Załącznik nr 7 do SWZ- Opis przedmiotu zamówienia

SPECYFIKACJA TECHNICZNA

Zakres zamówienia obejmuje:

- **I – Dostawa, wstępna konfiguracja oraz uruchomienie serwerów wraz z wymaganymi licencjami, konfiguracja usługi katalogowej wraz z migracją profili lokalnych oraz wirtualizacja posiadanej infrastruktury serwerowej wraz z dostawą systemu podtrzymania bateryjnego**
- **II – konfiguracja systemu kopii zapasowej**
- **III - usługa wsparcia środowiska IT Zamawiającego**
- **IV – Zapewnienie systemu monitoringu stanu infrastruktury IT Zamawiającego**
- **V - Szkolenia z zakresu rozwiązań technicznych**
- **VI - Modernizacja infrastruktury sieciowej**
- **VII - Szkolenia z zakresu cyberbezpieczeństwa**
- **VIII - Dostarczenie stacji roboczych**
- **IX - Dostawa licencji Microsoft 365 Business Basic (lub rozwiązania równoważnego)**

I

Dostawa, wstępna konfiguracja oraz uruchomienie serwerów wraz z wymaganymi licencjami, konfiguracja usługi katalogowej wraz z migracją profili lokalnych oraz wirtualizacja posiadanej infrastruktury serwerowej wraz z dostawą systemu podtrzymania bateryjnego

1.1 Przedmiot zamówienia

Przedmiotem zamówienia jest:

1) dostawa fabrycznie nowego Sprzętu, nie używanego w innych środowiskach ani projektach;
2) konfiguracja, instalacja serwerów oraz wirtualizacja wskazanych zasobów Zamawiającego wraz z uruchomieniem środowiska;
3) dostarczenie systemu podtrzymania bateryjnego w ilościach według typu:
    a) typ 1 – 1 sztuka
    b) typ 2 – 1 sztuka
4) konfiguracja usługi katalogowej;
5) migracja profili lokalnych stacji roboczych używanych przez pracowników Zamawiającego do usługi katalogowej w kooperacji z Działem IT Zamawiającego;
6) utworzenie polityki bezpieczeństwa w dziedzinie haseł;
7) konfiguracja polityk w oparciu o wskazania Zamawiającego (4 polityki);
8) dostarczenie przez Wykonawcę dokumentacji dostarczonego Sprzętu;
9) dostawa Oprogramowania i zapewnienie możliwości korzystania przez Zamawiającego z Oprogramowania na warunkach licencyjnych mających zastosowanie do Oprogramowania.

1.2 Termin realizacji zamówienia oraz liczba dostarczanego sprzętu

Zamawiający wymaga, aby dostawa sprzętu, o którym mowa w pkt 1.1 do Zamawiającego nastąpiła w terminie do 18 tygodni od podpisania umowy. W terminie 2 tygodni od dostarczenia sprzętu Dostawca jest zobligowany do ustalenia terminu wdrożenia z Zamawiającym.

1.3 Wymagania wobec Wykonawcy

O udzielenie zamówienia mogą ubiegać się Wykonawcy, który posiadają niezbędną wiedzę i kwalifikacje do realizacji zamówienia.

1.4 Wymagania szczegółowe Zamawiającego

Zestawienie wymaganych parametrów technicznych serwera (2 sztuki)

Nazwa elementu lub cechy	Parametry
Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych;
Procesor	• Zainstalowany 1 procesor w architekturze x86, maksymalnie 8-rdzeniowy, o TDP nie większym niż 105W. Wynik wydajności procesora instalowanego w oferowanym serwerze nie powinien być niższy niż 130 punktów w teście SPECrate®2017_int_base, opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org; • Możliwość rozbudowy serwera o drugi procesor tego samego typu;
Płyta główna	• Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera; • Z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje; • Wyposażona w moduł TPM 2.0; • Minimum 32 sloty DIMM na pamięć DDR4;
Pamięć operacyjna	• Zainstalowane minimum 64GB pamięci RAM o częstotliwości minimum 3200MHz w modułach o pojemności 16GB każdy; • Możliwość rozbudowy/rekonfiguarcji serwera do 8TB pamięci RAM DDR4;
Zabezpieczenie pamięci	Wsparcie dla: memory mirroring, ECC, SDDC lub Advanced ECC;
Procesor	• Zintegrowana karta graficzna z minimum 16MB pamięci, osiągająca rozdzielczość 1920x1200 przy 60 Hz;

Graficzny	• 1 port VGA na tylnym panelu serwera oraz jeden port VGA na panelu przednim; • Możliwość instalacji dodatkowej karty GPU posiadającą 4 porty mDP lub DP lub HDMI;
Zatoki dyskowe i dyski	• Serwer wyposażony w 8 zatok dyskowych hot-plug 2.5” umożlwiających instalację dysków SSD/HDD interfejsem SAS/SATA; • Serwer wyposażony w min. 4 dyski SATA SSD o pojemności min. 960GB każdy. Dyski klasy Enterprise dedykowane do pracy w oferowanym serwerze i o parametrze DWPD min. 1; • Możliwość rozbudowy serwera o 2 dyski M.2 SSD NVMe o pojemności min. 960GB. Rozwiązanie dedykowane jako nośnik boot, musi umożliwiać konfigurację sprzętowego mirroringu (RAID 1).
Kontroler dyskowy	• Serwer wyposażony w sprzętowy kontroler RAID obsługujący dyski SAS 3.0 i pozwalający na konfigurację RAID 0,1,10,5; • Serwer umożliwiający rozbudowę/rekonfigurację o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 2 GB pamięci cache z podtrzymywaniem bateryjnym. Kontroler obsługujący funkcjonalność SSD Cache na poziomie sprzętowym tj. możliwość wykorzystania dysku SSD do przyśpieszenia operacji odczytu dla grupy RAID na dyskach HDD.
Zasilacz	Minimum dwa redundantne zasilacze o mocy min. 800W z certyfikatem minimum Platinum.
Interfejsy sieciowe	• Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej. • Karta LAN posiadająca 2 porty 10GbE BASE-T oraz dwa porty 1GbE BASE-T nie zajmujące slotów PCIe serwera;
Sloty PCIe	• Serwer posiadający – w momencie dostarczenia – min. 2 sloty PCIe generacji 4.0 w tym 1 slot działający z prędkością x16; • W momencie dostarczenia min. jeden slot PCIe powinien być wolny, dostępny dla użytkownika;
Dodatkowe porty	• z przodu obudowy: 1x USB 3.0, 1x VGA • z tyłu obudowy: 2x USB 3.0, 1x VGA • wewnętrzne: 1 x USB 3.0
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
Zarządzanie	Serwer musi posiadać moduł zarządzający wyposażony w minimum jeden port 10/100/1000 Base-T Ethernet, pozwalający na zdalny dostęp i zarządzanie serwerem przy użyciu graficznego interfejsu Web. Moduł musi umożliwiać: • monitorowanie podzespołów serwera: temperatura, zasilacze,

	wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub • dostęp do karty możliwy: - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend (SSH lub IPMI) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz SNMP • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB • funkcja zdalnej konsoli szeregowej przez SSH (wirtualny port szeregowy) • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • możliwość równoczesnej obsługi przez min. 2 administratorów • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Funkcje zabezpieczeń	• Czujnik otwarcia obudowy; • Ramka zabezpieczająca przed nieautoryzowanym dostępem do dysków serwera;
Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.
Wspierane systemy operacyjne	Microsoft Windows Server 2019, 2022, Red Hat Enterprise Linux 8, VMware vSphere (ESXi) 7.0;
Gwarancja	• 36 miesięcy wsparcia producenta w trybie pełnego serwisu on-site NBD. Przy czym NBD określa czas reakcji w miejscu instalacji sprzętu; • W przypadku awarii dyski twarde pozostają własnością zamawiającego; • Usługa wsparcia technicznego musi być świadczona przez producenta lub

	autoryzowany serwis producenta oferowanych urządzeń;
Inne	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001; • Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA; • Możliwość rozbudowy serwerów zgodnie z ww. wyżej specyfikacją musi być możliwa przy użyciu certyfikowanych komponentów oraz zachowaniu pełnego wsparcia i gwarancji producenta serwera; • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce;
Licencje	Dostarczenie 4 sztuk Licencji Windows Server 2022 Standard 16 core pack lub równoważnych. Licencje muszą być nie przypisane do sprzętu.

Punktacja dodatkowa:

Parametr dodatkowy 1	Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanych serwerów, nawet po wygaśnięciu 3-letniego okresu wsparcia.
Parametr dodatkowy 2	Oprogramowanie diagnostyczne producenta serwera (lub wbudowana funkcja karty zarządzającej) posiadające funkcjonalność predykcji awarii wszystkich kluczowych komponentów serwera: procesorów, pamięci RAM, dysków wewnętrznych HDD/SSD/M.2 SSD, wentylatorów, zasilaczy, kontrolerów dyskowych.
Parametr dodatkowy 3	Serwer wyposażony w wbudowany panel LCD umieszczony na froncie obudowy i pozwalający na wyświetlenie informacji o: stanie serwera, konfiguracji sieciowej karty zarządzającej, zasilaniu, temperaturze.
Parametr dodatkowy 4	Możliwość zarządzania – monitoring parametrów pracy i konfiguracja najważniejszych komponentów - z poziomu urządzania mobilnego przy użyciu dedykowanej aplikacji dostępnej na Android i/lub iOS.

1.5 Zestawienie wymaganych parametrów technicznych odnośnie systemów operacyjnych:

1) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości.
2) Wbudowane wsparcie instalacji i pracy na wolumenach które:
   a) pozwalają na zmianę rozmiaru w czasie pracy systemu,

   b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   c) umożliwiają kompresję „w locie" dla wybranych plików i/lub folderów,
   d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
3) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
4) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
5) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
6) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
7) Wbudowana zapora internetowa (firewall) z obsługi definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
8) Graficzny interfejs użytkownika.
9) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
10) Możliwość zmiany języka interfejsu po zainstalowaniu systemu dla co najmniej języka polskiego i angielskiego.
11) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
12) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
13) Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
14) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
   a) podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
   b) usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarzadzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
      i) podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
      ii) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
      iii) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
15) Zdalna dystrybucja oprogramowania na stacje robocze.
16) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
17) PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
   a) dystrybucję certyfikatów poprzez http,
   b) konsolidację CA dla wielu lasów domeny,
   c) automatyczne rejestrowania certyfikat6w pomiędzy różnymi lasami domen.
18) Szyfrowanie plików i folderów.
19) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

20) Serwis udostępniania stron WWW
21) Wsparcie dla protokołu IP w wersji 6 (Ipv6).
22) Wbudowane usługi VPN pozwalające na zestawienie równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.

Zestawienie wymaganych parametrów technicznych systemu podtrzymania bateryjnego Typ 1

Nazwa komponentu	Wymagane minimalne parametry techniczne
Moc znamionowa w W	minimum 1980 W
Moc znamionowa w VA	minimum 2200 VA
Rodzaj akumulatora	kwasowo-ołowiowy
Typowy czas pełnego ładowania	3 godziny
Żywotność baterii	minimum 5 lat
Ilość gniazd sieciowych	minimum 9 sztuk
Znamionowa energia przepięcia	375 J
Czas przełączania zasilania	maksymalnie 8ms
Ochrona linii danych	Ochrona kabli sieci Ethernet RJ45 10/100/1000 Base-T
Masa produktu	Maksymalnie 43 kg
Sposób montażu	Szafa RACK 19”
Maksymalna wysokość	2U
Komunikacja i zarządzanie	• Dioda led wskazująca status zasilania • Alarm niskiego poziomu naładowania akumulatora
Certyfikaty produktu	CE, EAC, IRAM, RCM, VDE
Normy produktu	EN/IEC 62040-1 EN/IEC 62040-2 EN 60950
Gwarancja	minimum 24 miesiące

Zestawienie wymaganych parametrów technicznych systemu podtrzymania bateryjnego Typ 2

Nazwa komponentu	Wymagane minimalne parametry techniczne
Moc znamionowa w W	minimum 410 W
Moc znamionowa w VA	minimum 750 VA
Rodzaj akumulatora	kwasowo-ołowiowy
Typowy czas pełnego ładowania	8 godzin
Napięcie akumulatora	12 V
Pojemność baterii	minimum 7 Ah
Żywotność baterii	minimum 3 lata
Znamionowa energia przepięcia	273 J
Ochrona linii danych	Ochrona kabli sieci Ethernet RJ45 10/100/1000 Base-T
Masa produktu	Maksymalnie 5,2 kg
Sposób montażu	wolnostojący
Komunikacja i zarządzanie	• Dioda led wskazująca status zasilania • Alarm niskiego poziomu naładowania akumulatora
Certyfikaty produktu	CE, CB, EAC
Normy produktu	EN/IEC 62040-1 EN/IEC 62040-2 CE
Gwarancja	minimum 24 miesiące

1.6 Wymagane prace wdrożeniowe

1) **Dostarczenie sprzętu wraz z konfiguracją i wirtualizacją zasobów**
   a) Zinwentaryzowanie i walidacja aktualnego środowiska serwerowego objętego migracją
   b) Zamawiający zobowiązuje się do wskazania osób kontaktowych, świadczących wsparcie dla aplikacji dziedzinowych, celem ich migracji do nowego środowiska serwerowego.
   c) Dedykowane wsparcie aplikacji dziedzinowych realizuje migrację aplikacji do nowego środowiska na wniosek Zamawiającego
   d) Podłączenie serwerów do infrastruktury elektrycznej i sieciowej Zamawiającego
   e) Wstępna konfiguracja serwerów polegająca na nadaniu dostępów, adresacji oraz aktualizacji oprogramowaniu sprzętowego do najnowszej zalecanej przez producenta wersji
   f) Przygotowanie środowiska wirtualizacji na nowo dostarczonych serwerach
   g) Przygotowanie 4 maszyn wirtualnych opartych o system Microsoft Windows Server w najnowszej, dostępnej wersji
   h) Przekazanie dostępów Zamawiającemu
   i) Testy po uruchomieniu środowiska wirtualnego polegające na sprawdzeniu poprawności uruchamiania się środowiska systemowego i poprawności pracy systemu replikacji
   j) Uruchomienie replikacji dla wskazanych 4 maszyn wirtualnych
   k) Drugi dostarczony serwer pełnić ma rolę repozytorium replik i ma służyć awaryjnemu uruchomieniu środowiska
   l) Przygotowanie dokumentacji powdrożeniowej zawierającej opis wdrożonej konfiguracji wirtualizacji zasobów

2) **Wymagania odnośnie środowiska wirtualizacji:**
   a) Możliwość obsługi Secure Boot oraz Trusted Platform Module
   b) Możliwość rozruchu PXE z syntetyczną kartą sieciową
   c) Możliwość rozruchu z dysku SCSI
   d) Możliwość obsługi dysków wirtualnych w formacie .vhdx
   e) Wsparcie dla UEFI z GPT
   f) Obsługa 32-bitowych i 64-bitowych systemów operacyjnych
   g) Obsługa do 12TB pamięci RAM
   h) Obsługa do 240 procesorów wirtualnych
   i) Wsparcie systemów Linux oraz Windows
   j) Wsparcie dla Intel VT oraz AMD-V
   k) Obsługa replikacji między hostami oraz klastrów wysokiej dostępności (failover cluster)
   l) Wirtualizator musi pozwalać na zmianę parametrów maszyny wirtualnej
   m) Wirtualizator musi zapewniać możliwość zatrzymywania, uruchamiania i restartowania maszyn wirtualnych
   n) Wirtualizator musi umożliwiać tworzenie wirtualnych przełączników
   o) Wirtualizator musi zapewniać wbudowane mechanizmy do migracji na żywo maszyn wirtualnych, migracji magazynu oraz funkcję importu/eksportu maszyny wirtualnej
   p) Wirtualizator musi zapewniać możliwość tworzenia kopii maszyn wirtualnych w innych lokalizacjach fizycznych (mechanizmy replikacji), kopiowania woluminów w tle oraz budowanie klastrów wysokiej dostępności

Wdrożenie usługi katalogowej w infrastrukturze Zamawiającego

a) Wykonawca zobowiązuje się do dostarczenia 40 licencji USER CAL potrzebnych do wdrożenia usługi katalogowej
b) Utworzenie maszyny wirtualnej na hypervisorze pełniącej rolę kontrolera domeny
c) Utworzenie domeny usługi katalogowej
d) Utworzenie schematu organizacyjnego oraz nadanie odpowiednich uprawnień poszczególnym użytkownikom, po ustaleniach z Zamawiającym
e) Konfiguracja polityki bezpieczeństwa haseł
f) Utworzenie 4 polityk w oparciu o wskazania zamawiającego
g) Podłączenie komputerów do utworzonej domeny – proces wykonywany wspólnie z administratorem IT Zamawiającego, na bazie ustalonego harmonogramu
h) Migracja profili lokalnych ze stacji roboczych użytkowników do usługi katalogowej – proces wykonywany wspólnie z administratorem IT Zamawiającego, na bazie ustalonego harmonogramu
i) Instalacja odpowiednich, wskazanych przez Zamawiającego drukarek na poszczególnych stacjach roboczych wraz z działem IT Zamawiającego
j) Dokumentowanie wykonanych prac

II

Konfiguracja systemu kopii zapasowej

2.1 Przedmiot zamówienia

Przedmiotem zamówienia jest:
1) dostawa sytemu kopii zapasowych;
2) wdrożenie oraz konfiguracja systemu kopii zapasowych w środowisku IT Zamawiającego
3) dostarczenie przez Wykonawcę dokumentacji konfiguracji wdrożonego systemu

2.2 Termin realizacji zamówienia oraz liczba dostarczanego sprzętu

Zamawiający wymaga, aby dostawa systemu, o którym mowa w pkt 2.1 do Zamawiającego nastąpiła w terminie 4 tygodni od daty wdrożenia sprzętu dostarczonego i skonfigurowanego w ramach Części I niniejszego dokumentu

2.3 Wymagania wobec Wykonawcy

O udzielenie zamówienia mogą ubiegać się Wykonawcy, który posiadają niezbędną wiedzę i kwalifikacje do realizacji zamówienia.

2.4 Wymagania szczegółowe Zamawiającego:

1) Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
2) Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.

3) Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.
4) Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
5) Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
6) Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
7) Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-incremental)
8) Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
9) Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
10) Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy aktualizowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
11) Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania migawki.
12) Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
13) Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
14) Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
15) Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
16) Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
17) Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
18) Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
19) Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
20) Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
21) Repozytoria oparte o XFS muszą pozwalać na zmienność danych przez określoną ilość czasu (tzw. Immutability)

22) Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
23) Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
24) Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
25) Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
26) Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
27) Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
28) Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
29) Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
30) Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
31) Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
32) Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
33) Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
34) Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
    a) Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
    b) BSD: UFS, UFS2
    c) Solaris: ZFS, UFS
    d) Mac: HFS, HFS+
    e) Windows: NTFS, FAT, FAT32, ReFS
    f) Novell OES: NSS
35) Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
36) Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.

37) Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
38) Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
39) Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
40) Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
41) Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
42) Oprogramowanie musi zapewniać możliwość wykonywania kopii zapasowych do 10 maszyn wirtualnych

2.5 Wymagane prace wdrożeniowe

1) instalacja oprogramowania do kopii zapasowych na zasobie wirtualnym wskazanym przez Zamawiającego;
2) skonfigurowanie repozytorium kopii zapasowych wskazanego przez Klienta
3) zaprojektowanie i wdrożenie polityki tworzenia kopii zapasowych z wykorzystaniem dostarczonego oprogramowania do kopii zapasowych dla przynajmniej 4 maszyn wirtualnych
4) przeprowadzenie testów akceptacyjnych poprawności działania operacji, kopii zapasowych i odzyskiwania danych;
5) konfiguracja powiadomień systemu kopii zapasowej oraz weryfikacja ich działania;
6) szkolenie z systemu kopii zapasowych obejmujące:
   a) przybliżenie interfejsu rozwiązania i funkcjonalności
   b) tworzenie zadań kopii zapasowych
   c) tworzenie powiadomień, walidacji wykonywania się kopii zapasowych
   d) dobrych praktyk w dziedzinie administracji i obsługi systemów kopii zapasowych

III

Usługa wsparcia środowiska IT Zamawiającego

3.1 Przedmiot zamówienia

Przedmiotem zamówienia jest:
1) Świadczenie kompleksowej usługi wsparcia w zakresie merytoryczno–konsultacyjnym w dziedzinie infrastruktury IT Zamawiającego

3.2 Wymagania wobec Wykonawcy

O udzielenie zamówienia mogą ubiegać się Wykonawcy, który posiadają niezbędną wiedzę i kwalifikacje do realizacji zamówienia.

3.3 Szczegółowe wymagania odnośnie usługi

1) Usługa wsparcia ma być realizowana w następujących obszarach:
   a) Wsparcie utrzymaniowe infrastruktury IT – pomoc w analizie i rozwiązywaniu problemów infrastrukturalnych (urządzenie brzegowe, urządzenia sieciowe typu przełącznik, serwery fizyczne, serwery z wirtualizacją, NAS)
   b) Wsparcie konsultacyjne – umożliwienie realizacji konsultacji odnośnie ścieżek rozwoju i zmian w infrastrukturze Zamawiającego, propozycje zmian konfiguracyjnych, zakupowych i aktualizacyjnych wedle potrzeb
   c) Dostęp do 5 webinariów dotyczących problematyki administracyjnej i bezpieczeństwa zasobów IT
2) Rozpoczęcie współpracy i wdrożenie usługi wsparcia musi wiązać się z inwentaryzacją zasobów IT Zamawiającego przez Oferenta, dopuszcza się realizację procesu inwentaryzacji zdalnie lub w siedzibie Zamawiającego wraz z osobą odpowiedzialną za obszar IT po stronie Zamawiającego
3) Wsparcie ma być realizowane w zakresie 36 godzin przypadających na okres 18 miesięcy trwania umowy, to jest w pakiecie 2 godzin roboczych w miesiącu
4) Niewykorzystane godziny w 1 miesięcznym okresie rozliczeniowym nie przechodzą do następnego okresu rozliczeniowego
5) Zamawiający akceptuje formę zdalną poprzez udostępniony przez Wykonawcę kanał elektroniczny lub dedykowaną aplikację, z możliwością późniejszego odtworzenia spotkania (nagranie szkolenia), z zastrzeżeniem nierozpowszechniania nagrania poza obszar organizacji Zamawiającego
6) W ramach pakietu miesięcznej liczby godzin wsparcia realizowane są działania dotyczą diagnostyki i naprawy problemów występujących w infrastrukturze Klienta oraz spotkania konsultacyjne
7) Kontakt w ramach usługi wsparcia musi być realizowany za pośrednictwem infolinii, komunikacji e-mail lub systemu formularzy, przy czym Zamawiający wymaga utrzymania minimum 2 form kontaktu z wcześniej wymienionych
8) Wsparcie musi być realizowane w oparciu o SLA jak w tabeli poniżej:

Priorytet	Czas realizacji (rh)	Czas reakcji (rh)
Krytyczny	4	1
Wysoki	6	1
Średni	10	1
Niski	24	1
Wniosek	40	1
Zdarzenie	--	1

* rh – roboczogodzina

Natomiast sam status nadawania priorytetów zgłaszanym zadaniom ma odbywać się w oparciu o niniejszą tabelę priorytetów:

	Pilność				
WPŁYW	**Praca uniemożliwiona**	**Utrudnienie pracy (istnieje alternatywa)**	**Prace Planowe**	**Wniosek o usługę**	**Zdarzenie**
Cała organizacja	Krytyczny	Krytyczny	Średni	Wniosek	Zdarzenie
Kilka Lokacji	Krytyczny	Wysoki	Średni	Wniosek	Zdarzenie
Grupa użytkowników	Wysoki	Wysoki	Niski	Wniosek	Zdarzenie
Pojedynczy użytkownik	Średni	Niski	Niski	Wniosek	Zdarzenie

Gdzie zamawiający definiuje pojęcia jak niżej:

Wpływ – jest jednostką mierzalności krytyczności dla biznesu, dotyczącą incydentów lub problemów. Wpływ jest mierzony liczbą ludzi lub systemów zaangażowanych.

Wpływ	Opis
1. Cała organizacja	Wszyscy autoryzowani użytkownicy.
2. Kilka lokacji	Wszyscy autoryzowani użytkownicy z kilku lokacji.
3. Niewielka grupa użytkowników	Wszyscy autoryzowani użytkownicy z jednej lokacji / zespołu.
4. Pojedynczy użytkownik	Indywidualne zgłoszenie.

Pilność – jest określeniem szybkości rozwiązywania incydentów posiadających konkretny wpływ.

Pilność	Opis
1. Praca uniemożliwiona	Poważny defekt prowadzący do całkowitego przerwania procesów biznesowych po stronie klienta. Nie istnieje obejście problemu / doraźne rozwiązanie. Wykonywanie pracy jest niemożliwe.
2. Utrudnienie pracy (istnieje obejście)	Defekt mający wpływ na procesy biznesowe po stronie klienta, przerwany przepływ operacyjny. Dysfunkcja podstawowych narzędzi lub aplikacji. Praca jest utrudniona, ale możliwa.
3. Niska pilność / planowane	Utrudnienie mające wpływ na pracę użytkownika, lecz jego pilność jest niewysoka i rozwiązanie może być zaplanowane w czasie.
4. Wniosek o usługę / pytanie	Dotyczy wniosku o usługę lub zapytania, a nie incydentu.

9) Dostęp do wsparcia musi być realizowany w systemie 24/7/365, zgłoszenia w charakterze incydentów, wniosków i zdarzeń muszą być podejmowane i realizowane od poniedziałku do piątku w godzinach 7:00 – 17:00, natomiast w godzinach 17:00 – 7:00 oraz w dni wolne od pracy i weekendy, podmiot świadczący musi zapewnić inżyniera dyżurnego, który jest w stanie podjąć działania na wypadek zdarzeń krytycznych, które wystąpią w czasie poza godzinami pracy zamawiającego lub na wypadek incydentów zgłoszonych w tych porach przez administratora zasobów IT Zamawiającego

IV

Zapewnienie systemu monitoringu stanu infrastruktury IT Zamawiającego

4.1 Przedmiot zamówienia

Przedmiotem zamówienia jest:

1) dostawa systemu monitoringu dla infrastruktury IT Zamawiającego;
2) przeprowadzenie szkolenia z posługiwania się dostarczonym rozwiązaniem i interpretacji danych prezentowanych przez system monitoringu.

4.2 Szczegółowe wymagania odnośnie proponowanego rozwiązania

1) System powinien być uruchomiony na zasobach infrastruktury IT Zamawiającego.
2) System powinien być zrealizowany na środowisku nie wymagającym licencjonowania systemu operacyjnego maszyny wirtualnej
3) System powinien agregować dane o statusie maszyn wirtualnych realizowanych na wirtualizatorze Microsoft HYPER-V oraz VMWare
4) W przypadku systemów z rodziny Microsoft Windows Server oraz Linux, system powinien zapewniać możliwość zdefiniowania kluczowych usług, których wyłączenie lub przerwa w działaniu będzie monitowana - serwisów uruchomionych na powłoce Windows/Linux, statusu baz danych MSSQL Express i Standard, PostgresSQL, Firebird
5) System musi zapewniać możliwość odczytu danych z urządzeń przy wykorzystaniu protokołu SNMP, IMPI, JMX
6) System musi zapewniać możliwość ostrzegania w przypadku braku odpowiedzi z monitorowanego urządzenia, maszyny wirtualnej, serwera fizycznego
7) W przypadku rozwiązań serwerowych system musi zapewniać możliwość odczytu danych o statusie temperatury procesora, płyty głównej dla wiodących vendorów takich jak Lenovo, HP, DELL
8) System powinien integrować się z rozwiązaniami do zdalnego zarządzania serwerami takimi jak: iDRAC, iLO, XClarity Controller
9) System powinien pozwalać. na uzyskiwanie informacji o utylizacji CPU, RAM, przestrzeni pamięci masowej, interfejsów sieciowych maszyn wirtualnych opartych o Linux, Windows
10) System powinien zapewniać możliwość odczytu stanu CPU, wentylatorów, temperatury, utylizacji interfejsów urządzeń sieciowych wiodących producentów jak Ubiquiti, DELL, Extreme, Fortinet, CISCO i innych zapewniających komunikację SNMP z urządzeniem
11) System powinien umożliwiać dla monitorowanych elementów natychmiastowe graficzne przedstawienie na wykresie za pomocą wbudowanej funkcjonalności
12) System graficznego przedstawienia (wykresy) powinien posiadać funkcje:
    a. możliwości tworzenia niestandardowych wykresów;
    b. łączenia wielu elementów w jeden widok
    c. tworzenia mapy sieci
    d. tworzenia raportów

13) System powinien mieć funkcjonalność pozwalającą na tworzenie szablonów konfiguracji serwerów
14) System powinien zapewniać możliwość wykonania automatycznego wyrywania urządzeń sieciowych w danym obszarze
15) System powinien zapewniać możliwość automatycznej rejestracji agenta
16) System powinien zapewniać programowalny interfejs API
17) System musi zapewniać możliwość definiowania czasu retencji przechowywania danych oraz progów ostrzeżeń:
    a. Warning – rozumianych jako ostrzeżenie
    b. Critical – rozumianych jako rzutujących na całą infrastrukturę Zamawiającego i uniemożliwiające wykonywanie czynność)
18) System powinien zapewniać możliwość wysyłki monitów w postaci e-mail oraz opcjonalnie powinien zapewniać możliwość integracji z rozwiązaniami typu bramka sms
19) System powinien zapewniać możliwość bezpiecznego uwierzytelniania oraz nadawania wielopoziomowych uprawnień
20) System powinien zapewniać możliwość monitorowania minimum 100.000 obiektów w ramach jednej instancji

4.3 Wymagane prace wdrożeniowe

1) instalacja przez oferenta rozwiązania na dedykowanym zasobie wirtualnym Zamawiającego;
2) konfiguracja wstępna i nadanie dostępów do logowania dla Zamawiającego;
3) przygotowanie po konsultacji z Zamawiającym monitoringu dla 10 urządzeń wytypowanych przez Zamawiającego (serwery, przełączniki, urządzenie brzegowe klasy UTM);
4) konfiguracja progów alarmów zgodnie z wymogami Zamawiającego oraz po konsultacji z Wykonawcą i wdrożeniem w oparciu o najlepsze praktyki;
5) konfiguracja powiadomień na wskazaną przez Zmawiającego skrzynkę pocztową za pośrednictwem dedykowanej skrzynce technicznej dostarczonej przez Zamawiającego.

V
Szkolenia z zakresu rozwiązań technicznych

5.1 Przedmiot zamówienia

Przedmiotem zamówienia jest:
1) Przeprowadzenie szkolenia z zakresu rozwiązań technicznych takich jak: Microsoft Active Directory, rozwiązania Fortinet Fortigate, rozwiązań kopii zapasowych dedykowanych środowiskom zwirtualizowanym, bezpieczeństwa sieci

5.2 Szczegółowe wymagania odnośnie usługi

1) Szkolenie - minimalne wymagania:
   a) szkolenia będą zrealizowane jako szkolenia zamknięte;

b) szkolenia będą przeprowadzone w języku polskim;
c) szkolenia muszą odbyć się w formie zdalnej poprzez udostępniony przez Wykonawcę kanał elektroniczny lub dedykowaną aplikację, z możliwością późniejszego odtworzenia spotkania (nagranie szkolenia), z zastrzeżeniem nierozpowszechniania nagrania poza obszar organizacji Zamawiającego;
d) Musi tworzyć cykl 5 (słownie pięciu) szkoleń, trwających minimum 1 godzinę każde, gdzie łączna liczba godzin poświęcona na szkolenia nie może być mniejsza niż 25 godzin
e) Zamawiający dopuszcza udział uczestników szkolenia w ramach większej grupy szkoleniowej
f) agenda szkoleń musi dotykać tematyki technologicznej, w tym przynajmniej: Microsoft Active Directory, rozwiązania Fortinet Fortigate, Rozwiązań kopii zapasowych dedykowanych środowiskom zwirtualizowanym, bezpieczeństwa sieci
g) obowiązek sprawdzania obecności w trakcie każdego ze szkoleń np. w postaci zrzutów ekranowych listy zalogowanych uczestników szkolenia pozwalającej potwierdzić obecność uczestników. Oryginalne wersje list obecności zostaną przekazane Zamawiającemu po zakończeniu każdej edycji szkolenia;
h) wykonawca gwarantuje, że osoba prowadząca szkolenia posiada odpowiednie predyspozycje do prowadzenia szkoleń oraz wyczerpującą wiedzę, co najmniej na poziomie wymaganym do realizacji szkoleń;
i) wykonawca jest zobowiązany przeprowadzić szkolenie w oparciu o zaakceptowane przez Zamawiającego materiały dydaktyczne;
j) wykonawca zobowiązany jest w porozumieniu z Zamawiającym ustalić dokładną datę przeprowadzenia szkoleń. Zamawiający ustali na zasadzie negocjacji z Wykonawcą, w terminie maksymalnie 15 dni roboczych od daty podpisania umowy ramowy harmonogram szkoleń;
k) po ukończeniu szkolenia uczestnicy otrzymają zaświadczenie lub certyfikat ukończenia szkolenia w formie papierowej bądź elektronicznej. Zaświadczenia zostaną przesłane na wskazany przez Zamawiającego adres fizyczny lub adres skrzynki poczty elektronicznej.

VI

Modernizacja infrastruktury sieciowej

6.1 Przedmiot zamówienia

Przedmiotem zamówienia jest:
1) dostawa fabrycznie nowego Sprzętu, nie używanego w innych środowiskach ani projektach, w ilościach:
    a. Punkt dostępowy wifi – 2 sztuki
2) konfiguracja urządzeń oraz fizyczna instalacja w infrastrukturze IT Zamawiającego;
3) udzielenie przez Wykonawcę gwarancji i zapewnienie w jej ramach serwisu gwarancyjnego oraz wsparcia technicznego na dostarczony Sprzęt;
4) dostarczenie przez Wykonawcę dokumentacji dostarczonego Sprzętu;

6.2 Termin realizacji zamówienia oraz liczba dostarczanego sprzętu

Zamawiający wymaga, aby dostawa sprzętu, o którym mowa w pkt 6.1 do Zamawiającego nastąpiła w terminie 6 tygodni od dnia podpisania Umowy

6.3 Wymagania wobec Wykonawcy

O udzielenie zamówienia mogą ubiegać się Wykonawcy, który posiadają niezbędną wiedzę i kwalifikacje do realizacji zamówienia.

6.4 Wymagania szczegółowe Zamawiającego

Zestawienie wymaganych parametrów technicznych dla punktu dostępowego wifi (2 sztuki)

Obsługiwane standardy IEEE	802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.1Q, 802.1X, 802.3af, 802.3az
Interfejsy	1x 10/100/1000 Base-T RJ45,
Liczba Anten	4 wewnętrzne WIFI + 1 wewnętrzna BLE
Obsługiwane rodzaje autentykacji użytkownika/urządzenia	WPA, WPA2, and WPA3 with 802.1x or preshared key, WEP, Web Captive Portal, MAC lista zezwolonych i zablokowanych urządzeń
Liczba maksymalna rozgłaszanych SSID	Do 16 lub 14 przy włączonym skanowaniu w tle
Parametry dla 1 zakresu radiowego	2,4 GHz b/g/n (2x2:2 stream) 20/40 MHz (256 QAM)
Parametry dla 2 zakresu radiowego	5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz (256 QAM)
Maksymalna liczba użytkowników podłączona do kanału radiowego	Do 512
PoE – Pover over Ethernet	Zgodne ze standardem IEEE 802.3af
Maksymalna przepustowość danych	Dla zakresu 2,4 GHz – 400 Mbit/s, dla zakresu 5 GHz – 867 Mbit/s
Dodatkowe wymagania	- Obsługa 802.11ac Wave 2 MU-MIMO - Obsługa TxBF Transmit Beam Forming - Obsługa LDPC Low-Density Parity Check Encoding - Obsługa MLD Maximum Likelihood Demodulation MLD - Obsługa MRC Maximum Ratio Combining - Możliwość montażu na suficie, ścianie
Maksymalne wymiary	165x165x48 mm
Maksymalny waga	0,6 kg
Maksymalny pobór mocy	12,4 W

6.5 Wymagania ogólne dla punktów dostępowych oraz wykonywanych prac:

1) Dostarczone urządzenia muszą pochodzić z autoryzowanego kanały sprzedaży producentów na rynek polski – do oferty należy dołączyć odpowiednie oświadczenie producenta sprzętu
2) Dostarczone urządzenia muszą być objęte gwarancją opartą o świadczenia gwarancyjne producenta sprzętu, niezależnie od statusu partnerskiego Wykonawcy przez okres co najmniej 12 miesięcy
3) Zamawiający zobowiązuje Wykonawcę do dostarczenia sprzętu kompatybilnego z obecnie zainstalowanymi urządzeniami Fortinet FortiAP oraz Fortigate
4) Wykonawca w ramach działań wdrożeniowych zobowiązany jest do montażu urządzeń w wyznaczonych miejscach przez Zamawiającego
5) W wyznaczonych miejscach Zamawiający deklaruje doprowadzenie okablowania celem zasilenia i podłączenia punktów dostępowych do sieci
6) Na zainstalowanych 2 urządzeniach Wykonawca zobligowany jest do odtworzenia konfiguracji, odwzorowując aktualną konfigurację urządzeń FortiAp 321C
7) Zamawiający akceptuje możliwość zasugerowania przez Wykonawcę zmian konfiguracyjnych w oparciu o dobre praktyki i aktualne trendy w dziedzinie bezpieczeństwa sieci
8) Wykonawca zobowiązuje się do przekazania zamawiającemu dokumentacji opisującej wykonane prace

VII

Szkolenia z zakresu cyberbezpieczeństwa

7.1 Przedmiot zamówienia

Przedmiotem zamówienia jest:

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

7.2 Wymagania wobec Wykonawcy

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

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

7.3 Szczegółowe wymagania odnośnie usługi

1) Szkolenie - minimalne wymagania:
    a) szkolenia będą zrealizowane jako szkolenia zamknięte;
    b) szkolenia będą przeprowadzone w języku polskim;

c) szkolenia muszą odbyć się w formie zdalnej poprzez udostępniony przez Wykonawcę kanał elektroniczny lub dedykowaną aplikację, z możliwością późniejszego odtworzenia spotkania (nagranie szkolenia), z zastrzeżeniem nierozpowszechniania nagrania poza obszar organizacji Zamawiającego;
d) Musi tworzyć cykl 5 (słownie pięciu) szkoleń, trwających minimum 1 godzinę każde
e) Zamawiający dopuszcza udział uczestników szkolenia w ramach większej grupy szkoleniowej
f) agenda szkoleń musi dotykać tematyki cyberbezpieczeństwa, w tym przynajmniej: socjotechniki, phishingu, ransomware, bezpieczeństwa poczty elektronicznej oraz korzystania z urządzeń mobilnych, sieci Wi-Fi, bezpieczeństwa nośników danych;
g) obowiązek sprawdzania obecności w trakcie każdego ze szkoleń np. w postaci zrzutów ekranowych listy zalogowanych uczestników szkolenia pozwalającej potwierdzić obecność uczestników. Oryginalne wersje list obecności zostaną przekazane Zamawiającemu po zakończeniu każdej edycji szkolenia;
h) wykonawca gwarantuje, że osoba prowadząca szkolenia posiada odpowiednie predyspozycje do prowadzenia szkoleń oraz wyczerpującą wiedzę, co najmniej na poziomie wymaganym do realizacji szkoleń;
i) wykonawca jest zobowiązany przeprowadzić szkolenie w oparciu o zaakceptowane przez Zamawiającego materiały dydaktyczne;
j) wykonawca zobowiązany jest w porozumieniu z Zamawiającym ustalić dokładną datę przeprowadzenia szkoleń. Zamawiający ustali na zasadzie negocjacji z Wykonawcą, w terminie maksymalnie 15 dni roboczych od daty podpisania umowy ramowy harmonogram szkoleń;
k) po ukończeniu szkolenia uczestnicy otrzymają zaświadczenie lub certyfikat ukończenia szkolenia w formie papierowej bądź elektronicznej. Zaświadczenia zostaną przesłane na wskazany przez Zamawiającego adres fizyczny lub adres skrzynki poczty elektronicznej.

2) Etap II (testy socjotechniczne) - minimalne wymagania:
a) wykonanie testu weryfikacyjnego poziomu świadomości cyberzagrożeń Pracowników Zamawiającego poprzez nakłanianie ich do niestosowania się do obowiązujących zasad i procedur bezpieczeństwa obowiązujących u Zamawiającego;
b) przygotowanie i wdrożenie indywidualnych scenariuszy kontrolowanego ataku hakerskiego, na wybraną grupę Pracowników Zamawiającego;
c) opracowanie raportu po realizacyjnego zawierającego:
i) wyniki przeprowadzonych testów oraz stan poziomu zabezpieczenia zasobów systemu informatycznego Zamawiającego;
ii) rekomendacje oraz zalecenia dla posiadanego środowiska;
iii) propozycje modernizacji środowiska lub jego zabezpieczeń;
d) spotkanie organizacyjne pomiędzy Zleceniodawcą a Wykonawcą, mające na celu omówienie wyników testów socjotechnicznych oraz zaleceń i rekomendacji zawartych w raporcie po realizacyjnym.

VIII

Dostarczenie stacji roboczych

8.1 Przedmiot zamówienia

Przedmiotem zamówienia jest:

1) dostawa fabrycznie nowego Sprzętu, nie używanego w innych środowiskach ani projektach:
    a. Komputer typu Notebook – 7 sztuk

8.2 Wymagania szczegółowe Zamawiającego

Zestawienie wymaganych parametrów technicznych komputera typu Notebook

Typ	Notebook
Taktowanie procesora	2.4 GHz
Taktowanie procesora (Boost)	4.2 GHz
Pozostałe informacje o procesorze	Minimalna wartość testu PassMark CPU Mark dla wielu wątków - 10060 punktów, dla pojedynczego wątku - 2720
Przekątna ekranu	15,6''
Rozdzielczość (minimum)	1920 x 1080 (FHD 1080)
Powierzchnia matrycy	Matowa
Technologia podświetlania	Diody LED
Rodzaj karty graficznej	Zintegrowana
Zainstalowana pamięć RAM (minimum)	8 GB
Maks. wielkość pamięci	32 GB
Liczba obsadzonych gniazd pamięci	1
Liczba wolnych gniazd pamięci	1
Rodzaj pamięci	SODIMM DDR4
Częstotliwość szyny pamięci (minimum)	2666 MHz
Typ dysku	SSD
Pojemność SSD (minimum)	512 GB
Format szerokości SSD	M.2
Interfejs dysku SSD	PCI-Express
Komunikacja	• LAN 10/100/1000 • Minimum w standardzie WiFi 802.11 ac • Bluetooth
Porty USB (wartości minimalne)	• 1 x USB 2.0 Type-A • 2 x USB 3.1 Type-A
Porty wideo	1 x HDMI

Czytnik kart pamięci	Tak
Pozostałe porty we/wy (wartości minimalne)	• 1 x Audio (Combo) • 1 x RJ-45
Kamera internetowa	Tak
Podświetlana klawiatura	Tak
Czytnik linii papilarnych	Tak
Pojemność baterii	41 Wh
Liczba komór	3-komorowa
System operacyjny	Microsoft Windows 10 Pro 64-bit lub nowszy z uwagi na wykorzystywane aktualnie w infrastrukturze środowisko pracy oparte o rozwiązania systemowe firmy Microsoft lub równoważne. Opis równoważności został umieszczony pod tabelą.
Wysokość	18.9 mm
Szerokość	358.5 mm
Głębokość	235.56 mm
Waga maksymalna	1.75 kg
Akcesoria w zestawie	• Zasilacz 65W • Europejski przewód zasilający • Dokumentacja
Informacje o gwarancji	Minimum 3-letnia
Pozostałe informacje	Preinstalowany system Microsoft Windows 10 Pro (obejmuje licencję na system Microsoft Windows 11 Pro)

Oprogramowanie typu MS Windows 10 Professional 64bit PL lub równoważne, spełniające poniższe warunki:

1. System operacyjny dla komputerów przenośnych, z graficznym interfejsem użytkownika.
2. System operacyjny ma pozwalać na uruchomienie i pracę z aplikacjami użytkowanymi przez Zamawiającego, w szczególności: MS Office 2010, 2013, 2016; MS Visio 2007, 2010, 2016; MS Project 2007, 2010, 2016; EMID, AutoCAD.
3. System ma udostępniać dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
4. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim.
5. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe.
6. Wbudowany system pomocy w języku polskim.
7. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.
8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z

możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne.
9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).
14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.
15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.
16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.
17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe.
18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
19. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.
20. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
21. Obsługa standardu NFC (near field communication).
22. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
23. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
24. Mechanizmy logowania do domeny w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
25. Mechanizmy wieloelementowego uwierzytelniania.
26. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu.
27. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.
28. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.
29. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
30. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
31. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.

32. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.
33. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.
34. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
35. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
36. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
37. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
38. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
39. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
40. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
41. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.
42. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
43. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.
44. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
45. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

IX

Dostawa licencji Microsoft 365 Business Basic (lub rozwiązania równoważnego)

9.1 Przedmiot zamówienia

Przedmiotem zamówienia jest:

1) Dostawa 4 licencji rocznych pakietu biurowego Microsoft 365 Business Basic (lub rozwiązania równoważnego).

9.2 Wymagania wobec Wykonawcy

O udzielenie zamówienia mogą ubiegać się Wykonawcy, który posiadają niezbędną wiedzę i kwalifikacje do realizacji zamówienia.

9.3 Szczegółowe wymagania odnośnie dostawy licencji

1) Ilekroć jest mowa o modelu licencyjnym należy przez to rozumieć pakiet biurowy Microsoft 365 Business Basic (lub rozwiązanie równoważne).
2) Ilekroć jest mowa o oprogramowaniu należy przez to rozumieć usługi pakietu biurowego Microsoft 365 Business Basic (lub rozwiązania równoważnego).
3) Wymagane składowe pakietu biurowego Microsoft 365 Business Basic zwane przez Producenta usługami (zgodnie ze specyfikacją producenta):
    a) Poczta e-mail i kalendarze - pojemność skrzynki 50GB, maksymalny rozmiar wiadomości 150MB,
    b) Przechowywanie i udostępnianie plików - każda licencja posiada przestrzeń w rozmiarze 1TB, dostępnej w postaci rozwiązania chmurowego w infrastrukturze Producenta
    c) Konferencje Online (Teams) – do 300 osób,
    d) Wiadomości błyskawiczne i komunikator (Teams),
    e) Firmowa sieć społecznościowa (Yammer),
    f) Witryny zespołów (SharePoint),
    g) Subskrypcja umożliwia dostęp do internetowych wersji aplikacji pakietu Office: Outlook, Word, Excel, PowerPoint, OneNote
    h) Usługa pocztowa (Exchange),
    i) Zarządzanie pracą (Planner),
    j) Tworzenie biuletynów i prezentacji multimedialnych (Sway, PowerPoint)
    k) Interfejs API dla usług wchodzących w skład oferowanego pakietu (Microsoft Graph).
4) Równoważność:
    a) Wykonawca powołujący się na rozwiązania równoważne musi wykazać, że spełniają one warunki określone w pkt. 3) niniejszego dokumentu.
    b) W celu wykazania równoważności Wykonawca jest zobligowany podać nazwę pakietu równoważnego, a także przeprowadzić dowód równoważności poprzez opis porównawczy. Wykonawca ma obowiązek wykazać w jaki sposób oferowany model licencyjny jest równoważny z modelem licencyjnym wyspecyfikowanym przez Zamawiającego w pkt. 3). Produkt równoważny powinien umożliwiać zarządzanie dostępem użytkowników do aplikacji, który umożliwia synchronizację poświadczeń z usługą katalogową Active Directory.
    c) Zamawiający zastrzega sobie w przypadku jakichkolwiek wątpliwości, prawo sprawdzenia pełnej zgodności warunków i zakresu równoważności oferowanego rozwiązania. W takim przypadku, Zamawiający wezwie Wykonawców do przedstawienia dodatkowych dokumentów dotyczących oferowanego rozwiązania.
    d) Negatywny wynik sprawdzenia oferty w zakresie równoważności oferowanych Produktów skutkować będzie odrzuceniem tej oferty.

1) Zamawiający wymaga dostępu do najnowszych wersji modelu licencyjnego przez cały okres jej ważności, tj. przez 12 miesięcy od dnia ich dostarczenia.
2) Dostarczone licencje muszą być aktywne przez okres 12 miesięcy od daty przekazania ich Zamawiającemu, określonej umową (nie później niż 14 dni od jej podpisania).
3) Wymagana jest możliwość korzystania z pomocy w dowolnym momencie, dzięki całodobowej telefonicznej i internetowej pomocy technicznej od firmy Producenta.
4) Wykonawca musi zapewnić, że dostarczone licencje są wolne od wad, dobrej jakości oraz ich parametry i cechy są zgodne z założeniami niniejszego dokumentu