

Załącznik nr 4 do SWZ**OPIS PRZEDMIOTU ZAMÓWIENIA****ZAMÓWIENIE PODZIELONE JEST NA 3 CZĘŚCI:**

<u>Część I Zamówienia: Dostawa sprzętu oraz szkolenie pracowników Urzędu Miejskiego w Więcborku</u>	2
<u>Zadanie 1 - Szkolenie dla administratora</u>	2
<u>Zadanie 2 - Szkolenie pracowników z zasad cyberbezpieczeństwa</u>	2
<u>Zadanie 3 - Modernizacja sieci LAN</u>	4
<u>Zadanie 4 - Rejestracja Incydentów</u>	14
<u>Zadanie 5 – System do agregacji logów / SIEM</u>	16
<u>Zadanie 6 – Wykonanie skanów podatności</u>	18
<u>Zadanie 7 - Wdrożenie systemu Data Leak Protection – DLP</u>	20
<u>Zadanie 8 - Zakup i konfiguracja UPS</u>	23
<u>Część II Zamówienia – Dostawa serwera dla Środowiskowego Domu Samopomocy w Więcborku</u>	25
<u>Część III Zamówienia – Dostawa serwera dla Centrum Usług Społecznych w Więcborku</u>	33

Część I Zamówienia: Dostawa sprzętu oraz szkolenie pracowników Urzędu Miejskiego w Więcborku

Zadanie 1 - Szkolenie dla administratora

1. Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. Przeprowadzenie szkolenia z zakresu rozwiązań technicznych takich jak: Microsoft Active Directory, rozwiązania Fortinet Fortigate, rozwiązań kopii zapasowych dedykowanych środowiskom zwirtualizowanym, bezpieczeństwa sieci, rozwiązań klasy xDR/EDR.

2. Szczegółowe wymagania odnośnie usługi

Szkolenie - minimalne wymagania:

- a. szkolenia będą zrealizowane jako szkolenia zamknięte;
- b. szkolenia będą przeprowadzone w języku polskim;
- c. szkolenia muszą odbyć się w formie zdalnej poprzez udostępniony przez Wykonawcę kanał elektroniczny lub dedykowaną aplikację, z możliwością późniejszego odtworzenia spotkania (nagranie szkolenia), z zastrzeżeniem nierozpowszechniania nagrania poza obszar organizacji Zamawiającego;
- d. Musi tworzyć cykl 3 (słownie trzech) szkoleń, trwających minimum 1 godzinę każde, gdzie łączna liczba godzin poświęcona na szkolenia nie może być mniejsza niż 10 godzin
- e. Zamawiający dopuszcza udział uczestników szkolenia w ramach większej grupy szkoleniowej
- f. agenda szkoleń musi dotyczyć tematyki technologicznej, w tym przynajmniej: Microsoft Active Directory, rozwiązania Fortinet Fortigate, rozwiązań kopii zapasowych dedykowanych środowiskom zwirtualizowanym, bezpieczeństwa sieci, rozwiązań klasy xDR/EDR.
- g. obowiązek sprawdzania obecności w trakcie każdego ze szkoleń np. w postaci zrzutów ekranowych listy zalogowanych uczestników szkolenia pozwalającej potwierdzić obecność uczestników. Oryginalne wersje list obecności zostaną przekazane Zamawiającemu po zakończeniu każdej edycji szkolenia;
- h. wykonawca gwarantuje, że osoba prowadząca szkolenia posiada odpowiednie predyspozycje do prowadzenia szkoleń oraz wyczerpującą wiedzę, co najmniej na poziomie wymaganym do realizacji szkoleń;
- i. wykonawca zobowiązany jest w porozumieniu z Zamawiającym ustalić dokładną datę przeprowadzenia szkoleń. Zamawiający ustali na zasadzie negocjacji z Wykonawcą, w terminie maksymalnie 15 dni roboczych od daty podpisania umowy ramowy harmonogram szkoleń;
- j. po ukończeniu szkolenia uczestnicy otrzymają zaświadczenie lub certyfikat ukończenia szkolenia w formie papierowej bądź elektronicznej. Zaświadczenia zostaną przesłane na wskazany przez Zamawiającego adres fizyczny lub adres skrzynki poczty elektronicznej.

Zadanie 2 - Szkolenie pracowników z zasad cyberbezpieczeństwa

1.1 Przedmiot zamówienia

Przedmiotem zamówienia są:

1. przeprowadzenie szkolenia zwiększającego świadomość pracowników Zamawiającego w dziedzinie cyberbezpieczeństwa;
2. wykonanie testów socjotechnicznych na wybranej grupie kontrolnej pracowników Zamawiającego.

1.2 Wymagania wobec Wykonawcy

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy posiadają niezbędną wiedzę i kwalifikacje do realizacji zamówienia. Wykonawca musi spełniać wszystkie poniższe warunki:

- wykonawca zatrudnia osobę posiadającą certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według ISO/IEC 27001 lub równoważnym
- wykonawca zatrudnia osobę posiadającą certyfikat CompTIA Security+ lub równoważny

1.3 Szczegółowe wymagania odnośnie usługi

1. Szkolenie - minimalne wymagania:

- a. szkolenia będą zrealizowane jako szkolenia zamknięte;
- b. szkolenia będą przeprowadzone w języku polskim;
- c. szkolenia muszą odbyć się w formie zdalnej poprzez udostępniony przez Wykonawcę kanał elektroniczny lub dedykowaną aplikację, z możliwością późniejszego odtworzenia spotkania (nagranie szkolenia), z zastrzeżeniem nierozpowszechniania nagrania poza obszar organizacji Zamawiającego;
- d. minimalny czas trwania szkolenia to trzy (3) pełne godziny zegarowe
- e. Zamawiający dopuszcza udział uczestników szkolenia w ramach większej grupy szkoleniowej
- f. agenda szkoleń musi dotyczyć tematyki cyberbezpieczeństwa, w tym przynajmniej: socjotechniki, phishingu, ransomware, bezpieczeństwa poczty elektronicznej oraz korzystania z urządzeń mobilnych, sieci Wi-Fi, bezpieczeństwa nośników danych;
- g. obowiązek sprawdzania obecności w trakcie każdego ze szkoleń np. w postaci zrzutów ekranowych listy zalogowanych uczestników szkolenia pozwalającej potwierdzić obecność uczestników. Oryginalne wersje list obecności zostaną przekazane Zamawiającemu po zakończeniu każdego szkolenia;
- h. wykonawca gwarantuje, że osoba prowadząca szkolenia posiada odpowiednie predyspozycje do prowadzenia szkoleń oraz wyczerpującą wiedzę, co najmniej na poziomie wymaganym do realizacji szkoleń;
- i. wykonawca zobowiązany jest w porozumieniu z Zamawiającym ustalić dokładną datę przeprowadzenia szkoleń. Zamawiający ustali na zasadzie negocjacji z Wykonawcą, w terminie maksymalnie 15 dni roboczych od daty podpisania umowy ramowy harmonogram szkoleń;
- j. po ukończeniu szkolenia uczestnicy otrzymają zaświadczenie lub certyfikat ukończenia szkolenia w formie papierowej bądź elektronicznej. Zaświadczenia zostaną przesłane na wskazany przez Zamawiającego adres fizyczny lub adres skrzynki poczty elektronicznej.

2. Etap II (testy socjotechniczne) - minimalne wymagania:

- a. wykonanie testu weryfikacyjnego poziomu świadomości cyberzagrożeń Pracowników Zamawiającego poprzez nakłanianie ich do niestosowania się do obowiązujących zasad i procedur bezpieczeństwa obowiązujących u Zamawiającego;
- b. przygotowanie i wdrożenie indywidualnych scenariuszy kontrolowanego ataku hakerskiego, na wybraną grupę Pracowników Zamawiającego;
- c. opracowanie raportu po realizacyjnego zawierającego:
 - i. wyniki przeprowadzonych testów oraz stan poziomu zabezpieczenia zasobów systemu informatycznego Zamawiającego;
 - ii. rekomendacje oraz zalecenia dla posiadanego środowiska;
 - iii. propozycje modernizacji środowiska lub jego zabezpieczeń;

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

- d. spotkanie organizacyjne pomiędzy Zleceniodawcą a Wykonawcą, mające na celu omówienie wyników testów socjotechnicznych oraz zaleceń i rekomendacji zawartych w raporcie po realizacyjnym.

Zadanie 3 - Modernizacja sieci LAN

1. Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. dostawa fabrycznie nowego Sprzętu, nie używanego w innych środowiskach ani projektach, w ilościach:
 - a) Przełącznik sieciowy – 1 sztuka
 - b) Punkt dostępowy WiFi 6 – 5 sztuk
2. konfiguracja urządzeń oraz fizyczna instalacja w infrastrukturze IT Zamawiającego;
3. Dostarczenie oprogramowania klasy Network Access Control (NAC)
4. Konfiguracja oprogramowania NAC, implementacja w środowisku zamawiającego
5. udzielenie przez Wykonawcę gwarancji i zapewnienie w jej ramach serwisu gwarancyjnego oraz wsparcia technicznego na dostarczony Sprzęt;
6. dostarczenie przez Wykonawcę dokumentacji dostarczonego Sprzętu;

2. Termin realizacji zamówienia

Zamawiający wymaga, aby dostawa sprzętu do Zamawiającego nastąpiła w terminie 8 tygodni od dnia podpisania Umowy.

3. Wymagania wobec Wykonawcy

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy posiadają niezbędną wiedzę i kwalifikacje do realizacji zamówienia. Wykonawca musi spełniać wszystkie poniższe warunki:

- Wymaga się, aby wykonawca wykazał się doświadczeniem w podobnych realizacjach, tzn. Wykaże referencje, że w okresie 2 lat przed terminem składania ofert, a jeżeli okres działalności jest krótszy w tym okresie - zrealizował dostawy urządzeń sieciowych dla minimum 3 klientów, gdzie wartość jednostkowa zamówienia wynosiła minimum 50 000 zł netto

4. Wymagania szczegółowe Zamawiającego

Zestawienie wymaganych parametrów technicznych dla przełącznika sieciowego (1 sztuki)

Interfejs sieciowy	48x 1Gb Ethernet (10/100/1000 Mbps) 4x SFP+ (1/10 Gbps)
Interfejs zarządzania	Ethernet, In-Band
Łączna przepustowość (non-blocking)	Minimum 88 Gbps
Przepustowość przełączania	Minimum 176 Gbps
Prędkość przekazywania	Minimum 130 Mpps
Sposób zasilania	Uniwersalny: 100 - 240 V AC / 50 - 60 Hz USP RPS DC: 11.5 VDC, 5.22A
Zasilacz	Wbudowany, AC/DC Moc minimum 60 W
Maksymalny pobór mocy	60 W
Diody LED	System: Status RJ45: Speed / Link / Activity

*SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCIBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II*

	SFP+: Speed / Link / Activity RPS: Status
Waga	Z uchwytyami montażowymi: maksymalnie 4,15 kg Bez uchwytów montażowych: maksymalnie 4,10kg
Dopuszczalna temperatura pracy	Od -5 do 45 st. C
Certyfikaty	IC, FCC, CE
Możliwość montażu w szafie RACK	Tak, maksymalnie 1U

Zestawienie wymaganych parametrów technicznych dla punktu dostępowego0 (5 sztuk)

Parametr	Wartość
Wymiary	Ø206 x 46 mm (Ø8.1 x 1.8")
Materiał obudowy	Poliwęglan
Materiał uchwytu	Stal nierdzewna (SUS304)
Odporność na warunki atmosferyczne	IP54
Interfejs sieciowy	1x port GbE RJ45
Interfejs zarządzania	Ethernet, Bluetooth
Metoda zasilania	PoE+
Zasilanie	Przełącznik PoE lub adapter PoE 48V, 0.5A (nie w zestawie)
Zakres obsługiwanego napięcia	44–57V DC
Maks. pobór mocy	21W
Maks. moc nadawania	2.4 GHz: 23 dBm; 5 GHz: 26 dBm; 6 GHz: 23dBm
MIMO	2.4 GHz: 2x2; 5 GHz: 2x2; 6 GHz: 2x2
Maks. przepustowość	2.4 GHz: 688 Mbps; 5 GHz: 4.3 Gbps; 6 GHz: 5.8 Gbps
Zysk anteny	2.4 GHz: 4 dBi; 5 GHz: 6 dBi; 6 GHz: 5.8 dBi
Dioda LED	Biała/niebieska
Przycisk	Reset fabryczny
Montaż	Ściana, sufit (elementy montażowe w zestawie)
Temperatura pracy	-30 do 40°C (-22 do 104°F)
Wilgotność otoczenia	5–95% (bez kondensacji)
Certyfikaty	CE, FCC, IC
Standardy WiFi	802.11n/ac/ax/be
Zabezpieczenia sieci bezprzewodowej	WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3)
BSSID	8 na każde radio
VLAN	802.1Q
Zaawansowane QoS	Ograniczanie prędkości dla użytkownika
Izolacja ruchu gości	Obsługiwane
Obsługa klientów jednocześnie	300+
Obsługiwane prędkości	802.11n: 6,5 Mbps do 300 Mbps
	802.11ac: 6,5 Mbps do 1,7 Gbps
	802.11ax: 7,3 Mbps do 2,4 Gbps
	802.11be: 7,3 Mbps do 5.8 Gbps

5. Wymagania ogólne dla wszystkich typów urządzeń sieciowych oraz wykonywanych prac:

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCIBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

1. Dostarczone urządzenia muszą pochodzić z autoryzowanego kanału sprzedaży producentów na rynek polski – do oferty należy dołączyć odpowiednie oświadczenie producenta sprzętu
2. Dostarczone urządzenia muszą być objęte gwarancją opartą o świadczenia gwarancyjne producenta sprzętu, niezależnie od statusu partnerskiego Wykonawcy przez okres co najmniej 12 miesięcy
3. Urządzenie musi mieć możliwość zarządzania i konfigurowania poprzez dedykowane rozwiązanie zarządzające, posiadające funkcje takie jak:
 - a. podgląd statusu urządzeń w czasie rzeczywistym
 - b. centralne zarządzanie wieloma sieciami z poziomu interfejsu graficznego
 - c. możliwość zdalnej aktualizacji oprogramowania urządzeń
 - d. wersję mobilną aplikacji
4. Urządzenia (przełączniki) muszą być zarządzalne w warstwie 2 i 3
5. Dostarczający jest zobowiązany do podłączenia urządzeń sieciowych w infrastrukturze Zamawiającego do wskazanych miejsc połączeń sieciowych i elektrycznych
6. Dostarczający jest zobowiązany do aktualizacji oprogramowania sprzętowego dostarczonych urządzeń do najnowszej dostępnej i zalecanej przez producenta wersji
7. Dostarczający musi utworzyć dostępy administracyjne do urządzeń oraz przekazać je Zamawiającemu
8. W ramach wykonywanych prac Wykonawca zobowiązuje się do skonfigurowania urządzenia brzegowego w zakresie nowych VLAN-ów, dla przekazanych urządzeń
 1. Utworzenie interfejsów w warstwie L3 na urządzeniu brzegowym – do 5 VLAN-ów
 2. Utworzenie polityk pomiędzy stworzonymi VLAN-ami na urządzeniu brzegowym, zgodnie z wymaganiami zamawiającego (do 15 polityk)
9. W ramach przekazanych urządzeń, Wykonawca zobowiązuje się - na wskazanych przez Zamawiającego interfejsach - zdefiniować do 5 VLAN-ów
10. Na wskazanym przez Zamawiającego zasobie serwerowym, Wykonawca zobowiązany jest do instalacji, konfiguracji i dodania urządzeń sieciowych do dedykowanego centralnego rozwiązania zarządzającego.

6. Wymagania wobec Wykonawcy - NAC

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy posiadają niezbędną wiedzę i kwalifikacje do realizacji zamówienia. Wykonawca musi spełniać wszystkie poniższe warunki:

- Wymaga się, aby wykonawca wykazał się doświadczeniem w podobnych realizacjach, tzn. Wykaże referencje, że w okresie 5 lat przed terminem składania ofert, a jeżeli okres działalności jest krótszy w tym okresie - zrealizował dostawy urządzeń sieciowych dla minimum 2 klientów, gdzie wartość jednostkowa zamówienia wynosiła minimum 50 000 zł netto

7. Wymagania szczegółowe Zamawiającego - NAC

Zestawienie wymaganych parametrów technicznych odnośnie systemu NAC:

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.

*SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II*

5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 250 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 1000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
 - VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x
 - Maszyny fizyczne - serwery wspierane przez producenta.
11. System musi posiadać funkcjonalność serwerów:
 - serwera RADIUS dla infrastruktury sieciowej,
 - serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
 - serwera SYSLOG,
 - serwera TACACS+,
 - serwera Monitoringu,
 - serwera DHCP,
 - serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
 - serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.
13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google Workspace, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznymi systemami (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC), CheckPoint, Service Now.
16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.

*SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II*

17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługi wielu PKI dla różnych grup użytkowników.
20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.
35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook, Google, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.

*SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II*

39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestrację gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzenia, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minimum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.
59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
 - Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
 - Czy włączony jest firewall
 - Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
 - Czy jest włączone szyfrowanie dysku systemowego

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

- Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
 - Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
 - Czy w systemie są uruchomione procesy wskazane przez administratora
 - Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
 - Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
 - Wartości klucza rejestru
 - Typu wartości: Number, String, Version
60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
61. System musi współpracować z serwerem tokenów.
62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfigurator sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działu IT dla systemów co najmniej:
- Microsoft Windows
 - Mac OS
 - iOS
 - Android
63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfigurator sieci).
64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

Mechanizmy uwierzytelniania

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
 - MAC,
 - PAP/ASCII,
 - CHAP,
 - SNMP,
 - 802.1X.
3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.
4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X SupPLICANT, Apple iOS SupPLICANT, Google Android SupPLICANT, Ubuntu SupPLICANT).
7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
 - Tożsamość/Urządzenie końcowe,
 - Grupa tożsamości/urządzeń końcowych,
 - Parametry urządzeń końcowych, min: system operacyjny, wersja,
 - Atrybuty Active Directory,

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

- Jednostka organizacyjna tożsamości/urządzeń końcowych,
 - Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
 - Grupy urządzeń sieciowych,
 - Porty urządzeń sieciowych,
 - Grupy portów urządzeń sieciowych,
 - Jednostka organizacyjna portów,
 - Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
 - Data, czas ważności polityki,
 - Wewnętrzny Captive Portal,
 - Metoda autoryzacji.
8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.
 9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
 10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
 11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
 12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
 13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
 14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
 15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
 16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
 17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
 18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
 19. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
 20. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

Obsługa serwerów certyfikatów CA

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

- możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
- możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
- Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
- usługę OCSP (Online Certificate Status Protocol).

Obsługa serwerów DHCP

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
 - Uruchamianie usługi dla wybranych podsieci,
 - Przypisanie ustalonego adresu IP dla adresu MAC.
 - Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
 - Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
 - Możliwość określania braku dostępu dla wybranych adresów MAC,
 - Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
 - Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
 - Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
 - Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
 - Dokonywanie zmian bez konieczności wyłączania usług.

Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępu urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.
8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.

*SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II*

4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadanym adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności VLANów w urządzeniach sieciowych działających w środowisku.
14. System musi wspierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory, minimum:
 - ☐ Logowania, wylogowania z system w tym błędne logowania
 - ☐ Logowania do sieci 802.1X

Alarmy

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
 - wiadomości e-mail,
 - Syslog,
 - notyfikacji systemowych.
2. Alarmy mogą być generowane w sytuacjach, min:
 - Ilości obsługiwanych transakcji RADIUS,
 - Opóźnienie obsługi transakcji RADIUS,
 - Statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
 - badanie łączności IP za pomocą ping, traceroute,
 - tcpdump protokołów RADIUS, TACACS+,
 - wyszukiwanie zdarzeń RADIUS z uwzględnieniem:

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

- nazwy użytkownika,
- adresu MAC,
- statusu uwierzytelnienia (udana lub nieudana),
- powodu, jeżeli uwierzytelnienie nieudane,
- zakresu czasowego, co do dnia, godziny i minuty,
- wykonanie zdalnego polecenia na urządzeniu sieciowym.

Licencja wsparcia technicznego producenta oprogramowania:

Wykonawca dostarczy wraz dożywotnią licencją systemu NAC – 12 miesięczną licencję na wsparcie producenta oprogramowania. Licencja ta powinna obejmować minimum:

1. Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC
2. Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
3. Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.
4. Dostęp do dokumentacji i instrukcji na stronie internetowej.
5. Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

Wymagane prace wdrożeniowe związane z oprogramowaniem klasy NAC:

1. Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta.
2. Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji).
3. Konfiguracja urządzenia firewall (dodatkowo VLAN-u gościnnego, ustawienie polityk).
4. Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego - lista).
5. Integracja dostarczanych urządzeń sieciowych (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach.
6. Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy.
7. Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.
8. Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia.

Zadanie 4 - System Rejestracji Incydentów

1. Przedmiot zamówienia

Przedmiotem zamówienia jest:

- 1) dostawa oprogramowania do rejestrowania i zarządzania incydentów w infrastrukturze IT Zamawiającego;
- 2) przeprowadzenie szkolenia z posługiwania się dostarczonym rozwiązaniem.

2. Szczegółowe wymagania odnośnie proponowanego rozwiązania

1. instalacja na własnym środowisku serwerowym (tzw. on-premise)
2. własny wbudowany mechanizm wykonywania kopii zapasowych

*SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II*

3. instalacja na systemach Windows i Linux
 4. własna baza postgreSQL
 5. wbudowana funkcjonalność bazy wiedzy
 6. Możliwość utworzenia minimum do 5 unikalnych techników
 7. możliwość logowania bez potrzeby ponownego używania poświadczeń do aplikacji dzięki autentykacji poprzez integrację Active Directory, LDAP
 8. aplikacja integruje się z dowolną skrzynką pocztową działająca na protokole POP, POPS, IMAP, IMAPS, SMTP, SMTPS, jak również obsługuje Exchange Web Services (EWS)
 9. kalendarz przeznaczony dla serwisantów, pozwalający na rejestrowanie nieobecności i wyznaczanie zastępstw. System pozwala na automatyczne przekierowanie zgłoszeń do wskazanego technika zapasowego (bazując na dacie zarejestrowania zgłoszenia bądź dacie rozwiązania zgłoszenia) lub wyłączenie umowy SLA dla zgłoszenia
 10. interfejs programowania aplikacji API (Application Programming Interface)
 11. analiza czasów: przypisania zgłoszenia do danego technika, przypisania zgłoszenia do danej grupy wsparcia, przypisania zgłoszenia do danego statusu
 12. Możliwość utworzenia macierzy priorytetów,
 13. rejestracja zgłoszenia przez użytkownika poprzez stronę www, załączenie dowolnej ilości dowolnego formatu załączników
 14. przeglądanie przez użytkownika na stronie www statusu własnych zgłoszeń, dodawania komentarzy oraz przeglądania bazy wiedzy
 15. interfejs zarejestrowanych zgłoszeń, w tym widok prezentujący listę zarejestrowanych zgłoszeń incydentów i zadań
 16. w ramach rozwiązywania zgłoszeń możliwość komunikacji z użytkownikiem poprzez pocztę elektroniczną i rejestrację wiadomości do właściwych wątków zgłoszeń
 17. automatyczna eskalacja zgłoszeń do grup wsparcia lub osób odpowiedzialnych za dany obszar
 18. przekierowanie zgłoszeń do innych serwisantów lub grup wsparcia celem dalszej obsługi
 19. możliwość zdefiniowania SLA
 20. automatyczne przypisywanie osób wymaganych do akceptacji zgłoszenia w oparciu o sposób wypełnienia zgłoszenia, akceptacje mogą być oparte o dowolne atrybuty zgłaszającego oraz dane osoby zgłaszającej
 21. tworzenie raportów zarejestrowanych incydentów, problemów i zmian filtrowanych według kategorii, centrów, statusu zgłoszenia, użytkownika oraz czasu pracy użytkowników w ramach rozwiązywania zgłoszeń, tworzenie raportów wg własnego zapotrzebowania
 22. wbudowaną funkcjonalność exportu utworzonych raportów do plików formatu PDF, XLS, CSV, XML, DOC i HTML
 23. funkcjonalność wykonywania zapytań SQL do bazy danych oprogramowania, funkcjonalność ta jest realizowana poprzez interfejs webowy oprogramowania
3. Wymagane prace wdrożeniowe
- 1) Instalacja przez oferenta rozwiązania na dedykowanym zasobie wirtualnym Zamawiającego;
 - 2) konfiguracja wstępna i nadanie dostępu do logowania dla Zamawiającego;
 - 3) przygotowanie po konsultacji z Zamawiającym podstawowych elementów system takich jak: kategorie, podkategorie, role;
 - 4) konfiguracja szablonów i formularzy zgodnie z wymogami Zamawiającego oraz po konsultacji z Wykonawcą i wdrożeniem w oparciu o najlepsze praktyki;
 - 5) konfiguracja powiadomień na wskazaną przez Zamawiającego skrzynkę pocztową za pośrednictwem dedykowanej skrzynki technicznej dostarczonej przez Zamawiającego.

Zadanie 5 – System do agregacji logów / SIEM

1. Przedmiot zamówienia

Przedmiotem zamówienia jest:

- 1) dostawa oprogramowania do logowania i analizowania dzienników zdarzeń i logów z infrastruktury IT Zamawiającego;
- 2) przeprowadzenie szkolenia z posługiwania się dostarczonym rozwiązaniem.

2. Termin realizacji zamówienia oraz liczba dostarczanego sprzętu

Zamawiający wymaga, aby dostawa systemu do Zamawiającego nastąpiła w terminie 8 tygodni od podpisania Umowy.

3. Wymagania wobec Wykonawcy

O udzielenie zamówienia mogą ubiegać się Wykonawcy, który posiadają niezbędną wiedzę i kwalifikacje do realizacji zamówienia. Wykonawca musi spełniać wszystkie poniższe warunki:

- Wymaga się, aby wykonawca wykazał się doświadczeniem w podobnych realizacjach, tzn. wykaże referencje, że w okresie 2 lat przed terminem składania ofert, a jeżeli okres działalności jest krótszy w tym okresie - zrealizował dostawy systemu backupu dla minimum 2 klientów, gdzie wartość jednostkowa zamówienia wynosiła minimum 10 000 zł netto

4. Szczegółowe wymagania odnośnie proponowanego rozwiązania

L.p.	Parametr lub warunek minimalny	Minimalne wymagania
1.	Wymagania ogólne	W ramach postępowania wymagany jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi wersje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).
2.	Interfejsy, Dysk:	1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB.
3.	Parametry wydajnościowe	1. System musi być w stanie przyjmować minimum 5 GB logów na dzień. 2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.
4.	Logowanie	W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje: 1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: a. Listę najczęściej wykrywanych ataków. b. Listę najbardziej aktywnych użytkowników. c. Listę najczęściej wykorzystywanych aplikacji. d. Listę najczęściej odwiedzanych stron www. e. Listę krajów, do których nawiązywane są połączenia.

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCIBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

		<p>f. Listę najczęściej wykorzystywanych polityk Firewall.</p> <p>g. Informacje o realizowanych połączeniach IPSec.</p> <p>4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.</p> <p>5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.</p> <p>6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.</p>
5.	Raportowanie	<p>W zakresie raportowania system musi zapewniać:</p> <ol style="list-style-type: none"> 1. Generowanie raportów co najmniej w formatach: PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Funkcję definiowania własnych raportów. 4. Możliwość spolszczenia raportów. 5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.
6.	Kolekcja logów	<p>W zakresie korelacji zdarzeń system musi zapewniać:</p> <ol style="list-style-type: none"> 1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: <ul style="list-style-type: none"> • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie vpn, utracone połączenie sieciowe. 4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.
7.	Zarządzanie	<ol style="list-style-type: none"> 1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. <ol style="list-style-type: none"> a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. 2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
8.	Serwisy i licencje	<ol style="list-style-type: none"> 1. System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. 2. Wsparcie: System musi być objęty serwisem producenta upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7 oraz mieć zalicencjonowaną funkcję analizy logów archiwalnych przez okres 24 miesięcy.
9.	Opisy wymagań ogólnych	<ol style="list-style-type: none"> 1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z

*SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCIBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II*

		<p>dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.</p> <p>2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.</p>
--	--	--

5. Wymagane prace wdrożeniowe

- 1) Analiza bieżącego stanu środowiska
- 2) Instalacja systemu w środowisku Zamawiającego
- 3) Konfigurację portów wymaganych przez SIEM
- 4) Instalację agenta SIEM na systemach Windows
- 5) Instalację agenta SIEM na Hyper-V
- 6) Instalację agenta SIEM na systemach Linux
- 7) Utworzenie reguły dla poszczególnych grup agentów
- 8) Podłączenie urządzeń sieciowych do SIEM
- 9) Dostosowanie reguł zbierania logów z urządzeń
- 10) Dostosowanie reguł zbierania logów z systemów Windows
- 11) Dostosowanie reguł zbierania logów z systemów Linux
- 12) Utworzenie reguł normalizacji logów, jeśli będzie taka potrzeba
- 13) Skonfigurowanie modułu integralności plików oraz rejestru na systemach Windows monitorowanych przez SIEM
- 14) Uruchomienie modułu wykrywającego podatności CVE na systemach monitorowanych przez SIEM

Zadanie 6 – Wykonanie skanów podatności

1. Przedmiot Zamówienia

Przedmiotem zamówienia jest przeprowadzenie jednorazowego skanu podatności z wykorzystaniem systemu klasy **Vulnerability Management**, umożliwiającego skanowanie podatności w środowisk IT, oraz analizę wyników. System ten musi być uruchomiony lokalnie w środowisku Zamawiającego, w celu wykonania sieci wewnętrznych. Dodatkowo wykonawca musi zapewnić wsparcie techniczne podczas realizacji projektu, a także wsparcie personelu Zamawiającego w zakresie przygotowanie infrastruktury IT do wykonania skanowania.

2. Termin realizacji zamówienia oraz liczba dostarczanego sprzętu

Zamawiający wymaga, aby dostawa sprzętu do Zamawiającego nastąpiła w terminie 8 tygodni od dnia podpisania Umowy.

3. Wymagania funkcjonalne systemu skanowania podatności

3.1. Skanowanie sieci i urządzeń

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

- System musi umożliwiać wykonywanie **nieograniczonej liczby skanów** sieci, w tym planowanych oraz skanów na żądanie.
- Skanowanie musi obejmować zarówno środowiska IPv4, jak i **IPv6**.
- Konieczna jest możliwość dodania urządzeń do skanowania poprzez wprowadzenie pojedynczego adresu IP, zakresu adresów IP oraz adresu sieci wraz z maską.
- Rozwiązanie musi umożliwiać **segmentację skanów** oraz obsługę skanów w rozproszonych geograficznie sieciach.

3.2. Funkcjonalność skanowania aplikacji webowych

- System musi posiadać możliwość dodawania aplikacji webowych do skanowania z opcjami takimi jak konfiguracja uwierzytelniania, tworzenie białych i czarnych list URL, a także definiowanie rozszerzeń, które mają być skanowane.
- System musi obsługiwać uwierzytelnione skanowanie aplikacji webowych, w tym **HTTP Basic** oraz **HTTP Form**.

3.3. Skanowanie urządzeń fizycznych i wirtualnych

- System musi umożliwiać dodanie urządzeń do skanowania za pomocą plików **CSV** oraz przypisywanie urządzeniom i aplikacjom webowym odpowiednich tagów oraz poziomu wpływu biznesowego (Neutral, Low, Medium, High).
- Konieczne jest wsparcie dla tworzenia dynamicznych znaczników/tagów na podstawie warunków takich jak nazwa urządzenia, zakres adresów IP, otwarte porty, czy system operacyjny.

3.4. Wymagania dotyczące sond skanujących

- Sonda skanująca musi być rejestrowana w centralnej konsoli zarządzającej przy użyciu wygenerowanego przez administratora tokena.

4. Wymagania Funkcjonalne

4.1. Zarządzanie podatnościami

- System musi posiadać funkcję priorytetyzacji oraz sortowania podatności, a także możliwość ich grupowania na podstawie różnych kryteriów, takich jak stan, typ, poziom krytyczności, status wykrycia, kategorie czy znaczniki.

4.2. Raportowanie

- System musi posiadać rozbudowane możliwości generowania raportów, w tym:
 - o Raporty z wyników skanowania sieci.
 - o Raporty z wyników skanowania aplikacji webowych.
 - o Raporty zgodności z regulacjami, takimi jak **ISO 27001, PCI DSS, OWASP**.
 - o Raporty delta (porównawcze) umożliwiające analizę zmian podatności w czasie.

4.3. Dodatkowe funkcje systemu

*SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II*

- System musi oferować możliwość dodawania nowych profili skanowania oraz korzystania z predefiniowanych profili producenta.
- Profil skanowania musi posiadać możliwość wyboru trybu skanowania (Full, Basic, Discovery), intensywności skanowania oraz wyboru testów podatności.
- System musi zapewniać co najmniej **105 tys. testów**.
- Rozwiązanie musi zapewniać możliwość przypisywania etykiet (tagów) do zasobów oraz edytowania informacji o aktywach, w tym takich, które mogą dotyczyć danych osobowych (zgodność z **RODO**).

5. Warunki realizacji

5.1. Instalacja i konfiguracja

- Wykonawca dokona instalacji oraz pełnej konfiguracji systemu na środowisku Zamawiającego wymaganego do skanu wewnętrznego sieci, zgodnie z przyjętymi założeniami oraz wymogami technicznymi producenta,
- Wykonawca wspomaga IT Zamawiającego w zakresie przygotowanie infrastruktury IT do prawidłowego wykonania skanowania.

5.2. Przeprowadzenie skanowania

- W ramach realizacji zamówienia Wykonawca przeprowadzi jednorazowy skan podatności zgodnie z ustalonym harmonogramem oraz profilami skanowania wskazanymi przez Zamawiającego.
- Wykonawca przygotowuje raport na podstawie zebranych danych dla Zamawiającego o stanie podatności w ramach realizowanego skanowania.

Zadanie 7 - Wdrożenie systemu Data Leak Protection – DLP

Wdrożenie DLP (Safetica) oraz konfiguracja polityk bezpieczeństwa.

1. Przedmiot zamówienia

1. Dostarczenie oprogramowania klasy DLP – 40 licencji bezterminowych z rocznym wsparciem
2. Implementacja rozwiązania w środowisku zamawiającego
3. Konfiguracja oprogramowania

2. Termin realizacji zamówienia oraz liczba dostarczanego sprzętu

Zamawiający wymaga, aby dostawa systemu do Zamawiającego nastąpiła w terminie 8 tygodni od daty podpisania Umowy.

3. Wymagania wobec Wykonawcy

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy posiadają niezbędną wiedzę i kwalifikacje do realizacji zamówienia. Wykonawca musi spełniać wszystkie poniższe warunki:

Wymaga się, aby wykonawca wykazał się doświadczeniem w podobnych realizacjach, tzn. wykaże referencje, że w okresie 2 lat przed terminem składania ofert, a jeżeli okres działalności jest krótszy w

*SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II*

tym okresie - zrealizował dostawy systemu backupu dla minimum 3 klientów, gdzie wartość jednostkowa zamówienia wynosiła minimum 10 000 zł netto.

Posiada co najmniej jednego pracownika z ważnym certyfikatem wystawionym przez producenta rozwiązania w zakresie wdrażania rozwiązania.

4. Wymagania szczegółowe Zamawiającego

Zestawienie wymaganych parametrów technicznych – system DLP

1. System operacyjny:

- a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
- b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
- c. MacOS 12 lub nowszy.

2. Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 (64-bit) i nowszych.

3. Serwer administracyjny musi obsługiwać bazy danych:

- a. MS SQL Server 2016 lub nowsze,
- b. MS SQL Express, c. AzureSQL S3 lub nowsze.

4. Pomoc i dokumentacja programu dostępne w języku angielskim.

5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.

6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.

7. Serwer administracyjny musi umożliwiać instalację/deinstalację zdalnego klienta na stacjach roboczych.

8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.

9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.

10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.

11. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.

12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.

13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.

14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).

15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.

16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.

*SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II*

17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.
19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
22. Dashboardsy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
23. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.
24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
26. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przysyłanie komunikatorami itp.
27. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.
28. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
29. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
30. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
31. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
32. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysłaną przez użytkowników Microsoft 365.

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCIBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

33. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
34. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach
35. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.)
36. System musi zapewniać możliwość zarządzania szyfrowaniem dysków twardych oraz urządzeń wymiennych.
5. Wymagane prace wdrożeniowe
1. Dostarczenie oprogramowania klasy DLP
 2. Implementacja rozwiązania w środowisku zamawiającego
 - a. Utworzenie i podstawowa konfiguracja VM
 - b. Instalacja konsoli centralnej
 - c. Wdrożenie agentów na wskazanych komputerach zamawiającego
 - d. Konfiguracja integracji dla Microsoft MS365
 3. Konfiguracja oprogramowania
 - e. Utworzenie do 5* reguł DLP
 - f. Utworzenie do 5* kategorii danych
 - g. Przygotowanie danych i oraz do 2 raportów, omówienie raportów i zebranych danych

Zadanie 8 - Zakup i konfiguracja UPS

Dostawa zasilacza awaryjnego UPS

1. Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. dostawa fabrycznie nowych sprzętów, nie używanych w innych środowiskach ani projektach;
2. udzielenie przez Wykonawcę gwarancji i zapewnienie w jej ramach serwisu gwarancyjnego oraz wsparcia technicznego na dostarczony Sprzęt;
3. dostarczenie przez Wykonawcę dokumentacji dostarczonego Sprzętu;
4. Podłączenie sprzętu w infrastrukturę elektryczną zamawiającego

2. Termin realizacji zamówienia oraz liczba dostarczanego sprzętu

Zamawiający wymaga, aby dostawa sprzętu do Zamawiającego nastąpiła w terminie 8 tygodni od dnia podpisania Umowy.

3. Wymagania wobec Wykonawcy

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy posiadają niezbędną wiedzę i kwalifikacje do realizacji zamówienia. Wykonawca musi spełniać wszystkie poniższe warunki:

- Wymaga się, aby wykonawca wykazał się doświadczeniem w podobnych realizacjach, tzn. Wykaże referencje, że w okresie 2 lat przed terminem składania ofert, a jeżeli okres

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCIBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

działalności jest krótszy w tym okresie - zrealizował dostawy urządzeń sieciowych dla minimum 3 klientów, gdzie wartość jednostkowa zamówienia wynosiła minimum 10 000 zł netto

4. Wymagania szczegółowe Zamawiającego

Zestawienie wymaganych parametrów technicznych systemu podtrzymania bateryjnego - Typ 1 – 1 sztuka

Nazwa komponentu	Wymagane minimalne parametry techniczne
Topologia	Line interactive
Typ przebiegu	Sinusoida
Liczba szaf rackowych	2U
Moc znamionowa w W	minimum 2700 W
Moc znamionowa w VA	minimum 3000 VA
Typowy czas ładowania do 90%	3 godziny
Rodzaj akumulatora	Akumulator kwasowo-ołowiowy
Masa produktu	Maksymalnie 37,5 kg
Sposób montażu	Montaż w szafie RACK (zestaw musi zawierać elementy montażowe)
Komunikacja i zarządzanie	<ul style="list-style-type: none"> Wielofunkcyjna konsola sterownicza i informacyjna LCD Wyświetlacz stanu LED ze wskaźnikiem zasilania Gniazdo karty zarządzania
Dostarczone wyposażenie	<ul style="list-style-type: none"> CD z oprogramowaniem Wsporniki montażowe do szaf przemysłowych Kabel do sygnalizacji RS-232 do Smart-UPS Czujnik temperatury podręcznik użytkownika Karta do zdalnego zarządzania Web SNMP Management Card
Certyfikaty produktu	C-Tick, CE, EAC, GOST, IRAM, VDE, UK PSTI
Normy	<ul style="list-style-type: none"> EN/IEC 62040-1:2019/A11:2021 EN/IEC 62040-2:2006/AC:2006 EN/IEC 62040-2:2018
Gwarancja	3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulator

Zestawienie wymaganych parametrów technicznych systemu podtrzymania bateryjnego - Typ 1 - 10 sztuk

Nazwa komponentu	Wymagane minimalne parametry techniczne
Topologia	Line interactive
Moc znamionowa w W	minimum 650 W
Moc znamionowa w VA	minimum 1200 VA
Typ przebiegu	Schodkowa aproksymacja sinusoidy
Typowy czas ładowania do 90%	8 godziny
Napięcie akumulatora	12 V
Masa produktu	Maksymalnie 8 kg

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

Sposób montażu	Wolnostojący
Rodzaj akumulatora	Akumulator kwasowo-ołowiowy
Typ połączenia wyjściowego	4 Schuko
Elementy zestawu	<ul style="list-style-type: none"> Podręcznik użytkownika
Komunikacja i zarządzanie	<ul style="list-style-type: none"> Dioda led wskazująca na status zasilania: zasilanie z sieci energetycznej: zasilanie z akumulatora
Certyfikaty produktu	CE, CB, EAC
Normy	<ul style="list-style-type: none"> EN/IEC 62040-1:2019/A11:2021 EN/IEC 62040-2:2006/AC:2006 EN/IEC 62040-2:2018
Gwarancja	2 lata na naprawę lub wymianę

CZEŚĆ II Zamówienia – Dostawa serwera dla Środowiskowego Domu Samopomocy w Więcborku

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa fabrycznie nowego serwera, nie finansowanego wcześniej z krajowych lub unijnych funduszy projektowych;

2. Termin realizacji zamówienia oraz liczba dostarczanego sprzętu

Zamawiający wymaga, aby dostawa systemu do Zamawiającego nastąpiła w terminie 6 tygodni.

3. Wymagania wobec Wykonawcy

O udzielenie zamówienia mogą ubiegać się Wykonawcy, który posiadają niezbędną wiedzę i kwalifikacje do realizacji zamówienia. Wykonawca musi spełniać wszystkie poniższe warunki:

- Wymaga się, aby wykonawca wykazał się doświadczeniem w podobnych realizacjach, tzn. wykaże referencje, że w okresie 2 lat przed terminem składania ofert, a jeżeli okres działalności jest krótszy w tym okresie - zrealizował dostawy sprzętu serwerowego dla minimum 3 klientów, gdzie wartość jednostkowa zamówienia wynosiła minimum 50 000 zł netto

4. Wymagania szczegółowe Zamawiającego:

Zestawienie wymaganych parametrów technicznych

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ul style="list-style-type: none"> Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3.5" Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Płyta główna	<ul style="list-style-type: none"> 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

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

Chipset	<ul style="list-style-type: none"> Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych
Procesor	<ul style="list-style-type: none"> Jeden procesor 8-rdzeniowy, min. 3.2GHz, umożliwiający osiągnięcie wyniku min. 95.1 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org w konfiguracji jednoprocessorowej.
Pamięć RAM	<ul style="list-style-type: none"> 2x16GB pamięci RAM DDR5 UDIMM o częstotliwości pracy 5600MT/s.
Kontroler RAID	<ul style="list-style-type: none"> Sprzętowy kontroler dyskowy, posiadający <ul style="list-style-type: none"> Min. 8GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących
Dyski twarde	<ul style="list-style-type: none"> Zainstalowane <ul style="list-style-type: none"> 3x dysk SSD SATA o pojemności min. 480GB, Hot-Plug. Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Sloty PCIe	<ul style="list-style-type: none"> Dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
Wbudowane porty	<ul style="list-style-type: none"> min. 4 porty USB w tym min: <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Zasilacze	<ul style="list-style-type: none"> Redundantne, o mocy maks. 700W klasy Titanium
Elementy montażowe	<ul style="list-style-type: none"> Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
System operacyjny/dodatki oprogramowania	<ul style="list-style-type: none"> Windows Server 2025 Standard - 16 Core License Pack

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCIBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

Bezpieczeństwo	<ul style="list-style-type: none"> • Zatrask 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. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 V3 • 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	<ul style="list-style-type: none"> • Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: <ul style="list-style-type: none"> o zdalny dostęp do graficznego interfejsu Web karty zarządzającej; o zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); o szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; o możliwość podmontowania zdalnych wirtualnych napędów; o wirtualną konsolę z dostępem do myszy, klawiatury; o wsparcie dla IPv6; o wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; o integracja z Active Directory; o możliwość obsługi przez dwóch administratorów jednocześnie; o wsparcie dla automatycznej rejestracji DNS o 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: <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> • Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> 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

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCIBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

	<ul style="list-style-type: none"> 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 przejścia 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. o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. o Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. o Zdalne uruchamianie diagnostyki serwera. o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania	<p>Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <ul style="list-style-type: none"> • Monitoring: <ul style="list-style-type: none"> o ilość podłączonych oraz rozłączonych systemów o stan podłączonych urządzeń o informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów o Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia o informacje o statusie gwarancji dla poszczególnych urządzeń o informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń o informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

	<ul style="list-style-type: none"> o Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych o Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. o Monitorowanie wydajności, przepustowości oraz opóźnień dla systemu pamięci masowych. o Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. o Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. o Monitoring parametrów serwerów z informacją o minimum: <ul style="list-style-type: none"> ♣ Obciążeniu procesora ♣ Zużyciu pamięci RAM ♣ Temperaturze procesorów ♣ Temperaturze powietrza wlotowego ♣ Zużyciu prądu ♣ Zmianach w fizycznej konfiguracji serwera ♣ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. o Monitoring parametrów pamięci masowych z informacją o minimum: <ul style="list-style-type: none"> ♣ Opóźnieniach ♣ IOPS ♣ Przepustowości ♣ Utylizacji kontrolerów ♣ Pojemność całkowita i dostępna ♣ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ♣ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ♣ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ♣ Informacje o poziomie redukcji danych ♣ Informacje o statusie replikacji oraz snapshotów o Monitoring parametrów przełączników sieciowych z informacją o minimum: <ul style="list-style-type: none"> ♣ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ♣ Stanie komponentów: zasilacze, wentylatory ♣ Podłączonych hostach ♣ Ilości i statusu portów ♣ Utylizacji procesora ♣ Utylizacji poszczególnych portów ♣ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware <ul style="list-style-type: none"> o możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania
--	---

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

	<ul style="list-style-type: none"> o możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty <ul style="list-style-type: none"> o Możliwość generowania raportów dla serwerów zawierających informację o: <ul style="list-style-type: none"> ♣ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ♣ Średnim obciążeniu: procesorów, pamięci RAM, IO, o Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: <ul style="list-style-type: none"> ♣ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji o Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo <ul style="list-style-type: none"> o Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. o Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. o Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. o Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia <ul style="list-style-type: none"> o Urządzenie Producenta dostarczane w ramach postępowania o Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent <ul style="list-style-type: none"> o Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności <ul style="list-style-type: none"> o Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne <ul style="list-style-type: none"> o Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	<ul style="list-style-type: none"> • 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

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCIBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

	<p>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 spełnianie wymogu.</p> <ul style="list-style-type: none"> 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.
Dokumentacja użytkownika	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 4 lat. Wymagana możliwość zachowania dysku twardego w ramach świadczonej usługi wsparcia serwisowego dla sprzętu, obejmująca 4-letni okres wsparcia serwisowego z gwarancją producenta. Usługa ma na celu umożliwienie zamawiającemu zachowania nośników danych (dysków twardych) po ich awarii. 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: <ul style="list-style-type: none"> Możliwość 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.

*SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCIBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II*

	<ul style="list-style-type: none"> o 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 autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
--	--

Zestawienie wymaganych parametrów technicznych odnośnie systemu operacyjnego:

- 1) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości.
- 2) Wbudowane wsparcie instalacji i pracy na wolumenach które:
 - a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - c) umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów,
 - d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
- 3) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- 4) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
- 5) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
- 6) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
- 7) Wbudowana zapora internetowa (firewall) z obsługi definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- 8) Graficzny interfejs użytkownika.
- 9) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
- 10) Możliwość zmiany języka interfejsu po zainstalowaniu systemu dla co najmniej języka polskiego i angielskiego.
- 11) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- 12) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
- 13) Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
- 14) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
 - a) podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 - b) usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - c) podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA – DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

- d) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
- e) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
- 15) Zdalna dystrybucja oprogramowania na stacje robocze.
- 16) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
- 17) PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - a) dystrybucję certyfikatów poprzez http,
 - b) konsolidację CA dla wielu lasów domeny,
 - c) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
- 18) Szyfrowanie plików i folderów.
- 19) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
- 20) Serwis udostępniania stron WWW
- 21) Wsparcie dla protokołu IP w wersji 6 (Ipv6).
- 22) Wbudowane usługi VPN pozwalające na zestawienie równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.

CZĘŚĆ III Zamówienia – Dostawa serwera dla Centrum Usług Społecznych w Więcborku

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa fabrycznie nowego serwera, nie finansowanego wcześniej z krajowych lub unijnych funduszy projektowych;

2. Termin realizacji zamówienia oraz liczba dostarczanego sprzętu

Zamawiający wymaga, aby dostawa systemu do Zamawiającego nastąpiła w terminie 6 tygodni.

3. Wymagania wobec Wykonawcy

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy posiadają niezbędną wiedzę i kwalifikacje do realizacji zamówienia. Wykonawca musi spełniać wszystkie poniższe warunki:

- Wymaga się, aby wykonawca wykazał się doświadczeniem w podobnych realizacjach, tzn. wykaże referencje, że w okresie 2 lat przed terminem składania ofert, a jeżeli okres działalności jest krótszy w tym okresie - zrealizował dostawy sprzętu serwerowego dla minimum 3 klientów, gdzie wartość jednostkowa zamówienia wynosiła minimum 50 000 zł netto

4. Wymagania szczegółowe Zamawiającego:

Zestawienie wymaganych parametrów technicznych

Parametr	Wymagania
Płyta główna	Dwuprocesorowa oparta na chipsecie do zastosowań serwerowych, pełni kompatybilna z dostarczonymi procesorami posiadająca możliwością instalacji modułu TPM min 2 złączy USB 3.2 min 16 złączy DIMM

SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II

	zintegrowany kontroler IPMI 2.0 z dedykowanym złączem RJ45
Procesor	<p>Zainstalowany procesor typu Intel XEON Gen 4 posiadający min 12rdzeni taktowany zegarem minimum 2.0GHz pamięć podręczną cache o wielkości minimum 30MB osiągający w teście PassMark - CPU Mark min .22000 punktów – wynik na dzień składania oferty</p> <p>ze względu na wymogi oprogramowania wymagane są procesory Intela</p>
Liczba procesorów	2 szt
Karta graficzna	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli – współpracująca z karta zarządzającą
Karty sieciowa	Wbudowane min. 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT
Zarządzanie	<p>Niezależna od zainstalowanego systemu operacyjnego dedykowana karta zarządzająca z dostępem przez dedykowany port RJ-45 Gigabit Ethernet zgodna z IPMI 2.0 umożliwiającą</p> <p>Zdalny dostęp do graficznego interfejsu Web karty zarządzającej</p> <p>Zdalne monitorowanie i informowanie o statusie stacji(temperaturze, prędkości obrotowej wentylatorów itd.)</p> <p>szyfrowane połączenie w sieci (SSL v3 lub TLS)</p> <p>włączenie, wyłączenie i restart serwera, aktualizacja Biosu</p> <p>podgląd logów sprzętowych serwera</p> <p>przejście pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS)</p> <p>możliwość podmontowania zdalnych wirtualnych napędów, plików ISO</p> <p>integracja z Active Directory</p>
Pamięć RAM	Minimum 256GB DDR5 RDIMM w modułach minimum 32GB,w konfiguracji wielokanałowej, pracująca z maksymalną częstotliwością obsługiwaną przez dostarczony procesor
Kontroler RAID	kontroler VROC obsługa poziomów Raid 0,1,10,
Dyski	<p>Dwa serwerowe dyski NVME U.2 o pojemności min 1.9TB i 5 letniej gwarancji producenta zainstalowane w kieszeniach hot swap serwera</p> <p>Dwa dyski o pojemności min 10TB ,prędkości obrotowej 7200rpm i MTBF min 2.0 miliona godzin zainstalowane w kieszeniach hot swap</p>
Obudowa-	<p>Typu „rack” 19’’ o wysokość max 2U wraz z zestawem szyn montażowym umożliwiającym montaż w typowej, 19-calowej szafie serwerowej,</p> <p>w tym pełne wysunięcie serwera z szafy posiadająca</p> <p>Dwa zasilacze Hot Swap o mocy co najmniej 1000W każdy i sprawności min 95% przy obciążeniu 50%</p> <p>Zasilacze muszą posiadać certyfikat Titanium Level Certified -wymagane załączenie do oferty raportu.</p> <p>Poprawna praca przy zasilaniu 200-240V (nominalne napięcie) AC 50 Hz</p> <p>Obudowa musi umożliwiać instalację min 8 dysków hot swap SAS 12Gb/s / SATA/SSD w tym 4 dysków NVME U.2 . (wolne zatoki na dyski obsadzone ramkami hot-swap, możliwość dodania własnego dysku przez użytkownika bez konieczności zakupu specjalnej ramki)</p>

*SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II*

	Zasilacze, dyski , wentylatory muszą być elementami Hot Swapowymi
Gniazda PCI-e	• Min. 6 slotów PCIe w tym minimum 4 sloty PCIe 5.0 x16
System operacyjny	Preinstalowany system operacyjny Windows Server 2025 STD PL + licencje CAL 40szt. Per device
Certyfikaty	Producent serwera powinien posiadać certyfikaty: PN-EN ISO 9001:2015, PN-EN ISO14001:2015 oraz PN-ISO/IEC 27001:2014 lub nowsze na procesy projektowania, produkcję, sprzedaż i serwis, PN-EN ISO 50001:2018 SA 8000:2014 Oferowany model serwera musi znajdować się na liście Windows Server Catalog i posiadać status Certified for Windows dla systemów Windows Server /2025 – wymagany wydruk ze strony https://www.windowsservercatalog.com Oznaczenie CE
Gwarancja	Minimum 36miesięcy + serwis on-site, czas reakcji 4h, czas naprawy w następnym dniu roboczym . Możliwość telefonicznego zgłaszania usterek w serwisie producenta komputera. Wymagany okres przyjmowania zgłoszeń serwisowych we wszystkie dni robocze.
Wsparcie techniczne	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Inne	Dostarczony sprzęt musi być fabrycznie nowy. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne
Oprogramowanie	Instalacja systemu oparta na wirtualizatorze Proxmox Oprogramowanie do kopii zapasowych dla wszystkich VM – Xopero/TerraCloud

5. Zestawienie wymaganych parametrów technicznych odnośnie systemów operacyjnych:

- 23) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości.
- 24) Wbudowane wsparcie instalacji i pracy na wolumenach które:
 - a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - c) umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów,
 - d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
- 25) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- 26) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
- 27) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
- 28) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
- 29) Wbudowana zaporę internetową (firewall) z obsługi definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

*SB.271.18.2025 ZAMAWIAJĄCY: GMINA WIĘCIBORK – TRYB PODSTAWOWY – DOSTAWA –
DOSTAWA SPRZĘTU W RAMACH PROJEKTU CYBERBEZPIECZNY SAMORZĄD – Etap II*

- 30) Graficzny interfejs użytkownika.
- 31) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
- 32) Możliwość zmiany języka interfejsu po zainstalowaniu systemu dla co najmniej języka polskiego i angielskiego.
- 33) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- 34) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
- 35) Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
- 36) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
 - a) podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 - b) usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - c) połączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - d) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - e) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
- 37) Zdalna dystrybucja oprogramowania na stacje robocze.
- 38) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
- 39) PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - a) dystrybucję certyfikatów poprzez http,
 - b) konsolidację CA dla wielu lasów domeny,
 - c) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
- 40) Szyfrowanie plików i folderów.
- 41) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
- 42) Serwis udostępniania stron WWW
- 43) Wsparcie dla protokołu IP w wersji 6 (IPv6).
- 44) Wbudowane usługi VPN pozwalające na zestawienie równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.