IZ.271.9.1.2025.

Skórcz, 28.05.2025 r.

ZAPYTANIE OFERTOWE

Dotyczy projektu pn. Dostawa sprzętu i oprogramowania w ramach projektu „Cyberbezpieczny samorząd" w Gminie Skórcz w ramach: Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd"

I. ZAMAWIAJĄCY : Gmina Skórcz

II. OPIS PRZEDMIOTU ZAMÓWIENIA

Gmina Skórcz występuje z zapytaniem ofertowym dotyczącym dostawy sprzętu komputerowego i oprogramowania.

Przedmiot zamówienia:

1. Serwer – 1 sztuka

Parametr	Charakterystyka (wymagania minimalne)

Obudowa	• Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków 3.5" Hot-Plug • Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania minimum jednego procesora. • Możliwość obsługi procesorów 128 rdzeniowych • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do min. 3TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	• Zainstalowany jeden procesor, min. 16-rdzeniowy, min. 3.0GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 177 w teście SPECrate2017_int_base w konfiguracji jedno procesorowej, dostępnym na stronie www.spec.org.
RAM	• 256GB DDR5 RDIMM 5600MT/s,

Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający
	  ○ Min. 8GB nieulotnej pamięci cache,
	  ○ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
	  ○ Wsparcie dla dysków samoszyfrujących.

Dyski twarde	• Zainstalowane: ○ 2x dysk SATA o pojemności min. 8TB, Hot-Plug. • Możliwość zainstalowania, w dedykowanym slocie, dwóch dysków M.2 NVMe o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Gniazda PCI	• Osiem slotów PCIe
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)

Wbudowane porty	• 4 porty USB w tym min:
	  ○ 1 port USB 3.0 z tyłu obudowy,
	  ○ 1 port micro USB z przodu obudowy
	• 2 port VGA z czego jeden z przodu obudowy
	• Możliwość rozbudowy o port RS232

Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1080
Wentylatory	• Redundantne
Zasilacze	• Redundantne, Hot-Plug min. 700W klasy Titanium
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
System operacyjny/dodatkowe oprogramowanie	• Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO. • Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. • SSO musi być wspierany przez producenta co najmniej do 2034 roku. SSO musi posiadać następujące, wbudowane cechy: • a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, • b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, • c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, • d) 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, • e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, • f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, • g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), • i) wbudowane wsparcie instalacji i pracy na wolumenach, które: • I. pozwalają na zmianę rozmiaru w czasie pracy systemu, • II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, • III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,

	• IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), • j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, • k) wbudowane szyfrowanie dysków • l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, • m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, • n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, • o) graficzny interfejs użytkownika, • p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, • r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), • s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, • t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, • u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: • I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, • II. 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: • 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, • 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, • 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, • III. zdalna dystrybucja oprogramowania na stacje robocze, • IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, • V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: • 1) dystrybucję certyfikatów poprzez http, • 2) konsolidację CA dla wielu lasów domeny, • 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, • VI. szyfrowanie plików i folderów, • VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), • VIII.możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, • IX. serwis udostępniania stron WWW, • X. wsparcie dla protokołu IP w wersji 6 (IPv6), • XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych 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: • 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, • 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, • 3) obsługi 4-KB sektorów dysków,

	• 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, • 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, • 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), • v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, • w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), • x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, • y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, • z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Licencje dostępowe	• 19 szt. najnowszej dostępnej licencji zdalnego dostępu dla Windows Server 2025 - 1 Device CAL , kompatybilna z najnowszym dostępnym serwerowym systemem operacyjnym tego samego producenta. Licencja dożywotnia. Licencje fabrycznie nowe, wolne od wad i uszkodzeń oraz nieobciążone prawami osób trzecich. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowych licencji nieużywanych oraz nieaktywowanych nigdy wcześniej na innym urządzeniu oraz pochodzących z legalnego źródła sprzedaży.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).

Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego, karta zarządzająca, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:
	  ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
	  ○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
	  ○ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
	  ○ możliwość podmontowania zdalnych wirtualnych napędów;
	  ○ wirtualną konsolę z dostępem do myszy, klawiatury;

	○ wsparcie dla IPv6; ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie; ○ wsparcie dla automatycznej rejestracji DNS ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB

	○ Przesyłanie alertów „as-is" do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych

	○ 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. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania

	○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których

	nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku – **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres min. 5 lat.
	• Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.
	• Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
	• Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
	• Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.
	• Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
	• Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.
	• Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
	• Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
	  ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
	  ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w

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

2. NAS – 1 sztuka

Funkcjonalność	Wymagania minimalne
Procesor	Procesor czterordzeniowy 64 bitowy o taktowaniu nie niższym niż 2.2GHz
Obudowa	Desktop
Pamięć RAM	Min. 16GB DDR4 ECC z możliwością rozbudowy o drugą kość pamięci 16GB do łącznej wielkości 32 GB RAM
Całkowita liczba gniazd pamięci	2
Liczba zatok na dyski twarde	8
Kieszenie dysków M.2	2 (NVMe)
Możliwość podłączenia modułu rozszerzającego	Tak
Dodatkowa karta rozszerzeń	Dwa gniazda NVMe SSD M.2 Interfejs magistrali hosta: PCIe 3.0 x8 Interfejs pamięci masowej: PCIe NVMe Wysokość mocowania: Niskoprofilowe i o pełnej wysokości Obsługiwane obudowy: 22110 / 2280 Gwarancja: 5 lat
Maksymalna ilość dysków z opcjonalnymi modułami rozszerzającymi, nie mniej niż:	18
Porty na karty rozszerzeń	1 x Gen3 x8 PCIe (x4 link)
Porty LAN	Wbudowane min. 4 x RJ-45 1GbE
Porty USB 3.2	min. 4
Port eSATA	min. 2
Zasilanie	Zasilacz o mocy max. 250W
Mechanizm szyfrowania sprzętowego	Tak, min AES-NI
Wewnętrzny system plików	BTRFS, EXT4
Obsługiwane tryby RAID	Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcje backup	Możliwość tworzenia kopii bezpieczeństwa urządzeń pod Windows (Bare Metal), Linux, MacOS oraz usług chmur publicznych, portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), serwer Apple Time

	Machine, backup na zewnętrzne dyski twarde, obsługa minimum 1024 migawek na folder udostępniony, obsługa minimum 65000 migawek na cały system
Usługa katalogowa	Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/FTP/WebDAV/File Station
Minimum obsługiwane aplikacje/usługi	Serwer plików, Serwer FTP, WebDav, Serwer WEB, Serwer kopii zapasowych, Serwer Monitoringu (min. 2 licencje), możliwość utworzenia klastra wysokiej dostępności z 2 identycznych urządzeń, Serwer pocztowy (min. 5 licencji w cenie)
Bezpieczeństwo	Obsługa WORM (Write Once Read Many - jeden zapis, wiele odczytów) dla folderów współdzielonych i migawek, zapora sieciowa, szyfrowanie folderu współdzielonego, szyfrowanie całego woluminu, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów HTTP, HTTPS, SMB, SSH, Telnet, rsync, FTP, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania), dwuetapowa weryfikacja logowania (2FA), adaptacyjna metoda logowania dla konta administratora (AMFA), możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2, U2F, grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail.
Oprogramowanie do kopii zapasowej	Oferowany serwer powinien mieć oprogramowanie do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów. Minimalne wymagane funkcje oprogramowania do backupu: - kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal, - kopia zapasowa środowisk MacOS - kopia zapasowa maszyn wirtualnych (VMware, Hyper-V) - kopia zapasowa serwerów fizycznych (Windows, Linux) - obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania, - obsługa wielu wersji i retencji, - możliwość wyzwalania kopii zapasowej według harmonogramu, - obsługa klastra przełączania awaryjnego Microsoft Hyper-V, - automatyczna weryfikacja utworzonych kopii zapasowych maszyn wirtualnych i serwerów fizycznych, za pomocą utworzonego nagrania wideo z odtworzenia w formie maszyny wirtualnej, - centralne zarządzanie, - konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji, harmonogramu i woluminów objętych backupem dla poszczególnych zadań, - portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), - delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla użytkowników bez uprawnień administratora, - kopia zapasowa usług chmur publicznych Microsoft 365 i Google Workspace

VPN	VPN Server dla min. 40 połączeń
Gwarancja producenta na serwer	Min. 3 lata

3. Dyski twarde do macierzy dyskowej – 8 sztuk

Minimalne wymagania:	
Pojemność	min. 12 000 GB
Typ	HDD
Format	Format 3,5 cala
Interfejs	SATA
Pobór mocy (W)	Maks.: 7,9 praca oraz 4.3 bezczynność
Prędkość obrotowa	7200 obr./ min.
Obciążenie roczne	550TB
Odporność na wstrząsy	Podczas pracy 70G – czas trwania 2ms
Niezawodność MTTF	Min. 2 000 000
Dodatkowe informacje	Dyski muszą się znajdować na liście kompatybilności producenta oferowanego NAS-a z pkt 3. Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego serwera. Gwarancja producenta dysku: min. 5 lat

4. UPS – 1 sztuka

Nazwa komponentu	Wymagane minimalne parametry techniczne
Technologia	VFI (true on-line, podwójne przetwarzanie energii)
Moc znamionowa	40kVA / 40kW
Konfiguracja faz	3:3
Możliwość rozbudowy w pracy równoległej	Do 8 urządzeń.
Wyjściowy współczynnik mocy (PF)	1.0
Napięcie wejściowe	380 / 400 / 415 VAC
Zakres napięcia wejściowego	216 – 498 VAC
Częstotliwość wejściowa	Wymagana 50-60 Hz
Sprawność AC-AC w trybie pracy on-line z obciążeniem 100%	nie mniejsza niż 96%
Sprawność AC-AC w trybie pracy Oszczędzania energii Eco Mode	nie mniejsza niż 99%
Tryb pracy z konwersją częstotliwości	Wymagana praca ze stałą częstotliwością wyjściową 50Hz, przy zasilaniu 60Hz lub odwrotnie.
Napięcie wyjściowe	380 / 400 / 415 VAC
Częstotliwość wyjściowa	50/60Hz (programowalna)

Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem	Wymagane
Baterie	Szczelne, bezobsługowe, w technologii AGM, o projektowanej żywotności min. 10-12 lat i pojemności minimalnej 11520 V*Ah.
Szafa baterii	Brak, akumulatory wewnątrz urządzenia
Stabilizacja napięcia wyjściowego w stanie ustalonym	± 1%
Stabilizacja napięcia wyjściowego w stanie nieustalonym	± 3%
Współczynnik szczytu	3:1
Panel sterujący z wyświetlaczem ciekłokrystalicznym LCD w języku polskim oraz sygnalizacją akustyczną	Wymagane
Złącze interfejsów	RS232, USB, REPO
Wyjściowa listwa do wpięcia UPS do instalacji stałej	Wymagana możliwość podłączenia przewodów o przekroju min 25 mm2
Karta sieciowa SNMP	Wymagana
Wyłącznik awaryjny REPO	Wymagane
Zabezpieczenie przed prądem wstecznym	Wymagane
Czujnik warunków środowiskowych	Wymagane, pomiar temperatury i wilgoci w pomieszczeniu, kompatybilny z kartą SNMP
Diagnostyka parametrów urządzenia UPS i baterii	Automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-a i z wykorzystaniem oprogramowania do zarządzania i monitorowania UPS
Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego	Wymagane
Zewnętrzny bypass serwisowy	Wymagany
Poziom hałasu w odległości 1m,	< 58 dBA

	Wentylatory o regulowanej prędkości obrotowej w zależności od obciążenia i temperatury
Możliwość regulacji z panelu sterującego tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu	Wymagane
Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa ,kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE	Wymagane, załączyć do oferty
Producent zasilacza UPS z siedzibą w Polsce, posiadający biuro dystrybucji i serwisu na terenie kraju.	Wymagane
Certyfikat ISO 9001 oraz 14001 producenta zasilacza UPS	Wymagane, załączyć do oferty
Wymiary zasilacza UPS [S x G x W] (mm)	Maksymalnie 500 x 850 x 1400
Instrukcja w języku polskim	Wymagane
Gwarancja na elektronikę i akumulatory.	Minimum 48 miesięcy W ramach gwarancji konieczne jest dokonywanie - bez dodatkowych opłat - przeglądów corocznych wymaganych do utrzymania prawidłowego funkcjonowania urządzenia oraz gwarancji. Usługa taka winna obejmować, podstawowe czynności konserwacyjne, ocenę stanu jakości urządzeń, a także wymianę elementów eksploatacyjnych niezbędnych dla prawidłowego działania urządzenia w okresie gwarancyjnym.
Usługa	Dostawa, instalacja w przygotowanej lokalizacji zabezpieczonej w odpowiednią instalację elektryczną, rozruch techniczny ze szkoleniem.

5. UTM – 1 sztuka

Minimalne wymagania Zamawiającego	
PARAMETRY SPRZĘTOWE	- Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. - Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. - Liczba portów Ethernet 2,5Gbps – min. 8. - Liczba portów światłowodowych 1Gbps – min. 1. - Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. - Przepustowość Firewall (1518 bajtów UDP) – minimum 8Gbps.

	- Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps. - Przepustowość filtrowania Antywirusowego – minimum 1Gbps. - Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2Gbps. - Liczba tuneli VPN IPSec – minimum 100. - Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 100. - Obsługa interfejsów 802.11q (VLAN) – minimum 128 - Liczba równoczesnych sesji – minimum 400 000 i nie mniej niż 25 000 nowych sesji/sekundę. - Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. - Urządzenie nie ma limitu na liczbę użytkowników. - Liczba reguł filtrowania – minimum 8 192. - Liczba tras statycznego routingu – minimum 512. - Liczba tras dynamicznego routingu – minimum 10 000. - Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia. - Urządzenie musi być wyposażone w moduł TPM.
Obsługa Sieci	Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
ZAPORA KORPORACYJNA (Firewall)	- Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. - Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. - Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). - Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. - Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. - Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. - Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. - Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. - Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. - Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). - System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
INTRUSION PREVENTION SYSTEM (IPS)	- System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy

	pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. - Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. - Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. - Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. - Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. - Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. - Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. - Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. - Moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). - Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
KSZTAŁTOWANIE PASMA (Traffic Shapping)	- Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. - Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. - Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). - Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
OCHRONA ANTYWIRUSOWA	- Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie. - Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania). - Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem. - Skaner antywirusowy ma pochodzić od europejskiego producenta. - Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. - Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

OCHRONA ANTYSPAM	- Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). - Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. Skaner heurystyczny. - W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. - Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
WIRTUALNE SIECI PRYWATNE (VPN)	- Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). - Urządzenie ma wspierać co najmniej następujące typy sieci VPN: a. PPTP VPN, b. IPSec VPN, c. SSL VPN. - SSL VPN ma działać w trybie tunelu. - Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. - Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) - Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). - Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. - Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
FILTR DOSTĘPU DO STRON WWW	- Urządzenie ma posiadać wbudowany filtr URL. - Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych. - Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu. - Administrator ma mieć możliwość dodawania własnych kategorii URL. - Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. - Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. - Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. - Filtr URL musi uwzględniać komunikację po protokole HTTPS. - Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. - Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. - Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.

UWIERZYTELNIANIE	Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. - Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. - Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. - Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. - Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. - Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. - Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). - Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH. - Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.
ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)	- Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). - Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. - Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. - Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). - Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. - W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). - Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
ROUTING (TRASOWANIE)	- Urządzenie ma umożliwiać statyczne trasowanie pakietów. - Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

	- Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). - Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. - Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.
ADMINISTRACJA URZĄDZENIEM	- Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. - Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. - Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. - Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. - Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. - Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) - Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. - Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. - Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. - Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. - Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. - Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). - System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). - Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. - Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). - Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. - Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: a. manualnego eksportu do pliku w dowolnym momencie czasu, b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu - Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. - Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

	- Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
RAPORTOWANIE	- Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. - System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. - System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. - System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. - System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. - System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. - Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. - Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. - Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
POZOSTAŁE USŁUGI I FUNKCJE	- Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. - Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. - Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). - Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. - Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). - Urządzenie ma posiadać usługę DNS Proxy. - Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). - Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. - Urządzenie musi mieć zaimplementowane Open API. - Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie
WDROŻENIE	W cenie urządzenia wykonawca zapewni wdrożenie urządzenia w poniższym zakresie: - Konfiguracja sieci (interfejsy i routing). - Konfiguracja firewalla (min. 20 reguł). - Konfiguracja NAT (min. 10 reguł). - Konfiguracja IPS - Konfiguracja dodatkowych usług sieciowych tj. DHCP, DNS Proxy. - Integracja z AD lub założenie wewnętrznej bazy użytkowników - Konfiguracja dostawców Internetu (min. 2 dostawców). - Konfiguracja transparentnej autoryzacji w Active Directory – co najmniej instruktaż przebiegu instalacji. - Konfiguracja VPN: IPSec Site-to-Site (limit 2 tuneli) – zgodnie z otrzymanymi od Zamawiającego parametrami tuneli; Client-to-Site – konfiguracja urządzenia i co najmniej jednej wzorcowej stacji klienckiej

GWARANCJA I SERWIS	- Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich wyspecyfikowanych funkcji bezpieczeństwa na okres min. Do 30.06.2026r. - W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

III Kod i nazwa zamówienia według Wspólnego Słownika Zamówień (CPV)

CPV 48820000-2 serwery
CPV 48000000-8 pakiety oprogramowania i systemy informatyczne
CPV 72268000-1 usługi dostawy oprogramowania

IV. TERMIN REALIZACJI UMOWY

Zamówienie będzie wykonane w miejscu siedziby zamawiającego. Dostawy sprzętu i oprogramowania będą realizowane w ciągu 21 dni od podpisania umowy w Wykonawcą.

Przedmiot umowy będzie dostarczany przez Wykonawcę do miejsc wskazanych przez Zamawiającego w zakresie dostawy sprzętu.

Terminy realizacji zamówienia mogą ulec zmianie, w zależności od wystąpienia okoliczności, których nie można było przewidzieć w dniu zawarcia umowy lub w sytuacjach nieprzewidzianych lub uzasadnionych, za zgodą obu stron.

V Warunki udziału w postępowaniu

1. Na potwierdzenie spełnienia warunku udziału w postępowaniu, dotyczącego zdolności technicznej lub zawodowej Zamawiający wymaga, aby Wykonawca wykazał się odpowiednim doświadczeniem, tj. w ciągu ostatnich 3 lat przed upływem terminu składania ofert, w tym okresie realizuje, bądź zrealizował należycie co najmniej dwie usługi w zakresie dostawy sprzętu komputerowego na kwotę co najmniej 100 000 złotych brutto. w ramach jednego zamówienia, kontraktu, umowy.

VI Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty wraz z podaniem wag tych kryteriów i sposobu oceny ofert

1. Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami:

Lp.	Nazwa kryterium	Waga (pkt)
1.	Cena (całkowity koszt wykonania zamówienia)	90
2.	Przyjmowanie możliwości wykonania zamówienia poza godzinami 8.00-17.00 tj. przez całą dobę	10

2. Przy wyborze oferty Zamawiający będzie stosować zasadę, że oferta nieodrzucona, zawierająca najwyższą liczbę punktów przyznanych według powyższych kryteriów, jest ofertą najkorzystniejszą.
3. W toku dokonywania badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień treści złożonych przez nich ofert.
4. Przy ocenie ofert w kryterium „Cena" (C) punkty zostaną przyznane w poniższy sposób:
   - Cena – znaczenie 90% (maksymalnie do 90 pkt)
   - Kryterium ceny będzie rozpatrywane na podstawie ceny brutto podanej przez Wykonawcę w Formularzu Ofertowym.
   - Punkty w kryterium „Cena" będą obliczane na podstawie wzoru:

C = CC min/ CC of x 90

gdzie:

C – punkty przyznane Wykonawcy w ramach kryterium „Cena"

CC min – najniższa cena brutto spośród badanych ofert

CC of – cena brutto badanej ofert

   - Do wzoru zostaną przyjęte ceny podane przez Wykonawców w Formularzu Oferty stanowiącym Załącznik nr 1 do SWZ.

5. Kryterium „Przyjmowanie możliwości wykonania zamówienia poza godzinami 8.00-17.00 tj. przez całą dobę" stanowi 10 możliwych do uzyskania punktów.
6. Sumaryczna liczba punktów zostanie obliczona według wzoru:
   W = C + E

   gdzie:

   W – łączna liczba punktów przyznanych w poszczególnych kryteriach,

   C – liczba punktów przyznanych w kryterium „Cena",

   E – wartość punktowa kryterium „Przyjmowanie możliwości wykonania zamówienia poza godzinami 8.00-17.00 tj. przez całą dobę",

   Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku
7. Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku.
8. W związku z zaistnieniem przesłanki o której mowa w art. 246 ust. 2 PZP możliwe było zastosowanie kryterium ceny jako kryterium o wadze przekraczającej 60%, ze względu na określenie w opisie przedmiotu zamówienia wymagań jakościowych odnoszących się do co najmniej głównych elementów składających się na przedmiot zamówienia.

VII Wykaz oświadczeń lub dokumentów, jakie mają złożyć wykonawcy w celu wykazania spełniania warunków udziału w postępowaniu

1. W celu potwierdzenia spełniania warunków udziału w postępowaniu Wykonawca przedłoży wykaz dostaw wraz z podaniem ich rodzaju, wartości, daty i miejsca wykonania oraz podmiotów, na rzecz których dostawy te zostały wykonane oraz załączeniem dowodów określających, czy te usługi zostały wykonane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego usługi zostały wykonane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest wstanie uzyskać tych dokumentów– wzór załącznik nr 2 do Zapytania ofertowego.

VIII. ZGŁASZANIE PYTAŃ I WĄTPLIWOŚCI

Wszelkie pytania i wątpliwości dotyczące prowadzonego postępowania należy kierować poprzez portal https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/.

Oferenci mogą zadawać pytania do przedmiotu zamówienia najpóźniej 2 dni robocze przed zakończeniem terminu składania ofert.

Jeżeli wniosek o wyjaśnienie treści zapytania ofertowego wpłynie po upływie terminu, o którym mowa powyżej lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.

Odpowiedzi będą udzielane za pośrednictwem portalu https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl w ciągu 2 dni roboczych.

W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść zapytania ofertowego.

Zapytanie ofertowe wraz ze zmianami upublicznione zostanie w Bazie Konkurencyjności.

IX. TERMIN ZWIĄZANIA OFERTĄ

Wykonawca pozostaje związany złożoną ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z zakończeniem terminu składania ofert.

X. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

a) Do oferty winny być dołączone wszystkie dokumenty i oświadczenia wskazane w zapytaniu ofertowym.
b) Oferta oraz załączniki do oferty muszą być sporządzone w języku polskim.
c) Oświadczenia mają być złożone w oryginale. Kopie wymaganych dokumentów winny być poświadczone „za zgodność z oryginałem" przez składającego ofertę, z datą poświadczenia.
d) W przypadku składania ofert przez Bazę Konkurencyjności dopuszcza się:
   - złożenie oferty wraz z załącznikami podpisanych kwalifikowanym podpisem elektronicznym lub
   - złożenie oferty wraz z załącznikami podpisanych elektronicznym podpisem zaufanym.
e) Wszelkie koszty związane z przygotowaniem oferty i inne koszty ponosi Oferent.

XI. MIEJSCE I TERMIN SKŁADANIA OFERT

Ofertę należy złożyć poprzez portal https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl, do dnia **05.06.2025r**

Otwarcie złożonych ofert nastąpi niezwłocznie po wyznaczonym terminie ich składania w siedzibie Zamawiającego.

XII. WYTYCZNE ODNOŚNIE CENY PRZEDSTAWIONEJ W OFERCIE

1. Cena musi uwzględniać wszystkie wymagania zapytania ofertowego oraz obejmować wszelkie koszty jakie poniesie Wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia.
2. Cena musi być wyrażona w polskich złotych, liczbowo, z dokładnością do dwóch miejsc po przecinku. Oferta musi zawierać należny podatek VAT. Prawidłowe ustalenie stawki

należnego podatku VAT należy do obowiązków Wykonawcy, zgodnie z przepisami ustawy o podatku od towarów i usług oraz o podatku akcyzowym.

INFORMACJE DOTYCZĄCE WALUTY ROZLICZENIA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCĄ

Rozliczenia między Zamawiającym a Wykonawcą dokonywane będą w walucie polskiej, w złotych (PLN).

XIII. OCENA OFERT POD WZGLĘDEM FORMALNYM I DOPUSZCZENIE DO OCENY PUNKTOWEJ

1. Zamawiający dokona oceny ofert pod względem formalnym oraz zgodności z niniejszym zapytaniem ofertowym.
2. Oferta zostanie odrzucona, jeśli:
   a) została złożona po wyznaczonym terminie;
   b) została złożona w niewłaściwym miejscu;
   c) jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji;
   d) do oferty nie załączono wszystkich wymaganych dokumentów przewidzianych w Zapytaniu ofertowym;
   e) zaoferowana cena przez danego Wykonawcę przewyższa kwotę, którą Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia.
   f) jest niezgodna z wymaganiami określonymi w Zapytaniu ofertowym;
   g) jest niezgodna z obowiązującymi przepisami prawa;
   h) jest niekompletna lub nie będzie zawierała wszystkich wymaganych przez Zamawiającego dokumentów, oświadczeń, podpisów.
   i) Oferent nie spełnia warunków udziału w postępowaniu;
3. Zamawiający może wezwać Oferentów, którzy w określonym terminie nie złożyli wymaganych przez Zamawiającego oświadczeń lub dokumentów, lub którzy nie złożyli pełnomocnictw, albo którzy złożyli wymagane przez Zamawiającego oświadczenia i dokumenty, zawierające błędy, omyłki pisarskie bądź rachunkowe, niespójności lub nie potwierdzające spełnienia przez Oferentów warunków udziału w postępowaniu lub którzy złożyli wadliwe pełnomocnictwa, do ich złożenia w wyznaczonym terminie, chyba, że mimo ich złożenia oferta podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.

4. Zamawiający może w toku badania i oceny ofert żądać od Oferentów wyjaśnień dotyczących treści złożonych ofert.
5. Z tytułu odrzucenia oferty Wykonawcom nie przysługują żadne roszczenia przeciw Zamawiającemu.
6. Żadne informacje dotyczące procesu oceny oraz wyboru ofert nie zostaną ujawnione Oferentom lub innym osobom, niezaangażowanym oficjalnie w proces oceny i wyboru oferty.
7. Zamawiający odrzuci ofertę Oferenta, który nie złożył wyjaśnień lub jeżeli dokonana ocena wyjaśnień wraz z dostarczonymi dowodami potwierdzi, że oferta zawiera informacje nieprawdziwe lub niemożliwe do udokumentowania.
8. Zamawiający wymaga, aby ofertę wraz z załącznikami podpisała osoba uprawniona do reprezentowania Wykonawcy. Jeżeli upoważnienie nie wynika z dokumentów rejestrowych, Wykonawca zobowiązany jest dołączyć do oferty stosowne pełnomocnictwo.

XIV. FORMALNOŚCI JAKIE POWINNY ZOSTAĆ DOPEŁNIONE W CELU ZAWARCIA UMOWY

1. Zamawiający zastrzega prawo do unieważnienia postępowania bez podania przyczyny oraz do odrzucenia oferty, jeżeli zaoferowana cena przekroczy kwotę przeznaczoną na sfinansowanie całości zamówienia lub danej części zamówienia, w przypadku złożenia oferty częściowej.
2. O unieważnieniu postępowania ofertowego Zamawiający zawiadomi równocześnie wszystkich Wykonawców, którzy:
    a. ubiegali się o udzielenie zamówienia – w przypadku unieważnienia postępowania przed upływem terminu składania ofert;
    b. złożyli oferty – w przypadku unieważnienia postępowania po upływie terminu składania ofert;
3. Zamawiający podpisze umowę z Wykonawcą, który przedłoży najkorzystniejszą ofertę z punktu widzenia kryteriów przyjętych w zapytaniu ofertowym, chyba że Zamawiający unieważni postępowanie.
4. Niezwłocznie po wyborze najkorzystniejszej oferty, Zamawiający poinformuje o wynikach postępowania umieszczając informację na Bazie Konkurencyjności.
5. Wykonawca, którego oferta zostanie uznana za najkorzystniejszą, przed podpisaniem umowy zobowiązany jest do złożenia informacji o osobach umocowanych do zawarcia umowy i okazania ich pełnomocnictwa, jeżeli taka konieczność zaistnieje.
6. Termin i miejsce podpisania umowy:
    a. Wykonawca, którego oferta została wybrana jest zobowiązany do zawarcia umowy z Zamawiającym w terminie i miejscu wskazanym przez Zamawiającego, lecz nie

później niż w terminie 7 dni od wskazanego terminu pod rygorem nie zawarcia umowy. Odpowiednio stosuje się pkt poniżej;

b. jeżeli Wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert bez przeprowadzenia ich ponownego badania i oceny.

XV. OCHRONA DANYCH OSOBOWYCH

1. Administratorem danych osobowych w związku z realizacją **postępowania zakupowego** pod nazwą: pn. **Dostawa sprzętu i oprogramowania w ramach projektu „Cyberbezpieczny samorząd dla Gminy Skórcz ” realizowanego w ramach projektu grantowego pt.: „Cyberbezpieczny Samorząd”,** dofinansowanego ze środków zewnętrznych z w ramach FUNDUSZY EUROPEJSKICH NA ROZWÓJ CYFROWY 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa - konkurs grantowy „Cyberbezpieczny Samorząd” o numerze o numerze FERC.02.02-CS.01-001/23 Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/1132/ FERC.02.02-CS.01- 001/23/2024, jest **Gmina Skórcz Wójt Gminy Skórcz, ul. Dworcowa 6, 83-220 Skórcz, tel.: 58 582 46 45, adres e- mail: gminaskorcz@gminaskorcz.pl**
2. Zobowiązuje się Wykonawcę do spełnienia obowiązku informacyjnego z art. 13 i 14 RODO, stanowiącego **załączniki nr 4 i 5** do **zapytania ofertowego** wobec osób, których dane osobowe zostaną przekazane przez Wykonawcę w związku z realizacją niniejszego postępowania.
3. Wykonawca oświadcza, że wypełnił obowiązek informacyjny przewidziany w art. 13 RODO i art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu, o którym mowa w punkcie 2.
4. Wykonawca przekaże Zamawiającemu **w załączeniu do oferty**, podpisany przez osobę/by, której dane dotyczą odpowiednio obowiązek informacyjny z art. 13 lub 14 RODO, stanowiący **załącznik nr 4 i 5** do zapytania ofertowego.
5. Wykonawca przyjmuje do wiadomości, że zamówienie jest współfinansowane ze środków ze środków zewnętrznych z FUNDUSZY EUROPEJSKICH NA ROZWÓJ CYFROWY 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa - konkurs grantowy „Cyberbezpieczny Samorząd” o numerze o numerze FERC.02.02-CS.01-001/23 Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/1132/ FERC.02.02-CS.01- 001/23/2024. W związku z powyższym w ramach badania kwalifikowalności wydatków dojdzie do udostępnienia dokumentacji w tym danych osobowych następującym instytucjom:

   1) Ministrowi Funduszy i Polityki Regionalnej (dalej jako MFiPR), w zakresie w jakim pełni funkcję Instytucji Zarządzającej (IZ) Funduszami Europejskimi na Rozwój Cyfrowy 2021- 2027 (dalej jako FERC) oraz Funduszy Europejskich dla Funduszu Społecznego 2021- 2027 (dalej jako FERS), z siedzibą przy ul. Wspólnej 2/4, 00-926 Warszawa; 2) Centrum Projektów Polska Cyfrowa (dalej jako CPPC) w

zakresie w jakim pełni funkcje Instytucji Pośredniczącej (IP) FERC i FERS, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa, które staną się wówczas Administratorem danych osobowych.

6. Zgodnie z zapisami umowy powierzenia grantu, Zamawiający został zobowiązany do spełnienia obowiązku informacyjnego przez Grantodawcę w imieniu Administratorów, o których mowa w pkt. 5.
7. Zobowiązuje się Wykonawcę do spełnienia obowiązku informacyjnego z art. 13 i 14 RODO, stanowiącego **załączniki nr 6 do zapytania ofertowego** wobec osób, których dane osobowe zostaną przekazane przez Wykonawcę w związku z realizacją niniejszego postępowania.
8. Wykonawca oświadcza, że wypełnił obowiązek informacyjny przewidziany w art. 13 RODO i art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowania, o którym mowa w punkcie7.
9. Wykonawca przekaże Zamawiającemu **w załączeniu do oferty**, podpisany przez osobę/by, której dane dotyczą obowiązek informacyjny z art. 13 i 14 RODO, stanowiący **załącznik nr 6** do zapytania ofertowego.

10. Wykonawca zobowiązuje się do każdorazowego spanienia obowiązku informacyjnego z Art. 13 i 14 RODO, o którym mowa w **zał. 4 i 5 oraz 6 do zapytania ofertowego** , również w trakcie realizacji umowy w przypadku jej zawarcia w wyniku niniejszego postepowania i zobowiązuje się do przekazania Zamawiającemu podpisanego obowiązku informacyjnego w dniu przekazania danych, nie później niż 10 dni od przekazania danych Zamawiającemu z zastrzeżeniem, że Wykonawca przekaże Zamawiającemu jako załącznik do podpisywanej umowy, podpisany przez osobę/by, której dane dotyczą odpowiednio obowiązek informacyjny z art. 13 lub 14 RODO.

XVI. Załączniki:

- Załącznik nr 1 – Formularz oferty
- Załącznik nr 2 - Wykaz usług
- Załącznik nr 3 – Projekt umowy
- Załącznik nr 4 - OBOWIĄZEK INFORMACYJNY z art. 13 ust. 1 i 2 RODO
- Załącznik nr 5 - OBOWIĄZEK INFORMACYJNY z art. 14 ust. 1 i 2 RODO (pracownicy do kontaktu, podwykonawcy, pełnomocnicy itp.)
- Załącznik nr 6 - Klauzula_informacyjna_FERC_FERS

SŁAWOMIR CZECHOWSKI; UG SKÓRCZ

Elektronicznie podpisany przez SŁAWOMIR CZECHOWSKI; UG SKÓRCZ
Data: 2025.05.28 12:21:36 +02'00'