

Nr referencyjny ZP.271.3.2026

Załącznik nr 3 do SWZ

## **OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest: „Zakup, wdrożenie, konfiguracja oraz utrzymanie urządzeń (serwera redundancji, przełączników sieciowych, dyski NVMe, zasilacz UPS, router) w ramach projektu grantowego Cyberbezpieczny Samorząd” w ramach projektu grantowego Cyberbezpieczny Samorząd”.

Przedmiotowe zamówienie realizowane jest w ramach projektu współfinansowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa, Konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd”.

1. Przystępując do udziału w niniejszym postępowaniu oświadczam, iż spełniam wszystkie niżej określone wymagania w zakresie przedmiotu zamówienia oraz oferuję przedmiot zamówienia w pełni zgodny z określonym poniżej:
  - a) Dostarczane oprogramowanie i sprzęt muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich, rok produkcji nie starszy niż Q4 2025.
  - b) Dostarczony sprzęt i oprogramowanie pochodzić będą z oficjalnych kanałów dystrybucyjnych producenta obejmujących również rynek Unii Europejskiej, zapewniających w szczególności realizację uprawnień gwarancyjnych.
  - Zamawiający zastrzega, że sprzęt jak i podzespoły nie muszą być wyprodukowane na terenie UE, lecz muszą być dopuszczone do obrotu na terenie UE oraz musi być zapewniony dostęp do części zamiennych.
  - Wszystkie urządzenia muszą posiadać oznakowanie CE.
  - Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL)
  - Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V  $\pm$  10%, 50 Hz.
  - Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, w którym nie wskazano szczegółowych warunków gwarancji, musi być objęte minimum 24 miesięczną gwarancją, jeśli w opisie parametrów nie wskazano inaczej.
  - c) Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, aby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
  - d) Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
  - e) Do każdego urządzenia oraz oprogramowania musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekazać adresy WWW, pod którymi można je pobrać.
2. **Wykonawca zobowiązany jest do wdrożenia urządzeń do pracy w ramach infrastruktury IT jednostki, wykonania właściwych technicznych i logicznych połączeń urządzeń z siecią teleinformatyczną jednostki, wprowadzenie wszystkich ustawień z uwzględnieniem**

**prawidłowego działania reguł oraz regulacji ruchu zgodnie z wymaganiami i wskazówkami administratora sieci jednostki.**

3. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.
4. Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).

## Spis treści

<b>CZĘŚĆ PIERWSZA ZAMÓWIENIA DOSTAWA I KONFIGURACJA INFRASTRUKTURY IT</b>	<b>3</b>
1. Serwer - liczba sztuk: 1	3
2. Serwer NAS z backupem – liczba sztuk: 1	9
3. Router UTM z firewall – liczba sztuk: 1	10
4. Przełącznik sieciowy warstwy L2/L3 – 1 sztuka	12
5. Przełącznik sieciowy warstwy L2/L3 48 portowy – 2 sztuki	13
<b>CZĘŚĆ DRUGA ZAMÓWIENIA DOSTAWA I WDROŻENIE ZASILACZY AWARYJNYCH</b>	<b>14</b>
1. Zasilacz awaryjny UPS - liczba sztuk: 6	14
2. Zasilacz awaryjny UPS 2-stanowiskowy - liczba sztuk: 18	16
3. Zasilacz awaryjny UPS 1-stanowiskowy - liczba sztuk: 10	18
<b>CZĘŚĆ TRZECIA ZAMÓWIENIA</b>	<b>19</b>
1. Wdrożenie systemu klasy SIEM – szt. 1	19

## Opis parametrów minimalnych dostarczanej infrastruktury oraz oprogramowania:

Wymagania dla Wykonawcy, który dostarczy infrastrukturę sprzętową oraz oprogramowanie:

# CZĘŚĆ PIERWSZA ZAMÓWIENIA

## DOSTAWA I KONFIGURACJA INFRASTRUKTURY IT

### 1. Serwer - liczba sztuk: 1

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<p>Obudowa RACK o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych, oraz organizatorem do kabli.</p> <ul style="list-style-type: none"> <li>8 wnęk na dyski 2.5" z interfejsem NVMe;</li> <li>Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI</li> </ul>
Płyta główna	<ul style="list-style-type: none"> <li>Dwuprocessorowa, zaprojektowana i wyprodukowana przez producenta serwera,</li> <li>Obsługująca do 1 TB RAM przy wykorzystaniu 32 slotów</li> <li>Złącza PCI Express generacji 5,</li> <li>Wszystkie złącza PCI Express muszą być aktywne;</li> <li>Zainstalowany moduł TPM 2.0</li> </ul>
Procesor	<ul style="list-style-type: none"> <li>Dwa procesory typu skalownego z uwagi na licencjonowanie posiadający dokładnie 8 rdzeni działającego co najmniej z częstotliwością minimum 3.5 GHz i dającego w teście Passmark Dual CPU dostępnym na stronie <a href="https://www.cpubenchmark.net/">https://www.cpubenchmark.net/</a> wynik nie mniejszy niż 53 600 pkt. na dzień 21.01.2026 r.</li> </ul>
RAM	<ul style="list-style-type: none"> <li>Min 256GB DDR5, RDIMM, 6400 MT/s, ECC przy zachowaniu 24 wolnych slotów</li> </ul>
Dyski twarde	<ul style="list-style-type: none"> <li>Serwer ma mieć przewidzianą przez producenta możliwość dodania modułu pozwalającego na startowanie systemu z kart SD lub dysków M.2 skonfigurowanych w RAID1 nie zajmujących slotów na dyski.</li> <li>Zainstalowane co najmniej 6 dysków minimum 1.92TB SSD NVMe Read Intensive</li> </ul>
Karty sieciowe	<ul style="list-style-type: none"> <li>min. 4 interfejsy sieciowe 10Gb Ethernet w standardzie BASE-T</li> <li>min. 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (powyższe porty nie mogą być osiągnięte poprzez karty w slotach PCIe)</li> </ul>
Kontroler RAID	<ul style="list-style-type: none"> <li>Sprzętowy kontroler dyskowy 8 GB cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60</li> </ul>
Kontroler zdalnego zarządzania oraz oprogramowanie do zarządzania	<p>Tak, zapewnia dostęp do wirtualnej konsoli i możliwość montowania zdalnych nośników. To pozwala zdalnemu administratorowi na pełne sterowanie serwerem, w tym rozruch z montowanego zdalnie nośnika, przy użyciu przeglądarki internetowej i intuicyjnego interfejsu opartego na HTML5.</p> <p>Licencja na zarządzanie umożliwia wygodne zarządzanie całym środowiskiem z jednego miejsca, integrując rozwiązania różnych producentów. Wersja konsoli pozwala na raportowanie, inwentaryzację urządzeń i aktualizację firmware, sterowników oraz automatyczne wdrażanie nowych serwerów oraz tworzenie i wdrażanie schematów konfiguracyjnych i planów aktualizacji (Baseline), a dodatkowo oferuje integrację z wtyczkami partnerów, takich jak VMware Center i Microsoft System Center.</p>

	<ul style="list-style-type: none"> <li>• Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: <ul style="list-style-type: none"> <li>o wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych;</li> <li>o możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;</li> <li>o wsparcie dla protokołów – WMI, SNMP, IPMI, WSMAN, Linux SSH;</li> <li>o możliwość oskryptowywania procesu wykrywania urządzeń;</li> <li>o możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram;</li> <li>o szczegółowy opis wykrytych systemów oraz ich komponentów;</li> <li>o możliwość eksportu raportu do CSV, HTML, XLS;</li> <li>o grupowanie urządzeń w oparciu o kryteria użytkownika;</li> <li>o automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń;</li> <li>o szybki podgląd stanu środowiska;</li> <li>o podsumowanie stanu dla każdego urządzenia;</li> <li>o szczegółowy status urządzenia/elementu/komponentu;</li> <li>o generowanie alertów przy zmianie stanu urządzenia;</li> <li>o filtry raportów umożliwiające podgląd najważniejszych zdarzeń;</li> <li>o integracja z service desk producenta dostarczonej platformy sprzętowej;</li> <li>o możliwość przejęcia zdalnego pulpitu;</li> <li>o możliwość podmontowania wirtualnego napędu;</li> <li>o kreator umożliwiający dostosowanie akcji dla wybranych alertów;</li> <li>o możliwość importu plików MIB;</li> <li>o przesyłanie alertów „as-is” do innych konsol firm trzecich;</li> <li>o aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania);</li> <li>o możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta;</li> <li>o możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów;</li> </ul> </li> <li>• moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.</li> </ul>
Aplikacja do zarządzania	<p><b>Aplikacja mobilna do zarządzania serwerami powinna umożliwiać:</b></p> <ul style="list-style-type: none"> <li>o Monitorowanie stanu serwerów, w tym odczyt parametrów zdrowia, inwentarza i konfiguracji.</li> <li>o Konfigurowanie ustawień serwera, takich jak parametry sieci, hasła administratora i kolejność urządzeń rozruchowych.</li> <li>o Bezpośrednią komunikację z kontrolerem serwera za pomocą technologii bezprzewodowej.</li> <li>o Zdalne zarządzanie serwerami poprzez połączenie z konsolą zarządzania.</li> <li>o Pobieranie informacji o serwerach takich jak inwentarz, status, alerty oraz logi.</li> <li>o Konfigurowanie serwerów zdalnie.</li> <li>o Wysyłanie poleceń sterowania zasilaniem i innych poleceń.</li> <li>o Otrzymywanie powiadomień o alertach z systemów zarządzania.</li> <li>o Pobieranie informacji o gwarancji.</li> <li>o Uruchamianie zewnętrznych aplikacji, takich jak klienty zdalnego pulpitu.</li> </ul>

	<ul style="list-style-type: none"> <li>o Zabezpieczenie danych w aplikacji poprzez szyfrowanie z użyciem klucza specyficznego dla urządzenia.</li> <li>o Opcjonalne zabezpieczenie dostępu do aplikacji za pomocą hasła i biometrii.</li> <li>o Automatyczne wylogowanie w przypadku braku aktywności.</li> <li>o Połączenie z serwerami za pomocą technologii Bluetooth Low Energy (BLE) lub Wi-Fi.</li> <li>o Wyświetlanie szczegółowych informacji o serwerze oraz dzienników.</li> <li>o Otrzymywanie automatycznych powiadomień z konsoli zarządzania.</li> <li>o Przypisywanie adresów IP i modyfikowanie haseł.</li> <li>o Konfigurowanie atrybutów BIOS.</li> <li>o Wyłączanie i włączanie serwera oraz dostęp do konsoli systemowej.</li> <li>o Pobieranie danych z systemów zarządzania typu "jeden do wielu".</li> <li>o Wyświetlanie certyfikatu systemu w celu weryfikacji tożsamości przy pierwszym połączeniu.</li> <li>• Aplikacja powinna być dostępna do pobrania w popularnych sklepach z aplikacjami</li> </ul>
Wbudowane porty	<p>Z przodu:</p> <ul style="list-style-type: none"> <li>• 1 × USB 2.0 Type-C</li> <li>• 1 × Dedykowany port Ethernet do iDRAC (zarządzanie)</li> </ul> <p>Z tyłu:</p> <ul style="list-style-type: none"> <li>• 1 × Dedykowany port Ethernet do iDRAC</li> <li>• 1 × VGA</li> <li>• 2 × USB 3.1 Type-A</li> </ul>
Zasilacze	<ul style="list-style-type: none"> <li>• Podwójny nadmiarowy (1+1) z możliwością wymiany bez wyłączania systemu 800W w Hot-Plug Titanium</li> </ul>
System operacyjny/dodatkowe oprogramowanie	<ul style="list-style-type: none"> <li>• System obsługujący wszystkie rdzenie, wersja wielojęzyczna Hyper-V, AD DS, DNSSEC, DHCP, Failover Clustering, 50 licencji CAL użytkownika na system. System najnowszy na czas składania oferty. Licencja na serwerowy system operacyjny, w wersji najnowszej oferowanej przez producenta musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego.</li> <li>• Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na zaoferowanym serwerze. Dostarczona licencja powinna umożliwiać korzystanie z usług wszystkich rdzeni serwera.</li> <li>• Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.</li> <li>• Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.</li> <li>• Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.</li> <li>• Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</li> <li>• Możliwość dynamicznego obniżania poboru energii przez rdzenie procesora niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.</li> <li>• Wbudowane wsparcie instalacji i pracy na wolumenach, które:</li> <li>• pozwalają na zmianę rozmiaru w czasie pracy systemu,</li> <li>• b) umożliwiają tworzenie w czasie pracy systemu migawek, dających</li> </ul>

	<p>użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,</p> <ul style="list-style-type: none"> <li>• umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,</li> <li>• umożliwiają zdefiniowanie list kontroli dostępu (ACL).</li> <li>• Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</li> <li>• Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.</li> <li>• Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.</li> <li>• Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</li> <li>• Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.</li> <li>• Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play).</li> <li>• Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</li> <li>• Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.</li> <li>• Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).</li> <li>• Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:</li> <li>• Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,</li> <li>• 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:</li> <li>• Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,</li> <li>• Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,</li> <li>• Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.</li> <li>• Zdalna dystrybucja oprogramowania na stacje robocze.</li> <li>• Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej</li> <li>• Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:</li> <li>• Dystrybucję certyfikatów poprzez http</li> <li>• Konsolidację CA dla wielu lasów domeny,</li> <li>• Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,</li> <li>• Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.</li> <li>• Szyfrowanie plików i folderów.</li> <li>• Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).</li> <li>• Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.</li> <li>• Serwis udostępniania stron WWW.</li> </ul>
--	---



	<ul style="list-style-type: none"> <li>• Wsparcie dla protokołu IP w wersji 6 (IPv6),</li> <li>• Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:</li> <li>• Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,</li> <li>• Obsługi ramek typu jumbo frames dla maszyn wirtualnych.</li> <li>• Obsługi 4-KB sektorów dysków</li> <li>• Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra</li> <li>• Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.</li> <li>• Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)</li> <li>• Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.</li> <li>• 17) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</li> </ul>
Bezpieczeństwo	<ul style="list-style-type: none"> <li>• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.</li> <li>• Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</li> <li>• BIOS powinien mieć możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła</li> <li>• Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</li> <li>• Moduł TPM 2.0</li> <li>• Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera</li> </ul>
Certyfikaty	<ul style="list-style-type: none"> <li>• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001</li> <li>• Serwer musi posiadać deklaracja CE.</li> <li>• Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2025.</li> </ul>
Dokumentacja użytkownika	<ul style="list-style-type: none"> <li>• Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</li> <li>• Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</li> </ul>
Warunki gwarancji	<ul style="list-style-type: none"> <li>• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat.</li> <li>• Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.</li> <li>• Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.</li> <li>• Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</li> <li>• Certyfikowany Technik Producenta z właściwym zestawem części do naprawy</li> </ul>

	<p>(potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.</p> <ul style="list-style-type: none"> <li>Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</li> <li>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.</li> <li>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii.</li> </ul> <p>Charakterystyka usługi diagnostyki:</p> <ul style="list-style-type: none"> <li>Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.</li> <li>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.</li> <li>Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.</li> <li>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.</li> <li>Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.</li> </ul> <ul style="list-style-type: none"> <li>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</li> <li>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.</li> </ul>
Montaż	<ul style="list-style-type: none"> <li>Dostawa urządzeń do siedziby Zamawiającego.</li> <li>Montaż serwera w szafie przy użyciu dedykowanych szyn.</li> <li>Wykonanie okablowania strukturalnego i zasilającego wewnątrz szafy (estetyczne ułożenie kabli w prowadnicach).</li> <li>Aktualizacja oprogramowania układowego (firmware/BIOS) do najnowszych wersji stabilnych.</li> <li>Wstępna konfiguracja kontrolera iDRAC oraz macierzy RAID zgodnie z wytycznymi Zamawiającego.</li> <li>Testy poprawności działania wentylatorów oraz zasilania redundantnego</li> </ul>



## 2. Serwer NAS z backupem – liczba sztuk: 1

Element / Cecha	Minimalne wymagane parametry techniczne
Obudowa i zasilanie	<ul style="list-style-type: none"> <li>• Typu Rack 2U z szynami montażowymi w standardzie 19". Nadmiarowe zasilacze (2 szt.) o mocy min. 550W każdy.</li> </ul>
Procesor	<ul style="list-style-type: none"> <li>• min 3,4 GHz x86 8 wątków PassMark CPU min. 12000 w trybie Multithread Rating oraz min. 3000 w trybie Single Thread Rating (<a href="https://www.cpubenchmark.net/">https://www.cpubenchmark.net/</a>)</li> <li>• Wynik testu załączyć do oferty</li> </ul>
Pamięć RAM	<ul style="list-style-type: none"> <li>• Minimum 16 GB DDR4 z obsługą korekcji błędów (ECC). Możliwość rozbudowy do min. 128 GB.</li> </ul>
Zatoki na dyski	<ul style="list-style-type: none"> <li>• Minimum 18 zatok na dyski SATA (3,5" SATA oraz 2,5" SATA)</li> </ul>
Dyski twarde	<ul style="list-style-type: none"> <li>• Min. 6 szt. dysków klasy Enterprise/NAS o poj. min. 12TB każdy (łącznie min. 72TB surowej). Prędkość 7200 RPM, MTBF min. 2 mln h</li> </ul>
Pamięć flash	<ul style="list-style-type: none"> <li>• Min 5GB</li> </ul>
Interfejsy sieciowe	<ul style="list-style-type: none"> <li>• Minimum 2 porty o przepustowości min. 10 GbE każdy. Minimum 2 porty o przepustowości 2,5 GbE</li> </ul>
System operacyjny	<ul style="list-style-type: none"> <li>• System producenta z graficznym interfejsem zarządzania przez WWW, w języku polskim, obsługujący system plików z obsługą migawek (Snapshots).</li> </ul>
Ilość portów USB	<ul style="list-style-type: none"> <li>• Min. 4 szt</li> </ul>
System backupu	<ul style="list-style-type: none"> <li>• Zintegrowane rozwiązanie bezagentowe do backupu maszyn wirtualnych (VMware/Hyper-V) oraz stacji roboczych Windows. Obsługa deduplikacji i kompresji danych.</li> </ul>
Protokoły	<ul style="list-style-type: none"> <li>• Obsługa SMB/CIFS, NFS, iSCSI, HTTP/HTTPS, FTP, SNMP, SSH.</li> </ul>
Bezpieczeństwo	<ul style="list-style-type: none"> <li>• Szyfrowanie wolumenów kluczem AES-256 bit, dwuetapowa weryfikacja logowania, zintegrowany system monitorowania stanu zdrowia dysków.</li> </ul>
Gwarancja	<ul style="list-style-type: none"> <li>• Minimum 60 miesięcy gwarancji producenta lub autoryzowanego serwisu świadczącej w miejscu instalacji.</li> </ul>

Wykonawca zobowiązany jest do przeprowadzenia pełnej konfiguracji zakupionego urządzenia w celu integracji z istniejącą infrastrukturą Zamawiającego.

**Wymagania dotyczące kompatybilności i wsparcia:**

Urządzenie musi być fabrycznie nowe, nieużywane.  
Musi pochodzić z oficjalnej polskiej dystrybucji,  
Producent musi udostępniać oprogramowanie i dokumentację.

### 3. Router UTM z firewall – liczba sztuk: 1

Lp.	Kategoria / Cecha	Wymagany parametr minimalny	Uwagi
<b>1.</b>	<b>Wydajność</b>		
1.1	Przepustowość Firewall	Min. 20 Gbps	Dla pakietów 1518 bajtów
1.2	Przepustowość IPS	Min. 2.6 Gbps	Zgodnie z testami producenta
1.3	Przepustowość NGFW	Min. 1.6 Gbps	Firewall, IPS, Kontrola aplikacji
1.4	Przepustowość Threat Protection	Min. 1 Gbps	Pełen pakiet UTP włączony
1.5	Liczba jednoczesnych sesji TCP	Min. 1,5 miliona	
1.6	Nowe sesje na sekundę (CPS)	Min. 56 000	
<b>2.</b>	<b>Interfejsy fizyczne</b>		
2.1	Porty Ethernet RJ-45 (1 Gbps)	Min. 12 portów	Dowolna konfiguracja portów (WAN/LAN/DMZ)
2.2	Porty SFP (1 Gbps)	Min. 4 porty	
2.3	Porty SFP+ (10 Gbps)	Min. 2 porty	
<b>3.</b>	<b>Niezawodność i budowa</b>		
3.1	Zasilanie	Podwójne, redundantne AC	Dwa wbudowane zasilacze
3.2	Format obudowy	Montaż w szafie RACK 19" (1U)	Wymagany zestaw montażowy
3.3	Pamięć masowa	Wbudowany dysk SSD (dla	Min. 1x 480 GB SSD

		logów/cache)	
--	--	--------------	--

### Wymagania dotyczące Pakietu Usług Bezpieczeństwa

Wykonawca dostarczy wraz z urządzeniem subskrypcję usług bezpieczeństwa na okres 12 miesięcy, obejmującą następujące funkcjonalności:

System zapobiegania włamaniom (IPS): Automatyczna aktualizacja sygnatur w czasie rzeczywistym, ochrona przed atakami typu exploit oraz ochrona przed lukami w oprogramowaniu.

Zaawansowana ochrona przed złośliwym oprogramowaniem: Wykrywanie i blokowanie wirusów, spyware oraz zagrożeń typu ransomware na poziomie bramy sieciowej.

Usługa piaskownicy (Sandbox) w chmurze: Mechanizm analizy behawioralnej podejrzanych plików w odizolowanym środowisku wirtualnym w celu wykrywania zagrożeń typu "zero-day".

### Filtrowanie treści WWW:

- Klasyfikacja witryn internetowych na podstawie kategorii (min. 75 kategorii tematycznych) oraz możliwość blokowania dostępu do stron szkodliwych i zainfekowanych.
- Filtrowanie treści wideo: Możliwość granularnej kontroli i filtrowania dostępu do portali strumieniowych (np. na podstawie kategorii treści).

### Kontrola aplikacji:

- Rozpoznawanie i kontrola (blokowanie/limitowanie) aplikacji sieciowych niezależnie od używanego portu lub protokołu.
- Ochrona przed niechcianą pocztą (Antispam):
- Weryfikacja nadawców oraz filtrowanie treści wiadomości e-mail w celu blokowania spamu i phishingu.

### Wsparcie Techniczne i Gwarancja

Serwis Producenta:

Dostęp do pomocy technicznej w trybie 24/7 (całodobowo) realizowanej przez inżynierów producenta urządzenia.

Aktualizacje:

Możliwość pobierania i instalowania aktualizacji oprogramowania układowego (firmware) oraz poprawek bezpieczeństwa przez cały okres trwania subskrypcji.

Wymiana sprzętowa:

W przypadku awarii fizycznej urządzenia, Wykonawca zapewni dostarczenie sprawnego urządzenia zastępczego lub naprawę w terminie do następnego dnia roboczego (tryb NBD - Next Business Day).

### Usługa konfiguracji polityk UTM i wdrożenia: polityk Port Security, DHCP Snooping, VLAN, DNS Spoofing, segmentacja sieci LAN .

Montaż urządzenia w szafie RACK oraz podłączenie do infrastruktury Zamawiającego.

Inicjalna konfiguracja systemu operacyjnego, aktualizacja do najnowszej stabilnej wersji.

Migracja lub stworzenie nowych polityk bezpieczeństwa (reguły filtrowania ruchu, translacja adresów NAT).

Konfiguracja bezpiecznego dostępu zdalnego (VPN) z wykorzystaniem uwierzytelniania dwuskładnikowego (MFA).

Uruchomienie i dostrojenie wszystkich systemów bezpieczeństwa

Przeprowadzenie szkolenia stanowiskowego dla administratorów (min. 4h) oraz przekazanie dokumentacji powykonawczej wraz z kopią zapasową konfiguracji.

#### 4. Przełącznik sieciowy warstwy L2/L3 – 1 sztuka

Urządzenie musi być zarządzalnym przełącznikiem sieciowym warstwy 2 z funkcjonalnością L2 oraz obsługą warstwy 3, przeznaczonym do montażu w szafie rack 19”.

Kategoria	Wymagany parametr minimalny
Konstrukcja	Obudowa typu Rack 19”, wysokość max 1U.
Procesor	4-rdzeniowy min 1.7 GHz
Pamięć RAM	Min 4 GB DDR4
Porty dostępne	Minimum 1 port RJ-45 10/100/1000 Mbps 12x 10 Gbps 2x 25 Gbps
Zasilanie	Redundantne (2x) AC 100-240V, wbudowane zasilacze
Wymiar	Max 443 x 224 x 44 mm
Mirroring portów	Możliwość duplikacji ruchu na port w celu analizy
Zarządzanie	Dostęp przez dedykowaną aplikację, przeglądarkę WWW oraz interfejs linii komend
Protokoły STP	Obsługa STP, RSTP, MSTP (zapobieganie pętlom).
Pobór mocy	Maksymalnie 49 W
Okablowanie	Do każdego przełącznika należy dostarczyć 12 kabli do stackowania dwóch urządzeń za pomocą portów SFP+ o długości 3 m
Gwarancja	24 miesiące

Wykonawca zobowiązany jest do przeprowadzenia pełnej konfiguracji zakupionych przełączników sieciowych w celu integracji z istniejącą infrastrukturą Zamawiającego.

#### Wymagania dotyczące kompatybilności i wsparcia:

Urządzenie musi być fabrycznie nowe, nieużywane, Musi pochodzić z oficjalnej polskiej dystrybucji, Producent musi udostępniać oprogramowanie i dokumentację.

## 5. Przełącznik sieciowy warstwy L2/L3 48 portowy – 2 sztuki

Urządzenie musi być zarządzalnym przełącznikiem sieciowym warstwy 2 z funkcjonalnością L2 oraz obsługą warstwy 3, przeznaczonym do montażu w szafie rack 19”.

Kategoria	Wymagany parametr minimalny
Typy portów Ethernet	48 portów Gigabit Ethernet (10/100/1000 Mb/s) RJ45 z PoE+
Porty światłowodowe SFP+	4 sloty SFP+ (10 Gb/s)
Porty światłowodowe QSFP+	2 sloty QSFP+ (40 Gb/s)
Przepustowość	168 Gb/s
Zdolność przełączania	336 Gb/s
Prędkość przekazywania pakietów	235 Mp/s
Zasilanie PoE	48 wyjść PoE (na każdym porcie Ethernet), tryby 802.3af/at lub pasywny
Maksymalna łączna moc PoE	750 W
Zarządzanie	Zarządzanie L3 (przełącznik warstwy 3)
Montaż	Możliwość montażu w szafie rack 19"
Zasilanie	wbudowany zasilacz AC 100-240 V
Zarządzanie	Dostęp przez dedykowaną aplikację, przeglądarkę WWW oraz interfejs linii komend
Gwarancja	24 miesiące

Wykonawca zobowiązany jest do przeprowadzenia pełnej konfiguracji zakupionych przełączników sieciowych w celu integracji z istniejącą infrastrukturą Zamawiającego.

### Wymagania dotyczące kompatybilności i wsparcia:

Urządzenie musi być fabrycznie nowe, nieużywane.

Musi pochodzić z oficjalnej polskiej dystrybucji.

Producent musi udostępniać oprogramowanie i dokumentację.



## CZĘŚĆ DRUGA ZAMÓWIENIA

### DOSTAWA I WDROŻENIE ZASILACZY AWARYJNYCH

#### 1. Zasilacz awaryjny UPS - liczba sztuk: 6

L.p.	Nazwa komponentu	Wymagane parametry techniczne
1	2	3
1.	Model, symbol, producent urządzenia	
2.	Technologia	online, VFI-SS-111,
3.	Moc wyjściowa	3kVA/3kW; PF=1
4.	Obudowa	Rack/Tower Zestaw do montażu w szafie rack na wyposażeniu dla urządzenia oraz modułu bateryjnego
5.	Napięcie wejściowe	110 ÷ 300 V AC ± 2 %
6.	Napięcie znamionowe (wartość skuteczna)	230V AC
7.	Prąd znamionowy (wejście)	15,6A
8.	Częstotliwość napięcia wejściowego (zakres oraz tolerancja)	45 ÷ 55 / 55 ÷ 65 Hz ± 1 Hz
9.	Częstotliwość znamionowa napięcia wejściowego	50Hz / 60Hz
10.	Zniekształcenia prądu wejściowego THDi	< 5%
11.	Zakres napięcia wyjściowego	200/208/220/230/240V AC konfigurowalne z poziomu oprogramowania oraz z menu zasilacza na wyświetlaczu LCD (domyślnie 230V AC)
12.	Zniekształcenia napięcia wyjściowego THDu	< 1% dla Pmax (liniowe) < 5% (nieliniowe wg PN EN 62040-3)
13.	Gniazda wyjściowe	4x IEC320 C13 (10A) sterowalne + 4x IEC320 C13 (10A) + 1x IEC320 C19 (16A)
14.	Akumulatory wewnętrzne UPS	Minimum 6szt akumulatorów 12V9Ah
15.	Moduły bateryjne	możliwość podpięcia do 4szt modułów (każdy z minimum 12szt akumulatorów 12V9Ah)
16.	Wymagany czas podtrzymania oferowanego zestawu dla obciążenia 3kW/2,4kW/1,5kW	17 / 23 / 40 min (akumulatory umieszczone w UPS i maksymalnie 1 Module Bateryjnym)



17.	Przeciążalność	105-125% - 5min / 125-150% - 30s / >150% - 500ms
18.	EPO	Wymagane – standard NC
19.	Sygnalizacja	akustyczno-diodowa, wyświetlacz LCD oraz diody sygnalizujące usterkę, pracę baterijną, pracę w trybie online, obejście bypass
20.	Język oprogramowania	polski i angielski do wyboru z poziomu interfejsu użytkownika
21.	Konfiguracja minimalnego poziomu naładowania baterii po powrocie zasilania sieciowego (po rozładowaniu baterii przed ponownym samoczynnym załączeniem zasilania na wyjściu)	Wymagane, konfigurowalne z poziomu oprogramowania (przez USB)
22.	Wymagane certyfikaty	CE, ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu; (załączyć dokument)
23.	Komunikacja z urządzeniem	RS232, USB HID, styki bezpotencjałowe 1-wejście; 1-wyjście; SNMP – wymagana na wyposażeniu
24.	Wymiary UPS (rack) (wys x szer x gł)	Nie więcej niż 86 x 439 x 600 mm
25.	Oprogramowanie do monitorowania pracy zasilacza UPS	Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na min. 75 stanowiskach komputerowych w sieci; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów (potwierdzone oświadczeniem producenta oprogramowania)
26.	Oprogramowanie - funkcjonalność	możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPS'ów w oprogramowaniu
27.	Oprogramowanie - funkcjonalność	Konfiguracja minimalnego poziomu naładowania baterii. UPS po rozładowaniu baterii przed samoczynnym załączeniem zasilania wyjść (po powrocie zasilania sieciowego) będzie musiał naładować baterie do tego poziomu. Parametr ten ma zastosowanie w przypadku, gdy załączenie zasilania wyjść może nastąpić tylko wtedy, gdy UPS zgromadzi niezbędny zapas energii na wypadek kolejnego zaniku.
28.	Oprogramowanie - funkcjonalność	Uruchom poprzez Bypass - Aktywacja tej funkcji powoduje, że UPS zawsze przed załączeniem zasilania wyjść na kilka sekund załączy zasilanie poprzez Bypass i po chwili przełączy się w zasilanie wyjść poprzez falownik (normalny tryb pracy). Funkcja ta umożliwia załączenie urządzeń o zwiększonym prądzie rozruchowym bez przeciążania falownika UPS.
29.	Serwis producenta	Wymagany, zlokalizowany na terenie Polski



30.	Gwarancja	Minimum 24 miesięcy elektronika, 24 miesięcy akumulatory, serwis door to door
31.	Dokumentacja	Instrukcja w języku polskim
32.	Oświadczenie (załączyć do oferty)	Oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji

## 2. Zasilacz awaryjny UPS 2-stanowiskowy - liczba sztuk: 18

PARAMETRY \ TYP	
Moc wyjściowa (pozorna / czynna)	minimum 1600 VA
	minimum 1040 W
DANE OGÓLNE I ŚRODOWISKOWE	
Topologia	VI (line interactive)
Typ obudowy	TOWER
Temperatura pracy	0 ÷ +40 °C
WEJŚCIE	
Napięcie znamionowe (wartość skuteczna)	230 V AC
Zakres napięcia wejściowego (wartości skuteczne) i tolerancja	160 ÷ 264 V (~ 145 ÷ 280 V) ± 2 %
Częstotliwość znamionowa napięcia wejściowego	50 Hz
Zakres częstotliwości i tolerancja	45 ÷ 55 Hz ± 1 Hz
Progi przełączania: sieć – UPS	160 ÷ 264 V (~ 145 ÷ 280 V) ± 2 %
WYJŚCIE	
Napięcie znamionowe (wartość skuteczna)	230 V AC
Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa	184 ÷ 264 V (~ 167 ÷ 280 V) ± 2 %
Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca rezerwowa	230 V ± 5 %
Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej)	Sinusoidalny / Tak jak na wejściu
Częstotliwość znamionowa napięcia wyjściowego	50 Hz
Filtracja napięcia wyjściowego	LC, Filtr przeciwzakłóceńowy RFI/EMI, tłumik warystorowy
Progi przełączania: UPS – sieć	165 V / 259 V (~ 150 V / 275 V) ± 2 %
Czas przełączenia na pracę rezerwową	< 3 ms
Czas powrotu na pracę sieciową	0 ms
CZASY PODTRZYMANIA	
Czas podtrzymania z baterii wewnętrznych ( 100 % / 80 % / 50 %	minimum 4/ 5 / 8 min

Pmax)	
<b>PARAMETRY MECHANICZNE</b>	
Wymiary - tower (wys. x szer. x gł.)	nie większe niż 190 x 165 x 480 mm
Masa zasilacza	nie większa niż 17 kg
<b>ZABEZPIECZENIA</b>	
Zabezpieczenie wejściowe	Przeciwzwarciove - Bezpiecznik szklany 5 x 20 mm 10 A / 250 V AC
	Przeciwprzepięciowe
Zabezpieczenie wyjściowe	Elektroniczne – przeciwzwarciove i przeciążeniowe
<b>WYPOSAŻENIE I FUNKCJE DODATKOWE</b>	
Przyłącze zasilania UPS	Przewód zakończony wtyczką z uziemieniem 16A (PN-E-93201:1997) + uni-schuko
Przyłącza wyjściowe (liczba i typ gniazd)	4 x PN-E-93201
Sygnalizacja	Akustyczno – optyczna; diody LED
Interfejsy komunikacyjne	USB HID
Oprogramowanie monitorująco-zarządzające	Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów (potwierdzone oświadczeniem producenta oprogramowania)
	Możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPSów
	Możliwość zarządzania różnymi UPSami tego samego producenta
Wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.	
<b>GWARANCJA ORAZ SERWIS</b>	
Gwarancja	Minimum 36 miesięcy na elektronikę i 24 miesiące na akumulatory;
Serwis	Autoryzowany serwis producenta zlokalizowany w Polsce.
	Serwis realizowany w systemie door to door
<b>NORMY</b>	
Spełnione normy: PN-EN 62040-1:2009, PN-EN 62040-2:2008	
<b>CERTYFIKATY PRODUCENTA (ZAŁĄCZYĆ DO OFERTY)</b>	
ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania;	
Deklaracja CE producenta sprzętu	
<b>OŚWIADCZENIA / DOKUMENTY (ZAŁĄCZYĆ DO OFERTY)</b>	
Oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji	
Oświadczenie producenta o posiadaniu licencji oraz pełnych praw do oprogramowania do monitorowania pracy UPS	
Karta katalogowa oferowanego sprzętu w języku polskim	

**3. Zasilacz awaryjny UPS 1-stanowiskowy - liczba sztuk: 10**

<b>UPS 1200VA (parametry minimalne)</b>	
<b>Parametr</b>	<b>Wymagania minimalne</b>
Moc pozorna	min. 1200VA
Moc rzeczywista	min. 600W
Technologia	VI (line interactive)
Typ obudowy	wolnostojąca
<b>Praca sieciowa</b>	
Napięcie wejściowe	170 ÷ 280 V AC ± 7 %
Częstotliwość napięcia wejściowego	45 ÷ 55 Hz ± 1 Hz
Zakres napięcia wyjściowego	230 V AC ± 10 %
Kształt napięcia wyjściowego	Schodkowa aproksymacja sinusoidy / Tak jak na wejściu
Progi przełączania sieć – UPS	170 ÷ 280 V AC ± 7 %
Czas przełączania sieć – UPS	<6ms
<b>Praca bateryjna</b>	
Napięcie wyjściowe	~230V ± 10%
Częstotliwość napięcia wyjściowego	50Hz ± 1Hz
Kształt napięcia wyjściowego na pracy bateryjnej	Schodkowa aproksymacja sinusoidy
Progi przełączania UPS – sieć	176 V ÷ 274 V AC ± 7 %
Zabezpieczenie wyjściowe przeciwzwarcowe	elektroniczne
Zabezpieczenie wyjściowe przeciążeniowe	elektroniczne
Czas podtrzymania (P 0,8max/P 0,5max)	minimum 4,5 / 11 min
akumulatory wewnętrzne	minimum 2szt 12V 7Ah; szczelne, bezobsługowe
<b>Pozostałe</b>	
Wejście zasilania	IEC320 C14
Ilość i typ gniazd wyjściowych	minimum 2 x PN-E-93201 oraz 2 x IEC 320 C13 (10 A)
Filtr telekomunikacyjny	minimum filtr RJ45 (LAN 10/100 Base-T)
Sygnalizacja	Akustyczno-optyczna, w tym minimum wyświetlacz LCD sygnalizujący napięcie wejściowe i wyjściowe, poziom obciążenia, stan naładowania baterii
Zimny start	tak
Interfejs komunikacyjny	USB (kabel w komplecie)
Waga UPS	do 9kg
Wymiary	Nie większe niż: wysokość 195mm; szerokość 139mm; głębokość 365mm
Gwarancja	Min 24 miesiące na elektronikę i 12 miesięcy na akumulatory;
Serwis	Autoryzowany serwis producenta zlokalizowany w Polsce.
	Serwis realizowany w systemie door-to-door



Oprogramowanie	Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na min. 75 stanowiskach komputerowych w sieci; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów (potwierdzone oświadczeniem producenta oprogramowania)
	Wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.
Certyfikaty producenta (załączyć do oferty)	ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania;
	Deklaracja CE producenta sprzętu
Oświadczenia / dokumenty	Oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji
	Oświadczenie producenta o możliwości udostępnienia przed dostawą 1 sztuki wyrobu na testy w ciągu 3 dni roboczych od wezwania przez zamawiającego
	Oświadczenie producenta o posiadaniu licencji oraz pełnych praw do oprogramowania do monitorowania pracy UPS
	Karta katalogowa oferowanego sprzętu

## CZĘŚĆ TRZECIA ZAMÓWIENIA

### 1. Wdrożenie systemu klasy SIEM – szt. 1

Kategoria	Szczegółowe wymagania i zakres prac
Model licencjonowania i prawo własności	<ol style="list-style-type: none"> <li>System musi być dostarczony na licencji niewymagającej opłat subskrypcyjnych, czasowych ani zależnych od ilości przetwarzanych danych lub liczby podłączonych końcówek (licencja wieczysta/bezterminowa).</li> <li>Zamawiający musi otrzymać pełne uprawnienia administracyjne do systemu, umożliwiające jego dowolną modyfikację i rozbudowę bez udziału osób trzecich.</li> <li>Kod źródłowy rozwiązania musi być jawny, umożliwiający weryfikację bezpieczeństwa przez Zamawiającego.</li> </ol>
Platforma Serwerowa (Środowisko Wirtualne)	<ol style="list-style-type: none"> <li>Instalacja na systemie operacyjnym z rodziny Unix/Linux w najnowszej wersji stabilnej z długim wsparciem technicznym (LTS).</li> <li>Wykonawca dokona optymalizacji jądra systemu pod kątem wysokiej wydajności operacji wejścia/wyjścia (I/O).</li> <li>Konfiguracja bezpieczeństwa systemu operacyjnego (tzw. Hardening): usunięcie zbędnych usług, zamknięcie nieużywanych portów, konfiguracja mechanizmu kontroli dostępu do procesów oraz logowania operacji uprzywilejowanych.</li> <li>Przygotowanie struktury wolumenów dyskowych z uwzględnieniem separacji danych systemowych od bazy danych logów i indeksów (obsługa min. 500GB przestrzeni z</li> </ol>

	możliwością rozbudowy online).
Architektura Systemu Analizy Zdarzeń	<ol style="list-style-type: none"> <li>1. Wdrożenie silnika gromadzenia i korelacji zdarzeń w czasie rzeczywistym.</li> <li>2. Implementacja wydajnego mechanizmu indeksowania danych, pozwalającego na natychmiastowe przeszukiwanie zasobów historycznych (min. 100 tys. zdarzeń na sekundę).</li> <li>3. Uruchomienie interfejsu graficznego (webowego) umożliwiającego wizualizację zagrożeń, tworzenie raportów oraz zarządzanie konfiguracją systemu z poziomu przeglądarki.</li> <li>4. Zabezpieczenie panelu zarządzania za pomocą szyfrowania TLS oraz integracja z centralnym systemem uwierzytelniania (jeśli dotyczy).</li> </ol>
Funkcjonalność Monitorowania Bezpieczeństwa	<ol style="list-style-type: none"> <li>1. Monitorowanie Integralności (FIM): System musi wykrywać zmiany w kluczowych plikach systemowych, konfiguracjach i rejestrach w czasie rzeczywistym.</li> <li>2. Analiza Podatności: Automatyczna identyfikacja brakujących poprawek bezpieczeństwa oraz błędów w konfiguracji zainstalowanego oprogramowania na stacjach i serwerach.</li> <li>3. Detekcja Intruzów: Mechanizm wykrywania rootkitów, procesów ukrytych oraz anomalii w ruchu sieciowym na hostach.</li> <li>4. Mapowanie zagrożeń: Automatyczne przypisywanie wykrytych zdarzeń do globalnych baz wiedzy o taktykach i technikach ataków cybernetycznych.</li> </ol>
Wdrożenie Agentów i Integracja	<ol style="list-style-type: none"> <li>1. Automatyzacja wdrożenia: Wykonawca przygotowuje gotowe pakiety instalacyjne oraz skrypty umożliwiające masową dystrybucję oprogramowania agenta na systemy operacyjne z rodziny Windows oraz Linux.</li> <li>2. Komunikacja bezpieczna: Agenty muszą komunikować się z serwerem centralnym za pomocą szyfrowanego i uwierzytelnionego kanału (klucze RSA/AES).</li> <li>3. Pozyskiwanie danych bezagentowe: Konfiguracja zbierania logów z urządzeń sieciowych i systemów bezpieczeństwa niepozwalających na instalację agenta (poprzez protokoły strumieniowe).</li> <li>4. Dostrajanie (Tuning): Eliminacja fałszywych alarmów (false positives) poprzez stworzenie reguł wykluczeń dostosowanych do specyfiki środowiska Zamawiającego.</li> </ol>
Reagowanie na Incydenty i Powiadamianie	<ol style="list-style-type: none"> <li>1. Konfiguracja modułu aktywnej odpowiedzi, umożliwiającego automatyczne blokowanie adresów IP agresora lub izolację zainfekowanego hosta od sieci po przekroczeniu progu krytyczności zdarzenia.</li> <li>2. Uruchomienie wielokanałowego systemu powiadomień (e-mail/komunikatory/systemy ticketowe) o wykrytych naruszeniach bezpieczeństwa.</li> </ol>
Przekazanie Wiedzy i Dokumentacja	<ol style="list-style-type: none"> <li>1. Dostarczenie kompletnej dokumentacji technicznej w języku polskim, zawierającej opis architektury, konfigurację ról i uprawnień oraz procedurę odtwarzania awaryjnego (Disaster Recovery).</li> <li>2. Przeprowadzenie warsztatów stanowiskowych dla personelu IT w zakresie: obsługi incydentów, tworzenia własnych reguł analizy oraz diagnostyki pracy agentów.</li> <li>3. Udzielenie wsparcia technicznego i merytorycznego w okresie 30 dni od daty wdrożenia systemu poprzez telefon, e-mail lub asysta zdalna.</li> </ol>



Skalowalność	Architektura musi pozwalać na dołożenie kolejnych węzłów indeksujących bez konieczności reinstalacji całego środowiska.
Zgodność	Rozwiązanie musi umożliwiać generowanie raportów zgodności z powszechnie obowiązującymi normami ochrony danych osobowych oraz standardami bezpieczeństwa informacji.