Załącznik nr 2 do SWZ

Szczegółowy opis przedmiotu zamówienia

Dostawa sprzętu i oprogramowania w ramach Projektu „Cyfrowy Powiat"
Część 1: Zasilacz Centralny
Część 2: Serwer i zasilacz awaryjny
Część 3: Urządzenie UTM
Część 4: Stacje robocze, Dysk SSD i oprogramowanie

Zadanie realizowane w ramach projektu „Cyfrowy Powiat", projekt realizowany przez Powiat Kościerski w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój Cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, Działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczącej realizacji projektu grantowego ,,Cyfrowy Powiat".

1 Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

a. Całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
b. Całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana wcześniej;

2 Wymagania gwarancyjne.

Sprzęt

a. O ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona min. dwuletnia gwarancja (chyba, że zapisy szczegółowe stanowią inaczej) oparta na gwarancji producenta rozwiązanie; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
b. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych co najmniej jednym z wymienionych kanałów: telefon (w godzinach pracy Zamawiającego), e-mail serwis internetowy (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
c. Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego;

3 Miejsce instalacji sprzętu i oprogramowania/systemu.

a. Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części załącznika w budynku Starostwa Powiatowego w Kościerzynie w miejscach wskazanych przez Zamawiającego.

Termin realizacji: 30 dni od dnia zawarcia umowy

Część 1.

Zasilacz Centralny

Lp.	Opis wymagań techniczno-funkcjonalnych	Konfiguracja minimalna Zamawiającego	Konfiguracja proponowana przez Wykonawcę

1.	Technologia	VFI (true on-line, podwójne przetwarzanie energii)	
2.	Budowa	Beztransformatorowa, prostownik IGBT. UPS musi być wyposażony w podwójny tor zasilający niezależny dla prostownika i Bypassu.	
3.	Moc znamionowa	30 kVA / 30kW	
4.	Wyjściowy współczynnik mocy (PF)	1,0	
5.	Współczynnik mocy wejściowej 0.99.	0,99	
6.	Napięcie wejściowe trójfazowe	400 VAC 3F + N	
7.	Tolerancja napięcia wejściowego przy obciążeniu 100%; bez przechodzenia na baterie	172 – 287 Vac (L-N)	
8.	Zakres częstotliwości wejściowej	Wymagana 40-70 Hz	
9.	Sprawność AC-AC w trybie pracy on-line z obciążeniem 100%	nie mniejsza niż 96%	
10.	Tryb pracy ECO mode, zapewniający podwyższoną sprawność zasilacza	Wymagany	
11.	Możliwość rozbudowy mocy w okresie eksploatacji	Do minimum 8 sztuk w układzie pracy równoległej	
12.	Montażu modułu pracy równoległej w oferowanej jednostce	Wymagane – pozwala na dołączenie kolejnej jednostki.	
13.	Napięcie wyjściowe trójfazowe	400 VAC 3F + N	
14.	Częstotliwość wyjściowa	50/60Hz (programowalna)	
15.	Zintegrowane bezprzerwowe przełączniki obejściowe (by-pass)	Statyczny przełącznik (SCR) oraz ręczny rozłącznik serwisowy	
16.	Zewnętrzny bezprzerwowy Bypass serwisowy	Wymagany Bypass bezprzerwowy w postaci jednego przełącznika, z informacją o położeniu dla zabezpieczenia falownika UPS przed uszkodzeniem w przypadku nieprawidłowego użycia.	
17.	Wejście komunikacyjne na UPS do podłączenia sygnalizacji położenia przełącznika zewnętrznego Bypassu serwisowego, dla ochrony falownika UPS przed przypadkowym przełączeniem	Wymagane	
18.	Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem.	Wymagane, wraz z funkcją restingu baterii (nieciągłe ładowanie baterii z okresem restingu wynoszącymi minimum 10 dni)	
19.	Możliwość regulacji prądu ładowania baterii z poziomu panelu LCD w UPS-ie.	Wymagane – podać maksymalną wartość prądu ładowania baterii	
20.	Czas podtrzymania	30 minut przy obciążeniu 30kW	
21.	Lokalizacja baterii	Baterie umieszczone w module zewnętrznym. Należy stosować baterie szczelne AGM VRLA o żywotności 10-12 lat. Każdy łańcuch baterii zabezpieczony niezależnym rozłącznikiem bezpiecznikowym.	
22.	Autonomia pracy zasilacza UPS przy pracy z baterii podawana w minutach na panelu LCD zasilacza	Wymagane	
23.	W przypadku uszkodzenia pojedynczych akumulatorów w stosie, wymagana poprawna praca urządzenia ze zmniejszonym łańcuchem baterii	Wymagane, poprzez konfigurację, zmianę długości łańcucha baterii 30-40 sztuk	
24.	Stabilizacja napięcia wyjściowego w stanie ustalonym	± 1%	
25.	Stabilizacja napięcia wyjściowego w stanie nieustalonym	± 3%	
26.	Stabilność częstotliwości	bez synchronizacji: ± 0,05 Hz	

	wyjściowej:		
27.	Współczynnik szczytu	3:1	
28.	Minimalne przeciążenie falownika w trybie pracy normalnej	115% przez 60 minut 130% przez 10 minut 150% przez 1 minutę >150% - 0,2 sek	
29.	Panel sterujący z wyświetlaczem dotykowym oraz sygnalizacją diodową i akustyczną	Wymagane	
30.	Złącze interfejsów	SNMP, Dry Contact In/OUT, Modbus RTU, RS485	
31.	Karta sieciowa SNMP wbudowana w UPS.	Wymagane	
32.	Interfejs EPO (do wyłącznika ppoż.)	Wymagane – zestyk NO oraz NC. UPS zintegrowany z systemem ppoż budynku.	
33.	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	
34.	Dedykowane oprogramowanie do wysyłania SMS	Wymagane	
35.	Poziom hałasu w odległości 1m	< 50 dBA	
36.	Rejestr zdarzeń	Dziennik zdarzeń w UPS-ie + komunikaty serwisowe	
37.	Możliwość regulacji z panelu sterującego tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu	Wymagane	
38.	Monitorowanie stanu baterii i czasu autonomii	Stan baterii + dostępna autonomia mierzona w czasie rzeczywistym	
39.	UPS wyposażony w dotykowy, kolorowy wyświetlacz zabezpieczony hasłem przed ingerencją osób postronnych	Wymagane	
40.	UPS wyposażony w programowany tryb pracy ECO mode o podwyższonej sprawności z możliwością zaprogramowania dni tygodnia oraz godzin w jakich UPS przechodzi automatycznie w tryb oszczędnej pracy o podwyższonej sprawności.	Wymagane	
41.	UPS wyposażony w funkcję automatycznego czyszczenia z możliwością zaplanowania okresowego samoczynnego załączenia się tej funkcji.	Wymagane	
42.	UPS wyposażony w zdalny wyłącznik REPO	Wymagane – dostawa po stronie dostawcy UPS.	
43.	Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa ,kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE	Wymagane zarówno dla zasilacza UPS jak i baterii	
44.	Producent zasilacza UPS z siedzibą w Polsce, posiadający biuro dystrybucji i serwisu na terenie kraju.	Wymagane	
45.	Certyfikat ISO 9001 i 14001 dystrybutora i producenta sprzętu	Wymagane	
46.	Rozłączniki manewrowe	Zasilacz UPS powinien być wyposażony w komplet rozłączników pozwalających na bezpieczne włączenie i wyłączenie UPSa. Wymaga się co najmniej czterech rozłączników zamontowanych na UPS: zasilanie prostownika, zasilanie bypass, bypass serwisowy, rozłącznik wyjściowy z UPS.	
47.	Podłączenie zasilania i odbiorów	Podłączenie okablowania z tyłu zasilacza, z możliwością podłączenia dwóch oddzielnych	

		torów do zasilania prostownika i bypassu wewnętrznego.	
48.	UPS powinien posiadać funkcję umożliwiającą samo dociążenie bez podłączania dodatkowych odbiorników w celu przetestowania podzespołów pod pełnym obciążeniem w trakcie każdej wizyty serwisu.	Wymagane	
49.	Zasilacz wyposażony w kółka transportowe pozwalające na łatwe przemieszczanie w czasie konserwacji	Wymagane	
50.	Instrukcja w języku polskim	Wymagane	
51.	Przeglądy gwarancyjne	Wymaganie min. 3 przez okres gwarancji. (należy wkalkulować w cenę urządzenia)	
52.	Gwarancja	60 miesięcy na cały system UPS + baterie	
53.	Dostawa, wniesienie, podłączenie, uruchomienie oraz szkolenie	Wymagane	

Część 2.

Serwer

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 2U. Możliwość instalacji minimum 16 dysków 2.5”. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów 3rd Generacji Intel Xeon. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowany jeden procesor min. 8-rdzeniowy klasy x86, min. 2.8GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 131 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	Minimum 128GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	Min. 2 sloty PCIe z czego przynajmniej jeden x16 generacji 4.
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Dyski twarde	Zainstalowane: 2x dysk SSD SATA o pojemności min. 960GB, 6Gb, 2,5“ Hot-Plug. 5x dysk SAS o pojemności min. 2.4TB, 12Gb, 2,5“ Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 4GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
Wbudowane porty	4xUSB, w tym min. 1 port USB 3.0 2 porty VGA z czego 1 na panelu przednim

	Możliwość rozbudowy o Serial Port
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 800W każdy.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; - 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; - integracja z Active Directory; - wsparcie dla dynamic 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
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej

	• Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is" do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze 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 2016, 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	5 lat gwarancji producenta

	Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi sie na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowyych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. 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 przez producenta do 7 lat. 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. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

Zasilacz awaryjny

L P.	Opis wymagań techniczno-funkcjonalnych	Konfiguracja minimalna Zamawiającego
1.	Technologia	VFI (true on-line, podwójne przetwarzanie energii)
2.	Moc znamionowa	6 kVA / 6 kW
3.	Wyjściowy współczynnik mocy (PF)	1.0
4.	Napięcie wejściowe	230 Vac
5.	Tolerancja napięcia wejściowego przy obciążeniu 70-100%; bez przechodzenia na baterie	138– 299 Vac
6.	Tolerancja napięcia wejściowego przy obciążeniu mniejszym od 70%; bez przechodzenia na baterie	110 – 299 Vac
7.	Częstotliwość wejściowa	Wymagana 40-70 Hz
8.	Sprawność AC-AC w trybie pracy on-line z obciążeniem 100%	nie mniejsza niż 95%
9.	Sprawność AC-AC w trybie pracy Oszczędzania energii Eco Mode	nie mniejsza niż 99%
10.	Tryb pracy z konwersją częstotliwości	Wymagana praca ze stałą częstotliwością wyjściową 50Hz, przy zasilaniu 60Hz lub odwrotnie.
11.	Napięcie wyjściowe	230 Vac
12.	Częstotliwość wyjściowa	50/60Hz (programowalna)

13.	Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem	Wymagane
14.	Czas podtrzymania	8 minut dla 6 kW
15.	Baterie	Szczelne, bezobsługowe, w technologii AGM, o projektowanej żywotności min. 10-12 lat,
16.	Moduł baterii	Montowany w szafie rack
17.	Wymiary zestawu w szafie rack '	Maks 5 U
18.	Stabilizacja napięcia wyjściowego w stanie ustalonym	± 1%
19.	Stabilizacja napięcia wyjściowego w stanie nieustalonym	± 3%
20.	Współczynnik szczytu	3:1
21.	Panel sterujący z wyświetlaczem ciekłokrystalicznym LCD w języku polskim oraz sygnalizacją akustyczną	Wymagane
22.	Złącze interfejsów	RS232, USB, REPO
23.	Wyjściowa listwa do wpięcia UPS do instalacji stałej	Wymagana możliwość podłączenia przewodów o przekroju min 6mm2
24.	Karta sieciowa SNMP	Wymagana
25.	Interfejs EPO (do wyłącznika ppoż.)	Wymagane
26.	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
27.	Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego	Wymagane
28.	Poziom hałasu w odległości 1m,	< 50 dBA Wentylatory o regulowanej prędkości obrotowej w zależności od obciążenia i temperatury
29.	Możliwość regulacji z panelu sterującego tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu	Wymagane
30.	Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa ,kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE	Wymagane
31.	Producent zasilacza UPS z siedzibą w Polsce, posiadający biuro dystrybucji i serwisu na terenie kraju.	Wymagane
32.	Certyfikat ISO 9001 oraz 14001 producenta zasilacza UPS	Wymagane
33.	Instrukcja w języku polskim	Wymagane
34.	Gwarancja	60 miesięcy
35.	Przeglądy gwarancyjne	Wymaganie min. 3 przez okres gwarancji. (należy wkalkulować w cenę urządzenia)

Część 3

UTM

Urządzenie UTM firmy Fortinet FortiGate-80F (lub równoważny)

Lp.	Minimalne wymagania:	jednostka miary	liczba
1	Wymagania Ogólne: • Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. • System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. • W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu. • System musi wspierać IPv4 oraz IPv6 w zakresie: – Firewall. – Ochrony w warstwie aplikacji. – Protokołów routingu dynamicznego.	**szt.**	1
2	Redundancja, monitoring i wykrywanie awarii • W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. • Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. • Monitoring stanu realizowanych połączeń VPN.	**szt.**	1
3	Interfejsy, Dysk, Zasilanie: • System realizujący funkcję Firewall musi dysponować minimum 8 portami Gigabit Ethernet RJ-45 oraz 2 portami SFP Gigabit Ethernet. • System Firewall musi posiadać wbudowane gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. • W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. • System musi być wyposażony w zasilanie AC.	**szt.**	1
4	Parametry wydajnościowe: • W zakresie Firewall'a obsługa nie mniej niż 1,5 mln jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę. • Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. • Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.8 Gbps. • Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps. • Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. • Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps. • Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTPS – minimum 715 Mbps.	**szt.**	1
5	Funkcje Systemu Bezpieczeństwa: W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: • Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. • Kontrola Aplikacji.	**szt.**	1

	• Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. • Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. • Ochrona przed atakami - Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. • Zarządzanie pasmem (QoS, Traffic shaping). • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). • Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. • Analiza ruchu szyfrowanego protokołem SSL.		
6	Polityki, Firewall • Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. • System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: – Translację jeden do jeden oraz jeden do wielu. – Dedykowany ALG (Application Level Gateway) dla protokołu SIP. • W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. • Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. – Amazon Web Services (AWS). – Microsoft Azure – Cisco ACI. – Google Cloud Platform (GCP). – OpenStack. – VMware vCenter (ESXi).	**szt.**	1
7	Połączenia VPN • System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: – Wsparcie dla IKE v1 oraz v2. – Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). – Obsługa protokołu Diffie-Hellman grup 19 i 20. – Wsparcie dla pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. – Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. – Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. – Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. – Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. – Mechanizm „Split tunneling” dla połączeń Client-to-Site. • System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: – Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. – Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. – Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.	**szt.**	1
8	Routing i obsługa łączy WAN • W zakresie routingu rozwiązanie powinno zapewniać obsługę: – Routingu statycznego. – Policy Based Routingu.	**szt.**	1

	– Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.		
9	Zarządzanie pasmem • System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. • Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. • System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.	**szt.**	1
10	Ochrona przed malware • Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). • System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. • System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). • System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. • System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	**szt.**	1
11	Ochrona przed atakami • Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. • System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. • Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. • System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. • Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. • Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	**szt.**	1
12	Kontrola aplikacji • Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. • Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. • Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. • Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	**szt.**	1
13	Kontrola WWW • Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. • W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. • Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. • Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. • Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. • Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.	**szt.**	1

	• W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.		
14	Uwierzytelnianie użytkowników w ramach sesji • System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: – Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. – Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. – Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. • Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. • Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.	**szt.**	1
15	Zarządzanie • Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. • Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. • Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. • System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. • System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. • Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. • Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	**szt.**	1
16	Logowanie • Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. • W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. • Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. • Musi istnieć możliwość logowania do serwera SYSLOG.	**szt.**	1
17	Certyfikaty Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.	**szt.**	1
18	Serwisy i licencje W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów na okres 12 miesięcy. Powinny one obejmować: • Kontrola Aplikacji, IPS, Antywirus, Analiza typu Sandbox, Antyspam, Web Filtering	**szt.**	1
19	Gwarancja oraz wsparcie • Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać	**szt.**	1

	również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. • Minimum dodatkowe 4 godziny na rok wsparcia telefonicznego w języku polskim. • Wdrożenie zdalne obejmujące, – Aktualizacja firmaware – Podłączenie UTM do sieci – Konfiguracja interfejsów urządzenia – Konfiguracja routingu oraz NAT – Konfiguracja usługi DHCP – Konfiguracja VPN – IPsec – SSL VPN – Konfiguracja profili: – Deep Packet Inspection – Web filtering – DNS filtering – Application Control – Antivirus – IPS – DoS prevention		
20	Opisy do wymagań ogólnych Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.	**szt.**	1
21	Dostawa na koszt Wykonawcy	**szt.**	1

Część 4
Stacje robocze

Komputer firmy Dell Inspiron 5415 (lub równoważny) – 4 szt.

Lp.	Minimalne wymagania:	jednostka miary	liczba
1	Procesor: AMD Ryzen™ 5 5625U (6 rdzenie, 12 wątków, 2.30-4.30 GHz, 19 MBcache)	**szt.**	1
2	Pamięć RAM: 16 GB (SO-DIMM DDR4, 3200 MHz)	**szt.**	1
3	Grafika: Karta zintegrowana	**szt.**	1
4	Dysk: SSD PCIe, 256 GB	**szt.**	1
5	Karta sieciowa: 1GbE BASE-T	**szt.**	1
6	Zasilacz: Dołączony w zestawie	**szt.**	1
7	Typ obudowy: All-in-One	**szt.**	1
8	Ekran: • Typ: Matowy, LED, WVA • Przekątna ekranu: 23,8" • Rozdzielczość: 1920 x 1080 (FullHD)	**szt.**	1
9	Dźwięk: • Wbudowane dwa mikrofony • Zintegrowana karta dźwiękowa • Wbudowane głośniki stereo	**szt.**	1
10	Kamera internetowa: 2.1 Mpix	**szt.**	1
11	Złącza: • USB 3.2 Gen. 1 - 2 szt. • USB 3.2 Gen. 2 - 1 szt. • Wyjście słuchawkowe/głośnikowe - 1 szt. • RJ-45 (LAN) - 1 szt.	**szt.**	1
12	Mysz i klawiatura w zestawie	**szt.**	1
13	System operacyjny: Microsoft Windows 11 Pro	**szt.**	1
14	Gwarancja: 24 miesiące	**szt.**	1
15	Dostawa na koszt Wykonawcy	**szt.**	1

Dyski:

Dysk SSD firmy GOODRAM 256GB 2,5" SATA SSD CX400 (lub równoważny) wraz z uchwytem do montażu – 11 szt.

Lp.	Minimalne wymagania:	jednostka miary	liczba
1	Rodzaj dysku: SATA SSD	**szt.**	1
2	Pojemność: 256 GB	**szt.**	1
3	Format: 2.5"	**szt.**	1
4	Interfejs: 2,5" SATA	**szt.**	1
5	Prędkość odczytu (maksymalna): 550 MB/s	**szt.**	1
6	Prędkość zapisu (maksymalna): 480 MB/s	**szt.**	1
7	Rodzaj kości pamięci: TLC	**szt.**	1
8	Niezawodność MTBF: 2 000 000 godz.	**szt.**	1
9	Gwarancja: 36 miesięcy	**szt.**	1
10	Wyposażenie dodatkowe – uchwyt montażowy (sanki): • Typ: Sanki do montażu dysku 2,5" w zatoce 3,5" • Dołączone śrubki do montażu dysku • Gwarancja: 24 miesiące	**szt.**	11
11	Dostawa na koszt Wykonawcy	**szt.**	1

Oprogramowanie:

Dodatkowa licencja oprogramowania do tworzenia kopii zapasowych - Xopero One Backup&Recovery

Lp.	Minimalne wymagania:	jednostka miary	liczba
1	Bezterminowa licencja Xopero One Virtual Protection do robienia kopii z maszyny wirtualnej	**szt.**	1
2	Wsparcie techniczne (aktualizacje, pomoc techniczna) producenta dla Xopero One Virtual Protection do 28.02.2023 r.	**szt.**	1
3	Wdrożenie zdalne obejmujące: • Instalację oprogramowania • Utworzenie planu kopii zapasowej w programie	**szt.**	1
4	Dostawa na koszt Wykonawcy	**szt.**	1