Cyberbezpieczny Samorząd

Szczegółowy Opis Przedmiotu Zamówienia

POWIAT KALISKI

Plac Św. Józefa 5, 62-800 Kalisz

„Dostawa sprzętu i oprogramowania”

Nr sprawy ZP.272.1.29.2026

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

WYKAZ ZAGADNIEŃ

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA

1. Przedmiot zamówienia.

Przedmiotem zamówienia jest Zwiększenie Cyberbezpieczeństwa w Powiecie Kaliskim poprzez dostawę, montaż i wdrożenie sprzętu oraz udzielenie licencji na oprogramowanie zapewniające Zamawiającemu prawo do korzystania z rozwiązań sprzętowych (zwanych dalej Rozwiązaniami) i oprogramowania (zwanego dalej Oprogramowaniem). Wykonawca na własny koszt dostarczy we wskazane przez Zmawiającego miejsca sprzęt i oprogramowanie. Dostarczony sprzęt i oprogramowanie muszą być fabrycznie nowe, wyprodukowane najpóźniej w 2026 r.

2. Miejsce realizacji przedmiotu zamówienia.

Montaż i konfiguracja sprzętu muszą być wykonane w terminach i miejscach uzgodnionych z Zamawiającym, zgodnie z wymaganiami Szczegółowego Opisu Przedmiotu Zamówienia i umowy. Wykonawca podłączy wszystkie elementy do sieci. Wykonawca dokona konfiguracji fizycznej i logicznej, podłączy i skonfiguruje urządzenia pozwalając na rozpoczęcie pracy. Dostawa, montaż i konfiguracja sprzętu muszą być wykonane w terminie uzgodnionym z Zamawiającym. Elementy zostaną dostarczone na adres: Starostwo Powiatowe w Kaliszu, plac Świętego Józefa 5, 62-800 Kalisz. W celu poprawnej realizacji zamówienia Wykonawca przeprowadzi analizę przedwdrożeniową.

3. Termin realizacji.

Przedmiot zamówienia zostanie zrealizowana w terminie wskazanym w Formularzu ofertowym przez Wykonawcę, jednak nie dłuższej niż w terminie 40 dni kalendarzowych od dnia zawarcia umowy. Usługi wsparcia technicznego będą świadczone przez producenta sprzętu w okresie trwania gwarancji.

4. Równoważność.

Rozwiązania równoważne:

4.1 Wszędzie tam, gdzie przedmiot zamówienia opisany jest przez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych dopuszcza się rozwiązania równoważne opisywanym.

4.2 Jeżeli w jakimkolwiek miejscu dokumentacji stanowiącej opis przedmiotu zamówienia, zostały wskazane nazwy producenta, nazwy własne, znaki towarowe, patenty lub pochodzenie materiałów czy urządzeń służących do wykonania niniejszego zamówienia, które wskazują lub mogłyby wskazywać na konkretnego producenta, nie stanowi to preferowania wyrobu czy materiałów danego producenta, lecz ma na celu wskazanie na cechy – parametry techniczne i jakościowe nie gorsze od podanych w opisie. Ewentualne operowanie przykładowymi nazwami producenta

ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Zamawiający dopuszcza w takim przypadku składanie ofert równoważnych z zastosowaniem innych materiałów i urządzeń niż opisane nazwą producenta, nazwą własną, znakiem towarowym, patentem lub pochodzeniem materiałów czy urządzeń służących do wykonania niniejszego zamówienia, pod warunkiem, że zagwarantują one uzyskanie parametrów technicznych, eksploatacyjnych i jakościowych nie gorszych od założonych w dokumentacji. To samo dotyczy sytuacji, gdy przedmiot zamówienia opisany jest za pomocą norm, aprobat, specyfikacji technicznych i systemów odniesienia.

4.3 Jeżeli w jakimkolwiek miejscu dokumentacji stanowiącej opis przedmiotu zamówienia został określony sposób postępowania użytkownika i/lub realizacji określonej funkcjonalności należy traktować go wyłącznie poglądowo. Opis ma na celu określenie pożądanego efektu końcowego. Sposób jego osiągnięcia może być dowolny.

4.4 W przypadku, gdy do opisu przedmiotu zamówienia zostały użyte określenia norm właściwych dla Europejskiego Obszaru Gospodarczego, Zamawiający dopuszcza każde inne rozwiązanie, o ile wykonawca udowodni w swojej ofercie, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w zapytaniu ofertowym.

4.5 Wykonawca składając ofertę z zastosowaniem rozwiązań równoważnych składa wraz z ofertą oświadczenie o zastosowaniu materiałów równoważnych wraz z przedłożeniem (załączeniem do oferty) dokumentów, iż zastosowane materiały spełniają wymogi zawarte w opisie przedmiotu zamówienia (DTR urządzeń, karty katalogowe, certyfikaty, rysunki zamienne - jeśli zakres proponowanych zmian wymaga zmian projektowych).

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

5. Zakup i konfiguracja serwera do replikacji z oprogramowaniem systemowym

5.1 Serwer – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• serwerowa do montażu w szafie RACK 19" o wysokości maksymalnie 2U • Obudowa powinna posiadać zainstalowany panel LCD umieszczony na froncie obudowy i pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera (umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze). • Obudowa z możliwością wyposażenia w kartę do bezpośredniej komunikacji z urządzeniem mobilnym. • 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. • W obudowie powinien być zainstalowany zestaw redundantnych wentylatorów.
Zasilanie	• W obudowie powinien być zainstalowany zestaw redundantnych zasilaczy o mocy co najmniej 1100W w standardzie Titanium każdy wymienialnych podczas pracy oraz 2 kable C13/C14 10A minimum 2m
Płyta główna	• Płyta główna z możliwością zainstalowania minimum dwóch procesorów. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • musi być wyposażona w zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust), • Musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o konfigurację wewnętrznego oprogramowania komponentów serwera. • Zintegrowany z płytą główną moduł TPM w wersji co najmniej 2.0 V3
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Procesor	• Dwa procesory typu skalowalnego z uwagi na licencjonowanie posiadający dokładnie 8 rdzeni działającego co najmniej z częstotliwością minimum 2.6 GHz i dającego w teście Passmark dostępnym na stronie https://www.cpubenchmark.net/ wynik nie mniejszy niż 40 400 pkt. dla wersji Dual CPU *(należy dołączyć benchmark przeprowadzony najpóźniej 60 dni od dnia złożenia oferty)*
RAM	• Na płycie głównej powinno znajdować się minimum 32 slotów przeznaczone do instalacji pamięci taktowaną przynajmniej z częstotliwością 5600MT/s przy użyciu odpowiednich procesorów. • 128GB pamięci RAM w modułach 32GB RDIMM przygotowanych na działanie z częstotliwością co najmniej 5600MT/s
Dyski twarde	• 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. • Miejsce na co najmniej 8 dysków 3.5" z przodu obudowy oraz co najmniej 4 dyski 2.5” z tyłu obudowy • Zainstalowane co najmniej 2 dyski minimum 480GB SSD SATA Read Intensive 6Gbps Hot-Plug • Zainstalowane dyski HDD SAS ISE 12 Gbps Hot-plug o łącznej minimalnej pojemności 144TB w RAID 5 (np. 7 x 24TB)
Kontroler RAID	• Serwer powinien posiadać kontroler RAID umożliwiający konfigurację RAID 0, 1, 10, 5, 50, 6, 60.
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT • min. 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 • (powyższe porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA

	• 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).
Kontroler eksploatacji serwera	• Serwer powinien być standardowo wyposażony w kontroler eksploatacji • Konfigurowanie ustawień BIOS i sprzętu. • Uproszczoną instalację systemów operacyjnych z wbudowanymi sterownikami, z opcją instalacji bezobsługowej dla systemów Microsoft Windows i Red Hat Enterprise Linux 7. • Aktualizację oprogramowania niezależnie od systemu operacyjnego, z możliwością przywrócenia poprzedniej wersji. • Ciągłą dostępność diagnostyki bez zależności od dysku twardego, z automatyczną aktualizacją oprogramowania podczas wymiany komponentów. • Usunięcie danych związanych z serwerem i pamięcią masową na wybranych komponentach. Możliwe jest usunięcie informacji z BIOS. • Dostarczenie informacji o bieżącej i fabrycznej konfiguracji systemu. • Udostępnianie logów sprzętowych w celu rozwiązywania problemów. • Zdalne zarządzanie cyklem życia serwera co najmniej za pomocą interfejsu WS-Man • Konfigurację ustawień sieci dla wbudowanej karty NIC, w tym ustawienia VLAN. • Wykonywanie diagnostyki pamięci, urządzeń we/wy, procesora i dysków fizycznych. • Aktualizację komponentów systemu za pomocą repozytoriów lub pojedynczych pakietów DUP. • Powrót do poprzedniej wersji oprogramowania układowego. • Umożliwia zabezpieczenie konfiguracji systemu - "System Configuration Lockdown mode"

	• Automatyczną aktualizację oprogramowania i konfiguracji wymienionych części. • Trwałe usunięcie danych przed ponownym wykorzystaniem lub wycofaniem systemu. • Obsługę różnych metod aktualizacji, za pomocą różnych źródeł, takich jak FTP, udziały sieciowe (CIFS, NFS, HTTP, HTTPS) lub lokalne napędy USB/DVD
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: o Uwierzytelnianie dwuskładnikowe RSA SecurID (2FA). o Dostęp do zdalnej konsoli HTML5. o Obsługa wirtualnych nośników danych. o Zdalne udostępnianie plików (RFS). o Współpraca wirtualnej konsoli (do sześciu użytkowników). o Czat w ramach wirtualnej konsoli o Zarządzanie kluczami o Zarządzanie z poziomu portu USB Dual-Mode Type-C znajdującego się na panelu przednim serwera. o Wirtualny schowek. o Możliwość uwierzytelniania z wykorzystaniem Simple 2-Factor Authentication (Simple 2FA) o Zarządzanie kluczami: Secure Enterprise Key Management (SEKM) i Local Key Management (iLKM). o Automatyczna rejestracja certyfikatów SSL. o Zaawansowane zarządzanie termiczne. o Graficzne wyświetlanie zużycia energii w czasie rzeczywistym. o Historyczne dane zużycia energii. o Limitowanie zużycia energii (Power Capping). o Dostosowanie przepływu powietrza PCIe (LFM). o Zdalne wdrażanie systemu operacyjnego. o Zapisywanie wideo z awarii systemu. o Zarządzanie jednostkami przetwarzania danych (DPU). o Konfiguracja progów zużycia dysków SSD. o Dynamiczna konfiguracja wirtualnych adresów pamięci masowej.
Oprogramowanie do zarządzania	• Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: o wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; o możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta; o wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH; o możliwość oskryptowywania procesu wykrywania urządzeń;

	○ możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram; ○ szczegółowy opis wykrytych systemów oraz ich komponentów; ○ możliwość eksportu raportu do CSV, HTML, XLS; ○ grupowanie urządzeń w oparciu o kryteria użytkownika; ○ automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń; ○ 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; ○ aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania); ○ możliwość instalacji sterowników i 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 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.
Aplikacja do zarządzania	• Aplikacja mobilna do zarządzania serwerami powinna umożliwiać: ○ Monitorowanie stanu serwerów, w tym odczyt parametrów zdrowia, inwentarza i konfiguracji. ○ Konfigurowanie ustawień serwera, takich jak parametry sieci, hasła administratora i kolejność urządzeń rozruchowych. ○ Bezpośrednią komunikację z kontrolerem serwera za pomocą technologii bezprzewodowej. ○ Zdalne zarządzanie serwerami poprzez połączenie z konsolą zarządzania. ○ Pobieranie informacji o serwerach takich jak inwentarz, status, alerty oraz logi.

	○ Konfigurowanie serwerów zdalnie. ○ Wysyłanie poleceń sterowania zasilaniem i innych poleceń. ○ Otrzymywanie powiadomień o alertach z systemów zarządzania. ○ Pobieranie informacji o gwarancji. ○ Uruchamianie zewnętrznych aplikacji, takich jak klienci zdalnego pulpitu. ○ Zabezpieczenie danych w aplikacji poprzez szyfrowanie z użyciem klucza specyficznego dla urządzenia. ○ Opcjonalne zabezpieczenie dostępu do aplikacji za pomocą hasła i biometrii. ○ Automatyczne wylogowanie w przypadku braku aktywności. ○ Połączenie z serwerami za pomocą technologii Bluetooth Low Energy (BLE) lub Wi-Fi. ○ Wyświetlanie szczegółowych informacji o serwerze oraz dzienników. ○ Otrzymywanie automatycznych powiadomień z konsoli zarządzania. ○ Przypisywanie adresów IP i modyfikowanie haseł. ○ Konfigurowanie atrybutów BIOS. ○ Wyłączanie i włączanie serwera oraz dostęp do konsoli systemowej. ○ Pobieranie danych z systemów zarządzania typu "jeden do wielu". ○ Wyświetlanie certyfikatu systemu w celu weryfikacji tożsamości przy pierwszym połączeniu. • Aplikacja powinna być dostępna do pobrania w popularnych sklepach z aplikacjami • Kryterium stanowi dodatkową punktację.
Opcjonalny moduł do podłączenia aplikacji mobilnej	• Moduł powinien umożliwiać następujące funkcjonalności: • Bezprzewodową komunikację z urządzeniami mobilnymi wykorzystując technologie Bluetooth Low Energy (BLE) lub Wi-Fi. • Zapewnienie fizycznego bezpieczeństwa poprzez wymóg fizycznej obecności administratora przy serwerze i naciśnięcia przycisku aktywacyjnego na serwerze lub wirtualnego przycisku na wyświetlaczu LCD w przypadku obudów. Bez aktywacji nie jest możliwa wymiana danych. • Ograniczenie zasięgu komunikacji BLE przed uwierzytelnieniem do około 1 metra, a po uwierzytelnieniu do około 5 metrów. Zasięg Wi-Fi wynosi około 5 metrów. • Ograniczenie liczby jednoczesnych połączeń BLE do jednego urządzenia mobilnego na serwer. • Blokowanie dostępu po wielokrotnych próbach połączenia z użyciem nieprawidłowych danych uwierzytelniających, co skutkuje koniecznością ręcznej reaktywacji modułu.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

	• Zabezpieczenie komunikacji BLE z wykorzystaniem protokołu TLS 1.2, wymiany kluczy Diffie-Hellmana (2048-bitowe lub większe liczby pierwsze) oraz szyfrowania AES (128-bitowe klucze symetryczne). • Wykorzystanie trybu szyfrowania GCM z unikalnymi numerami sekwencyjnymi w celu ochrony przed nieautoryzowaną ingerencją, ujawnieniem informacji oraz atakami typu replay. • Aktywację Wi-Fi tylko w przypadku komunikacji wymagającej większej przepustowości lub komunikacji opartej na IP. • Generowanie nowego, losowego klucza WPA2PSK za każdym razem, gdy aktywowane jest Wi-Fi, który jest przesyłany do aplikacji mobilnej za pośrednictwem połączenia BLE. • Uwierzytelnianie użytkowników za pomocą tych samych danych uwierzytelniających co do kontrolera zdalnego dostępu. • Identyfikację serwera za pomocą certyfikatu PKI w formacie x509 oraz wyświetlanie znacznika serwisowego podczas łączenia. • Możliwość aktywacji diody ID LED w celu potwierdzenia połączenia z właściwym systemem. • Umożliwienie administratorom zdalnego wyłączania i włączania serwerów za pomocą poleceń.
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. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Windows Server 2025.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat.
	• Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.
	• Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
	• Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
	• Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.
	• Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
	• Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.
	• Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
	• Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
	  ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
	  ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.
	  ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.
	  ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.

	○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
Portal wsparcia produktu	• W ramach wsparcia technicznego wymagana jest usługa polegająca na przygotowaniu i dostarczeniu spersonalizowanego panelu w chmurze • Usługa powinna pozwalać na identyfikowanie priorytetów i potencjalnych zagrożeń technicznych sprzętu • co pomoże w podejmowanie właściwych działań. • Usługa powinna spełniać następujące założenia/funkcje: ○ Proaktywne zarządzanie priorytetami usług serwisowych w tym graficzną reprezentację poziomu zagrożeń. ○ Możliwość personalizacji widoku przez członków zespołu do zarządzanych przez nich lokalizacji i zasobów. ○ Dostęp do szczegółów dotyczących sprzętu i oprogramowania, w tym incydentów krytycznych, wsparcia technicznego, eskalacji, konserwacji na miejscu, poziomów kodu, poradników bezpieczeństwa i technicznych, zakresu wsparcia, wymiany części, łączności urządzeń i bram. ○ Dostęp do danych historycznych i analiz na potrzeby planowania IT
Aplikacja do zarządzania wsparciem	• Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego, automatycznie tworzące zgłoszenia serwisowe w przypadku awarii. • Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera. • Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów. • Konfiguracja i zaoferowany poziom wsparcia powinien po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie

	serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia powinien się kontaktować z klientem w celu rozwiązania problemu. • Oprogramowanie musi współpracować z kartą do zarządzania w urządzeniu, która będzie działać niezależnie od zainstalowanego systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit. Karta musi umożliwiać podmontowanie zdalnych wirtualnych napędów oraz wirtualną konsolę z dostępem do myszy, klawiatury. • Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające: o Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień. o Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów. o Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta. • upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, • możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji: • poprawkach i usprawnieniach dotyczących aktualizacji o dacie wydania ostatniej aktualizacji • priorytecie aktualizacji o zgodność z systemami operacyjnymi o jakiego komponentu sprzętu dotyczy aktualizacja o wszystkie poprzednie aktualizacje z informacjami jak powyżej o wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne • możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. • rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) • sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) • dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml

	raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.

5.2 System serwerowy - 1 sztuka

Licencja Microsoft Windows Server 2025 16-core Datacenter Reseller Option Kit en/cs/pl/ru/sv SW lub równoważna

Równoważność:

System operacyjny	Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO. Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym minimum dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. Wymagania: • możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, ○ możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, ○ możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, ○ 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, ○ wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, ○ wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, ○ 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), ○ wbudowane wsparcie instalacji i pracy na wolumenach, które: ▪ pozwalają na zmianę rozmiaru w czasie pracy systemu,

	▪ umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, ▪ umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, ▪ umożliwiają zdefiniowanie list kontroli dostępu (ACL), • wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, • wbudowane szyfrowanie dysków • możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, • możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, • wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, • graficzny interfejs użytkownika, • zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, • wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), • możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, • dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, • możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: • podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, • 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: o podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, o ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, o odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, • zdalna dystrybucja oprogramowania na stacje robocze, • praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, • szyfrowanie plików i folderów, • szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), • możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, • serwis udostępniania stron WWW, • wsparcie dla protokołu IP w wersji 6 (IPv6),

	• 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: ○ dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ○ obsługi ramek typu jumbo frames dla maszyn wirtualnych, ○ obsługi 4-KB sektorów dysków, ○ nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra. ○ możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, ○ możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), • 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, • wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), • możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, • mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, • możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

5.3 Konfiguracja serwera z systemem operacyjnym

W ramach realizacji zamówienia Wykonawca przeprowadzi:

1. Instalację i konfigurację serwera fizycznego.
2. Instalację i konfigurację systemu operacyjnego.
3. Przygotowanie, w systemie do kopii zapasowych, planów replikacji danych między magazynami danych.
4. Testy poprawności działania infrastruktury.
5. Instruktaż stanowiskowy pracowników IT z obsługi wdrożonych rozwiązań.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA

6. Zakup i konfiguracja switchy zarządzalnych i punktów dostępowych.

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

Zamawiający jest w posiadaniu rozwiązania FortiGate model 120G. W ramach rozbudowy istniejącego systemu, której celem jest rozszerzenie mechanizmów bezpieczeństwa o warstwę dostępową, wymaganym jest dostarczenie przełączników oraz innych elementów funkcjonalnych, współpracujących z istniejącym rozwiązaniem Fortigate, o następujących parametrach.

6.1 Switch Zarządzalny 8 portowy – 6 szt.:

Parametry fizyczne platformy:

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

Interfejsy sieciowe - wymagania minimalne

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

- 8 porty GE RJ-45,
- 2 porty GE, SFP.

Zarządzanie

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

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

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

Parametry wydajnościowe

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

Wymagane funkcje

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

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf

w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

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

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

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

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

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewniony serwis gwarancyjny producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

6.2 Punkt dostępowy wifi – 4 szt.:

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

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
   a) Temperatura 0–50°C,
   b) Wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać co najmniej następujące standardy:
   a) 2.4 GHz 802.11b/g/n/ax,
   b) 5 GHz 802.11a/n/ac/ax,
   c) 6 GHz 802.11ax/be
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.
5. Urządzenie musi być wyposażone w moduł BLE.
6. Urządzenie musi być wyposażone w co najmniej jeden interfejs Ethernet (RJ45) wspierający co najmniej szybkości 1G/2.5G/5.0G.
7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz. Maksymalne zużycie energii nie może przekraczać 17W przy wykorzystaniu wszystkich funkcji urządzenia.
8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
   a) Tunnel,
   b) Bridge,
   c) Mesh.
9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST).
11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    a) MIMO – 2x2,
    b) Wymagana przepustowość dla poszczególnych modułów radiowych:
       - min. 688 Mbps;
       - min. 2882 Mbps;
       - min. 5765 Mbps;
    c) Wymagana moc nadawania:
       - min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;

- min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
- min. 22 dBm dla pasma 6GHz z możliwością zmiany co 1dBm

d) Wsparcie dla kanałów 20/40/80/160/320MHz,
e) Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5dBi dla pasma 6GHz.
f) Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy.
g) Każdy z modułów radiowych musi posiadać możliwość pracy jako dedykowany skaner.

12. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512
13. Funkcje dodatkowe:
    a) OFDMA UL i DL,
    b) Spatial Reuse (BSS Coloring),
    c) UL-MU-MIMO,
    d) DL-MU-MIMO,
    e) Enhanced Target Wake Time (TWT),
    f) Wbudowany analizator widma,
    g) Wbudowane mechanizmy WIPS/WIDS.

Wykonawca dostarczy zasilacze do każdego punktu dostępowego.

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewniony serwis gwarancyjny producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2023, poz. 1582) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu,

transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

6.3 Wdrożenie switchy i punktów dostępowych.

Zakres Wdrożenia:

Przełączniki:

- Konfiguracja agregacji,
- Rejestracja oraz upgrade urządzeń,
- Konfiguracja VLAN,
- Weryfikacja działania VLAN na portach.

Acces Pointy:

-Rejestracja oraz upgrade urządzeń,
- Konfiguracja Profilu WiFi,
- Konfiguracja SSID oraz zasad bezpieczeństwa.

Dla zapewnienia wysokiego poziomu usług zamówienie musi być realizowane przez wykonawcę na poziomie min. zaawansowanym, posiadającego aktywne specjalizacje:

a) w zakresie Zdefiniowanej Programowo Sieci Rozległej (SD-WAN),
b) w zakresie Krawędzi Usługi Bezpiecznego Dostępu (SASE).

7. Zakup systemu zasilania awaryjnego.

7.1 Zasilacze awaryjne SERWEROWE – 2 szt

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań
1	Moc pozorna	1000 VA
2	Moc rzeczywista	1000 W
3	Topologia (klasyfikacja IEC 62040-3)	Line-interactive z AVR
4	Współczynnik mocy	1
5	Czas przełączenia na baterię	<4 ms
6	Liczba, typ gniazd wyjściowych	8 x IEC C13 (2 grupy po 2 gniazda IEC C13)

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

7	Typ gniazda wejściowego	IEC C20 16A
8	Czas podtrzymania dla 100% obciążenia dla pf=1	6 min
9	Czas podtrzymania przy 50% obciążenia dla pf=1	17 min
10	Dodatkowe baterie	Możliwość dodania do 4 dodatkowych modułów baterii w celu wydłużenia czasu podtrzymania do 148 minut dla 100% obciążenia przy pf=1
11	Napięcie znamionowe	200/208/220/230/240 V
12	Tolerancja napięci prostownika	160 V – 294 V (regulacja programowa 150-294 V)
13	Częstotliwość znamionowa	50/60 Hz autodetekcja
14	Tolerancja częstotliwości	47– 70 Hz
15	Kształt napięcia	Sinusoidalny
16	Napięcie znamionowe wyjściowe	200/208/220230/240 V do wyboru przez użytkownika
17	Zakres zmian napięcia	+6/-10% napięcia nominalnego
18	Częstotliwość wyjściowa	50/60 Hz
19	Współczynnik szczytu	3:1
20	Baterie wymieniane przez użytkownika "na gorąco"	Tak
21	Ochrona przed przeładowaniem	Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
22	Ochrona przed głębokim rozładowaniem	Tak
23	Okresowy automatyczny test baterii	Tak
24	System zarządzania pracą baterii	System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
26	Możliwość uruchomienia bez napięcia w sieci	Tak
27	Baterie wewnętrzne o pojemności nie mniejszej niż	7Ah 12V, minimum 4 szt.
29	Interfejs komunikacyjny	• USB
		• RS232 DB-9 żeński (HID)

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

		• styki przekaźnikowe
		• miniport wyłącznik ON/OFF
		• SNMP/Ethernet
30	Panel sterowania z wyświetlaczem LCD	• Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe , częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny,napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii w kWh).
		• Poziomy rząd przycisków sterowania
		• Poziomy rząd wskaźników stanu : zasialanie z siec(zielony), trybu bateryjnego (żółty), usterki (czerwony)
		• Sygnalizator akustyczny
31	Sygnały akustyczne	• Awaria
		• Niski stan naładowania baterii
		• Przeciążenie
		• Serwis
32	Przyciski sterujące i wskaźniki diodowe LED	• Przycisk Escape (anulowanie)
		• Przyciski funkcyjne (przewijanie w górę i w dół)
		• Przycisk Enter (potwierdzający)
		• Przycisk ON/OFF załączenia i wyłączenia
		• LED trybu zasilania z siec i(kolor zielony)
		• LED trybu baterii (kolor żółty)
		• LED usterki (kolor czerwony)
33	Kolor	Czarny RAL 9023 / RAL 9005
34	Typ obudowy	Uniwersalna Tower/Rack 2U
		1 x kabel szeregowy RS-232,
		1 x kabel komunikacyjny USB
		2 x kable wyjściowe IEC 10A
		2 x uchwyty kablowe
		1 x zestaw szyn montażowych 19’
		1x karta sieciowa SNMP/Ethernet
38	Dane techniczne karty SNMP	**Network Support:** Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP/

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

		Tymczasowe hasła: Nadawanie użytkownikowi dostępu za pomocą konta. Konto może wygasać po odpowiedniej, wprowadzonej liczbie dni (hasło przestaje być aktywne). **Blokowanie konta:** Po określonej liczbie nieudanych prób wpisania hasła lub określonej liczbie dni.
		Protokoły: MQTT/RNDIS/LDAP/NVD/SSH/PKI
		Kamptybilność: SNMP v1/v3 i IP v4/v6
		Interfejs: HTML5
		Adresowanie IP: DHCP/BootP/Manualne
		Szyfrowanie: pakiet szyfrów TLS 1.2 z minimum SHA256
		Dostępny port USB (microUSB - port serwisowy)
		Certyfikaty: CE, IEC 62443-4-2
36	Dołączone oprogramowanie	Tak, monitorujące i zarządzające UPS
37	Zgodność ze standardem Energy Star	Tak
38	Maksymalna szerokość	438 mm
39	Maksymalna wysokość	86 mm
40	Maksymalna głębokość	448 mm
41	Maksymalny ciężar	20 kg
42	Poziom hałasu w odl. 1m	do 45 dBA dla pracy normalnej
43	Znaki bezpieczeństwa	CE, TUV, CB Report, IEC/EN 62040-1-1, IEC/EN 62040-2
44	Gwarancja	36 miesięcy dla elektroniki
45	Możliwość montażu ręcznego bypassu serwisowego	Tak
47	Inne	Wszystkie elementy mają być nowe, nieużywane i wyprodukowane przez producenta UPS-a. Do oferty należy załączyć oświadczenie producenta potwierdzające ten fakt i o pochodzeniu sprzętu z oficjalnego kanału dystrybucji na rynek Polski.
		Możliwość integracji UPS z rozwiązaniem pozwalającym na masową aktualizację firmware i masową konfigurację parametrów pracy. Rozwiązanie musi umożliwiać monitoring parametrów pracy w środowisku mieszanym UPS - różni producenci UPS za pomocą protokołu SNMP. Serwer zarządzający rozwiązania musi występować w postaci dedykowanej wirtualnej maszyny dla systemów Vmware i Microsoft Hyper-V.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

7.2 Zasilacze awaryjne do szaf krosowych – 3 szt.

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań
1	Moc pozorna	1150 VA
2	Moc rzeczywista	920 W
3	Topologia (klasyfikacja IEC 62040-3)	Line-interactive z AVR
4	Liczba, typ gniazd wyjściowych	6 x IEC320 C13 (10A)
6	Czas podtrzymania dla 100% obciążenia	3 min
7	Czas podtrzymania przy 50% obciążenia	12 min
8	Napięcie znamionowe	230 V
9	Tolerancja napięcia wejściowego	160 V – 294 V (regulacja programowa 150-294 V)
10	Częstotliwość znamionowa	50/60 Hz autodetekcja
11	Tolerancja częstotliwości wejściowej	47-70 Hz (system 50 Hz), 56,5-70 Hz (system 60 Hz), 40 Hz w trybie niskiej czułości
12	Kształt napięcia w trybie pracy normalnej	Sinusoidalny
13	Napięcie znamionowe wyjściowe	230 V (domyślnie) / 200/208/220/240 V
14	Zakres zmian napięcia wyjściowego	maks. +6/-10% napięcia nominalnego
15	Częstotliwość wyjściowa	50/60 Hz +/-0,1%
17	Czas przełączania miedzy pracą sieciową a bateryjną	typowo 6ms
18	Baterie wymieniane przez użytkownika "na gorąco"	Tak
19	Ochrona przed głębokim rozładowaniem	Tak
20	Okresowy automatyczny test baterii	Tak
21	System zarządzania pracą baterii	System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

		jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
22	Zdolność zwarciowa w trybie bateryjnym	30 A
23	Zimny start	Tak
24	Baterie wewnętrzne o pojemności	2 x 9Ah/12V
25	Czas ładowania baterii do poziomy 90%	< 3 godz. do 90% pojemności użytkowej
26	Interfejs komunikacyjny	• USB
		• RS232 DB-9 żeński (HID)
		• mini-blok zacisków do zdalnego załączania
		• zdalny wyłącznik awaryjny
27	Panel sterowania z wyświetlaczem LCD	• Ekran z wyświetlaczem ciekłokrystalicznym LCD Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach.
		• Rząd przycisków sterowania
		• Rząd wskaźników stanu
		• Sygnalizator akustyczny
28	Sygnały akustyczne	• Awaria
		• Niski stan naładowania baterii
		• Przeciążenie
		• Serwis
29	Kolor	Czarny
30	Typ obudowy	Rack 1U
31	Dane techniczne karty SNMP (opcjonalnie wyposażenie)	**Network Support:** Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP/
		Tymczasowe hasła: Nadawanie użytkownikowi dostępu za pomocą konta. Konto może wygasać po odpowiedniej, wprowadzonej liczbie dni (hasło przestaje być aktywne). **Blokowanie konta:** Po określonej liczbie nieudanych prób wpisania hasła lub określonej liczbie dni.
		Protokoły: HTTPS1.1, MQTTS, TLS1.2, SNMPv1, SNMPv2c, SNMPv3, NTP, SMTPS, BOOTP/DHCP, CLI, SSH, ARP and Syslog

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA

		Kamptybilność: IPv4/v6, TLSv1.2, HTTP(S)v1.1, NTP, SMTP(S), BOOTP/DHCP, SSH, SysLog(S), LDAP, AD, RADIUS
		Interfejs: HTML5
		Adresowanie IP: DHCP/BootP/Manualne
		Szyfrowanie: pakiet szyfrów TLS 1.2 z minimum SHA256
		Dostępny port USB (microUSB - port serwisowy)
		Certyfikaty: IEC 62443-4-2
32	Dołączone oprogramowanie	Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie serwerów.
31	Wyposażenie standardowe	UPS, instrukcja obsługi, instrukcja bezpieczeństwa, inst. „Quick start”
		1 x kabel szeregowy RS-232,
		1 x kabel komunikacyjny USB
		Zestaw do montażu w szafie rack
		2 x kable wyjściowe IEC 10A
32	Maksymalna szerokość	438 mm
33	Maksymalna wysokość	43,2 mm
34	Maksymalna głębokość	509 mm
35	Maksymalny ciężar	14,3 kg
36	Poziom hałasu w odl. 1m	do 35 dBA dla pracy normalnej w odległosci 1m
37	Temperatura pracy	0 do 40 stopni C.
38	Znaki bezpieczeństwa / certyfikaty	CE, TUV, Reach / ROHS, ISO 140001
39	Bezpieczeństwo	IEC/EN 62040-1
40	Kompatybilność EMC	IEC/EN 62040-2/-3
41	Gwarancja	36 miesięcy dla elektroniki
42	Możliwość montażu bypassu serwisowego	Tak
43	Inne	Wszystkie elementy mają być nowe, nieużywane i wyprodukowane przez producenta UPS-a. Do oferty należy załączyć oświadczenie producenta potwierdzające ten fakt i o pochodzeniu sprzętu z oficjalnego kanału dystrybucji na rynek Polski.

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

		Możliwość integracji UPS z rozwiązaniem pozwalającym na masową aktualizację firmware i masową konfigurację parametrów pracy. Rozwiązanie musi umożliwiać monitoring parametrów pracy w środowisku mieszanym UPS - różni producenci UPS za pomocą protokołu SNMP. Serwer zarządzający rozwiązania musi występować w postaci dedykowanej wirtualnej maszyny dla systemów Vmware i Microsoft Hyper-V.

8. DODATKOWE ELEMENTY NIEZBĘDNE DO REALIZACJI ZAMÓWIENIA

W przypadku konieczności użycia dodatkowych komponentów, takich jak patchcordy, wkładki, przełączniki sieciowe (switch) lub inne elementy niezbędne do prawidłowego funkcjonowania wdrażanego rozwiązania **Wykonawca zobowiązany jest do uwzględnienia ich w cenie oferty.**

Zamawiający nie ponosi dodatkowych kosztów za komponenty wymagane do poprawnego działania wdrażanego rozwiązania.

<u>Wymagania dotyczące zespołu realizacyjnego Wykonawcy:</u>

8.1. Zamawiający planuje wdrożyć wyżej wymienione rozwiązania zgodnie z zaleceniami DYREKTYWY PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS2). Do tego niezbędne mogą być konsultacje dotyczące zgodności z wyżej wymienioną dyrektywą lub Systemem Zarządzania Bezpieczeństwem Informacji Zamawiającego, wobec czego w zespole realizującym zamówienie wymagana jest przynajmniej jedna osoba posiadająca aktualny certyfikat Audytora Wiodącego Systemu Bezpieczeństwa Informacji zgodnie z normą PN-EN ISO/IEC 27001:2023-08.

8.2. Zamawiający wymaga technicznego doświadczenia i kompetencji Wykonawcy wobec czego wymaganym jest, by dostawca dysponował osobami zdolnymi do wykonywania zamówienia, tj.:

- co najmniej jednym certyfikowanym inżynierem z zakresu oferowanego serwera **dla części nr 1**,
- co najmniej jednym certyfikowanym inżynierem z zakresu oferowanych switchy zarządzalnych i punktów dostępowych dla **części nr 2**.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

9. DOKUMENTACJA POWYKONAWCZA

Po zakończeniu wdrożenia (instalacji, konfiguracji, instruktażów stanowiskowych z obsługi sprzętu i oprogramowania) Wykonawca przygotuje dokumentację powykonawczą z przeprowadzonych pracy w formie zestawu dokumentów i raportów, które są przygotowywane po zakończeniu wdrożenia systemu informatycznego, projektu IT lub innego rodzaju prac technicznych. Jest ona kluczowa dla zapewnienia przejrzystości, utrzymania i dalszego rozwoju systemu.

Zamawiający będzie wymagał następujących opisów:

1. **Instrukcje instalacji i konfiguracji**
   - Kroki związane z instalacją i konfiguracją oprogramowania oraz sprzętu.
   - Wersje używanych narzędzi, frameworków oraz systemów operacyjnych.
2. **Zmiany wprowadzone podczas realizacji**
   - Opis modyfikacji w stosunku do pierwotnego planu, w tym zmiany w zakresie funkcjonalności, konfiguracji lub architektury systemu.
3. **Plany awaryjne i odzyskiwanie po awarii**
   - Procedury dotyczące radzenia sobie z krytycznymi awariami i przywracania systemu do działania.
4. **Zasady bezpieczeństwa**
   - Polityki bezpieczeństwa, w tym konfiguracja zapór sieciowych, zabezpieczenia dostępu, monitorowanie logów oraz zarządzanie hasłami.
5. **Lista komponentów i licencje**
   - Szczegółowy spis wszystkich komponentów sprzętowych i programowych użytych w projekcie, wraz z informacjami o licencjach i ich okresie ważności.
6. **Kontakt do wsparcia technicznego**
   - Informacje kontaktowe do osób lub firm odpowiedzialnych za utrzymanie systemu lub jego poszczególnych części.

Dokumentacja powykonawcza w IT jest niezbędna do dalszej eksploatacji i wsparcia systemu, umożliwiając nowym zespołom szybkie zapoznanie się z wdrożeniem oraz umożliwiając efektywne zarządzanie systemem w przyszłości.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa