Załącznik nr 4 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Zadanie 1 - Szkolenie pracowników - socjotechniki - 20 osób

Szkolenia z zakresu cyberbezpieczeństwa

Przedmiot zamówienia

Przedmiotem zamówienia jest:

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

Szczegółowe wymagania

1. Szkolenie - minimalne wymagania:
   a. Szkolenie zamknięte
   b. Szkolenie musi być przeprowadzone w języku polskim;
   c. szkolenie musi 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. Czas trwania szkolenia minimum 2 godziny
   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. wykonawca gwarantuje, że osoba prowadząca szkolenia posiada odpowiednie predyspozycje do prowadzenia szkoleń oraz wyczerpującą wiedzę, popartą 2-letnim doświadczeniem
   h. wykonawca zobowiązany jest w porozumieniu z Zamawiającym ustalić dokładną datę przeprowadzenia szkoleń.
   i. 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:
d. wyniki przeprowadzonych testów oraz stan poziomu zabezpieczenia zasobów systemu informatycznego Zamawiającego;
e. rekomendacje oraz zalecenia dla posiadanego środowiska;
f. propozycje modernizacji środowiska lub jego zabezpieczeń;
g. spotkanie organizacyjne pomiędzy Zleceniodawcą a Wykonawcą, mające na celu omówienie wyników testów socjotechnicznych oraz zaleceń i rekomendacji zawartych w raporcie po realizacyjnym.

Zadanie 2 - Szkolenia dla Administratorów

Przedmiot zamówienia

Przedmiotem zamówienia jest:

- Przeprowadzenie szkolenia z zakresu rozwiązań technicznych takich jak: Microsoft Active Directory, rozwiązania Fortinet Fortigate, rozwiązań kopii zapasowych dedykowanych środowiskom zwirtualizowanym, bezpieczeństwa sieci.

Szczegółowe wymagania

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 3 (słownie trzech) szkoleń, trwających minimum 1 godzinę każde, gdzie łączna liczba godzin poświęcona na szkolenia nie może być mniejsza niż 10 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, rozwiązań klasy xDR/EDR.
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, popartą 2-letnim doświadczeniem w obszarze technologicznym
i. wykonawca zobowiązany jest w porozumieniu z Zamawiającym ustalić dokładną datę przeprowadzenia szkoleń
j. 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.

Zadanie 3 - Backup

Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. dostawa serwera fabrycznie nowego, nie finansowanego wcześniej z krajowych lub unijnych funduszy projektowych,
2. dostawa macierzy NAS fabrycznie nowej, nie finansowanej wcześniej z krajowych lub unijnych funduszy projektowych,
3. konfiguracja, instalacja serwera,
4. konfiguracja, instalacja macierzy NAS,
5. dostawa sytemu kopii zapasowych – licencja wieczysta z dwuletnim wsparciem umożliwiający kopie minimum 10 VM,
6. wdrożenie oraz konfiguracja systemu kopii zapasowych w środowisku IT Zamawiającego,
7. dostarczenie przez Wykonawcę dokumentacji konfiguracji wdrożonego rozwiązania.

Zestawienie wymaganych parametrów technicznych – serwer (1 sztuka)

Parametr	**wymagania minimalne**
Typ urządzenia	Serwer kopii zapasowych umożliwiający jednoczesne uruchomienie oprogramowania do wykonywania kopii zapasowych oraz przechowywanie repozytorium kopii zapasowych na wewnętrznych zasobach dyskowych urządzenia.
Obudowa	Obudowa Rack o wysokości maksymalnie 2U, wyposażona w minimum 12 zatok dyskowych. Urządzenie należy dostarczyć z dedykowanymi, przesuwnymi szynami montażowymi do szafy Rack.
Procesor	Procesor klasy x86, o architekturze 64-bitowej, posiadający co najmniej 6 rdzeni fizycznych i taktowanie bazowe nie niższe niż 3,8 GHz.
Pamięć RAM	Minimum 32 GB pamięci DDR5 UDIMM.
Rozbudowa pamięci RAM	Minimum 4 gniazda pamięci RAM. Możliwość rozbudowy pamięci do co najmniej 192 GB.

Pamięć Flash	Minimum 5 GB pamięci Flash przeznaczonej na potrzeby systemu urządzenia.
Zatoki dyskowe	Minimum 12 zatok umożliwiających instalację dysków 3,5-calowych SATA oraz dysków 2,5-calowych SATA HDD lub SSD.
Gniazda M.2	Minimum 2 gniazda M.2 2280 PCIe Gen 5 x2, przeznaczone do instalacji dysków NVMe SSD.
Zainstalowane dyski	Minimum 4 dyski HDD SATA o pojemności co najmniej 8 TB każdy oraz minimum 2 dyski SSD o pojemności co najmniej 512GB każdy. Wszystkie zainstalowane dyski muszą znajdować się na oficjalnej liście kompatybilności oferowanego modelu urządzenia.
Maksymalna obsługiwana pojemność dysków	Obsługa dysków twardych o pojemności co najmniej 32 TB na pojedynczy dysk.
Rozbudowa pojemności	Możliwość podłączenia zewnętrznego modułu rozszerzającego pojemność pamięci masowej.
Interfejsy sieciowe	Minimum 2 porty Ethernet 2,5 Gb/s w standardzie RJ45 oraz minimum 2 porty 10GBASE-T w standardzie RJ45. Porty muszą obsługiwać agregację połączeń sieciowych oraz mechanizmy przełączania awaryjnego.
Porty USB	Minimum 2 porty USB 3.2 Gen 2 typu A.
Złącza PCIe	Minimum 3 gniazda rozszerzeń PCIe, umożliwiające instalację dodatkowych kart sieciowych, kart Fibre Channel lub innych kart rozszerzeń.
System plików	Obsługa systemu plików ZFS dla dysków wewnętrznych. Dla dysków zewnętrznych wymagana jest obsługa co najmniej EXT3, EXT4, NTFS, FAT32 i HFS+.
Zarządzanie macierzami RAID	Obsługa co najmniej RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50 i RAID 60, a także mechanizmów potrójnej parzystości i potrójnego lustra.
Ochrona i odbudowa RAID	Obsługa dysków Hot Spare i Global Hot Spare, konfiguracji priorytetu odbudowy macierzy, SSD TRIM, HDD S.M.A.R.T., skanowania uszkodzonych bloków oraz mechanizmów wykrywania i naprawy uszkodzeń danych.
Pamięć podręczna SSD	Możliwość wykorzystania dysków SSD jako pamięci podręcznej odczytu oraz jako pamięci podręcznej odczytu i dziennika zapisu.
Migawki	Obsługa migawek udziałów sieciowych oraz jednostek LUN, wraz z możliwością replikowania migawek na drugie urządzenie.
iSCSI	Wbudowana obsługa iSCSI, wielu jednostek LUN przypisanych do jednego celu iSCSI, mapowania i maskowania LUN, SPC-3 Persistent Reservation, MPIO oraz MC/S. Możliwość wykonywania migawek i kopii zapasowych jednostek LUN.

Szyfrowanie	Szyfrowanie udziałów sieciowych algorytmem co najmniej AES-256 oraz szyfrowanie danych na podłączonych dyskach zewnętrznych.
Usługi katalogowe	Integracja z Microsoft Active Directory i LDAP. Możliwość zarządzania kontami, grupami, limitami pojemności oraz uprawnieniami użytkowników, w tym zaawansowanymi uprawnieniami do podfolderów.
Protokoły dostępu	Logowanie użytkowników domenowych oraz dostęp do danych z wykorzystaniem co najmniej CIFS/SMB, FTP i sieciowego menedżera plików.
Funkcje backupu	Oprogramowanie producenta urządzenia do wykonywania kopii zapasowych danych z systemów Windows, wykonywania kopii na zewnętrzne dyski oraz przesyłania kopii do zewnętrznych usług chmurowych.
Usługi chmurowe	Obsługa co najmniej Amazon S3, Amazon Glacier, Microsoft Azure, Google Cloud Storage, Dropbox, OneDrive dla Firm oraz Google Drive.
Wirtualizacja	Możliwość uruchamiania maszyn wirtualnych z systemami Windows, Linux, Unix i Android. Obsługa importowania, klonowania oraz tworzenia migawek maszyn wirtualnych. Obsługa GPU pass-through dla dodatkowych kart graficznych.
Kontenery	Możliwość uruchamiania kontenerów Docker lub LXD oraz instalowania aplikacji z gotowych pakietów producenta i dostawców zewnętrznych.
Oprogramowanie do wykonywania kopii zapasowych	Urządzenie musi umożliwiać instalację i uruchomienie oferowanego systemu do wykonywania kopii zapasowych bezpośrednio na urządzeniu, z wykorzystaniem aplikacji natywnej, kontenera lub maszyny wirtualnej. Oprogramowanie musi mieć możliwość korzystania z wewnętrznej przestrzeni dyskowej urządzenia jako repozytorium kopii zapasowych.
Usługi sieciowe	Obsługa co najmniej funkcji serwera plików, serwera FTP, serwera WWW, serwera kopii zapasowych, serwera pobierania oraz klienta i serwera VPN.
Administracja	Zarządzanie przez HTTP i HTTPS, powiadomienia e-mail, możliwość powiadamiania przez SMS z wykorzystaniem zewnętrznych usług, DDNS, zdalny dostęp przez usługę chmurową producenta oraz obsługa SNMP v2 i SNMP v3.
Monitorowanie	Monitorowanie zasobów systemowych w czasie rzeczywistym, rejestr zdarzeń, informacje o aktywnych połączeniach użytkowników oraz zarządzanie zdarzeniami systemowymi.
Obsługa UPS	Obsługa zasilaczy UPS zarządzanych przez SNMP oraz urządzeń UPS podłączanych lokalnie przez USB.
Aktualizacje	Możliwość aktualizowania oprogramowania urządzenia wraz z powiadamianiem o aktualizacjach dostępnych na serwerach producenta. Możliwość wykonania kopii zapasowej ustawień systemowych, ich przywrócenia oraz resetowania urządzenia.

Zabezpieczenia	Filtrowanie adresów IP, automatyczne blokowanie nieautoryzowanych połączeń, obsługa HTTPS, FTP z SSL/TLS, SFTP, szyfrowanie AES-256 oraz możliwość importowania własnych certyfikatów SSL.
Wskaźniki i przyciski	Wskaźniki LED dla wszystkich zatok dyskowych, stanu urządzenia oraz interfejsów LAN. Przyciski zasilania i resetowania urządzenia.
Zasilanie	Dwa redundantne zasilacze o mocy minimum 550 W każdy, pracujące w zakresie napięcia 100–240 V AC.
Warunki środowiskowe	Temperatura pracy od 0°C do 40°C. Wilgotność względna podczas pracy w zakresie od 5% do 95%, bez kondensacji.
Gwarancja	Minimum 3 lata gwarancji na urządzenie główne.

Zestawienie wymaganych parametrów technicznych – macierz NAS (1 sztuka)

Typ urządzenia	Serwer NAS
Obudowa	Rack 2U
Procesor	Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark na lipiec 2025 co najmniej 4 550 punktów
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 4 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 8 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 12 dysków łącznie przy użyciu dodatkowej jednostki rozszerzającej podłączanej do jednostki głównej za pomocą portu eSATA.
Porty zewnętrzne	Minimum: • 2 porty USB 3.2.1 • 1 port eSATA lub USB-C (jako gniazdo rozszerzenia)
Porty sieciowe	Minimum: • 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 2.0	Min. 1x 4-liniowe gniazdo x8 gen. 3
Wentylator obudowy	Min. 2 wentylatory (80 × 80 × 25 mm)
System plików	Min.: • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Obsługiwane typy macierzy RAID	Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Zarządzanie pamięcią masową	• Maksymalny rozmiar pojedynczego wolumenu: 108 TB • Minimalny liczba wewnętrznych wolumenów: 32 • Minimalny liczba obiektów iSCSI Target: 64 • Minimalny liczba jednostek iSCSI LUN: 128

	• Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane protokoły	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, sesje Kerberized NFS, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Konto i folder współdzielony	• Minimalna liczba kont użytkowników: 1 024 • Minimalna liczba grup użytkowników: 256 • Minimalna liczba folderów współdzielonych: 256 • Minimalna liczba zadań synchronizacji folderów współdzielonych: 8
Usługi plików	• Protokół plików: SMB, AFP, NFS, FTP, WebDAV, Rsync • Minimalna liczba połączeń SMB (oparta na FSCT): 180 • Integracja z listą kontroli dostępu Windows (ACL) • Uwierzytelnianie Kerberos NFS
Wirtualizacja	Obsługa VMware vSphere with VAAI, Windows Server 2022, Citrix Ready, OpenStack
Bezpieczeństwo	Zapora, szyfrowanie folderów współdzielonych, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, wsparcie Let's Encrypt, HTTPS (konfigurowalny zestaw szyfrów)
Oprogramowanie	• Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów współdzielonych • Urządzenie musi wspierać funkcję WORM (Write Once, Read Many) oraz migawki niezmienne • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać

	udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. • Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Konserwacja	• Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack
Zasilanie	• Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz
Gwarancja	Wykonawca udzieli gwarancji: • 3 lata na urządzenia główne • 1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack

Zestawienie wymaganych parametrów technicznych – Dysk Typ1 - (8 sztuk)

Parametr	Wartość
Pojemność	4 TB
Format	3.5"
Interfejs	SATA 6 Gb/s
Prędkość obrotowa	5,400 obr./min
Maks. prędkość przesyłu danych	202 MB/s
Gwarancja	3 lata
Zużycie energii w trybie aktywnego bezczynności (typowe)	3.96 W
Zakres temperatury podczas pracy	0°C do 65°C (32°F do 149°F)
Zakre tempreatury podczas spoczynku	-40°C do 70°C (-40°F do 158°F)

Zestawienie wymaganych parametrów technicznych – system do Backupu

I. Wymagania minimalne:

1 Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji

a Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012
b Maszyny fizyczne: Windows Server 2025, 2022, 2019, 2016, 2012R2, 2012
c Microsoft 365 (Exchange online, One Drive for Business, Sharepoint, Teams)
d Proxmox Virtual Environment min. w wersji 8.0

2 Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowiska MS Hyper-V.

3 Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:

a na serwerze Windows lub Linux
c na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital.

4 Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS.

5 Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania.

6. Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).

II. Licencjonowanie

1 Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware, Hyper-V oraz Proxmox powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności.

2 Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 6 gniazd procesorów w obrębie środowiska.

3 W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 2 letniego wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania.

4 W ramach dostawy wymagane jest dostarczenie licencji na ochronę wszystkich gniazd procesorów serwera dostarczonego w ramach zadania nr 4 niniejszego postępowania.

5 Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska.

III. Ochrona danych

1 Oprogramowanie musi posiadać funkcje backupu i replikacji:
a Backup maszyn wirtualnych Vmware
b Replikacja maszyn wirtualnych Vmware (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
c Backup maszyn wirtualnych Hyper-V
d Replikacja maszyn wirtualnych Hyper-V (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
e Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
f Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
g Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
h Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
i "Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych
Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem"
j Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
k Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
l Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach.

IV. Optymalizacja wykorzystania miejsca na dane

1 Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
a Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
b Kompresja backupu, w tym konfigurowalny stopień kompresji
c Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne

V. Spójność danych

1 Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
a Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
b Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
c Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji:
d Microsoft Exchange 2013, 2016, 2019
e Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022
f Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
g Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
h Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania

i Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji

VI. Przywracanie danych

1 Oprogramowanie musi posiadać poniższe funkcje:
a Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
b Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)
c Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
d Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
e Microsoft Exchange
f MS Active Directory
g MS SQL
h Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.

VII. Wydajność

1 Oprogramowanie do backupu musi pozwalać na:
a Tworzenie backupu I replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
b Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
c Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN
d Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
e Wsparcie dla urządzeń oferujących dodatkową deduplikację danych

VIII. Zarządzanie

1 Oprogramowanie musi pozwalać na następujące formy zarządzania:
a Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
b Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
c Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania
d Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.
e Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
f Oprogramowanie musi umożliwiać integrację z Active Directory
g Oprogramowanie musi wspierać tzw. tryb multi tenant, umożliwiający podzielenie oprogramowania do backupu na kilka podinstancji zarządzanych z odrębnych interfejsów w celu rozłożenia zarządzania w złożonych środowiskach

Wymagane prace wdrożeniowe

1. Dostarczenie sprzętu wraz z konfiguracją
a. Zinwentaryzowanie i walidacja aktualnego środowiska serwerowego

b. Podłączenie serwera, macierzy, do infrastruktury elektrycznej i sieciowej Zamawiającego, z zastrzeżeniem, że pasywna część teletechniczna leży w gestii Wykonawcy tj. szafa rack oraz okablowanie sieci komputerowej
c. Wstępna konfiguracja serwera, macierzy, polegająca na nadaniu dostępów, adresacji oraz aktualizacji oprogramowaniu sprzętowego do najnowszej zalecanej przez producenta wersji
d. Przekazanie dostępów Zamawiającemu
e. Testy po uruchomieniu środowiska polegające na sprawdzeniu poprawności uruchamiania się środowiska systemowego
f. Przygotowanie dokumentacji powdrożeniowej zawierającej opis wdrożonej konfiguracji wirtualizacji zasobów
2. Wdrożenie backup
a. instalacja oprogramowania do kopii zapasowych na zasobie wskazanym przez Zamawiającego;
b. skonfigurowanie repozytorium kopii zapasowych wskazanego przez Klienta
c. zaprojektowanie i wdrożenie polityki tworzenia kopii zapasowych z wykorzystaniem dostarczonego oprogramowania do kopii zapasowych dla przynajmniej 2 maszyn wirtualnych;
d. przeprowadzenie testów akceptacyjnych poprawności działania operacji, kopii zapasowych i odzyskiwania danych;
e. konfiguracja powiadomień systemu kopii zapasowej oraz weryfikacja ich działania;

Zadanie 4 - Modernizacja DC

Przedmiot zamówienia

Przedmiotem zamówienia jest:

a. Dostawa serwera fabrycznie nowego, nie finansowanego wcześniej z krajowych lub unijnych funduszy projektowych;
b. Dostawa wymaganego oprogramowania
c. Konfiguracja, instalacja serwera;
d. Wdrożenie oraz konfiguracja środowiska wirtualizacji w środowisku IT Zamawiającego
e. Wsparcie w migracji obecnie posiadanych systemów
f. Dostarczenie przez Wykonawcę dokumentacji konfiguracji wdrożonego systemu

Wymagania szczegółowe Zamawiającego:

Zestawienie wymaganych parametrów technicznych – serwer

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U, 8 slotów na dyski 2.5" Hot-Swap. Obudowa z możliwością wyposażenia w panel wyświetlający informacje o stanie serwera (procesor, pamięć, dyski, BIOS, zasilanie, temperatura). Obudowa z możliwością wyposażenia w moduł umożliwiający bezpośredni dostęp z urządzenia mobilnego (Android/iOS) do konfiguracji i monitorowania kluczowych komponentów serwera za pośrednictwem dedykowanej aplikacji mobilnej, z wykorzystaniem połączenia USB.

Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 56 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym lub modelem serwera Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowany Jeden procesor min. 16-rdzeniowy, min. 2.0GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 266 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	128GB DDR5 RDIMM 5600MT/s
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający Min. 4GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących
Dyski twarde	Zainstalowane: 5× 960 GB SSD SATA 6 Gb/s 512 2.5″ do intensywnego odczytu, Hot-Plug. Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480 GB każdy z możliwością konfiguracji RAID 1.
Gniazda PCI	Min. 2 sloty PCIe LP
Interfejsy sieciowe/FC/SAS	min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz min. 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT
Wbudowane porty	Przynajmniej: 1 port USB 3.0 1 port USB 2.0 1 port VGA Możliwość rozbudowy o port RS232
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 1100W klasy Titanium
Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
System operacyjny/ dodatkowe oprogramowanie	Windows Server 2025 Standard w ilości umożliwiającej utworzenie 4 VM (z systemem z rodzinny Windows) zgodnie z licencją producenta.
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. Możliwość dynamicznego włączania i wyłączania portów USB bez potrzeby restartu serwera. Możliwość bezpiecznego wymazania danych z dysków wewnętrznych serwera niezależnie od zainstalowanego systemu operacyjnego, uruchamiana z poziomu zarządzania serwerem. Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania zgodne z zaleceniami NIST SP 800-147B. Serwer musi posiadać zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (sprzętowy Root of Trust).
Karta Zarządzania	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 uwierzytelnianie i autoryzację użytkowników; możliwość podmontowania zdalnych wirtualnych napędów; wirtualną konsolę z dostępem do myszy i klawiatury; wsparcie dla IPv6; wsparcie dla protokołów: SNMP, IPMI 2.0, SSH zdalne monitorowanie poboru prądu w czasie rzeczywistym; zdalne ustawianie limitu poboru prądu serwera; integrację z Active Directory/LDAP; jednoczesną obsługę przez co najmniej dwóch administratorów; wsparcie dla automatycznej rejestracji DNS; wysyłanie powiadomień e-mail do administratora w przypadku awarii lub zmiany konfiguracji sprzętowej; lokalne zarządzanie przez dedykowany port USB na przednim panelu serwera; zarządzanie wieloma serwerami bezpośrednio z konsoli karty zarządzającej
Oprogramowanie do zarządzania	wsparcie dla serwerów integracja z usługą katalogową (LDAP/Active Directory); zarządzanie serwerami bez udziału dedykowanego agenta; wsparcie dla protokołów SNMP, IPMI, SSH, Redfish; możliwość uruchamiania wykrywania urządzeń w oparciu o harmonogram lub ręcznie; szczegółowy opis wykrytych systemów i ich komponentów; możliwość eksportu danych inwentaryzacyjnych i dzienników zdarzeń do CSV lub HTML; filtrowanie i grupowanie urządzeń według kryteriów użytkownika (m.in. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, stan gwarancji); przegląd stanu środowiska na pulpicie nawigacyjnym oraz szczegółowy status każdego urządzenia; generowanie alertów i filtrowanie zdarzeń; integracja z centrum serwisowym producenta (automatyczne zgłaszanie incydentów); możliwość przejęcia zdalnego pulpitu serwera oraz podmontowania wirtualnego napędu; możliwość definiowania akcji dla alertów, ról i uprawnień administratorów; przekazywanie alertów do zewnętrznych systemów przez SNMP lub Syslog; zdalna aktualizacja firmware bez agenta, z wyborem źródła (lokalne lub online producenta); moduł raportujący: numery seryjne, konfiguracja, wersje firmware, obsadzenie slotów PCIe i pamięci, adresy IP i MAC, stan gwarancji, alerty, stan komponentów; tworzenie konfiguracji bazowej i weryfikacja środowiska pod kątem rozbieżności; wdrażanie serwerów w oparciu o profile konfiguracyjne; migracja ustawień serwera z wirtualnymi adresami sieciowymi (MAC, WWN, IQN); tworzenie paczek diagnostycznych i zdalne uruchamianie diagnostyki; dedykowana aplikacja mobilna (Android/iOS); oprogramowanie jako wirtualny appliance dla KVM, VMware ESXi i Microsoft 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 Silver według normy wprowadzonej w 2019 roku Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2025

Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. Wymagana możliwość zachowania dysku twardego w ramach świadczonej usługi wsparcia serwisowego dla sprzętu, obejmująca 3-letni okres wsparcia serwisowego z gwarancją producenta. Usługa ma na celu umożliwienie zamawiającemu zachowania nośników danych (dysków twardych) po ich awarii. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający 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. Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.

Wymagane prace wdrożeniowe

1. Dostarczenie sprzętu wraz z konfiguracją
a. Zinwentaryzowanie i walidacja aktualnego środowiska serwerowego
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. Konfiguracja serwera, polegająca na nadaniu dostępów, adresacji oraz aktualizacji oprogramowaniu sprzętowego do najnowszej zalecanej przez producenta wersji
f. Konfiguracja środowiska wirtualizacji wraz z replikacją aktualnych VM
g. Przekazanie dostępów Zamawiającemu
h. Testy po uruchomieniu środowiska wirtualnego polegające na sprawdzeniu poprawności uruchamiania się środowiska systemowego
i. Przygotowanie dokumentacji powdrożeniowej zawierającej opis wdrożonej konfiguracji wirtualizacji zasobów

Zadanie 5 - Sieć

Modernizacja sieci LAN

Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. dostawa fabrycznie nowego Sprzętu, nie używanego w innych środowiskach ani projektach, w ilościach:
   a. Przełącznik sieciowy 52p – 2 sztuki
   b. Przełącznik sieciowy 10p – 10 sztuk
   c. UTM z dwuletnim wsparciem – 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;

Wymagania szczegółowe Zamawiającego

Zestawienie wymaganych parametrów technicznych dla przełączników sieciowych - 52P (2 sztuki)

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 RPS: Status
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 przełączników sieciowych - 10P (10 sztuk)

Parametr	Wartość
Standardy i protokoły	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE802.3z, IEEE 802.3ad, IEEE 802.3x, IEEE 802.3af, IEEE 802.3at, IEEE 802.3az, IEEE 802.1d, IEEE 802.1s, IEEE 802.1w, IEEE 802.1q, IEEE 802.1x, IEEE 802.1p

Porty	8 x RJ45 10/100/1000 Mbps PoE+ (autonegocjacja MDI/MDIX), 2 x SFP 100/1000 Mbps
Okablowanie sieciowe	10BASE-T: kategoria 3, 4, 5 (do 100 m), 100BASE-TX/1000Base-T: kategoria 5, 5e (do 100 m), 100BASE-FX: MMF, SMF, 1000BASE-X: MMF, SMF
Wentylator	1 wentylator
Zabezpieczenia fizyczne	Tak
Zasilanie	100-240V AC, 50/60Hz
Porty PoE (RJ45)	8 portów PoE+ (802.3at/af), łączne zasilanie 150W
Wymiary (S x G x W)	294 x 180 x 44 mm (11.6 x 7.1 x 1.7 cali)
Montaż	Szafa Rack, Biurko
Wydajność przełączania	20 Gbps
Szybkość przekierowań pakietów	14.9 Mpps
Tablica adresów MAC	8K
Bufor pakietów	4.1 Mbit
Ramki jumbo	9 KB
QoS	Priorytetowanie 802.1p CoS/DSCP, 8 kolejek priorytetów
Funkcje L2 i L2+	DHCP relay, LACP, STP, Spanning Tree, Port Mirroring, Link Aggregation
VLAN	Max 4K grup VLAN, VLAN 802.1Q, GVRP, VLAN głosowy
ACL	Do 230 wpisów ACL, wsparcie dla ACL na IP, MAC, czasie
Bezpieczeństwo transmisji	AAA, 802.1X, IP/IPv6-MAC Binding, DHCP Snooping, DoS Defend
Zawartość opakowania	Przełącznik, kabel zasilający, instrukcja, elementy montażowe, gumowe podstawki
Środowisko pracy	Temperatura: 0–50 °C, wilgotność: 10–90% RH bez kondensacji
Certyfikaty	CE, FCC, RoHS

Wymagania ogólne dla wszystkich typów przełączników sieciowych 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. 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. Przełączniki 52p muszą posiadać możliwość zarządzania konfiguracją w warstwach 2 oraz 3 modelu OSI
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 5 VLAN-ów
9. Na wskazanym przez Zamawiającego zasobie serwerowym, Wykonawca zobowiązany jest do instalacji, konfiguracji i dodania urządzeń sieciowych do dedykowanego centralnego rozwiązania zarządzającego.

Wymagania ogólne dla zakupu urządzenia UTM wraz z wdrożeniem klastra HA

1. Dostarczone urządzenia muszą pochodzić z autoryzowanego kanały sprzedaży producentów na rynek polski – do oferty należy dołączyć odpowiednie oświadczenie producenta sprzętu
2. Zapewnienie dwuletniej subskrypcji licencji UTP do urządzenia
3. Zakres prac:
   a. Audyt istniejącej konfiguracji urządzenia
   b. Aktualizacja oprogramowania na nowym urządzeniu UTM
   c. Wyrównanie wersji oprogramowania na istniejącym urządzeniu
   d. Wdrożenie urządzenia UTM - Podstawowa konfiguracja urządzenia: przypisanie adresacji IP, ustawienie interfejsów sieciowych, konfiguracja dostępu do panelu administracyjnego.
   e. Konfiguracja klastra HA (High Availability) z istniejącym urządzeniem Fortigate FG 60F

f. Testowanie i weryfikacja nowej konfiguracji

4. Dostarczający musi utworzyć dostępy administracyjne do urządzeń oraz przekazać je Zamawiającemu

Zadanie 6 - Dostawa i wdrożenie systemu klasy DLP

Wdrożenie DLP oraz konfiguracja polityk bezpieczeństwa.

Przedmiot zamówienia

a. Dostarczenie oprogramowania klasy DLP
b. Implementacja rozwiązania w środowisku zamawiającego
c. Konfiguracja oprogramowania

Wymagania szczegółowe Zamawiającego

1. System operacyjny:

a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
c. MacOS 12 lub nowszy.

2. Serwer administracyjny musi obsługiwać instalację na systemach:
a. Windows Server 2016 (64-bit) i nowszych.
3. Serwer administracyjny musi obsługiwać bazy danych:
a. MS SQL Server 2016 lub nowsze,
b.MS SQL Express,
c. AzureSQL S3 lub nowsze.
4. Pomoc i dokumentacja programu dostępne w języku angielskim.
5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.
8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
11. System musi posiadać mechanizm usuwający najstarsze informacje, gdy rozmiar bazy osiągnie domyślny limit.
12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości e-mail oraz czynności na plikach.
19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
23. Serwer administracyjny musi posiadać możliwość połączenia z serwerem SMTP udostępnianym przez producenta.

24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już
skategoryzowanych plików.
25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
26. Administrator musi mieć możliwość tworzenia kategorii danych dla plików zaszyfrowanych lub dla takich gdzie zawartość pliku jest niemożliwa do odczytania.
27. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
28. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, numer REGON, NIP, wyrażenia regularne, określone ciągi znaków i numer IBAN.
29. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
30. Administrator musi mieć możliwość wyszukiwania danych wrażliwych w zasobach lokalnych
31 Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
32. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
33. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
34. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.
35. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
36. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach.
37. System musi umożliwiać synchronizacji grup bezpieczeństwa z Active Directory na potrzeby logowania do konsoli zarządzającej.
38. System musi umożliwiać administratorowi nadanie użytkownikowi uprzywilejowanego dostępu, przez co nie będzie obejmowany politykami przez określony czas – 1 godzinę, 6 godzin
lub do końca dnia.
39. System musi posiadać możliwość tworzenia polityk dynamicznych, pozwalających na dostosowywanie się akcji (takich jak zapisywanie logu, powiadomienie użytkownika, blokowanie lub blokowanie z możliwością zastąpienia przez użytkownika) w zależności od profilu pracy użytkownika wykonującego daną czynność, gdzie akcja dobierana jest w zależności od wyniku systemu uczenia maszynowego.
40. System musi umożliwiać dostosowanie polityk dynamicznych do dwóch trybów:
standardowy oraz łagodny. Możliwość taka musi istnieć per użytkownik.
41. System musi umożliwiać tworzenie raportów na podstawie logów zebranych w układach danych z możliwością dostosowania filtrów, użytkowników oraz zakresu czasu objętych raportowaniem.
42. System musi umożliwiać utworzenie raportu, który będzie zawierał podsumowanie stanu zabezpieczenia danych wraz z rekomendacjami w formie cyklicznej.
43. System musi zbierać informacje na temat podłączanych urządzeń do komputera,

odwiedzanych domen internetowych, ścieżek sieciowych, drukarek lokalnych oraz sieciowych, umożliwiając jednocześnie przypisanie takowych wpisów do bezpiecznych lub niezaufanych lokalizacji bez potrzeby manualnego wpisywania ścieżek lub numerów seryjnych urządzeń.
44. Dla każdej z wyżej wymienionych lokalizacji system powinien umożliwiać przypisanie indywidualnej polityki dostępu – np. umożliwiając przesyłanie danych do lokalizacji oznaczonej jako bezpieczna, jednocześnie blokując wysyłkę do lokalizacji oznaczonej jako niezaufana lub nieprzypisana.
45. System musi umożliwiać audyt operacji wykonywanych przez administratora w obszarze konsoli DLP.
46. System musi umożliwiać podłączenie archiwa logów w formacie plików o rozszerzeniu mdf

Wymagane prace wdrożeniowe

1. Dostarczenie oprogramowania klasy DLP
    a. 30 bezterminowych licencji on-prem, licencja zawierająca rok wsparcia producenta
2. Implementacja rozwiązania w środowisku zamawiającego
    a. Utworzenie i podstawowa konfiguracja VM
    b. Instalacja konsoli centralnej
    c. Wdrożenie agentów na wskazanych komputerach zamawiającego
    d. Konfiguracja integracji dla Microsoft MS365
3. Konfiguracja oprogramowania
    a. Utworzenie do 5 reguł DLP
    b. Utworzenie do 5 kategorii danych
    c. Przygotowanie danych i oraz do 2 raportów, omówienie raportów i zebranych danych

Zadanie 7 - Dostawa zasilacza awaryjnego UPS

Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. dostawa fabrycznie nowych sprzętów, nie używanych w innych środowiskach ani projektach;
2. udzielenie przez Wykonawcę gwarancji i zapewnienie w jej ramach serwisu gwarancyjnego oraz wsparcia technicznego na dostarczony Sprzęt;
3. dostarczenie przez Wykonawcę dokumentacji dostarczonego Sprzętu;

Wymagania szczegółowe Zamawiającego

Zestawienie wymaganych parametrów technicznych systemu podtrzymania bateryjnego - Typ 1 – 1 sztuka

Nazwa komponentu	Wymagane minimalne parametry techniczne
Topologia	Line interactive
Typ przebiegu	Sinusoida
Liczba szaf rackowych	2U
Moc znamionowa w W	minimum 2700 W
Moc znamionowa w VA	minimum 3000 VA

Typowy czas ładowania do 90%	3 godziny
Rodzaj akumulatora	Akumulator kwasowo-ołowiowy
Masa produktu	Maksymalnie 37,5 kg
Sposób montażu	Montaż w szafie RACK (zestaw musi zawierać elementy montażowe)
Komunikacja i zarządzanie	Wielofunkcyjna konsola sterownicza i informacyjna LCD Wyświetlacz stanu LED ze wskaźnikiem zasilania Gniazdo karty zarządzania
Dostarczone wyposażenie	CD z oprogramowaniem Wsporniki montażowe do szaf przemysłowych Kabel do sygnalizacji RS-232 do Smart-UPS Czujnik temperatury podręcznik użytkownika Karta do zdalnego zarządzania Web SNMP Management Card
Certyfikaty produktu	C-Tick, CE, EAC, GOST, IRAM, VDE, UK PSTI
Normy	EN/IEC 62040-1:2019/A11:2021 EN/IEC 62040-2:2006/AC:2006 EN/IEC 62040-2:2018
Gwarancja	3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulator

Zestawienie wymaganych parametrów technicznych systemu podtrzymania bateryjnego - Typ 2 - 25 sztuki

Nazwa komponentu	Wymagane minimalne parametry techniczne
Topologia	Line interactive
Moc znamionowa w W	minimum 650 W
Moc znamionowa w VA	minimum 1200 VA
Typ przebiegu	Schodkowa aproksymacja sinusiody
Typowy czas ładowania do 90%	8 godziny
Napięcie akumulatora	12 V
Masa produktu	Maksymalnie 8 kg
Sposób montażu	Wolnostojący
Rodzaj akumulatora	Akumulator kwasowo-ołowiowy
Typ połączenia wyjściowego	4 Schuko
Elementy zestawu	Podręcznik użytkownika
Komunikacja i zarządzanie	Dioda led wskazująca na status zasilania: zasilanie z sieci energetycznej: zasilanie z akumulatora
Certyfikaty produktu	CE, CB, EAC
Normy	EN/IEC 62040-1:2019/A11:2021 EN/IEC 62040-2:2006/AC:2006 EN/IEC 62040-2:2018
Gwarancja	2 lata na naprawę lub wymianę

Zadanie 8 - System rejestracji incydentów

Zapewnienie systemu rejestracji i zarządzania incydentami

Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. dostawa oprogramowania do rejestrowania i zarządzania incydentów w infrastrukturze IT Zamawiającego;
2. przeprowadzenie szkolenia z posługiwania się dostarczonym rozwiązaniem.

Szczegółowe wymagania rozwiązania

Integracja z posiadanym rozwiązaniem ochrony endpoint

Zamawiający posiada aktywną licencję na rozwiązanie ochrony endpoint Eset o kluczu publicznym: 33B-TK5-BT.

Oferowane rozwiązanie musi zapewniać pełną kompatybilność i integrację z posiadaną infrastrukturą ochrony, umożliwiającą rozszerzenie zakresu ochrony bez konieczności wymiany dotychczasowo wdrożonego oprogramowania.

Konsola zarządzająca

1. Rozwiązanie musi być dostępne w modelu chmurowym zarządzanym przez producenta oprogramowania, bez konieczności utrzymania dodatkowej infrastruktury serwerowej po stronie Zamawiającego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu przeglądarki internetowej (interfejs WWW), bez konieczności instalowania dodatkowego oprogramowania klienckiego.
3. Dostęp do konsoli zarządzającej musi być chroniony z wykorzystaniem protokołu szyfrowania SSL/TLS.
4. Rozwiązanie musi posiadać mechanizm wykrywania sklonowanych maszyn na podstawie unikalnego identyfikatora sprzętowego stacji roboczej, zapobiegający powstawaniu zduplikowanych wpisów w konsoli.
5. Rozwiązanie musi umożliwiać komunikację agenta zarządzającego z serwerem centralnym za pośrednictwem serwera proxy HTTP.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi (MDM) z poziomu konsoli centralnej.
7. Rozwiązanie musi posiadać mechanizm wymuszenia uwierzytelnienia wieloskładnikowego (MFA) przy logowaniu do konsoli administracyjnej.
8. Rozwiązanie musi posiadać granularny model uprawnień dla użytkowników konsoli, umożliwiający przypisanie uprawnień co najmniej w zakresie: zarządzania politykami, raportowaniem, zarządzaniem licencjami oraz zadaniami administracyjnymi. Każda z funkcji musi obsługiwać co najmniej następujące poziomy dostępu: odczyt, użycie, zapis oraz brak dostępu.
9. Rozwiązanie musi posiadać co najmniej 80 predefiniowanych szablonów raportów dostarczonych przez producenta.
10. Rozwiązanie musi umożliwiać tworzenie statycznych i dynamicznych grup urządzeń.
11. Dynamiczne grupy urządzeń muszą być tworzone w oparciu o szablony definiujące warunki kwalifikacji, obejmujące co najmniej: zakresy adresów IP, obecność aktywnych zagrożeń, stan ochrony i działania agenta, wersję systemu operacyjnego oraz parametry sprzętowe stacji.
12. Rozwiązanie musi umożliwiać uruchamianie zadań automatycznych z co najmniej następującymi wyzwalaczami: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia w dzienniku oraz po przypisaniu urządzenia do grupy dynamicznej.

Funkcjonalności rozwiązania

1. Wykrywanie i rejestrowanie incydentów bezpieczeństwa na serwerach i stacjach roboczych z systemem operacyjnym Windows.
2. Wykrywanie i rejestrowanie incydentów bezpieczeństwa na zarządzanych urządzeniach mobilnych.
3. Wykrywanie i rejestrowanie incydentów bezpieczeństwa w usługach Microsoft 365 (w tym Exchange Online, SharePoint Online, OneDrive).
4. Wykrywanie podatności w zainstalowanych aplikacjach i systemach operacyjnych zarządzanych urządzeń.
5. Możliwość zabezpieczenia dostępu do systemów operacyjnych i aplikacji z wykorzystaniem dodatkowego składnika uwierzytelnienia (MFA).

Monitorowanie i korelacja incydentów

1. Dostęp do konsoli centralnego zarządzania incydentami musi odbywać się z poziomu przeglądarki internetowej (interfejs WWW).
2. Serwer administracyjny musi posiadać natywny mechanizm przekazywania zdarzeń do konsoli zarządzającej tego samego producenta, umożliwiający scentralizowany podgląd wykrytych zagrożeń.
3. Interfejs konsoli musi być chroniony z wykorzystaniem protokołu szyfrowania SSL/TLS.
4. Serwer administracyjny musi umożliwiać definiowanie wykluczeń, których spełnienie zapobiega generowaniu alarmu bezpieczeństwa.
5. Wykluczenia muszą dotyczyć zarówno procesu będącego bezpośrednim źródłem zdarzenia, jak i procesu nadrzędnego (procesu „rodzica").
6. Utworzenie wykluczenia musi skutkować automatycznym rozwiązaniem istniejących alarmów spełniających kryteria tego wykluczenia.
7. Kryteria definiowania wykluczeń muszą obejmować co najmniej: nazwę procesu, ścieżkę procesu, parametry wiersza polecenia, wydawcę (sygnatariusza), typ podpisu cyfrowego, wartość skrótu SHA-1, nazwę komputera, grupę urządzeń oraz nazwę użytkownika.
8. Serwer administracyjny musi posiadać zestaw wbudowanych reguł detekcji dostarczonych przez producenta, wyzwalających alarmy bezpieczeństwa po ich spełnieniu. Liczba wbudowanych reguł dostarczanych przez producenta musi wynosić co najmniej 500. Administrator musi posiadać możliwość tworzenia własnych reguł detekcji oraz modyfikacji reguł dostarczonych przez producenta.
9. Serwer administracyjny musi umożliwiać blokowanie plików na podstawie ich sumy kontrolnej (hash). Mechanizm blokowania musi umożliwiać dodanie komentarza do wpisu oraz konfigurację akcji wykonywanej po wykryciu zablokowanej sumy kontrolnej.
10. Administrator musi posiadać możliwość przeglądania listy plików wykonywalnych uruchomionych na stacjach roboczych wraz ze szczegółami wybranego procesu, obejmującymi co najmniej: wartość SHA-1, typ podpisu cyfrowego, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz wskaźniki reputacji i popularności.
11. Administrator musi posiadać możliwość oznaczenia plików wykonywalnych oraz bibliotek DLL jako bezpieczne lub niebezpieczne, pobrania ich do analizy oraz ich zablokowania — bezpośrednio z poziomu konsoli.

12. Administrator musi posiadać możliwość przeglądania listy skryptów uruchomionych na stacjach roboczych wraz z informacją o parametrach ich uruchomienia oraz możliwość oznaczenia każdego skryptu jako bezpieczny lub niebezpieczny.
13. W ramach podglądu wykonanego skryptu administrator musi mieć możliwość przeglądania szczegółowych informacji o czynnościach wykonanych przez skrypt w formie tekstowej.
14. W ramach analizy skryptu lub pliku wykonywalnego administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń, obejmujących co najmniej: modyfikacje plików i rejestru systemowego, nawiązane połączenia sieciowe oraz utworzone procesy potomne.
15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu ochrony endpoint tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. Konsola zarządzająca musi umożliwiać podgląd co najmniej: szczegółów sprzętowych zarządzanego komputera (producent, model, numer seryjny, dane systemu operacyjnego, procesor, pamięć RAM, dyski, wyświetlacz, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz listy zainstalowanego oprogramowania firm trzecich.
16. Konsola administracyjna musi umożliwiać tagowanie obiektów (urządzeń, procesów, zdarzeń, incydentów) w celu ich kategoryzowania i filtrowania.
17. Konsola administracyjna musi umożliwiać zdalne połączenie ze stacją roboczą i wykonywanie poleceń z poziomu interfejsu wiersza poleceń lub sesji PowerShell.

Wymagane prace wdrożeniowe

1. Uruchomienie konsoli do Zarządzania wraz z integracją z istniejącym rozwiązaniem
2. konfiguracja wstępna i nadanie dostępów do logowania dla Zamawiającego;
3. przygotowanie po konsultacji z Zamawiającym definicji incydentów
4. konfiguracja 5 szablonów raportów zgodnych z wymogami Zamawiającego
5. konfiguracja powiadomień na wskazaną przez Zmawiającego skrzynkę pocztową za pośrednictwem dedykowanej skrzynce technicznej dostarczonej przez Zamawiającego.

Informacje dodatkowe:

Zamawiający wymaga, aby elementy przedmiotu zamówienia przeznaczone do użytku osób fizycznych, w tym pracowników Zamawiającego, były wykonane z uwzględnieniem wymagań dostępności dla osób z niepełnosprawnościami oraz projektowania z przeznaczeniem dla wszystkich użytkowników, zgodnie z art. 100 ustawy Prawo zamówień publicznych oraz ustawą o zapewnianiu dostępności osobom ze szczególnymi potrzebami. W szczególności Wykonawca zapewni dostępność cyfrową materiałów szkoleniowych, nagrań, dokumentacji, raportów, instrukcji, formularzy, komunikatów użytkownika, certyfikatów elektronicznych oraz interfejsów WWW/aplikacyjnych dostarczanych lub konfigurowanych w ramach zamówienia, w zakresie adekwatnym do ich przeznaczenia. Materiały i dokumenty elektroniczne powinny być przekazane w formatach umożliwiających odczyt maszynowy, posiadać logiczną strukturę nagłówków, poprawne tabele, teksty alternatywne dla istotnych elementów graficznych, odpowiedni kontrast, możliwość powiększania treści oraz obsługę przez technologie wspomagające. Nagrania szkoleń powinny posiadać co najmniej transkrypcję albo napisy, a platforma szkoleniowa powinna umożliwiać udział osobom

korzystającym z klawiatury i technologii wspomagających. Interfejsy systemów, konsol administracyjnych i portali WWW powinny być możliwe do obsługi z klawiatury, współpracować z aktualnymi przeglądarkami i technologiami wspomagającymi, posiadać czytelne komunikaty błędów, dostępne formularze, odpowiedni kontrast, skalowalność tekstu oraz dostępne mechanizmy uwierzytelniania, w tym MFA. Jeżeli ze względu na charakter danego elementu przedmiotu zamówienia pełne zapewnienie dostępności nie jest możliwe albo nie jest uzasadnione, Wykonawca wskaże ograniczenie i zaproponuje rozwiązanie alternatywne, a Zamawiający odnotuje uzasadnienie ograniczenia.