

*Załącznik nr 2  
do Zapytania Ofertowego*

## Szczegółowy opis zamówienia

Zamówienie podzielone jest na części:

- Część I – dostawa, wstępna konfiguracja oraz uruchomienie serwera wraz z wymaganymi licencjami oraz wirtualizacja posiadanej infrastruktury serwerowej
- Część II – Modernizacja infrastruktury sieciowej
- Część III - Usługa wsparcia środowiska IT Zamawiającego
- Część IV – Szkolenia z zakresu cyberbezpieczeństwa
- Część V - Zapewnienie systemu monitoringu stanu infrastruktury IT Zamawiającego

### Część I

**Dostawa, wstępna konfiguracja oraz uruchomienie serwera wraz z wymaganymi licencjami oraz wirtualizacja posiadanej infrastruktury serwerowej**

#### 1.1 Przedmiot zamówienia

Przedmiotem zamówienia jest:

- 1) dostawa Sprzętu fabrycznie nowego lub używanego, nie finansowanego wcześniej z krajowych lub unijnych funduszy projektowych;
- 2) konfiguracja, instalacja serwera oraz wirtualizacja wskazanych zasobów Zamawiającego wraz z uruchomieniem środowiska;
- 3) dostarczenie przez Wykonawcę dokumentacji dostarczonego Sprzętu;
- 4) 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 szczegółowe Zamawiającego

**Zestawienie wymaganych parametrów technicznych (1 sztuka)**

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 1U RACK 19 cali wraz z szynami montażowymi
Procesor	Procesor ośmiordzeniowy, szesnastowątkowy, x86 - 64 bity, o bazowym taktowaniu 2.10GHz i taktowaniu w trybie turbo 3.20GHz, cache 11MB, osiągający wynik co najmniej 11,137 w teście Passmark CPU Benchmarks, dla konfiguracji jednoprosesorowej <a href="https://www.cpubenchmark.net/cpu_list.php#single-cpu">https://www.cpubenchmark.net/cpu_list.php#single-cpu</a> Płyta główna wspierająca zastosowanie procesorów posiadających do 24 rdzeni
Liczba procesorów	1 procesor – 8 rdzeniowy (wymóg konieczny)

Pamięć operacyjna	64GB RDIMM DDR4 2400MT/s w modułach o pojemności przynajmniej 16GB każdy.  Płyta główna z minimum 16 slotami na pamięć i umożliwiającą instalację do minimum 1TB.
Sloty rozszerzeń	3 aktywne gniazda PCI-Express generacji 3
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5  Zamontowane dyski:  - 4x 960GB SAS SSD 2.5"
Kontroler	Serwer wyposażony w kontroler dyskowy, zapewniający obsługę 8 napędów dyskowych oraz obsługujący poziomy: RAID 0,1,5,6,10,50,60, z dwurdzeniowym procesorem, 12GB/s, 2GB cache.
Interfejsy sieciowe	Minimum 2 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.  Minimum 2 porty 10Gb Base-T
Karta graficzna	Zintegrowana karta graficzna
Porty	Porty od frontu:  1 x dedykowany port iDRAC Direct USB  1 x USB 2.0  1 x VGA  Porty od tyłu:  1 x dedykowany port sieciowy iDRAC  1 x Serial  2 x USB 3.0  1 x VGA
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 550W
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slotcie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: <ul style="list-style-type: none"> <li>• monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i</li> </ul>

	<p>dyski (fizyczne i logiczne), karty sieciowe</p> <ul style="list-style-type: none"> <li>wparcie dla agentów zarządzających oraz możliwość pracy w trybie bez agentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP</li> <li>dostęp do karty zarządzającej poprzez <ul style="list-style-type: none"> <li>dedykowany port RJ45 z tyłu serwera lub</li> <li>przez współdzielony port zintegrowanej karty sieciowej serwera</li> </ul> </li> </ul> <p>dostęp do karty możliwy</p> <ul style="list-style-type: none"> <li>z poziomu przeglądarki webowej (GUI)</li> <li>z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)</li> <li>z poziomu skryptu (XML/Perl)</li> <li>poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)</li> </ul> <ul style="list-style-type: none"> <li>wbudowane narzędzia diagnostyczne</li> <li>zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego</li> <li>obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przysyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie</li> <li>wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników</li> <li>przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)</li> <li>obsługa zdalnego serwera logowania (remote syslog)</li> <li>wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów</li> <li>mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie</li> <li>funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności</li> <li>monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji</li> <li>konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)</li> <li>zdalna aktualizacja oprogramowania (firmware)</li> <li>możliwość równoczesnej obsługi przez 6 administratorów</li> </ul>
--	--

	<ul style="list-style-type: none"> <li>• autentykacja dwuskładnikowa (Kerberos)</li> <li>• wsparcie dla Microsoft Active Directory</li> <li>• obsługa SSL i SSH</li> <li>• enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli</li> <li>• wsparcie dla IPv4 oraz IPv6, obsługa SNMP v3 oraz RESTful API</li> <li>• wsparcie dla Integrated Remote Console for Windows clients</li> </ul> <p>możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)</p>
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	<p>Microsoft Windows Server 2016, 2019, 2022</p> <p>Red Hat Enterprise Linux (RHEL) 7.6, 8.0</p> <p>SUSE Linux Enterprise Server (SLES) 12 SP3, 15</p> <p>ClearOS</p> <p>VMware ESXi 6.0 U3, 6.5 U2 through U.3 &amp; 6.7 U1 through U3, 7.0</p> <p>Ubuntu Server 16.04, LTS, 18.04 LTS, 20.04 LTS</p> <p>Citrix XenServer 7.1</p>
Wsparcie techniczne	Gwarancja świadczona na okres 36 miesięcy od dnia podpisania umowy, z usługą zachowania dysku twardego w razie awarii
Inne	W przypadku sprzętu używanego wymagane jest zaświadczenie, potwierdzające, że serwer nie został zakupiony wcześniej za pomocą środków pochodzących z grantów lub funduszy europejskich lub krajowych
Licencje	Dostarczenie 32 licencji 2 core pack Windows Server Standard 2022 lub równoważnych. Licencje nie mogą być przypisane do sprzętu.

#### **1.4 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 zaporę internetową (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 zarządzanie 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 certyfikatów 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.

### **1.5 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 serwera do infrastruktury elektrycznej i sieciowej Zamawiającego



- e) Wstępna konfiguracja serwera polegająca na nadaniu dostępów, adresacji oraz aktualizacji oprogramowaniu sprzętowego do najnowszej zalecanej przez producenta wersji
- f) Przygotowanie środowiska wirtualizacji na nowo dostarczonym serwerze
- 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) Po procesie migracji, przywrócenie do stanu fabrycznego dotychczasowego serwera produkcyjnego i uruchomienie wirtualizacji w ramach licencjonowania Windows (licencje w tym punkcie zapewnia Zamawiający)
- k) Uruchomienie replikacji dla wskazanych 2 maszyn wirtualnych
- 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

## **Część II**

### **Modernizacja infrastruktury sieciowej**

#### **2.1 Przedmiot zamówienia**

Przedmiotem zamówienia jest:

- 1) dostawa fabrycznie nowego Sprzętu, nie używanego w innych środowiskach ani projektach, w ilościach:
  - a. Przełącznik sieciowy Typ 1 - 1 sztuka
  - b. Przełącznik sieciowy Typ 2 - 1 sztuka
- 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;

### **2.2 Termin realizacji zamówienia oraz liczba dostarczanego sprzętu**

Zamawiający wymaga, aby dostawa sprzętu, o którym mowa w pkt 2.1 do Zamawiającego nastąpiła w terminie 6 tygodni od dnia podpisania Umowy.

### **2.3 Wymagania szczegółowe Zamawiającego**

#### **Zestawienie wymaganych parametrów technicznych dla przełącznika sieciowego Typ 1 (1 sztuka)**

Interfejs sieciowy	48x 1Gb Ethernet (10/100/1000 Mbps) 4x SFP+ (1/10 Gbps)
Interfejs zarządzania	Ethernet, In-Band
łączna przepustowość (non-blocking)	Minimum 88 Gbps
Przepustowość przełączania	Minimum 176 Gbps
Prędkość przekazywania	Minimum 130 Mpps
Sposób zasilania	Uniwersalny: 100 - 240 V AC / 50 - 60 Hz USP RPS DC: 11.5 VDC, 5.22A
Zasilacz	Wbudowany, AC/DC Moc minimum 60 W
Maksymalny pobór mocy	60 W
Diody LED	System: Status RJ45: Speed / Link / Activity SFP+: Link / Activity
Waga	Z uchwytami montażowymi: maksymalnie 4,15 kg Bez uchwytów montażowych: maksymalnie 4,10kg
Dopuszczalna temperatura pracy	Od -5 do 45 st. C
Certyfikaty	IC, FCC, CE
Możliwość montażu w szafie RACK	Tak, maksymalnie 1U

#### **Zestawienie wymaganych parametrów technicznych dla przełącznika sieciowego Typ 2 (1 sztuka)**

Interfejs sieciowy	24x 1Gb Ethernet (10/100/1000 Mbps) 2x SFP (1 Gbps)
Interfejs zarządzania	Ethernet, In-Band
łączna przepustowość (non-blocking)	Minimum 26 Gbps



Przepustowość przełączania	Minimum 52 Gbps
Prędkość przekazywania	Minimum 38 Mpps
Sposób zasilania	Uniwersalny: 100 - 240 V AC / 50 - 60 Hz
Zasilacz	Wbudowany, AC/DC Moc minimum 36 W
Maksymalny pobór mocy	25 W
Diody LED	System: Status RJ45: Speed / Link SFP: Speed / Link
Waga	Z uchwytami montażowymi: maksymalnie 2,75 kg Bez uchwytów montażowych: maksymalnie 2,70kg
Dopuszczalna temperatura pracy	Od -5 do 40 st. C
Certyfikaty	IC, FCC, CE
Możliwość montażu w szafie RACK	Tak, maksymalnie 1U

#### **2.4 Wymagania ogólne dla wszystkich typów przełączników sieciowych oraz wykonywanych prac:**

- 1) Dostarczone urządzenia muszą pochodzić z autoryzowanego kanału 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) Urządzenie musi mieć możliwość zarządzania i konfigurowania poprzez dedykowane rozwiązanie zarządzające, posiadające funkcje takie jak:
  - a. podgląd statusu urządzeń w czasie rzeczywistym
  - b. centralne zarządzanie wieloma sieciami z poziomu interfejsu graficznego
  - c. możliwość zdalnej aktualizacji oprogramowania urządzeń
  - d. wersję mobilną aplikacji
- 4) Urządzenie Typ 1 musi być zarządzalne w warstwie 2 i 3, urządzenie Typ 2 wyłącznie w warstwie 2
- 5) Dostarczający jest zobowiązany do podłączenia urządzeń sieciowych w infrastrukturze Zamawiającego do wskazanych miejsc połączeń sieciowych i elektrycznych
- 6) Dostarczający jest zobowiązany do aktualizacji oprogramowania sprzętowego dostarczonych urządzeń do najnowsze dostępnej i zalecanej przez producenta wersji
- 7) Dostarczający musi utworzyć dostępy administracyjne do urządzeń oraz przekazać je Zamawiającemu
- 8) W ramach przekazanych urządzeń, Wykonawca zobowiązuje się - na wskazanych przez Zamawiającego interfejsach - zdefiniować do 4 VLAN-ów





- 9) Na wskazanym przez Zamawiającego zasobie wirtualnym serwera, Wykonawca zobowiązany jest do instalacji, konfiguracji i dodania urządzeń sieciowych do dedykowanego centralnego rozwiązania zarządzającego

### Część 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 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 webinarów 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 54 godzin przypadających na okres 18 miesięcy trwania umowy, to jest w pakiecie 3 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



<b>Niski</b>	24	1
<b>Wniosek</b>	40	1
<b>Zdarzenie</b>	--	1

\* rh – roboczogodzina

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

WPŁYW	Pilność				
	Praca uniemożliwiona	Utrudnienie pracy (istnieje alternatywa)	Prace Planowe	Wniosek o usługę	Zdarzenie
<b>Cała organizacja</b>	Krytyczny	Krytyczny	Średni	Wniosek	Zdarzenie
<b>Kilka Lokacji</b>	Krytyczny	Wysoki	Średni	Wniosek	Zdarzenie
<b>Grupa użytkowników</b>	Wysoki	Wysoki	Niski	Wniosek	Zdarzenie
<b>Pojedynczy użytkownik</b>	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
<b>1. Cała organizacja</b>	Wszyscy autoryzowani użytkownicy.
<b>2. Kilka lokacji</b>	Wszyscy autoryzowani użytkownicy z kilku lokacji.
<b>3. Niewielka grupa użytkowników</b>	Wszyscy autoryzowani użytkownicy z jednej lokacji / zespołu.
<b>4. Pojedynczy użytkownik</b>	Indywidualne zgłoszenie.

Pilność – jest określeniem szybkości rozwiązywania incydentów posiadających konkretny wpływ.

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

## **Część IV**

### **Szkolenia z zakresu cyberbezpieczeństwa**

#### **4.1 Przedmiot zamówienia**

Przedmiotem zamówienia jest:

- 1) przeprowadzenie szkolenia zwiększającego świadomość pracowników Zamawiającego w dziedzinie cyberbezpieczeństwa;

#### **4.2 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
  - e) Zamawiający dopuszcza udział uczestników szkolenia w ramach większej grupy szkoleniowej
  - f) agenda szkoleń musi dotyczyć 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.

## **Część V**

### **Zapewnienie systemu monitoringu stanu infrastruktury IT Zamawiającego**

#### **5.1 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.

#### **5.2 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 monitorowana - serwisów uruchomionych na powłoce Windows/Linux, statusu baz danych MSSQL Express i Standard, PostgreSQL, 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 użyciu CPU, RAM, przestrzeni pamięci masowej, interfejsów sieciowych maszyn wirtualnych opartych o Linux, Windows
- 10) System powinien zapewniać możliwość odczytu stanu CPU, wentylatorów, temperatury, użycia 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 wrywania 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 czynności
- 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

### **5.3 Wymagane prace wdrożeniowe**

- 1) instalacja przez oferenta rozwiązania na dedykowanym zasobie wirtualnym Zamawiającego;
- 2) konfiguracja wstępna i nadanie dostępu 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 Zamawiającego skrzynkę pocztową za pośrednictwem dedykowanej skrzynki technicznej dostarczonej przez Zamawiającego.