzyczne materiałów katalogowych i dokumentacji technicznej dla zamawianego sprzętu i oprogramowania.

Zamawiający

Załączniki:

1. Wzór umowy dla części II
2. Wzór umowy dla części III
3. Opis Przedmiotu Zamówienia


mgr Damian Gochiniak
ZASTĘPCA BURMISTRZA

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotowe zamówienie realizowane jest w ramach projektu współfinansowanego z Funduszy Europejskich 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”.

1. Niniejszy dokument stanowi oświadczenie woli Wykonawcy wyrażające jego zobowiązanie do świadczenia przedmiotu zamówienia w sposób i w zakresie w pełni zgodnym z wymaganym przez Zamawiającego.
2. Wykonawca musi wykazać, że oferuje przedmiot zamówienia w pełni zgodny z wymaganym przez Zamawiającego.
3. Niespełnienie któregośkolwiek z poniższych wymagań spowoduje odrzucenie oferty jako niezgodnej z SWZ.
4. Przystępując do udziału w niniejszym postępowaniu oświadczamy, iż spełniamy wszystkie niżej określone wymagania w zakresie przedmiotu zamówienia oraz oferujemy przedmiot zamówienia w pełni zgodny z określonym poniżej:
 - a) Dostarczane oprogramowanie i sprzęt muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
 - b) Dostarczony sprzęt i oprogramowanie pochodzić będą z oficjalnych kanałów dystrybucyjnych producenta obejmujących również rynek Unii Europejskiej, zapewniających w szczególności realizację uprawnień gwarancyjnych.
 - Zamawiający zastrzega, że sprzęt jak i podzespoły nie muszą być wyprodukowane na terenie UE, lecz muszą być dopuszczone do obrotu na terenie UE oraz musi być zapewniony dostęp do części zamiennych.
 - c) Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, aby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
5. Wykonawca zobowiązany jest do wdrożenia urządzeń do pracy w ramach infrastruktury IT jednostki, wykonania właściwych technicznych i logicznych połączeń urządzeń z siecią teleinformatyczną jednostki, wprowadzenie wszystkich ustawień z uwzględnieniem prawidłowego działania reguł oraz regulacji ruchu zgodnie z wymaganiami i wskazówkami administratora sieci jednostki.
6. Wykonawca wyda Zamawiającemu instrukcje obsługi oprogramowania lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekaze adresy WWW, pod którymi można je pobrać.
7. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.

Opis zasad warunków równoważności:

- Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanym w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.

- Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
- Użycie w opisie przedmiotu zamówienia nazw rozwiązań, materiałów i urządzeń służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.
- Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne.
- Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
- W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
- Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
- Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. W tym przypadku należy do postępowania dołączyć wszelkie dowody wskazujące na spełnienie niniejszych wymagań.

PRZEDMIOTY ZAMÓWIENIA:

Część I

Punkty 1, 2, 3. Zakup licencji systemu monitorowania sieci, urządzeń sieciowych, drukarek i urządzeń drukujących, jednostek komputerowych, nośników pamięci, zabezpieczenie dostępu do urządzeń

- Moduł monitorowania sieci dla **nielimitowanej liczby urządzeń**,
- Moduł zarządzania zasobami IT,
- Moduł zarządzania użytkownikami i monitorowania aktywności,
- Moduł ochrony danych i zarządzania politykami bezpieczeństwa.

1. Wymagania ogólne:

- System działa w architekturze klient-serwer.
- Wspiera instalację w środowisku on-premises.
- Umożliwia zarządzanie z poziomu aplikacji desktopowej.
- Komunikacja między komponentami systemu odbywa się przy użyciu szyfrowanego protokołu (np. TLS 1.2 lub nowszy).
- System nie ogranicza liczby instalacji konsoli zarządzających ani liczby urządzeń w module Network.

2. Monitorowanie infrastruktury sieciowej:

- Wykrywanie urządzeń w sieci (ping, ARP, SNMP, Active Directory).
- Graficzne mapy sieci z możliwością konfiguracji warstw i ikon.
- Monitorowanie serwisów (HTTP/S, SMTP, SNMP, SQL, inne).
- Obsługa SNMP v1/v2c/v3 z autoryzacją i szyfrowaniem.
- Monitorowanie maszyn wirtualnych (VMware).
- Obsługa powiadomień i alarmów (e-mail, SMS, Teams,).
- Obsługa komunikatów Syslog, trapów SNMP i WMI.
- Integracja z bramkami SMS i możliwość wysyłania powiadomień przez API.

3. Zarządzanie zasobami IT:

- Automatyczna inwentaryzacja sprzętu i oprogramowania.
- Gromadzenie informacji o konfiguracji stacji roboczych, aplikacjach i licencjach.
- Zarządzanie cyklem życia zasobu IT (zakup, przypisanie, serwis, utylizacja).
- Obsługa kodów kreskowych/QR, mobilna aplikacja inwentaryzacyjna.
- Obsługa dokumentów, przypisanie zasobów do użytkowników i lokalizacji.
- Alarmowanie o zmianach sprzętowych i instalacjach oprogramowania.

4. Zarządzanie użytkownikami i monitorowanie:

- Monitorowanie czasu aktywności, aplikacji, stron WWW, wydruków.
- Identyfikacja podejrzanej aktywności (np. jigglery, powtarzalne zachowania).
- Zgodność z RODO (separacja danych, audyt dostępów administratorów).
- Blokowanie aplikacji, stron WWW, portów, transferu plików.
- Integracja z Active Directory i zarządzanie uprawnieniami.
- Historia pracy i ekranowe zrzuty aktywności.

5. Ochrona danych i polityki bezpieczeństwa:

- Zarządzanie prawami dostępu do nośników zewnętrznych (USB, CD, Wi-Fi, Bluetooth).
- Audyt operacji na plikach (USB, lokalnie, udziały sieciowe).
- Integracja z Windows Defender, BitLocker i Firewall.
- Zdalne szyfrowanie dysków (np. BitLocker), monitoring TPM.
- Definiowanie polityk dostępu, blokad i uprawnień.

6. Bezpieczeństwo i zgodność:

- Obsługa dwuskładnikowego uwierzytelniania (2FA) w konsoli.
- Logowanie działań administratorów.
- Eksport logów do zewnętrznych systemów (np. Syslog).

- Konfiguracja polityk haseł i uprawnień.
- Zgodność z wymogami RODO i możliwość anonimizacji danych.

7. Wymagania techniczne:

- Kompatybilność z systemami Windows (serwer, agent)
- Wersja 64-bitowa, przystosowana do działania na stacjach roboczych i serwerach.
- Interfejs webowy responsywny (obsługa Chrome, Firefox, Edge).

8. Inne wymagania:

- Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej jednego inżyniera z aktualnym certyfikatem producenta oferowanego rozwiązania oraz ISO 9001, 27001, 22301 w zakresie serwisowania oprogramowań informatycznych. Wszystkie certyfikaty należy dołączyć do oferty.

Część II – część sieciowa

Punkt 1 . Zakup urządzeń UTM wraz z licencjami i wsparciem- UM

Wymagania Ogólne

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

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy i Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45.
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 20 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.

3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,8 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1,4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 630 Mbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec 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

13. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
14. 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.
15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
17. 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

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.

Routing i obsługa łączy WAN

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 21).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
 - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
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.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: 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. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 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 24x7.
2. Wykonawca musi świadczyć pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest zatrudnianie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania oraz ISO 9001, ISO 27001 i ISO 22301 w zakresie

serwisowania urządzeń i oprogramowania informatycznego. Wszystkie certyfikaty należy dołączyć do oferty.

Punkt 2. Zakup licencji urządzeń klasy UTM – 4 m-ce

Przedłużenie licencji na Fortigate 60F na okres 4 m-cy od 02.02.2026 do 06.06.2026r.

Punkt 3. Zakup urządzenia sieciowego zarządzalnego w warstwie L2 L3 48p

Przełącznik sieciowy

W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 60 W.
- Minimalny zakres temperatury pracy: 0-45°C.

Interfejsy sieciowe - wymagania minimalne

Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 48 porty GE RJ-45.

b) 4 porty 10 GE SFP+

Zarządzanie

- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).

- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 260 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.

- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
 - Centralne zarządzanie konfiguracją urządzenia
 - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
 - Centralne zarządzanie sieciami VLAN.
 - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
 - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
 - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.

- Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
 - Automatyczna detekcja i rekomendacje konfiguracji.
 - Przesyłanie logów na zewnętrzny serwer syslog.
 - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
 - Obsługa białych i czarnych list adresów MAC.
 - Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 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 24x7.
2. Wykonawca musi świadczyć pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest zatrudnianie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania oraz ISO 9001, ISO 27001 i ISO 22301 w zakresie serwisowania urządzeń i oprogramowania informatycznego. Wszystkie certyfikaty należy dołączyć do oferty.

Punkt 4. Zakup urządzenia sieciowego zarządzalnego w warstwie L2 L3 24p**Przełącznik sieciowy**

W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 28 W.
- Minimalny zakres temperatury pracy: 0-45°C.

Interfejsy sieciowe - wymagania minimalne

Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

- a) 24 porty GE RJ-45.
- b) 4 porty 10 GE SFP+.

Zarządzanie

- Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3

- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.

- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
 - Centralne zarządzanie konfiguracją urządzenia
 - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
 - Centralne zarządzanie sieciami VLAN.
 - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
 - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
 - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
 - Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.

- Automatyczna detekcja i rekomendacje konfiguracji.
 - Przesyłanie logów na zewnętrzny serwer syslog.
 - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
 - Obsługa białych i czarnych list adresów MAC.
 - Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 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 24x7.
2. Wykonawca musi świadczyć pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest zatrudnianie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania oraz ISO 9001, ISO 27001 i ISO 22301 w zakresie serwisowania urządzeń i oprogramowania informatycznego. Wszystkie certyfikaty należy dołączyć do oferty.

Punkt 5. Zakup urządzenia sieciowego zarządzalnego w warstwie L2 L3 8p**Przełącznik sieciowy**

W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 10 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 8 porty GE RJ-45.

b) 2 porty GE, SFP.

Zarządzanie

- Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.

- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 20 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 30 Mpps.
- Tablica adresów MAC o pojemności co najmniej 8k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 5 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.

- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

- Centralne zarządzanie konfiguracją urządzenia
- Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
- Centralne zarządzanie sieciami VLAN.
- Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
- Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
- Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
- Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
- Automatyczna detekcja i rekomendacje konfiguracji.
- Przesyłanie logów na zewnętrzny serwer syslog.
- Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
- Obsługa białych i czarnych list adresów MAC.

- Wykrywanie aplikacji komunikujących się w sieci.
- 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
- 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 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 24x7.
2. Wykonawca musi świadczyć pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest zatrudnianie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania oraz ISO 9001, ISO 27001 i ISO 22301 w zakresie serwisowania urządzeń i oprogramowania informatycznego. Wszystkie certyfikaty należy dołączyć do oferty.

Punkt 6. Zakup urządzeń zarządzalnych do sieci bezprzewodowej wraz z konfiguracją kontrolera**Access Point**

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
 - a. Temperatura 0–50°C,
 - b. Wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać co najmniej następujące standardy:
 - a. 2.4 GHz 802.11b/g/n,
 - b. 5 GHz 802.11a/n/ac/ax,
 - c. 6 GHz 802.11ax/be
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.
5. Urządzenie musi być wyposażone w moduł BLE.
6. Urządzenie musi być wyposażone w co najmniej jeden interfejs Ethernet (RJ45) wspierający co najmniej szybkości 1G/2.5G/5.0G.
7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz. Maksymalne zużycie energii nie może przekraczać 17W przy wykorzystaniu wszystkich funkcji urządzenia.
8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
 - a. Tunnel,

- b. Bridge,
 - c. Mesh.
9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST).
11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
- a. MIMO – 2x2,
 - b. Wymagana maksymalna przepustowość dla poszczególnych modułów radiowych:
 - i. 688 Mbps;
 - ii. 2882 Mbps;
 - iii. 5765 Mbps;
 - c. Wymagana moc nadawania:
 - i. min. 26 dBm dla pasma 2.4GHz
 - ii. min. 23 dBm dla pasma 5GHz
 - iii. min. 22 dBm dla pasma 6GHz
 - d. Wsparcie dla kanałów 20/40/80/160/320MHz,
 - e. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4,2dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5,1dBi dla pasma 6GHz.
 - f. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy.
 - g. Każdy z modułów radiowych musi posiadać możliwość pracy jako dedykowany skaner.

12. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512

13. Funkcje dodatkowe:

- a. OFDMA UL i DL
- b. Spatial Reuse (BSS Coloring)
- c. UL-MU-MIMO
- d. DL-MU-MIMO
- e. Enhanced Target Wake Time (TWT)
- f. Wbudowany analizator widma
- g. Wbudowane mechanizmy WIPS/WIDS

Gwarancja oraz wsparcie

1. Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 12 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 24x7.
2. Wykonawca musi świadczyć pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest zatrudnianie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania oraz ISO 9001, ISO 27001 i ISO 22301 w zakresie serwisowania urządzeń i oprogramowania informatycznego. Wszystkie certyfikaty należy dołączyć do oferty.

Punkt 7 Wdrożenie polityk Port Security - DHCP Snooping, VLAN, DNS Spoofing

- przeniesienie konfiguracji z posiadanego UTM-a 60F i konfiguracja z drugim urządzeniem w klaster. Wdrożenie powyższych rozwiązań na 2 UTM-ach i switch-ach w jednostce Urząd Miejski,
- wdrożenie na urządzeniach UTM i switch zabezpieczeń sieciowych ograniczających dostęp do portów fizycznych, zezwalając na połączenie tylko zaufanym urządzeniom (Port Security)
- utworzenie 2 wirtualnych sieci (VLAN-ów) na przełącznikach i przypisaniu do nich portów, co pozwoli izolować różne grupy urządzeń
- Wdrożenie podstawowej konfiguracji na wszystkich UTM + 5 VPN

Część III – część serwerowa

- 1) Urządzenia muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych.
- 2) Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.
- 3) Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.
- 4) Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.
- 5) Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.
- 6) Urządzenia na etapie dostawy pomiędzy producentem, a zamawiającym nie mogą podlegać modyfikacjom.
- 7) Cały zaoferowany sprzęt (cztery serwery) musi posiadać jeden punkt świadczenia napraw gwarancyjnych.

Punkt 1 Serwer typ 1 o poniższej charakterystyce:

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	- Obudowa Rack o wysokości max 2U z możliwością instalacji min. 8 dysków 3.5" - Obudowa wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. - Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne.
Płyta główna	- Płyta główna z możliwością zainstalowania do dwóch procesorów. - Obsługa procesorów 32 rdzeniowych. - Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. - Na płycie głównej powinno znajdować się min. 16 slotów przeznaczonych do instalacji pamięci. - Płyta główna powinna obsługiwać do 1TB pamięci RAM.

Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych
Procesor	Zainstalowane dwa procesory 16-rdzeniowe, min. 2.8 GHz (częstotliwość bazowa), klasy x86, dedykowane do pracy z zaferowanym serwerem, umożliwiające osiągnięcie wyniku min. 333 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocessorowej.
RAM	Minimum 512 GB DDR5 RDIMM 5600MT/s,
Gniazda PCI	Min. cztery sloty PCIe, w tym min. trzy x16
Kontroler RAID	- Sprzętowy kontroler dyskowy, posiadający - Min. 8 GB nieulotnej pamięci cache, - Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. - Wsparcie dla dysków samoszyfrujących
Dyski twarde	- Zainstalowane: 3 x dysk SSD SATA o pojemności min. 1.92 TB, 6Gb, 2,5" Hot-Plug, 1 DWPD. 3 x dysk HDD SATA o pojemności min. 12 TB, 6Gb, 7.2 tys. obr./min., 3,5" Hot-Plug. - Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
Wbudowane porty	4 porty USB w tym min: 1 port USB 3.0 z tyłu obudowy, 1 port micro USB z przodu obudowy 2 port VGA z czego jeden z przodu obudowy
Video	Zintegrowana karta graficzna umożliwiającą wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne, Hot-Plug
Zasilacze	Redundantne, Hot-Plug min. 1100W klasy Titanium

Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
System operacyjny/dodatkowe oprogramowanie	Fabrycznie zainstalowany Windows Server 2025 Standard, licencja pokrywająca wszystkie fizyczne rdzenie w serwerze
Bezpieczeństwo	- Zatrzaśnięcie górnej pokrywy oraz blokada na ramce panelu 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).
Karta Zarządzania	- Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; - możliwość podmontowania zdalnych wirtualnych napędów; - wirtualną konsolę z dostępem do myszy, klawiatury; - wsparcie dla IPv6; - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; - integracja z Active Directory; - możliwość obsługi przez dwóch administratorów jednocześnie; - wsparcie dla automatycznej rejestracji DNS; - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.

- możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
- możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera

oraz z możliwością rozszerzenia funkcjonalności o:

- Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej
- Przesyłanie danych telemetrycznych w czasie rzeczywistym
- Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze
- Automatyczna rejestracja certyfikatów (ACE)

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.
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 według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnienie wymogu. - 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, 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 na okres 5 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:
 - Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
 - 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.
 - 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.
- Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
- 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.
- Możliwość rozszerzenia gwarancji producenta do 7 lat.

Wdrożenie usługi kolektowania logów sieciowych – na serwerze typ 1**I. Przedmiot zamówienia:**

1. Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja rozwiązania do centralnego zbierania, przechowywania i analizy logów z urządzeń i systemów informatycznych w infrastrukturze Zamawiającego. Rozwiązanie ma umożliwiać monitorowanie, analizę i raportowanie zdarzeń w czasie rzeczywistym oraz przechowywanie logów zgodnie z wymogami prawnymi i regulacyjnymi.
2. Wykonawca dostarczy licencje na oprogramowanie niezbędne do działania systemu, umożliwiające pełne wykorzystanie funkcjonalności opisanych w niniejszym dokumencie. Licencje muszą być ważne przez co najmniej 24 miesiące od momentu wdrożenia rozwiązania.

II. Wymagania techniczne dotyczące rozwiązania

1. Rozwiązanie powinno działać na systemie operacyjnym na licencji Open Source.
2. System centralnego składowania dzienników zdarzeń powinien być zainstalowany na fizycznym serwerze będącym na wyposażeniu Zamawiającego, ~~wirtualnej maszynie w środowisku Vmware lub wirtualnej maszynie w środowisku Hyper-V.~~
3. System powinien być oparty na komponentach z licencjonowaniem Open Source.
4. Zamawiający przeznaczy na potrzeby rozwiązania sprzętowego maszynę wirtualną ~~lub serwer fizyczny~~ o następujących parametrach:
 - Procesor (CPU): 8 rdzeni,
 - Pamięć RAM: 16 GB,
 - Dysk twardy (HDD): 2 TB.
5. System powinien umożliwiać tworzenie użytkowników za pomocą zewnętrznego źródła tożsamości (Active Directory) lub ręczne definiowanie kont w samym rozwiązaniu.
6. System powinien umożliwiać zdefiniowanie i skonfigurowanie dowolnej liczby źródeł danych, takich jak Syslog UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Powinna być dostępna opcja definiowania dowolnych portów komunikacji.
7. System powinien umożliwiać ekstrakcję fragmentów wpisów logów, które mogą być używane do filtrowania danych, tworzenia zapytań dla powiadomień i alertów, oraz budowania widoków w interfejsach.
8. System powinien umożliwiać tworzenie widoków w formie interfejsów, które mogą być udostępniane w trybie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV lub w dowolnej przeglądarce WWW.
9. System powinien pozwalać na tworzenie powiadomień (alertów) opartych na regułach uwzględniających napływające dane z dzienników systemowych.
10. System powinien umożliwiać tworzenie paczek, które będą składać się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe oraz interfejsów.

III. Wdrożenie systemu

1. Wykonawca przeprowadzi instalację oraz pełną konfigurację systemu do zbierania logów, zapewniając jego optymalne działanie zgodnie z wymaganiami Zamawiającego.
2. Wykonawca zobowiązuje się do przeprowadzenia integracji systemu z istniejącymi urządzeniami oraz systemami Zamawiającego, takimi jak serwery, urządzenia sieciowe, stacje robocze oraz inne systemy, które generują logi.
3. Wykonawca zainstaluje system operacyjny na wybranym przez Zamawiającego ~~serwerze fizycznym lub~~ maszynie wirtualnej.
4. Wykonawca zweryfikuje źródła czasu na urządzeniach i systemach wysyłających logi do systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie posiadają wspólnego zegara czasu, Wykonawca zaproponuje rozwiązanie uspinające zegary czasów w sieci Zamawiającego.
5. Wykonawca przeprowadzi instalację oraz wstępną konfigurację systemu, w tym konfigurację polityki dostępu dla pracowników zespołu IT Zamawiającego.

6. System zostanie skonfigurowany pod kątem retencji przechowywania danych zgodnie z przepisami prawnymi oraz dobrymi praktykami.
7. Wykonawca skonfiguruje urządzenia i systemy w sieci Zamawiającego do wysyłania dzienników zdarzeń (logów) do centralnego systemu składowania dzienników zdarzeń. Prace obejmą co najmniej:
 - 2 urządzenia klasy UTM firmy Fortinet,
 - 5 przełączników zarządzalnych firmy Fortinet,
 - 4 serwery Windows,
 - 80 stacji roboczych Windows 10 i 11,
 - 1 aplikację centralnego zarządzania ESET Endpoint Security,
 - 4 serwery wirtualizacji Hyper-V,
8. Definiowanie portów nasłuchu: System zostanie skonfigurowany w sposób umożliwiający segmentację nasłuchu logów, aby odseparować dane napływające z różnych typów urządzeń i systemów.
9. Analiza logów i konfiguracja ekstraktorów: Wykonawca przeprowadzi wstępną analizę napływających logów i skonfiguruje ekstraktory, które będą wydzielać wybrane segmenty danych.
10. Wykonawca skonfiguruje interfejsy prezentujące dane w postaci tabelarycznej lub graficznej oraz zautomatyzuje analizę napływających logów.
11. Wykonawca skonfiguruje mechanizmy powiadamiania oraz alertowania oparte na analizie logów.
12. System zostanie skonfigurowany do wysyłania powiadomień poprzez email lub Microsoft Teams w przypadku wykrycia niepokojących sytuacji.
13. Wykonawca przeprowadzi szkolenie dla pracowników Zamawiającego z obsługi wdrożonego systemu, w zakresie obsługi nowego systemu, w tym zarządzania logami, tworzenia raportów, obsługi interfejsów oraz zarządzania alertami
14. Po zakończeniu wdrożenia, Wykonawca przeprowadzi testy systemu w obecności Zamawiającego w celu potwierdzenia spełnienia wszystkich wymagań określonych w zamówieniu. Odbiór końcowy nastąpi po pozytywnym zakończeniu testów.

Punkt 2 Serwer typ 2 o poniższej charakterystyce:

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 2U z możliwością instalacji min. 8 dysków 3.5" • Obudowa wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 32 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się min. 16 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.

Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych
Procesor	Zainstalowany jeden procesor 16-rdzeniowe, min. 2.8 GHz (częstotliwość bazowa), klasy x86, dedykowany do pracy z zaoferowanym serwerem, umożliwiające osiągnięcie wyniku min. 333 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocessorowej.
RAM	Minimum 256 GB DDR5 RDIMM 5600MT/s,
Gniazda PCI	Min. dwa sloty PCIe, w tym min. jeden x16
Kontroler RAID	- Sprzętowy kontroler dyskowy, posiadający - Min. 8 GB nieulotnej pamięci cache, - Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. - Wsparcie dla dysków samoszyfrujących
Dyski twarde	- Zainstalowane: 3 x dysk SSD SATA o pojemności min. 1.92 TB, 6Gb, 2,5" Hot-Plug, 1 DWPD. 3 x dysk HDD SATA o pojemności min. 12 TB, 6Gb, 7.2 tys. obr./min., 3,5" Hot-Plug. - Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
Wbudowane porty	4 porty USB w tym min: 1 port USB 3.0 z tyłu obudowy, 1 port micro USB z przodu obudowy 2 port VGA z czego jeden z przodu obudowy
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne, Hot-Plug
Zasilacze	Redundantne, Hot-Plug min. 1100W klasy Titanium

Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
System operacyjny/dodatkové oprogramowanie	Fabrycznie zainstalowany Windows Server 2025 Standard, licencja pokrywająca wszystkie fizyczne rdzenie w serwerze
Bezpieczeństwo	- Zatrask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardech. - 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).
Karta Zarządzania	- Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; - możliwość podmontowania zdalnych wirtualnych napędów; - wirtualną konsolę z dostępem do myszy, klawiatury; - wsparcie dla IPv6; - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; - integracja z Active Directory; - możliwość obsługi przez dwóch administratorów jednocześnie; - wsparcie dla automatycznej rejestracji DNS; - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.

- możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
- możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera

oraz z możliwością rozszerzenia funkcjonalności o:

- Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej
- Przesyłanie danych telemetrycznych w czasie rzeczywistym
- Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze
- Automatyczna rejestracja certyfikatów (ACE)

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 modułarnych oraz przetworników 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.
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 według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnienie wymogu. - 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, 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 na okres 5 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:
 - Możliwość utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
 - 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.
 - 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 przekaze 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.
- Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
- 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.
- Możliwość rozszerzenia gwarancji producenta do 7 lat.

Dodatkowe licencje:

- Powyższe dwa serwery (typ 1 i typ 2) muszą zostać dostarczone z nowymi licencjami CAL dostarczonymi przez producenta oferowanych serwerów - łącznie 95 licencji na użytkownika Windows Server 2025 (Windows Server 2025 User CAL)

Punkt 3. Serwer typ 3 o poniższej charakterystyce:

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	- Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3.5" - Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Płyta główna	- Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. - Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych
Procesor	Jeden procesor 8-rdzeniowy, min. 2.7 GHz (częstotliwość bazowa), min. 24 MB pamięci podręcznej.
Pamięć RAM	64 GB pamięci RAM DDR5 UDIMM o częstotliwości pracy 5600MT/s.
Kontroler RAID	- Sprzętowy kontroler dyskowy, posiadający - Możliwość konfiguracji poziomów RAID: 0, 1, 10.
Dyski twarde	- Zainstalowane 2 x dysk SSD SATA o pojemności min. 960 GB, 6Gb, 2,5" Hot-Plug, 1 DWPD. 2 x dysk HDD SATA o pojemności min. 8 TB, 6Gb, 7.2 tys. obr./min., 3,5" Hot-Plug. - Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.

Sloty PCIe	Min. dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
Wbudowane porty	- min. 4 porty USB w tym min: 1 port USB 3.0 z tyłu obudowy, 1 port micro USB z przodu obudowy 1 port VGA na tylnym panelu, 1 port RS232
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Zasilacze	Redundantne, o mocy maks. 700W klasy Titanium
Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
System operacyjny/dodatkowe oprogramowanie	- Fabrycznie zainstalowany Windows Server 2025 Standard - Wraz z serwerem zamawiający wymaga dostarczenia łącznie 35 licencji CAL na użytkowników dostarczonych przez producenta serwera
Bezpieczeństwo	- Zatrzaśk 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. - Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. - Moduł TPM 2.0 - 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).
Karta Zarządzania	- Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;

- możliwość podmontowania zdalnych wirtualnych napędów;
 - wirtualną konsolę z dostępem do myszy, klawiatury;
 - wsparcie dla IPv6;
 - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
 - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
 - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
 - integracja z Active Directory;
 - możliwość obsługi przez dwóch administratorów jednocześnie;
 - wsparcie dla automatycznej rejestracji DNS
 - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
 - możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
 - możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
- oraz z możliwością rozszerzenia funkcjonalności o:
- Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej
 - Przesyłanie danych telemetrycznych w czasie rzeczywistym
 - Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze
 - Automatyczna rejestracja certyfikatów (ACE)

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.

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 według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnienie wymogu.**
- 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, 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 na okres 5 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 wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: ○ Możliwości utworzenia zgłoszenia serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. ○ 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. ○ 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 wystanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.

- Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
- 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.
- Możliwość rozszerzenia gwarancji producenta do 7 lat.

Wdrożenie usługi kolektowania logów sieciowych – na serwerze typ 3

II. Przedmiot zamówienia:

1. Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja rozwiązania do centralnego zbierania, przechowywania i analizy logów z urządzeń i systemów informatycznych w infrastrukturze Zamawiającego. Rozwiązanie ma umożliwiać monitorowanie, analizę i raportowanie zdarzeń w czasie rzeczywistym oraz przechowywanie logów zgodnie z wymogami prawnymi i regulacyjnymi.
2. Wykonawca dostarczy licencje na oprogramowanie niezbędne do działania systemu, umożliwiające pełne wykorzystanie funkcjonalności opisanych w niniejszym dokumencie. Licencje muszą być ważne przez co najmniej 24 miesiące od momentu wdrożenia rozwiązania.

V. Wymagania techniczne dotyczące rozwiązania

1. Rozwiązanie powinno działać na systemie operacyjnym na licencji Open Source.
2. System centralnego składowania dzienników zdarzeń powinien być zainstalowany na fizycznym serwerze będącym na wyposażeniu Zamawiającego, ~~wirtualnej maszynie w środowisku VMware lub wirtualnej maszynie w środowisku Hyper-V.~~
3. System powinien być oparty na komponentach z licencjonowaniem Open Source.
4. Zamawiający przeznaczy na potrzeby rozwiązania sprzętowego maszynę wirtualną ~~lub serwer fizyczny~~ o następujących parametrach:
 - Procesor (CPU): 8 rdzeni,
 - Pamięć RAM: 16 GB,
 - Dysk twardy (HDD): 2 TB.
5. System powinien umożliwiać tworzenie użytkowników za pomocą zewnętrznego źródła tożsamości (Active Directory) lub ręczne definiowanie kont w samym rozwiązaniu.
6. System powinien umożliwiać zdefiniowanie i skonfigurowanie dowolnej liczby źródeł danych, takich jak Syslog UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Powinna być dostępna opcja definiowania dowolnych portów komunikacji.
7. System powinien umożliwiać ekstrakcję fragmentów wpisów logów, które mogą być używane do filtrowania danych, tworzenia zapytań dla powiadomień i alertów, oraz budowania widoków w interfejsach.
8. System powinien umożliwiać tworzenie widoków w formie interfejsów, które mogą być udostępniane w trybie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV lub w dowolnej przeglądarce WWW.
9. System powinien pozwalać na tworzenie powiadomień (alertów) opartych na regułach uwzględniających napływające dane z dzienników systemowych.
10. System powinien umożliwiać tworzenie paczek, które będą składać się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe oraz interfejsów.

VI. Wdrożenie systemu

1. Wykonawca przeprowadzi instalację oraz pełną konfigurację systemu do zbierania logów, zapewniając jego optymalne działanie zgodnie z wymaganiami Zamawiającego.
2. Wykonawca zobowiązuje się do przeprowadzenia integracji systemu z istniejącymi urządzeniami oraz systemami Zamawiającego, takimi jak serwery, urządzenia sieciowe, stacje robocze oraz inne systemy, które generują logi.
3. Wykonawca zainstaluje system operacyjny na wybranym przez Zamawiającego ~~serwerze fizycznym lub~~ maszynie wirtualnej.
4. Wykonawca zweryfikuje źródła czasu na urządzeniach i systemach wysyłających logi do systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie posiadają wspólnego zegara czasu, Wykonawca zaproponuje rozwiązanie uspołniające zegary czasów w sieci Zamawiającego.
5. Wykonawca przeprowadzi instalację oraz wstępną konfigurację systemu, w tym konfigurację polityki dostępu dla pracowników zespołu IT Zamawiającego.
6. System zostanie skonfigurowany pod kątem retencji przechowywania danych zgodnie z przepisami prawnymi oraz dobrymi praktykami.
7. Wykonawca skonfiguruje urządzenia i systemy w sieci Zamawiającego do wysyłania dzienników zdarzeń (logów) do centralnego systemu składowania dzienników zdarzeń. Prace obejmą co najmniej:
 - 1 urządzenie klasy UTM firmy Fortinet,
 - 1 przełącznik zarządzalny firmy Fortinet,
 - 2 serwery Windows,
 - 30 stacji roboczych Windows 10 i 11,
 - 1 aplikację centralnego zarządzania ESET Endpoint Security,
 - 1 serwer wirtualizacji Hyper-V,
8. Definiowanie portów nasłuchu: System zostanie skonfigurowany w sposób umożliwiający segmentację nasłuchu logów, aby odseparować dane napływające z różnych typów urządzeń i systemów.
9. Analiza logów i konfiguracja ekstraktorów: Wykonawca przeprowadzi wstępną analizę napływających logów i skonfiguruje ekstraktory, które będą wydzielać wybrane segmenty danych.
10. Wykonawca skonfiguruje interfejsy prezentujące dane w postaci tabelarycznej lub graficznej oraz zautomatyzuje analizę napływających logów.
11. Wykonawca skonfiguruje mechanizmy powiadamiania oraz alertowania oparte na analizie logów.
12. System zostanie skonfigurowany do wysyłania powiadomień poprzez email lub Microsoft Teams w przypadku wykrycia niepokojących sytuacji.
13. Wykonawca przeprowadzi szkolenie dla pracowników Zamawiającego z obsługi wdrożonego systemu, w zakresie obsługi nowego systemu, w tym zarządzania logami, tworzenia raportów, obsługi interfejsów oraz zarządzania alertami
14. Po zakończeniu wdrożenia, Wykonawca przeprowadzi testy systemu w obecności Zamawiającego w celu potwierdzenia spełnienia wszystkich wymagań określonych w zamówieniu. Odbiór końcowy nastąpi po pozytywnym zakończeniu testów.

Punkt 4 Serwer typ 4 o poniższej charakterystyce:

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	- Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3.5" - Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Płyta główna	- Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. - Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych
Procesor	Jeden procesor 8-rdzeniowy, min. 2.7 GHz (częstotliwość bazowa), min. 24 MB pamięci podręcznej.
Pamięć RAM	32 GB pamięci RAM DDR5 UDIMM o częstotliwości pracy 5600MT/s.
Kontroler RAID	- Sprzętowy kontroler dyskowy, posiadający - Możliwość konfiguracji poziomów RAID: 0, 1, 10.
Dyski twarde	- Zainstalowane 2 x dysk SSD SATA o pojemności min. 960 GB, 6Gb, 2,5" Hot-Plug, 1 DWPD. 2 x dysk HDD SATA o pojemności min. 8 TB, 6Gb, 7.2 tys. obr./min., 3,5" Hot-Plug. - Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Sloty PCIe	Min. dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
Wbudowane porty	- min. 4 porty USB w tym min: 1 port USB 3.0 z tyłu obudowy, 1 port micro USB z przodu obudowy 1 port VGA na tylnym panelu,

	1 port RS232
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Zasilacze	Redundantne, o mocy maks. 700W klasy Titanium
Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
System operacyjny/dodatkowe oprogramowanie	- Fabrycznie zainstalowany Windows Server 2025 Standard - Wraz z serwerem zamawiający wymaga dostarczenia łącznie 20 licencji CAL na użytkowników dostarczonych przez producenta serwera
Bezpieczeństwo	- Zatrask 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. - Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. - Moduł TPM 2.0 - 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).
Karta Zarządzania	- Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; - możliwość podmontowania zdalnych wirtualnych napędów; - wirtualną konsolę z dostępem do myszy, klawiatury; - wsparcie dla IPv6; - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; - integracja z Active Directory; - możliwość obsługi przez dwóch administratorów jednocześnie; - wsparcie dla automatycznej rejestracji DNS - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.

- o możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
- o możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera

oraz z możliwością rozszerzenia funkcjonalności o:

- o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej
- o Przesyłanie danych telemetrycznych w czasie rzeczywistym
- o Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze
- o Automatyczna rejestracja certyfikatów (ACE)

Oprogramowanie do zarządzania

- Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:
 - o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
 - o integracja z Active Directory
 - o Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
 - o Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
 - o Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
 - o Szczegółowy opis wykrytych systemów oraz ich komponentów
 - o Możliwość eksportu raportu do CSV, HTML, XLS, PDF
 - o Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
 - o Grupowanie urządzeń w oparciu o kryteria użytkownika
 - o Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
 - o Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
 - o Szybki podgląd stanu środowiska
 - o Podsumowanie stanu dla każdego urządzenia
 - o Szczegółowy status urządzenia/elementu/komponentu
 - o Generowanie alertów przy zmianie stanu urządzenia.
 - o Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
 - o Integracja z service desk producenta dostarczonej platformy sprzętowej
 - o Możliwość przejęcia zdalnego pulpitu
 - o Możliwość podmontowania wirtualnego napędu
 - o Kreator umożliwiający dostosowanie akcji dla wybranych alertów
 - o Możliwość importu plików MIB
 - o Przesyłanie alertów „as-is” do innych konsol firm trzecich
 - o Możliwość definiowania ról administratorów
 - o Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
 - o Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
 - o Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
 - o Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
 - o 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 modułowych 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.
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 według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnienie wymogu. - 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, 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 na okres 5 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 wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
- Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
 - Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
 - 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.
 - 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.
- Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
- 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.
- Możliwość rozszerzenia gwarancji producenta do 7 lat.

Wdrożenie usługi kolektowania logów sieciowych – na serwerze typ 4

III. Przedmiot zamówienia:

1. Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja rozwiązania do centralnego zbierania, przechowywania i analizy logów z urządzeń i systemów informatycznych w infrastrukturze Zamawiającego. Rozwiązanie ma umożliwiać monitorowanie, analizę i raportowanie zdarzeń w czasie rzeczywistym oraz przechowywanie logów zgodnie z wymogami prawnymi i regulacyjnymi.
2. Wykonawca dostarczy licencje na oprogramowanie niezbędne do działania systemu, umożliwiające pełne wykorzystanie funkcjonalności opisanych w niniejszym dokumencie. Licencje muszą być ważne przez co najmniej 24 miesiące od momentu wdrożenia rozwiązania.

VIII. Wymagania techniczne dotyczące rozwiązania

1. Rozwiązanie powinno działać na systemie operacyjnym na licencji Open Source.
2. System centralnego składowania dzienników zdarzeń powinien być zainstalowany na fizycznym serwerze będącym na wyposażeniu Zamawiającego, ~~wirtualnej maszynie w środowisku Vmware lub wirtualnej maszynie w środowisku Hyper-V.~~
3. System powinien być oparty na komponentach z licencjonowaniem Open Source.
4. Zamawiający przeznaczy na potrzeby rozwiązania sprzętowego maszynę wirtualną ~~lub serwer fizyczny~~ o następujących parametrach:
 - Procesor (CPU): 8 rdzeni,
 - Pamięć RAM: 16 GB,
 - Dysk twardy (HDD): 2 TB.
5. System powinien umożliwiać tworzenie użytkowników za pomocą zewnętrznego źródła tożsamości (Active Directory) lub ręczne definiowanie kont w samym rozwiązaniu.
6. System powinien umożliwiać zdefiniowanie i skonfigurowanie dowolnej liczby źródeł danych, takich jak Syslog UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Powinna być dostępna opcja definiowania dowolnych portów komunikacji.
7. System powinien umożliwiać ekstrakcję fragmentów wpisów logów, które mogą być używane do filtrowania danych, tworzenia zapytań dla powiadomień i alertów, oraz budowania widoków w interfejsach.
8. System powinien umożliwiać tworzenie widoków w formie interfejsów, które mogą być udostępniane w trybie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV lub w dowolnej przeglądarce WWW.
9. System powinien pozwalać na tworzenie powiadomień (alertów) opartych na regułach uwzględniających napływające dane z dzienników systemowych.
10. System powinien umożliwiać tworzenie paczek, które będą składać się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe oraz interfejsów.

IX. Wdrożenie systemu

1. Wykonawca przeprowadzi instalację oraz pełną konfigurację systemu do zbierania logów, zapewniając jego optymalne działanie zgodnie z wymaganiami Zamawiającego.
2. Wykonawca zobowiązuje się do przeprowadzenia integracji systemu z istniejącymi urządzeniami oraz systemami Zamawiającego, takimi jak serwery, urządzenia sieciowe, stacje robocze oraz inne systemy, które generują logi.
3. Wykonawca zainstaluje system operacyjny na wybranym przez Zamawiającego ~~serwerze fizycznym lub maszynie wirtualnej.~~
4. Wykonawca zweryfikuje źródła czasu na urządzeniach i systemach wysyłających logi do systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie posiadają wspólnego zegara czasu, Wykonawca zaproponuje rozwiązanie uspinające zegary czasów w sieci Zamawiającego.
5. Wykonawca przeprowadzi instalację oraz wstępną konfigurację systemu, w tym konfigurację polityki dostępu dla pracowników zespołu IT Zamawiającego.
6. System zostanie skonfigurowany pod kątem retencji przechowywania danych zgodnie z przepisami prawnymi oraz dobrymi praktykami.
7. Wykonawca skonfiguruje urządzenia i systemy w sieci Zamawiającego do wysyłania dzienników zdarzeń (logów) do centralnego systemu składowania dzienników zdarzeń. Prace obejmą co najmniej:
 - 1 urządzenie klasy UTM firmy Fortinet,

- 1 przełącznik zarządczy firmy Fortinet,
 - 1 serwer Windows,
 - 15 stacji roboczych Windows 10 i 11,
 - 1 aplikację centralnego zarządzania ESET Endpoint Security,
 - 1 serwer wirtualizacji Hyper-V,
8. Definiowanie portów nasłuchu: System zostanie skonfigurowany w sposób umożliwiający segmentację nasłuchu logów, aby odseparować dane napływające z różnych typów urządzeń i systemów.
 9. Analiza logów i konfiguracja ekstraktorów: Wykonawca przeprowadzi wstępną analizę napływających logów i skonfiguruje ekstraktory, które będą wydzielać wybrane segmenty danych.
 10. Wykonawca skonfiguruje interfejsy prezentujące dane w postaci tabelarycznej lub graficznej oraz zautomatyzuje analizę napływających logów.
 11. Wykonawca skonfiguruje mechanizmy powiadamiania oraz alertowania oparte na analizie logów.
 12. System zostanie skonfigurowany do wysyłania powiadomień poprzez email lub Microsoft Teams w przypadku wykrycia niepokojących sytuacji.
 13. Wykonawca przeprowadzi szkolenie dla pracowników Zamawiającego z obsługi wdrożonego systemu, w zakresie obsługi nowego systemu, w tym zarządzania logami, tworzenia raportów, obsługi interfejsów oraz zarządzania alertami
 14. Po zakończeniu wdrożenia, Wykonawca przeprowadzi testy systemu w obecności Zamawiającego w celu potwierdzenia spełnienia wszystkich wymagań określonych w zamówieniu. Odbiór końcowy nastąpi po pozytywnym zakończeniu testów.

6. Montaż, konfiguracja, uruchomienie:

- Usługa wdrożenia musi obejmować montaż i uruchomienie oferowanego sprzętu w siedzibie zamawiającego (serwery typ 1 i typ 2) oraz dwóch jednostkach podległych (serwery typ 3 i typ 4),
 - Na wszystkich oferowanych urządzeniach musi zostać przeprowadzona aktualizacja firmware'u. Urządzenia zostaną skonfigurowane zgodnie z najlepszymi praktykami i wytycznymi zamawiającego, a na serwerach zainstalowane zostanie oprogramowanie do wirtualizacji (Windows Server Hyper-V).
 - Przy wykorzystaniu zaoferowanych licencji Microsoft muszą zostać utworzone dwie nowe maszyny wirtualne z systemem Windows Server 2025 Standard na serwerze typ 1,
 - Wykonawca dokona migracji domeny z obecnego serwera (maszyna wirtualna z systemem Windows Server 2019 Standard) na jedną z wcześniej utworzonych maszyn wirtualnych na serwerze typ 1,
 - Wykonawca skonfiguruje replikację asynchroniczną maszyn wirtualnych pomiędzy serwerem typ 1, a serwerem typ 2, aby zwiększyć odporność na awarie systemów,
-
- Przy wykorzystaniu zaoferowanych licencji Microsoft wykonawca utworzy na serwerach typ 3 oraz typ 4 po dwie nowe maszyny wirtualne z systemem Windows Server 2025,
 - Wykonawca na każdym z tych serwerów (na wybranych maszynach wirtualnych) uruchomi usługi kontrolera domeny wraz z usługami wymaganymi do ich prawidłowego działania,

- Wykonawca musi utworzyć konta dla wszystkich użytkowników (maksymalnie 35 kont dla serwera typ 3 oraz maksymalnie 20 dla serwera typ 4) oraz skonfigurować podstawową politykę domenową z uwzględnieniem wytycznych zamawiającego,
- W każdej z dwóch jednostek podległych (serwer typ 3 i typ 4) wybrane pięć komputerów zamawiającego z systemem w wersji Professional zostanie przez wykonawcę podłączone do domeny, a na każdym z tych komputerów przeprowadzona zostanie migracja profilu lokalnego do domenowego połączona z konfiguracją dla wybranych urządzeń profili mobilnych.
- Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00).
- Podczas wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonych systemów.

WZÓR UMOWY

UMOWA Nr

zawarta w Brześciu Kujawskim pomiędzy:

....., z siedzibą w, reprezentowaną przez:

..... - p.

przy kontrasygnacie Skarbnika – p.

NIP:

zwaną dalej „**Zamawiającym**”

a

.....,

z siedzibą w,

reprezentowanym/ą przez:

..... –

zwanym dalej „**Wykonawcą**”

o następującej treści:

PREAMBUŁA

- 1) Zgodnie z wynikiem przeprowadzenia postępowania przetargowego o nr rozstrzygniętego w dniu na realizację zadania pn.: „.....” w ramach umowy nr FERC..... „Cyberbezpieczny Samorząd”.
- 2) Zamawiający informuje, iż zamówienie dofinansowywane jest ze środków zewnętrznych Unii Europejskiej: Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC).

§ 1 PRZEDMIOT ZAMÓWIENIA

- 1) Przedmiotem umowy jest
 - a) Dostawa 2 urządzeń UTM wraz z licencjami i wsparciem dla Urzędu Miejskiego w Brześciu Kujawskim;
 - b) Dostawa licencji urządzeń klasy UTM na okres 6 miesięcy;
 - c) Dostawa 3 urządzeń sieciowych zarządzalnych w warstwie L2 L3 48p;
 - d) Dostawa 4 urządzeń sieciowych zarządzalnych w warstwie L2 L3 24p;
 - e) Dostawa 11 urządzeń sieciowych zarządzalnych w warstwie L2 L3 8p;
 - f) Dostawa 8 urządzeń zarządzalnych do sieci bezprzewodowej wraz z konfiguracją kontrolera;
 - g) Wdrożenie polityk Port Security - DHCP Snooping, VLAN, DNS Spoofing;

na potrzeby projektu pn.: „Cyberbezpieczny Samorząd”. w ramach realizacji projektu grantowego Cyberbezpieczny Samorząd, zwanych dalej: „sprzętem” lub „produktem”, spełniających warunki (parametry) techniczne określone w załączniku nr do SWZ i w ofercie Wykonawcy, stanowiących integralną część niniejszej umowy. Przedmiot umowy został określony w załączniku nr do SWZ – Opis przedmiotu zamówienia.

- 2) Wykonawca zobowiązuje się dostarczyć sprzęt fabrycznie nowy, nie pochodzący z wystawy lub z ekspozycji, kompletny, wraz z niezbędnymi do działania przewodami, z odpowiednim oprogramowaniem, posiadający wymagane prawem atesty i certyfikaty oraz gotowy do pracy.
- 3) Wykonawca zobowiązany jest do naprawiania wszelkich szkód powstałych w trakcie realizacji inwestycji z winy Wykonawcy.
- 4) Przedmiot umowy obejmuje również montaż (instalację), konfigurację sprzętu, wdrożenie oraz szkolenie dla pracowników.
- 5) Dostarczony sprzęt i oprogramowanie pochodzić będzie z oficjalnych kanałów dystrybucyjnych producenta obejmujących również rynek Unii Europejskiej, zapewniających w szczególności realizację uprawnień gwarancyjnych.

§ 2 OBOWIĄZKI WYKONAWCY

Wykonawca jest zobowiązany do:

- 1) Dostawy urządzeń wraz z usługą konfiguracji do Urzędu Miejskiego w Brześciu Kujawskim, pl. Władysława Łokietka 1, 87-880 Brześć Kujawski, w godzinach urzędowania Zamawiającego;

- 2) Skonfigurowania polityk Port Security - DHCP Snooping, VLAN, DNS Spoofing w godzinach urzędowania Zamawiającego;
- 3) Dostarczenia sprzętu wraz:
 - a) kartami gwarancyjnymi, instrukcjami obsługi oraz innymi dokumentami niezbędnymi do przejęcia sprzętu do używania,
 - b) ze wszystkimi akcesoriami stanowiącymi komplet sprzedażowy;
 - c) uruchomienia sprzętu i badania wykonanej instalacji;
 - d) zawiadomienia przedstawiciela Zamawiającego o planowanym terminie dostawy sprzętu, nie później niż na 3 dni przed tym terminem;
 - e) uzgodnienia z przedstawicielem Zamawiającego terminu dostawy sprzętu,
 - f) montażu (instalacji) i konfiguracji sprzętu i wdrożenia;
 - g) przygotowania protokołu odbioru, stanowiącego podstawę odbioru;
 - h) przeszkolenia wyznaczonych pracowników z obsługi sprzętu,
 - i) współpracy z Zamawiającym w trakcie realizacji umowy, a w szczególności udzielania wszelkich niezbędnych wyjaśnień i informacji dotyczących przedmiotu umowy na każde żądanie Zamawiającego lub osoby wskazanej przez Zamawiającego.

Wykonawca odpowiada za dostarczony sprzęt w czasie transportu. W przypadku uszkodzenia ponosi pełną odpowiedzialność za powstałe szkody.

§ 3 TERMIN REALIZACJI

- 1) Wykonawca jest zobowiązany do dostarczenia przedmiotów zamówienia w terminie do roku.
- 2) Za dzień wykonania umowy przez Wykonawcę uważa się dzień, w którym podpisany zostanie przez obie strony umowy protokół zdawczo - odbiorczy (protokół odbioru) sprzętu – bez uwag.
- 3) Protokół odbioru będzie obejmował nazwy, ilości oraz wartość dostarczonego sprzętu.
- 4) Prawo własności sprzętu, o którym mowa w § 1 przechodzi na Zamawiającego z dniem podpisania protokołu odbioru, o którym mowa w ust. 2.
- 5) W przypadku stwierdzenia, że dostarczony sprzęt:
 - a) jest niezgodny z opisem zawartym w Opisie przedmiotu zamówienia (OPZ), lub jest niekompletny,
 - b) posiada ślady użytkowania lub zewnętrznego uszkodzenia, są uszkodzone, posiadają wady uniemożliwiające użytkowanie, a wady i uszkodzenia te nie powstały z winy Zamawiającego,

- 6) Zamawiający odmówi odbioru części lub całości sprzętu, sporządzając protokół zawierający przyczyny odmowy odbioru (protokół rozbieżności). Zamawiający wyznaczy następnie termin (nie dłuższy niż 7 dni) dostawy oprogramowania fabrycznie nowego, wolnego od wad. Procedura czynności odbioru zostanie powtórzona.
- 7) Wyznaczenie Wykonawcy terminu określonego w ust. 5 nie zwalnia Wykonawcy z odpowiedzialności za nieterminowe wykonanie niniejszej umowy, w szczególności ze zobowiązania do zapłaty kar umownych z tego tytułu przewidzianych w § 9 niniejszej umowy.

§ 4 WYNAGRODZENIE I ROZLICZENIE PRZEDMIOTU UMOWY

- 1) Wynagrodzenie Wykonawcy za wykonanie przedmiotu umowy wynosi:
 - a) Dostawa 2 urządzeń UTM wraz z licencjami i wsparciem dla Urzędu Miejskiego w Brześciu Kujawskim - zł netto, stawka VAT...%, cena brutto zł.
 - b) Dostawa licencji urządzeń klasy UTM na okres 6 miesięcy- zł netto, stawka VAT...%, cena brutto zł.
 - c) Dostawa 3 urządzeń sieciowych zarządzalnych w warstwie L2 L3 48p- zł netto, stawka VAT...%, cena brutto zł.
 - d) Dostawa 4 urządzeń sieciowych zarządzalnych w warstwie L2 L3 24p- zł netto, stawka VAT...%, cena brutto zł.
 - e) Dostawa 11 urządzeń sieciowych zarządzalnych w warstwie L2 L3 8p- zł netto, stawka VAT...%, cena brutto zł.
 - f) Dostawa 8 urządzeń zarządzalnych do sieci bezprzewodowej wraz z konfiguracją kontrolera- zł netto, stawka VAT...%, cena brutto zł.
 - g) Wdrożenie polityk Port Security - DHCP Snooping, VLAN, DNS Spoofing- zł netto, stawka VAT...%, cena brutto zł.
- 2) Wynagrodzenie za przedmiot umowy obejmuje wszystkie koszty związane poniesione przez Wykonawcę, niezbędne do zrealizowania przedmiotu umowy. Oznacza to, że cena zawiera wszystkie koszty związane z realizacją dostawy i świadczeniem przez Wykonawcę usług objętych umową wynikających wprost z umowy, jak również nie ujęte w jej treści, a niezbędne do jej prawidłowego wykonania. tj. podatek VAT, wszelkie prace przygotowawcze, koszty transportu, itp.
- 3) Podstawą rozliczeń finansowych między Wykonawcą a Zamawiającym będzie faktura VAT wystawiona po wykonaniu całości przedmiotu umowy oraz po sporządzeniu i podpisaniu przez obie strony umowy protokołu zdawczo – odbiorczego (protokołu odbioru) – bez uwag.

- 4) Zapłata wynagrodzenia nastąpi w terminie 30 dni od dnia doręczenia Zamawiającemu faktury.
- 5) Za datę zapłaty przyjmuje się datę obciążenia rachunku bankowego Zamawiającego.
- 6) Faktura ma być wystawiona na:
Nabywca:, NIP:
Odbiorca:, NIP:
- 7) W przypadku powierzenia wykonania części zamówienia podwykonawcom lub dalszym podwykonawcom wraz z fakturą, Wykonawca przedstawi pisemny wykaz podwykonawców z ich udziałem finansowym i rzeczowym oraz dowody zapłaty wymagalnego wynagrodzenia podwykonawcom i dalszym podwykonawcom w zakresie wszelkich zobowiązań wynikających z udziału podwykonawcy i dalszego podwykonawcy w realizacji części zamówienia objętego fakturą. Brak potwierdzenia zapłaty wynagrodzenia podwykonawcom lub dalszym podwykonawcom wstrzymuje dokonanie zapłaty faktury. W przypadku gdy wykonawca realizuje zamówienia bez udziału podwykonawców do faktury Wykonawca przedłoży stosowne oświadczenie potwierdzające samodzielną realizację zamówienia.
- 8) Zamawiający wyraża zgodę na przekazanie faktur VAT drogą elektroniczną na wskazany adres e-mail:

§ 5 PODWYKONAWCY

- 1) Wykonawca może powierzyć wykonanie części zamówienia będącego przedmiotem niniejszej umowy podwykonawcom.
- 2) Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia.
- 3) Wykonawca ponosi pełną odpowiedzialność za część przedmiotu umowy, którą wykonuje przy pomocy podwykonawców.
- 4) Wykonawca ponosi odpowiedzialność na zasadach ogólnych za jakość i terminowość prac, które realizuje przy pomocy podwykonawców.
- 5) W przypadku powierzenia wykonania części zamówienia podwykonawcom lub dalszym podwykonawcom wraz z fakturą, Wykonawca przedstawi pisemny wykaz podwykonawców z ich udziałem finansowym i rzeczowym oraz dowody zapłaty wymagalnego wynagrodzenia podwykonawcom i dalszym podwykonawcom w zakresie wszelkich zobowiązań wynikających z udziału podwykonawcy i dalszego podwykonawcy w realizacji części zamówienia objętego fakturą. Brak potwierdzenia zapłaty wynagrodzenia podwykonawcom lub dalszym podwykonawcom

wstrzymuje dokonanie zapłaty faktury. W przypadku gdy wykonawca realizuje zamówienia bez udziału podwykonawców do faktury Wykonawca przedłoży stosowne oświadczenie potwierdzające samodzielną realizację zamówienia.

§ 6 GWARANCJA

- 1) Wykonawca udziela Zamawiającemu gwarancji na sprzęt będący przedmiotem umowy na okres 12 miesięcy.
 - a) W przypadku zakupu urządzeń zarządzalnych do sieci bezprzewodowej wraz z konfiguracją kontrolera, producent zapewnia ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy.
- 2) Okres gwarancji, o którym mowa w ust. 1 rozpoczyna się z dniem podpisania protokołu, o którym mowa w § 3 ust. 2.
- 3) Wykonawca, niezależnie od gwarancji, ponosi odpowiedzialność z tytułu rękojmi za wady fizyczne oraz wady prawne sprzętu zgodnie z kodeksem cywilnym.
- 4) Zamawiający będzie dokonywał zgłoszenia usterki na adres e-mail Wykonawcy lub telefonicznie
- 5) Wykonawca zobowiązuje się do podjęcia czynności serwisowych zgodnie z warunkami przedstawionymi w Opisie przedmiotu zamówienia.
- 6) Wykonawca zapewni bezpłatne usunięcie awarii w okresie trwania gwarancji.
- 7) Zamawiający w razie stwierdzenia w okresie gwarancji ewentualnych wad lub awarii w przedmiocie niniejszej Umowy, obowiązany jest do przedłożenia Wykonawcy, najpóźniej w ciągu 7 dni od dnia ich ujawnienia, stosowanej reklamacji.
- 8) Wykonawca zobowiązuje się w ramach gwarancji do usunięcia wad lub awarii w nieprzekraczalnym terminie 7 dni roboczych od dnia ich zgłoszenia przez Zamawiającego. Termin ten może ulec wydłużeniu do 14 dni roboczych tylko w uzasadnionych przypadkach, po uzyskaniu pisemnej zgody Zamawiającego.
- 9) W przypadku stwierdzenia wady ukrytej sprzętu Wykonawca zobowiązany jest do jego wymiany na nowy zgodnie z warunkami przedstawionymi w Opisie przedmiotu zamówienia.
- 10) Koszt dojazdu ekipy serwisowej w ramach napraw gwarancyjnych i koszt transportu sprzętu naprawianego w ramach gwarancji poza siedzibą Zamawiającego pokrywa Wykonawca.

- 11) Wykonawca ponosi wszelkie koszty związane z wykonaniem obowiązków wynikających z gwarancji.
- 12) Wykonawca zobowiązuje się do zapewnienia kontynuacji świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) w przypadku niemożności ich wypełnienia przez Wykonawcę.
- 13) Jeżeli Wykonawca w okresie gwarancji nie przystąpi do usunięcia wad lub awarii w ciągu 5 dni roboczych, Zamawiający może powierzyć ich usunięcie osobie trzeciej na koszt i ryzyko Wykonawcy oraz bez utraty gwarancji udzielonej przez Wykonawcę.
- 14) W przypadku zaistnienia w okresie gwarancji awarii sprzętu oraz konieczności przemieszczenia urządzenia w związku ze stwierdzeniem usterek, których nie można usunąć w siedzibie Zamawiającego, transportu sprzętu na własny koszt dokonuje Wykonawca.
- 15) W przypadku stwierdzenia ukrytych wad technicznych sprzętu koszty napraw pokryje Wykonawca.
- 16) Udzielona przez Wykonawcę gwarancja nie może zobowiązywać Zamawiającego do przechowywania opakowań, instrukcji bądź innych elementów dostawy, niemających wpływu na prawidłowe funkcjonowanie przedmiotu niniejszej Umowy.

§ 7 KARY UMOWNE

1. Strony postanawiają, że obowiązującą formę odszkodowania stanowią kary umowne, które będą naliczane w następujących wypadkach:
 - 1.1. Wykonawca płaci Zamawiającemu kary umowne:
 - a) 0,1% wynagrodzenia umownego netto, określonego w § 5 ust. 1 umowy, za każdy dzień zwłoki za przekroczenie terminu dostaw, o których mowa w § 3 ust. 1,
 - b) 0,05% wynagrodzenia umownego netto, określonego w § 5 ust. 1 umowy, za każdy dzień zwłoki w wykonaniu obowiązków Wykonawcy wynikających z gwarancji (m.in. zwłoka w usunięciu wad i usterek zgłoszonych w okresie gwarancji lub rękojmi);
 - c) 10% wynagrodzenia określonego w § 5 ust. 1 – w razie odstąpienia od umowy przez Wykonawcę lub przez Zamawiającego wskutek okoliczności, za które odpowiada Wykonawca.
 2. Łączna maksymalna wysokość kar umownych, których mogą dochodzić Strony nie może przekroczyć 10% wynagrodzenia netto, o którym mowa w § 5 ust. 1 umowy.
 3. Zamawiający zastrzega sobie możliwość dochodzenia odszkodowania uzupełniającego na zasadach określonych w Kodeksie cywilnym, jeżeli szkoda przewyższa wysokość kar umownych.

4. Zamawiający może naliczyć i potrącić z wynagrodzenia Wykonawcy, określonego w § 5 ust. 1 umowy, należność z tytułu kar umownych, o których mowa w ust. 1, po uprzednim wezwaniu Wykonawcy do ich zapłaty pod rygorem potrącenia, a Wykonawca wyraża na to zgodę.
5. Kary umowne płatne będą w terminie 10 dni od dnia otrzymania wezwania do zapłaty.

§ 8 SPOSÓB POROZUMIEWANIA SIĘ STRON

- 1) Wszelkie doręczenia związane z wykonaniem niniejszej Umowy dokonywane będą na adresu stron wypisane w komparycji lub adresy e-mail.
- 2) Strony zobowiązują się pisemnie informować o wszelkich zmianach danych adresowych. W razie zaniechania tego obowiązku korespondencja wysłana na adres zgodnie z ust. 1 będzie traktowana jako skutecznie doręczona.
- 3) Osobą do kontaktu ze strony Zamawiającego będzie:
 - a), e-mail:, tel.:
- 4) Osobą do kontaktu ze strony Wykonawcy będzie:
 - a), e-mail:, tel.:

§ 9 DOSTĘP DO INFORMACJI PUBLICZNEJ I PRZETWARZANIE DANYCH OSOBOWYCH

- 1) Wykonawca oświadcza, że znany jest mu fakt, iż treść niniejszej Umowy, a w szczególności dotyczące go dane identyfikujące, przedmiot niniejszej Umowy i wysokość wynagrodzenia podlegają udostępnieniu w trybie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej.
- 2) Strony oświadczają, że znane jest im i stosują w swojej działalności 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 (ogólne rozporządzenie o ochronie danych).
- 3) Strony oświadczają, że dane kontaktowe pracowników, współpracowników i reprezentantów Stron udostępniane wzajemnie w niniejszej Umowie lub udostępnione drugiej Stronie w jakikolwiek sposób w okresie obowiązywania niniejszej Umowy przekazywane są w związku z wykonywaniem zadania w interesie publicznym (wykonywania umowy) przez Zamawiającego lub prawnie uzasadnionego interesu Wykonawcy. Udostępniane dane kontaktowe mogą obejmować: imię i nazwisko, adres e-mail, stanowisko służbowe i numer telefonu służbowego. Każda ze Stron będzie administratorem danych kontaktowych, które zostały jej udostępnione w ramach Umowy. Strony zobowiązują się w związku z tym do przekazania wszystkim osobom, których dane udostępnił,

informacji, o których mowa w art. 14 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 (RODO).

§ 10 ZMIANY POSTANOWIEŃ UMOWY

- 1) Zamawiający dopuszcza możliwość wprowadzania zmiany umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy, w przypadku zaistnienia okoliczności niemożliwych do przewidzenia w chwili zawierania umowy lub w przypadku wystąpienia którejkolwiek z następujących okoliczności:
 - a) Zmiany terminu dostawy przedmiotu umowy, w przypadku:
 - i) skrócenia terminu realizacji zamówienia w przypadku wykonania przedmiotu zamówienia;
 - ii) wydłużenia terminu realizacji zamówienia w przypadku działania siły wyższej, mającej istotny wpływ na realizację przedmiotu umowy – nie więcej jednak niż o okres działania siły wyższej, do chwili jej ustąpienia;
 - b) wynagrodzenia, o którym mowa w § 5 ust. 1, w przypadku zmiany stawki podatku VAT, o wartość wynikającą ze zmiany stawki podatku VAT;
 - c) zmiany producenta lub modelu sprzętu (zastąpienie produktu lub rozszerzenie asortymentu o produkt równoważny lub wyższej jakości) w przypadku:
 - i) zaprzestania wytwarzania produktu objętego umową, w tym czasowego wstrzymania produkcji, pod warunkiem, iż odpowiednik jest tej samej lub wyższej jakości, za cenę nie wyższą niż cena produktu objętego umową,
 - ii) wprowadzenia do sprzedaży przez producenta zmodyfikowanego/udoskonalonego produktu, za cenę nie wyższą niż cena produktu objętego umową,
 - iii) wprowadzenia do sprzedaży przez producenta zmodyfikowanego/udoskonalonego produktu, obok dotychczas oferowanego za cenę nie wyższą niż cena produktu objętego umową,
 - iv) zmiany numeru katalogowego produktu, nazwy produktu, przy zachowaniu jego parametrów;
 - d) zmiany warunków realizacji i zakresu przedmiotu umowy niezbędne do prawidłowej realizacji zamówienia związane z:

- i) koniecznością spowodowaną zmianą obowiązujących przepisów prawa powodującą, że realizacja przedmiotu umowy w niezmienionej postaci stanie się niecelowa,
 - ii) wystąpieniem okoliczności powodujących, że niemożliwe jest zrealizowanie przedmiotu umowy w sposób określony w SWZ i złożonej ofercie, które nie były możliwe do przewidzenia w momencie zawarcia umowy,
 - iii) zaistnieniem okoliczności leżących po stronie Zamawiającego, w szczególności spowodowanych zdolnościami płatniczymi, warunkami organizacyjnymi lub okolicznościami, które nie były możliwe do przewidzenia w momencie zawarcia umowy,
 - iv) koniecznością modyfikacji zasad płatności wynagrodzenia umownego (m.in. wystawienia faktury, zasad i terminów rozliczeń i dokonywania płatności między stronami) oraz zasad i trybu odbioru przedmiotu zamówienia (m.in. rodzajów i terminów dokonywania czynności odbiorowych) wynikających w szczególności z zasad instytucji dofinansowujących lub zaistnienia innej okoliczności uzasadniającej wprowadzenie takiej modyfikacji,
 - v) zaistnieniem niemożliwych do wcześniejszego przewidzenia i niezależnych od stron okoliczności powodujących niemożliwość, niecelowość, zbędność czy bezzasadność realizacji poszczególnych elementów przedmiotu zamówienia z punktu widzenia realizowanego zamówienia czy interesu społecznego lub interesu Zamawiającego przy jednoczesnym obniżeniu wynagrodzenia umownego o wartość niezrealizowanych elementów przedmiotu zamówienia i/lub skrócenia terminu realizacji zamówienia,
 - vi) zaistnieniem innej niemożliwej do przewidzenia w momencie zawarcia umowy okoliczności prawnej, ekonomicznej lub technicznej, za którą żadna ze stron nie ponosi odpowiedzialności, skutkującej brakiem możliwości należytego wykonania umowy zgodnie z SWZ.
- e) Zmiany porządkujące i informacyjne zmiany postanowień umowy, w szczególności związane ze zmianą danych identyfikacyjnych (w tym adresowych i teleadresowych) stron umowy i osób reprezentujących strony (w szczególności z powodu nieprzewidzianych zmian organizacyjnych, choroby, wypadków losowych).
- 2) Zaistnienie któregośkolwiek zdarzenia lub okoliczności przewidzianych w ust. 1 oraz 2 upoważnia zarówno Wykonawcę, jak i Zamawiającego do żądania dokonania zmiany umowy, poprzez pisemne powiadomienie o tym drugiej Strony. Powiadomienie powinno zawierać opis wydarzenia lub okoliczności i uzasadnienie dające podstawę do dokonania zmiany umowy oraz powinno być przedstawione w ciągu 7 dni od dnia, w którym Strona umowy dowiedziała się lub powinna się dowiedzieć o danym zdarzeniu lub okolicznościach.

- 3) Wszelkie zmiany postanowień zawartej umowy mogą nastąpić za zgodą obydwu Stron wyrażoną na piśmie pod rygorem nieważności.

§ 11 ODSTĄPIENIE OD UMOWY

- 1) Zamawiającemu przysługuje prawo do odstąpienia od umowy lub rozwiązania umowy z zachowaniem 30 dniowego terminu, jeżeli:
 - a) Wykonawca nie realizuje zamówienia zgodnie z umową lub też nienależycie wykonuje swoje zobowiązania umowne i pomimo pisemnego lub przestanego drogą elektroniczną wezwania otrzymanego od Zamawiającego nie przystąpił do realizacji umowy zgodnie z jej warunkami – w terminie 14 dni od dnia stwierdzenia przez Zamawiającego danej okoliczności.
 - b) Wykonawca opóźnia się z usunięciem wad i/lub usterek więcej niż 14 dni od terminów określonych w § 3 ust 5 lub w § 8 - w terminie 14 dni od dnia powzięcia przez Zamawiającego informacji o upływie 14 -dniowego terminu zwłoki w realizacji przez Wykonawcę zobowiązań gwarancyjnych,
 - c) Wykonawca dokonał cesji wierzytelności wynikających z niniejszej umowy na rzecz osób trzecich bez pisemnej zgody Zamawiającego.
- 2) Odstąpienie Zamawiającego od umowy z przyczyn zależnych od Wykonawcy następuje z chwilą doręczenia Wykonawcy pisemnego oświadczenia wskazującego przyczynę odstąpienia od umowy. Odstąpienie od umowy z przyczyn, o których mowa w ust. 1.

§ 12 PRAWO WŁASNOŚCI INTELEKTUALNEJ

- 1) Wykonawca oświadcza, że na podstawie umowy udziela Zamawiającemu licencji opisanych umową, lub w inny sposób opisany umową upoważnia go do korzystania ze wszystkich dóbr własności intelektualnej wykonanych lub dostarczonych w ramach umowy. Celem jest zapewnienie Zamawiającemu możliwości korzystania z oprogramowania (systemu) w sposób i w celu opisanym w umowie. Wszystkie oświadczenia Wykonawcy i zapisy umowy należy interpretować zgodnie z powyższym celem umowy.
- 2) Wykonawca oświadcza, że przekazane w ramach umowy dobra własności intelektualnej nie będą posiadały żadnych wad prawnych ani nie będą ograniczać Zamawiającego w korzystaniu z tych dóbr w inny sposób niż wyraźnie opisany umową. Wykonawca pokryje wszelkie opłaty, koszty,

odszkodowania lub zadośćuczynienia, które będzie musiał zapłacić Zamawiający, jeżeli powyższe zapewnienia nie okażą się prawdziwe.

- 3) W celu uniknięcia wątpliwości Strony zgodnie postanawiają, że w przypadku, w którym możliwa jest modyfikacja sposobu działania oprogramowania za pomocą wbudowanych lub dostarczonych narzędzi, w tym parametryzacja i konfiguracja oprogramowania, tworzenie raportów itp. Zamawiający uprawniony jest do dokonania takich czynności bez konieczności zawierania odrębnych umów lub ponoszenia dodatkowych opłat.
- 4) Wykonawca oświadcza i gwarantuje, że warunki korzystania z oprogramowania są zgodne z wymaganiami opisanymi w umowie, w tym co do okresu korzystania, ograniczeń ilościowych (lub ich braku), takich jak liczba stanowisk komputerowych, użytkowników lub serwerów.
- 5) Wykonawca oświadcza i gwarantuje, że warunki korzystania z oprogramowania nie wymagają ponoszenia dodatkowych opłat na rzecz Wykonawcy lub producentów takiego oprogramowania. Wynagrodzenie obejmuje całość wynagrodzenia za korzystanie z oprogramowania.
- 6) Wykonawca oświadcza i gwarantuje, że jeżeli w ramach opłat należnych producentowi oprogramowania mieści się opłata za jakiegokolwiek dodatkowe świadczenia, w szczególności dostarczanie aktualizacji lub poprawek błędów lub inne usługi serwisowe, nieprzedłużenie korzystania z tych świadczeń przez Zamawiającego nie może powodować ustania licencji na korzystanie z oprogramowania lub uprawniać do wypowiedzenia umowy licencyjnej.
- 7) W przypadku, w którym w wyniku świadczenia przez Wykonawcę gwarancji dojdzie do zmiany oprogramowania, dokumentacji lub innych utworów, postanowienia umowne dotyczące odpowiednio przeniesienia praw lub udzielenia licencji na oprogramowanie, dokumentację lub inne utwory poddane zmianom stosuje się odpowiednio do takich zmian. Przeniesienie praw lub udzielenie licencji następuje z chwilą odbioru takich zmian.
- 8) Jakiegokolwiek postanowienie umowy, w tym załączników do niej, nie ogranicza uprawnień Zamawiającego wynikających z obowiązujących przepisów prawa, w tym z art. 75 ust. 1 do 3 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.

§ 13 POSTANOWIENIA KOŃCOWE

- 1) Wszelkie umowy nazwane uregulowane w Kodeksie cywilnym oraz umowy nienazwane, nieuregulowane przepisami prawa cywilnego (jak factoring, forfaiting i in.) mające na celu przeniesienie na osoby trzecie wierzytelności zarówno istniejących jak i przyszłych, wymagalnych jak

na Rozwój Cyfrowy

i niewymagalnych na dzień zawarcia umowy, zawarte przez Wykonawcę bez pisemnej zgody Zamawiającego są nieważne.

- 2) W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy kodeksu cywilnego oraz przepisy Ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tj. Dz.U. z 2023 r. poz. 1605 ze zm.) oraz przepisy wykonawcze do tej ustawy.
- 3) Wszelkie spory wynikające z niniejszej umowy lub powstające w związku z nią będą rozstrzygane przez sąd właściwy miejscowo dla siedziby Zamawiającego.
- 4) Umowę sporządzono w trzech jednobrzmiących egzemplarzach. Jeden egzemplarz dla Wykonawcy i dwa egzemplarze dla Zamawiającego.
- 5) Za datę Umowy przyjmuje się datę podpisu ostatniej osoby upoważnionej do podpisania.

Załączniki:

- 1) Oferta Wykonawcy
- 2) SWZ

ZAMAWIAJĄCY:

WYKONAWCA:

WZÓR UMOWY

UMOWA Nr

zawarta w Brześciu Kujawskim pomiędzy:

....., z siedzibą w, reprezentowaną przez:

..... - p.

przy kontrasygnacie Skarbnika – p.

NIP:

zwaną dalej „**Zamawiającym**”

a

.....,

z siedzibą w,

reprezentowanym/ą przez:

..... –

zwanym dalej „**Wykonawcą**”

o następującej treści:

PREAMBUŁA

- 1) Zgodnie z wynikiem przeprowadzenia postępowania przetargowego o nr rozstrzygniętego w dniu na realizację zadania pn.: „.....” w ramach umowy nr FERC..... „Cyberbezpieczny Samorząd”.
- 2) Zamawiający informuje, iż zamówienie dofinansowywane jest ze środków zewnętrznych Unii Europejskiej: Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC).

§ 1 PRZEDMIOT ZAMÓWIENIA

1) Przedmiotem umowy jest

- a) Dostawa i montaż serwera usług zarządzania użytkownikami i uprawnieniami dla Urzędu Miejskiego w Brześciu Kujawskim – typ 1;
- b) Dostawa i montaż zapasowego serwera na potrzeby replikacji danych w Urzędzie Miejskim w Brześciu Kujawskim – typ 2;
- c) Dostawa serwera logów sieciowych i systemowych dla jednostek podległych – typ 3;
- d) Dostawa serwera logów sieciowych i systemowych dla jednostek podległych – typ 4;

na potrzeby projektu pn.: „Cyberbezpieczny Samorząd”. w ramach realizacji projektu grantowego Cyberbezpieczny Samorząd, zwanych dalej: „sprzętem” lub „produktem”, spełniających warunki (parametry) techniczne określone w załączniku nr do SWZ i w ofercie Wykonawcy, stanowiących integralną część niniejszej umowy. Przedmiot umowy został określony w załączniku nr do SWZ – Opis przedmiotu zamówienia.

- 2) Wykonawca zobowiązuje się dostarczyć sprzęt fabrycznie nowy, nie pochodzący z wystawy lub z ekspozycji, kompletny, wraz z niezbędnymi do działania przewodami, z odpowiednim oprogramowaniem, posiadający wymagane prawem atesty i certyfikaty oraz gotowy do pracy.
- 3) Wykonawca zobowiązany jest do naprawiania wszelkich szkód powstałych w trakcie realizacji inwestycji z winy Wykonawcy.
- 4) Przedmiot umowy obejmuje również montaż (instalację), konfigurację sprzętu, wdrożenie oraz szkolenie dla pracowników.
- 5) Dostarczony sprzęt i oprogramowanie pochodzić będzie z oficjalnych kanałów dystrybucyjnych producenta obejmujących również rynek Unii Europejskiej, zapewniających w szczególności realizację uprawnień gwarancyjnych.

§ 2 OBOWIĄZKI WYKONAWCY

Wykonawca jest zobowiązany do:

- 1) Dostawy i montażu sprzętów w Urzędzie Miejskim w Brześciu Kujawskim, pl. Władysława Łokietka 1, 87-880 Brześć Kujawski, oraz w jednostkach podległych w godzinach urzędowania Zamawiającego;
- 2) Dostarczenia sprzętów wraz z:
 - a) kartami gwarancyjnymi, instrukcjami obsługi oraz innymi dokumentami niezbędnymi do przejęcia sprzętu do używania,

- b) ze wszystkimi akcesoriami stanowiącymi komplet sprzedażowy;
- c) uruchomienia sprzętu i badania wykonanej instalacji;
- d) zawiadomienia przedstawiciela Zamawiającego o planowanym terminie dostawy sprzętu, nie później niż na 3 dni przed tym terminem;
- e) uzgodnienia z przedstawicielem Zamawiającego terminu dostawy sprzętu,
- f) montażu (instalacji) i konfiguracji sprzętu i wdrożenia;
- g) przygotowania protokołu odbioru, stanowiącego podstawę odbioru;
- h) przeszkolenia wyznaczonych pracowników z obsługi sprzętu,
- i) współpracy z Zamawiającym w trakcie realizacji umowy, a w szczególności udzielania wszelkich niezbędnych wyjaśnień i informacji dotyczących przedmiotu umowy na każde żądanie Zamawiającego lub osoby wskazanej przez Zamawiającego.

Wykonawca odpowiada za dostarczony sprzęt w czasie transportu. W przypadku uszkodzenia ponosi pełną odpowiedzialność za powstałe szkody.

§ 3 TERMIN REALIZACJI

- 1) Wykonawca jest zobowiązany do dostarczenia przedmiotów zamówienia w terminie do roku.
- 2) Za dzień wykonania umowy przez Wykonawcę uważa się dzień, w którym podpisany zostanie przez obie strony umowy protokół zdawczo - odbiorczy (protokół odbioru) sprzętu – bez uwag.
- 3) Protokół odbioru będzie obejmował nazwy, ilości oraz wartość dostarczonego sprzętu.
- 4) Prawo własności sprzętu, o którym mowa w § 1 przechodzi na Zamawiającego z dniem podpisania protokołu odbioru, o którym mowa w ust. 2.
- 5) W przypadku stwierdzenia, że dostarczony sprzęt:
 - a) jest niezgodny z opisem zawartym w Opisie przedmiotu zamówienia (OPZ), lub jest niekompletny,
 - b) posiada ślady użytkowania lub zewnętrznego uszkodzenia, są uszkodzone, posiadają wady uniemożliwiające użytkowanie, a wady i uszkodzenia te nie powstały z winy Zamawiającego,
- 6) Zamawiający odmówi odbioru części lub całości sprzętu, sporządzając protokół zawierający przyczyny odmowy odbioru (protokół rozbieżności). Zamawiający wyznaczy następnie termin (nie dłuższy niż 7 dni) dostawy oprogramowania fabrycznie nowego, wolnego od wad. Procedura czynności odbioru zostanie powtórzona.

- 7) Wyznaczenie Wykonawcy terminu określonego w ust. 5 nie zwalnia Wykonawcy z odpowiedzialności za nieterminowe wykonanie niniejszej umowy, w szczególności ze zobowiązania do zapłaty kar umownych z tego tytułu przewidzianych w § 9 niniejszej umowy.

§ 4 WYNAGRODZENIE I ROZLICZENIE PRZEDMIOTU UMOWY

- 1) Wynagrodzenie Wykonawcy za wykonanie przedmiotu umowy wynosi:
- a) Dostawa i montaż serwera usług zarządzania użytkownikami i uprawnieniami dla Urzędu Miejskiego w Brześciu Kujawskim – typ 1- zł netto, stawka VAT...%, cena brutto zł.
 - b) Dostawa i montaż zapasowego serwera na potrzeby replikacji danych w Urzędzie Miejskim w Brześciu Kujawskim – typ 2- zł netto, stawka VAT...%, cena brutto zł.
 - c) Dostawa serwera logów sieciowych i systemowych dla jednostek podległych – typ 3- zł netto, stawka VAT...%, cena brutto zł.
 - d) Dostawa serwera logów sieciowych i systemowych dla jednostek podległych – typ 4- zł netto, stawka VAT...%, cena brutto zł.
- 2) Wynagrodzenie za przedmiot umowy obejmuje wszystkie koszty związane poniesione przez Wykonawcę, niezbędne do zrealizowania przedmiotu umowy. Oznacza to, że cena zawiera wszystkie koszty związane z realizacją dostawy i świadczeniem przez Wykonawcę usług objętych umową wynikających wprost z umowy, jak również nie ujęte w jej treści, a niezbędne do jej prawidłowego wykonania. tj. podatek VAT, wszelkie prace przygotowawcze, koszty transportu, itp.
- 3) Podstawą rozliczeń finansowych między Wykonawcą a Zamawiającym będzie faktura VAT wystawiona po wykonaniu całości przedmiotu umowy oraz po sporządzeniu i podpisaniu przez obie strony umowy protokołu zdawczo – odbiorczego (protokołu odbioru) – bez uwag.
- 4) Zapłata wynagrodzenia nastąpi w terminie 30 dni od dnia doręczenia Zamawiającemu faktury.
- 5) Za datę zapłaty przyjmuje się datę obciążenia rachunku bankowego Zamawiającego.
- 6) Faktura ma być wystawiona na:
- Nabywca:, NIP:
- Odbiorca:, NIP:
- 7) W przypadku powierzenia wykonania części zamówienia podwykonawcom lub dalszym podwykonawcom wraz z fakturą, Wykonawca przedstawi pisemny wykaz podwykonawców z ich udziałem finansowym i rzeczowym oraz dowody zapłaty wymagalnego wynagrodzenia podwykonawcom i dalszym podwykonawcom w zakresie wszelkich zobowiązań wynikających

z udziału podwykonawcy i dalszego podwykonawcy w realizacji części zamówienia objętego fakturą. Brak potwierdzenia zapłaty wynagrodzenia podwykonawcom lub dalszym podwykonawcom wstrzymuje dokonanie zapłaty faktury. W przypadku gdy wykonawca realizuje zamówienia bez udziału podwykonawców do faktury Wykonawca przedłoży stosowne oświadczenie potwierdzające samodzielną realizację zamówienia.

- 8) Zamawiający wyraża zgodę na przekazanie faktur VAT drogą elektroniczną na wskazany adres e-mail:

§ 5 PODWYKONAWCY

- 1) Wykonawca może powierzyć wykonanie części zamówienia będącego przedmiotem niniejszej umowy podwykonawcom.
- 2) Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia.
- 3) Wykonawca ponosi pełną odpowiedzialność za część przedmiotu umowy, którą wykonuje przy pomocy podwykonawców.
- 4) Wykonawca ponosi odpowiedzialność na zasadach ogólnych za jakość i terminowość prac, które realizuje przy pomocy podwykonawców.
- 5) W przypadku powierzenia wykonania części zamówienia podwykonawcom lub dalszym podwykonawcom wraz z fakturą, Wykonawca przedstawi pisemny wykaz podwykonawców z ich udziałem finansowym i rzeczowym oraz dowody zapłaty wymagalnego wynagrodzenia podwykonawcom i dalszym podwykonawcom w zakresie wszelkich zobowiązań wynikających z udziału podwykonawcy i dalszego podwykonawcy w realizacji części zamówienia objętego fakturą. Brak potwierdzenia zapłaty wynagrodzenia podwykonawcom lub dalszym podwykonawcom wstrzymuje dokonanie zapłaty faktury. W przypadku gdy wykonawca realizuje zamówienia bez udziału podwykonawców do faktury Wykonawca przedłoży stosowne oświadczenie potwierdzające samodzielną realizację zamówienia.

§ 6 GWARANCJA

- 1) Wykonawca udziela Zamawiającemu gwarancji na sprzęt będący przedmiotem umowy na okres 5 lat w zakresie wdrażanej technologii.
- 2) Okres gwarancji, o którym mowa w ust. 1 rozpoczyna się z dniem podpisania protokołu, o którym mowa w § 3 ust. 2.

- 3) Wykonawca, niezależnie od gwarancji, ponosi odpowiedzialność z tytułu rękojmi za wady fizyczne oraz wady prawne sprzętu zgodnie z kodeksem cywilnym.
- 4) Zamawiający będzie dokonywał zgłoszenia usterki na adres e-mail Wykonawcy lub telefonicznie
- 5) Wykonawca zobowiązuje się do podjęcia czynności serwisowych zgodnie z warunkami przedstawionymi w Opisie przedmiotu zamówienia.
- 6) Wykonawca zapewni bezpłatne usunięcie awarii w okresie trwania gwarancji.
- 7) Zamawiający w razie stwierdzenia w okresie gwarancji ewentualnych wad lub awarii w przedmiocie niniejszej Umowy, obowiązany jest do przedłożenia Wykonawcy, najpóźniej w ciągu 7 dni od dnia ich ujawnienia, stosowanej reklamacji.
- 8) Wykonawca zobowiązuje się w ramach gwarancji do usunięcia wad lub awarii w nieprzekraczalnym terminie 7 dni roboczych od dnia ich zgłoszenia przez Zamawiającego. Termin ten może ulec wydłużeniu do 14 dni roboczych tylko w uzasadnionych przypadkach, po uzyskaniu pisemnej zgody Zamawiającego.
- 9) W przypadku stwierdzenia wady ukrytej sprzętu Wykonawca zobowiązany jest do jego wymiany na nowy zgodnie z warunkami przedstawionymi w Opisie przedmiotu zamówienia.
- 10) Koszt dojazdu ekipy serwisowej w ramach napraw gwarancyjnych i koszt transportu sprzętu naprawianego w ramach gwarancji poza siedzibą Zamawiającego pokrywa Wykonawca.
- 11) Wykonawca ponosi wszelkie koszty związane z wykonaniem obowiązków wynikających z gwarancji.
- 12) Wykonawca zobowiązuje się do zapewnienia kontynuacji świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) w przypadku niemożliwości ich wypełnienia przez Wykonawcę.
- 13) Jeżeli Wykonawca w okresie gwarancji nie przystąpi do usunięcia wad lub awarii w ciągu 5 dni roboczych, Zamawiający może powierzyć ich usunięcie osobie trzeciej na koszt i ryzyko Wykonawcy oraz bez utraty gwarancji udzielonej przez Wykonawcę.
- 14) W przypadku zaistnienia w okresie gwarancji awarii sprzętu oraz konieczności przemieszczenia urządzenia w związku ze stwierdzeniem usterek, których nie można usunąć w siedzibie Zamawiającego, transportu sprzętu na własny koszt dokonuje Wykonawca.
- 15) W przypadku stwierdzenia ukrytych wad technicznych sprzętu koszty napraw pokryje Wykonawca.
- 16) Udzielona przez Wykonawcę gwarancja nie może zobowiązywać Zamawiającego do przechowywania opakowań, instrukcji bądź innych elementów dostawy, niemających wpływu na prawidłowe funkcjonowanie przedmiotu niniejszej Umowy.

§ 7 KARY UMOWNE

1. Strony postanawiają, że obowiązującą formę odszkodowania stanowią kary umowne, które będą naliczane w następujących wypadkach:
 - 1.1. Wykonawca płaci Zamawiającemu kary umowne:
 - a) 0,1% wynagrodzenia umownego netto, określonego w § 5 ust. 1 umowy, za każdy dzień zwłoki za przekroczenie terminu dostaw, o których mowa w § 3 ust. 1,
 - b) 0,05% wynagrodzenia umownego netto, określonego w § 5 ust. 1 umowy, za każdy dzień zwłoki w wykonaniu obowiązków Wykonawcy wynikających z gwarancji (m.in. zwłoka w usunięciu wad i usterek zgłoszonych w okresie gwarancji lub rękojmi);
 - c) 10% wynagrodzenia określonego w § 5 ust. 1 – w razie odstąpienia od umowy przez Wykonawcę lub przez Zamawiającego wskutek okoliczności, za które odpowiada Wykonawca.
2. Łączna maksymalna wysokość kar umownych, których mogą dochodzić Strony nie może przekroczyć 10% wynagrodzenia netto, o którym mowa w § 5 ust. 1 umowy.
3. Zamawiający zastrzega sobie możliwość dochodzenia odszkodowania uzupełniającego na zasadach określonych w Kodeksie cywilnym, jeżeli szkoda przewyższa wysokość kar umownych.
4. Zamawiający może naliczyć i potrącić z wynagrodzenia Wykonawcy, określonego w § 5 ust. 1 umowy, należność z tytułu kar umownych, o których mowa w ust. 1, po uprzednim wezwaniu Wykonawcy do ich zapłaty pod rygorem potrącenia, a Wykonawca wyraża na to zgodę.
5. Kary umowne płatne będą w terminie 10 dni od dnia otrzymania wezwania do zapłaty.

§ 8 SPOSÓB POROZUMIEWANIA SIĘ STRON

- 1) Wszelkie doręczenia związane z wykonaniem niniejszej Umowy dokonywane będą na adresy stron wypisane w komparycji lub adresy e-mail.
- 2) Strony zobowiązują się pisemnie informować o wszelkich zmianach danych adresowych. W razie zaniechania tego obowiązku korespondencja wysłana na adres zgodnie z ust. 1 będzie traktowana jako skutecznie doręczona.
- 3) Osobą do kontaktu ze strony Zamawiającego będzie:
 - a), e-mail:, tel.:
- 4) Osobą do kontaktu ze strony Wykonawcy będzie:
 - a), e-mail:, tel.:

§ 9 DOSTĘP DO INFORMACJI PUBLICZNEJ I PRZETWARZANIE DANYCH OSOBOWYCH

- 1) Wykonawca oświadcza, że znany jest mu fakt, iż treść niniejszej Umowy, a w szczególności dotyczące go dane identyfikujące, przedmiot niniejszej Umowy i wysokość wynagrodzenia podlegają udostępnieniu w trybie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej.
- 2) Strony oświadczają, że znane jest im i stosują w swojej działalności 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 (ogólne rozporządzenie o ochronie danych).
- 3) Strony oświadczają, że dane kontaktowe pracowników, współpracowników i reprezentantów Stron udostępniane wzajemnie w niniejszej Umowie lub udostępnione drugiej Stronie w jakikolwiek sposób w okresie obowiązywania niniejszej Umowy przekazywane są w związku z wykonywaniem zadania w interesie publicznym (wykonywania umowy) przez Zamawiającego lub prawnie uzasadnionego interesu Wykonawcy. Udostępniane dane kontaktowe mogą obejmować: imię i nazwisko, adres e-mail, stanowisko służbowe i numer telefonu służbowego. Każda ze Stron będzie administratorem danych kontaktowych, które zostały jej udostępnione w ramach Umowy. Strony zobowiązują się w związku z tym do przekazania wszystkim osobom, których dane udostępnił, informacji, o których mowa w art. 14 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 (RODO).

§ 10 ZMIANY POSTANOWIEŃ UMOWY

- 1) Zamawiający dopuszcza możliwość wprowadzania zmiany umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy, w przypadku zaistnienia okoliczności niemożliwych do przewidzenia w chwili zawierania umowy lub w przypadku wystąpienia którejkolwiek z następujących okoliczności:
 - a) Zmiany terminu dostawy przedmiotu umowy, w przypadku:
 - i) skrócenia terminu realizacji zamówienia w przypadku wykonania przedmiotu zamówienia;
 - ii) wydłużenia terminu realizacji zamówienia w przypadku działania siły wyższej, mającej istotny wpływ na realizację przedmiotu umowy – nie więcej jednak niż o okres działania siły wyższej, do chwili jej ustąpienia;
 - b) wynagrodzenia, o którym mowa w § 5 ust. 1, w przypadku zmiany stawki podatku VAT, o wartość wynikającą ze zmiany stawki podatku VAT;

- c) zmiany producenta lub modelu sprzętu (zastąpienie produktu lub rozszerzenie asortymentu o produkt równoważny lub wyższej jakości) w przypadku:
 - i) zaprzestania wytwarzania produktu objętego umową, w tym czasowego wstrzymania produkcji, pod warunkiem, iż odpowiednik jest tej samej lub wyższej jakości, za cenę nie wyższą niż cena produktu objętego umową,
 - ii) wprowadzenia do sprzedaży przez producenta zmodyfikowanego/udoskonalonego produktu, za cenę nie wyższą niż cena produktu objętego umową,
 - iii) wprowadzenia do sprzedaży przez producenta zmodyfikowanego/udoskonalonego produktu, obok dotychczas oferowanego za cenę nie wyższą niż cena produktu objętego umową,
 - iv) zmiany numeru katalogowego produktu, nazwy produktu, przy zachowaniu jego parametrów;
- d) zmiany warunków realizacji i zakresu przedmiotu umowy niezbędne do prawidłowej realizacji zamówienia związane z:
 - i) koniecznością spowodowaną zmianą obowiązujących przepisów prawa powodującą, że realizacja przedmiotu umowy w niezmienionej postaci stanie się niecelowa,
 - ii) wystąpieniem okoliczności powodujących, że niemożliwe jest zrealizowanie przedmiotu umowy w sposób określony w SWZ i złożonej ofercie, które nie były możliwe do przewidzenia w momencie zawarcia umowy,
 - iii) zaistnieniem okoliczności leżących po stronie Zamawiającego, w szczególności spowodowanych zdolnościami płatniczymi, warunkami organizacyjnymi lub okolicznościami, które nie były możliwe do przewidzenia w momencie zawarcia umowy,
 - iv) koniecznością modyfikacji zasad płatności wynagrodzenia umownego (m.in. wystawienia faktury, zasad i terminów rozliczeń i dokonywania płatności między stronami) oraz zasad i trybu odbioru przedmiotu zamówienia (m.in. rodzajów i terminów dokonywania czynności odbiorowych) wynikających w szczególności z zasad instytucji dofinansowujących lub zaistnienia innej okoliczności uzasadniającej wprowadzenie takiej modyfikacji,
 - v) zaistnieniem niemożliwych do wcześniejszego przewidzenia i niezależnych od stron okoliczności powodujących niemożliwość, niecelowość, zbędność czy bezzasadność realizacji poszczególnych elementów przedmiotu zamówienia z punktu widzenia realizowanego zamówienia czy interesu społecznego lub interesu Zamawiającego przy jednoczesnym obniżeniu wynagrodzenia umownego o wartość niezrealizowanych elementów przedmiotu zamówienia i/lub skrócenia terminu realizacji zamówienia,

- vi) zaistnieniem innej niemożliwej do przewidzenia w momencie zawarcia umowy okoliczności prawnej, ekonomicznej lub technicznej, za którą żadna ze stron nie ponosi odpowiedzialności, skutkującej brakiem możliwości należytego wykonania umowy zgodnie z SWZ.
 - e) Zmiany porządkujące i informacyjne zmiany postanowień umowy, w szczególności związane ze zmianą danych identyfikacyjnych (w tym adresowych i teleadresowych) stron umowy i osób reprezentujących strony (w szczególności z powodu nieprzewidzianych zmian organizacyjnych, choroby, wypadków losowych).
- 2) Zaistnienie któregokolwiek zdarzenia lub okoliczności przewidzianych w ust. 1 oraz 2 upoważnia zarówno Wykonawcę, jak i Zamawiającego do żądania dokonania zmiany umowy, poprzez pisemne powiadomienie o tym drugiej Strony. Powiadomienie powinno zawierać opis wydarzenia lub okoliczności i uzasadnienie dające podstawę do dokonania zmiany umowy oraz powinno być przedstawione w ciągu 7 dni od dnia, w którym Strona umowy dowiedziała się lub powinna się dowiedzieć o danym zdarzeniu lub okolicznościach.
- 3) Wszelkie zmiany postanowień zawartej umowy mogą nastąpić za zgodą obydwu Stron wyrażoną na piśmie pod rygorem nieważności.

§ 11 ODSTĄPIENIE OD UMOWY

- 1) Zamawiającemu przysługuje prawo do odstąpienia od umowy lub rozwiązania umowy z zachowaniem 30 dniowego terminu, jeżeli:
- a) Wykonawca nie realizuje zamówienia zgodnie z umową lub też nienależycie wykonuje swoje zobowiązania umowne i pomimo pisemnego lub przesłanego drogą elektroniczną wezwania otrzymanego od Zamawiającego nie przystąpił do realizacji umowy zgodnie z jej warunkami – w terminie 14 dni od dnia stwierdzenia przez Zamawiającego danej okoliczności.
 - b) Wykonawca opóźnia się z usunięciem wad i/lub usterek więcej niż 14 dni od terminów określonych w § 3 ust 5 lub w § 8 - w terminie 14 dni od dnia powzięcia przez Zamawiającego informacji o upływie 14 -dniowego terminu zwłoki w realizacji przez Wykonawcę zobowiązań gwarancyjnych,
 - c) Wykonawca dokonał cesji wierzytelności wynikających z niniejszej umowy na rzecz osób trzecich bez pisemnej zgody Zamawiającego.

- 2) Odstąpienie Zamawiającego od umowy z przyczyn zależnych od Wykonawcy następuje z chwilą doręczenia Wykonawcy pisemnego oświadczenia wskazującego przyczynę odstąpienia od umowy. Odstąpienie od umowy z przyczyn, o których mowa w ust. 1.

§ 12 PRAWO WŁASNOŚCI INTELEKTUALNEJ

- 1) Wykonawca oświadcza, że na podstawie umowy udziela Zamawiającemu licencji opisanych umową, lub w inny sposób opisany umową upoważnia go do korzystania ze wszystkich dóbr własności intelektualnej wykonanych lub dostarczonych w ramach umowy. Celem jest zapewnienie Zamawiającemu możliwości korzystania z oprogramowania (systemu) w sposób i w celu opisanym w umowie. Wszystkie oświadczenia Wykonawcy i zapisy umowy należy interpretować zgodnie z powyższym celem umowy.
- 2) Wykonawca oświadcza, że przekazane w ramach umowy dobra własności intelektualnej nie będą posiadały żadnych wad prawnych ani nie będą ograniczać Zamawiającego w korzystaniu z tych dóbr w inny sposób niż wyraźnie opisany umową. Wykonawca pokryje wszelkie opłaty, koszty, odszkodowania lub zadośćuczynienia, które będzie musiał zapłacić Zamawiający, jeżeli powyższe zapewnienia nie okażą się prawdziwe.
- 3) W celu uniknięcia wątpliwości Strony zgodnie postanawiają, że w przypadku, w którym możliwa jest modyfikacja sposobu działania oprogramowania za pomocą wbudowanych lub dostarczonych narzędzi, w tym parametryzacja i konfiguracja oprogramowania, tworzenie raportów itp. Zamawiający uprawniony jest do dokonania takich czynności bez konieczności zawierania odrębnych umów lub ponoszenia dodatkowych opłat.
- 4) Wykonawca oświadcza i gwarantuje, że warunki korzystania z oprogramowania są zgodne z wymaganiami opisanymi w umowie, w tym co do okresu korzystania, ograniczeń ilościowych (lub ich braku), takich jak liczba stanowisk komputerowych, użytkowników lub serwerów.
- 5) Wykonawca oświadcza i gwarantuje, że warunki korzystania z oprogramowania nie wymagają ponoszenia dodatkowych opłat na rzecz Wykonawcy lub producentów takiego oprogramowania. Wynagrodzenie obejmuje całość wynagrodzenia za korzystanie z oprogramowania.
- 6) Wykonawca oświadcza i gwarantuje, że jeżeli w ramach opłat należnych producentowi oprogramowania mieści się opłata za jakiegokolwiek dodatkowe świadczenia, w szczególności dostarczanie aktualizacji lub poprawek błędów lub inne usługi serwisowe, nieprzedłużenie korzystania z tych świadczeń przez Zamawiającego nie może powodować ustania licencji na korzystanie z oprogramowania lub uprawniać do wypowiedzenia umowy licencyjnej.

- 7) W przypadku, w którym w wyniku świadczenia przez Wykonawcę gwarancji dojdzie do zmiany oprogramowania, dokumentacji lub innych utworów, postanowienia umowne dotyczące odpowiednio przeniesienia praw lub udzielenia licencji na oprogramowanie, dokumentację lub inne utwory poddane zmianom stosuje się odpowiednio do takich zmian. Przeniesienie praw lub udzielenie licencji następuje z chwilą odbioru takich zmian.
- 8) Jakiegokolwiek postanowienie umowy, w tym załączników do niej, nie ogranicza uprawnień Zamawiającego wynikających z obowiązujących przepisów prawa, w tym z art. 75 ust. 1 do 3 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.

§ 13 POSTANOWIENIA KOŃCOWE

- 1) Wszelkie umowy nazwane uregulowane w Kodeksie cywilnym oraz umowy nienazwane, nieuregulowane przepisami prawa cywilnego (jak factoring, forfaiting i in.) mające na celu przeniesienie na osoby trzecie wierzytelności zarówno istniejących jak i przyszłych, wymagalnych jak i niewymagalnych na dzień zawarcia umowy, zawarte przez Wykonawcę bez pisemnej zgody Zamawiającego są nieważne.
- 2) W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy kodeksu cywilnego oraz przepisy Ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tj. Dz.U. z 2023 r. poz. 1605 ze zm.) oraz przepisy wykonawcze do tej ustawy.
- 3) Wszelkie spory wynikające z niniejszej umowy lub powstające w związku z nią będą rozstrzygane przez sąd właściwy miejscowo dla siedziby Zamawiającego.
- 4) Umowę sporządzono w trzech jednobrzmiących egzemplarzach. Jeden egzemplarz dla Wykonawcy i dwa egzemplarze dla Zamawiającego.
- 5) Za datę Umowy przyjmuje się datę podpisu ostatniej osoby upoważnionej do podpisania.

Załączniki:

- 1) Oferta Wykonawcy
- 2) SWZ

ZAMAWIAJĄCY:

WYKONAWCA: