Znak: GIR.271.1.3.2022 **Załącznik nr 1 do SWZ**

Szczegółowy opis przedmiotu zamówienia

Dostarczony sprzęt powinnien podlegać:
a) fizycznemu montażowi serwerów, macierzy, napędu taśmowego w wskazanym przez Zamawiającego miejscu
b) aktualizacji oraz konfiguracji BIOS na dostarczonych serwerach według najlepszych praktyk producenta,
c) update Firmware oraz konfiguracja według najlepszych praktyk producenta,
d) Konfiguracja automatycznego powiadamiania producenta i administratorów o usterkach za pomocą wiadomości wysłanych poprzez szyfrowany protokół
e) konfiguracja dysków w RAID na serwerach oraz macierzach,
f) instalacja systemu operacyjnego na dostarczonych serwerach oraz konfiguracja dysków logicznych według zaleceń Zamawiającego,
h) podłączenie i konfiguracja serwerów w sposób zapewniający redundancję
i) Sprawdzenie poprawności konfiguracji

A. Serwer – 2 szt.

Obudowa	• Typu RACK, wysokość nie więcej niż 2U; • Szyny umożliwiające wysunięcie serwera z szafy stelażowej; • Ramię porządkujące ułożenie przewodów z tyłu serwera; • Możliwość zainstalowania 16 dysków twardych hot plug 2,5"; • Fizycznego zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych; • Zainstalowane 5 szt. dysków SSD 960GB Hot-Plug; • Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray; • Możliwość zainstalowania wewnętrznego napędu LTO;
Płyta główna	• Dwuprocesorowa; • Wyprodukowana i zaprojektowana przez producenta serwera • Możliwość instalacji procesorów 38-rdzeniowych; • Zainstalowany moduł TPM 2.0; • 7 złącz PCI Express generacji 4 w tym: o 4 fizyczne złącza o prędkości x16; o 3 fizyczne złącza o prędkości x8; o Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości; o Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e; • 32 gniazda pamięci RAM; • Obsługa minimum 4TB pamięci RAM DDR4; • Obsługa minimum 12TB pamięci RAM DDR4 wraz z pamięcią nieulotną

	• Wsparcie dla technologii:
	  ○ Memory Scrubbing
	  ○ SDDC
	  ○ ECC
	  ○ Memory Mirroring
	  ○ ADDDC;
	• Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci)
	• Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug;

Procesory	• jeden procesor 8-rdzeniowe • Taktowanie 2,8GHz • architektura x86_64 osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base minimum 139 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/cpu2017.html
Pamięć RAM	• 128 GB pamięci RAM • DDR4 Registered • 3200Mhz
Kontrolery LAN	• Karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 10Gbit SFP+ obsadzona modułami MMF LC, możliwość wymiany zainstalowanych interfejsów na 2x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe; • Dodatkowa karta LAN 4x 1Gbit Base-T;
Kontrolery I/O	• Zainstalowany kontroler SAS RAID obsługujący poziomy 0,1,10,5,50,6,60 posiadający 2GB pamięci cache zabezpieczonej za pomocą baterii lub kondensatora
Porty	• Zintegrowana karta graficzna ze złączem VGA z tyłu i przodu serwera; • 2 port USB 3.0 wewnętrzne; • 2 porty USB 3.0 dostępne z tyłu serwera; • 1 Port serial, możliwość wykorzystania portu serial do zarządzania serwerem; • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; • 2 porty USB 3.0 na panelu przednim

Zasilanie, chłodzenie	• Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy minimalnej 900W; • Redundantne wentylatory hotplug;
Zarządzanie	• Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii o informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: ▪ karty rozszerzeń zainstalowane w dowolnym slocie PCI Express ▪ procesory CPU ▪ pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM ▪ wbudowany na płycie głównej nośnik pamięci M.2 SSD ▪ status karty zrządzającej serwera ▪ wentylatory ▪ bateria podtrzymująca ustawienia BIOS płyty główne ▪ zasilacze Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający zarządzanie, zdalny restart serwera; o Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; o Dostęp poprzez przeglądarkę Web, SSH; o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; o Zarządzanie alarmami (zdarzenia poprzez SNMP) o Możliwość przejęcia konsoli tekstowej o Możliwość zarządzania przez 6 administratorów jednocześnie o Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) o Obsługa serwerów proxy (autentykacja) o Obsługa VLAN o Możliwość konfiguracji parametru Max. Transmission Unit (MTU) o Wsparcie dla protokołu SSDP

	○ Obsługa protokołów TLS 1.2, SSL v3 ○ Obsługa protokołu LDAP ○ Integracja z HP SIM ○ Synchronizacja czasu poprzez protokół NTP ○ Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); • Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB; • Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; • Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. • BIOS UEFI w specyfikacji 2.7;
Wspierane OS	• Microsoft Windows Server 2022, 2019, 2016 • VMWare vSphere 6.7, 7.0 • Suse Linux Enterprise Server 15 • Red Hat Enterprise Linux 7.9, 8.3 • Hyper-V Server 2016, 2019
Gwarancja	• gwarancja producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. • Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; • Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; • Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego

	serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; • Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty);
Dokumentacja, inne	• Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy lub producenta; • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; • W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; • Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %; • Zgodność z normami: CB, RoHS, WEEE, GS oraz CE;
System operacyjny	Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.

	3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9) 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). 10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15) Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

	17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18) Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty z certyfikatami (smartcard), c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25) 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.
iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

c) Zdalna dystrybucja oprogramowania na stacje robocze.
d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
   i. Dystrybucję certyfikatów poprzez http
   ii. Konsolidację CA dla wielu lasów domeny,
   iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
   iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
f) Szyfrowanie plików i folderów.
g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
i) Serwis udostępniania stron WWW.
j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
k) Wsparcie dla algorytmów Suite B (RFC 4869),
l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
   i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

	ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

W ramach zamówienia Wykonawca dostarczy do serwerów:
- licencje dostępowe Windows Server 2022 CAL lub nowsze typu USER (na użytkowanie) lub równoważne dla 25 użytkowników
- licecncje Microsoft Windows Server 2022 Remote Desktop Services lub nowsze typu USER lub równoważne dla 5 użytkowników

B. Macierz dyskowa – 1 szt.

System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy

bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii. Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy lub musi być dostarczona licencja na dwukrotność dostarczanej pojemności. Dostarczana macierz musi umożliwiać takie podłączenie półek, aby awaria lub/i usunięcie jednej z półek nie powodowało utraty dostępu do danych znajdujących się na pozostałych modułach. Oferowana macierz musi obsługiwać min. 140 dysków wykonanych w technologii hot-plug. Wszystkie zainstalowane dyski hot-plug, z wyłączeniem dysków SSD stosowanych jako rozszerzenie pamięci Cache kontrolerów, muszą być dostępne dla zapisu danych Użytkownika. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów (tzw. „półek dyskowych") w rozmiarze 2U pozwalająca umieścić do 24 dysków 2,5" typu hotplug dla dysków SAS i SSD oraz w rozmiarze 2U dla 12 dysków 3,5" typu hotplug NL-SAS i SSD oraz półki gęstego upakowania dla 60 dysków typu hotplug NL-SAS; Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji wyżej wymienionych półek dyskowych (tj. 2,5" + 3,5" + gęstego upakowania).

Pojemność macierzy:

5 szt. dysków twardych NL-SAS lub SSD-SAS o pojemności 12TB każdy;

Kontrolery

- Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami;
- Każdy z kontrolerów macierzy musi posiadać po minimum 16GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu;
- Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 800GB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD,
- W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk.
- Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia;
- Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach.
- Każdy z kontrolerów RAID powinien posiadać dedykowany minimum 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.
- Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej z minimum 4 rdzeniami.
- Kontrolery macierzy muszą obsługiwać do 70 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów
- Oferowana macierz musi mieć wyprowadzone 2 porty iSCSI 10Gb/s SFP+ obsadzone wkładkami MMF LC do dołączenia serwerów bezpośrednio lub do sieci san na każdy kontroler RAID.
- Macierz musi umożliwiać dołożenie do każdego z kontrolerów portów do transmisji danych (bez konieczności usuwania istniejących):

    - 2x FC 16 Gb/s,
    - 2x iSCSI 10Gb/s SFP+,
    - 2x SAS 12Gb/s
    - 2x FC 32Gb/s,
- Dołożenie portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych
- Macierz posiada obsługę operacji plikowych I/O w sieci NAS w obrębie zainstalowanych kontrolerów. Protokoły dostępu: CIFS, NFS. W przypadku obsługi protokołów CIFS i NFS wymagana jest funkcjonalność agregacji przepustowości dla interfejsów dedykowanych do obsługi tych protokołów. Obsługa protokołów CIFS i NFS musi odbywać się jednocześnie. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy

Poziomy RAID

- Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:
    - Raid-1
    - Raid-10
    - Raid-5
    - Raid-50
    - Raid-6

Dyski

- Oferowana macierz musi wspierać dyski hot-plug:
    - dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS12Gb/s
    - dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm,
- Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania;
- Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex
- Macierz musi obsługiwać min. 140 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami;
- Możliwość rozbudowy oferowanego modelu macierzy do minimum 520 dysków bez migracji i przenoszenia danych - jedynie poprzez wymianę modułu kontrolerów macierzy (bez konieczności wymiany posiadanych dysków, półek dyskowych, bez konieczności przenoszenia danych/ istniejącej struktury grup dyskowych/LUN, jak również z zachowaniem istniejącej gwarancji producenta na półki dyskowe i dyski;
- Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) lub wirtualna przestrzeń zapasowa:
    - Macierz posiada możliwość konfiguracji dysku hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID
    - Macierz posiada możliwość konfiguracji dysku hot-spare dedykowanego dla zabezpieczenia tylko wybranej grupy dyskowej RAID
- W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować

powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess) lub nie wymaga zwolnienia zapasowej przestrzeni wirtualnej.
- Macierz musi pozwalać na zaszyfrowanie danych zapisanych na wszystkich obsługiwanych dyskach SSD-SAS, HDD-SAS oraz HDD NL-SAS minimum kluczem AES256-bit dla danych blokowych – jeżeli w tym celu niezbędne jest zakupienie dodatkowych licencji bądź komponentów sprzętowych to należy je dostarczyć wraz z macierzą.
- Macierz musi umożliwiać zaszyfrowanie całej dostępnej powierzchni użytkowej minimum kluczem AES256-bit.

Opcje programowe

- Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 2048 kopii migawkowych
- Macierz musi umożliwiać zdefiniowanie min. 4000 woluminów (LUN)
- Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 1024 ścieżek logicznych FC
- Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów
- Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową
- Macierz musi posiadać wsparcie dla systemów operacyjnych : Microsoft Windows Server 2016, 2019, 2022, SuSE Linux Enterprise Server, Red Hat Linux Enterprise Server, HP-UNIX, IBM AIX, SUN Solaris, Vmware Vsphere;
- Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.
- Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC oraz iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy;
- Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy;
- Macierz musi obsługiwać mechanizm ochrony priorytetów obsługi wybranych zasobów – za taki mechanizm uznaje się funkcję typu ‘cache partitioning’ lub ‘storage partitioning’.
- Macierz musi obsługiwać adresację IP v.4 i IP v.6
- Wraz z macierzą należy dostarczyć oprogramowanie lub moduły programowe typu plug-in pozwalające na integracje macierzy w środowiskach Vmware w zakresie

obsługi mechanizmów: Vmware VAAI, Vmware VVOL, Vmware MultiPath IO – z subskrypcją do bezpłatnej aktualizacji w całym okresie obowiązywania gwarancji

- Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy.
- Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy. Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SSAS, NLSAS. Macierz musi pozwalać na definiowanie różnych polityk i zasad migrowania danych w obrębie tej samej macierzy. Mechanizm AST musi pozwalać na definiowanie okna czasowego dla zbierania pomiarów wydajności operacji I/O oraz okna czasowego dla migrowania danych wg ustalonych zasad i polityk – minimalny definiowany czas trwania w/w operacji (długość okna czasowego) nie może być dłuższy niż 4 godziny. Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy
- Mechanizm AST musi być obsługiwać funkcję Quality-of-Services pozwalająca na zagwarantowaniu wydajności dla wybranych zasobów macierzy (woluminów) mierzonej jako maksymalny czas opóźnień operacji I/O wykonywanych przez serwer/środowisko/aplikację. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy
- Macierz musi wspierać usługi VSS (Volume ShadowCopy Services) w systemach klasy Microsoft Windows Sever – wymagane jest dostarczenie niezbędnego oprogramowania / sterowników VSS pozwalających na obsługę VSS przy maksymalnej pojemności i liczbie dysków obsługiwanych przez oferowaną. W czasie trwania gwarancji wymaga się bezpłatnego dostępu do nowych wersji oprogramowania i sterowników
- Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy tej klasy, z zachowaniem obsługi operacji I/O dla serwerów podłączonych do migrowanej macierzy tj. do migrowanych zasobów LUN
- Macierz wspiera rozwiązania klasy ‘klastra macierzowego’ tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami protokołami FC oraz iSCSI. Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC oraz iSCSI, zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy. Pod użytym pojęciem ‘wysoka dostępność zasobów dyskowych’ należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzą, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Funkcjonalność ‘klastra macierzowego’ musi pozwalać na automatyczne i ręczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii

macierzy podstawowej (tzw. Automated/manual failover). – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy.

Zarządzanie

- Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej
- Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.
- Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora
- Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI

Gwarancja i serwis

- Całe rozwiązanie musi być objęte gwarancją z naprawą w miejscu instalacji urządzenia i z gwarantowaną skuteczną naprawą do końca następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta macierzy.
- Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia.
- Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązania bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy oraz do kolejnych wersji oprogramowania zarządzającego w okresie minimum 2 lat.
- Jeśli uszkodzeniu ulegną dyski twarde nie podlegają one zwrotowi i pozostają w siedzibie Zamawiającego.
- System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez szyfrowany protokół. Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta – musi być do tego wykorzystany dedykowany system serwisowy macierzy.
- Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych
- Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia
- Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty);
- Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co

najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje;

C. Zasilacz UPS – 1 szt

Wymagania minimalne

a. Moc 3 KW

• elementy umożliwiające montaż w szafie RACK
• zajętość w szafie RACK nie więcej niż 2U
• moc pozorna 3kVA
• moc rzeczywista 2,7 kW
• technologia on-line
• podtrzymanie 3,8 minuty przy 100% obciążeniu
• podtrzymanie 11,5 minuty przy 50% obciążeniu
• wyjścia: 8x IEC 320 C13 (10A)
• 1x RJ45
• aplikacja do automatycznego zamykania wspieranych systemów operacyjnych w przypadku braku zasilania
• wspierane i certyfikowane systemy operacyjne: Microsoft Windows Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, VMware Infrastructure, Citrix XenServer
• zarządzanie przez SNMP
• automatyczny wewnętrzny bypass
• bezprzerwowa wymiana baterii
• możliwość dołączenia baterii wydłużających czas podtrzymania zasilania
• wyświetlacz LCD na froncie urządzenia, umożliwiający zarządzanie i monitoring urządzenia
• certyfikaty: CE, CB
• Gwarancja door-to-door

D. Napęd taśmowy -1 szt.

- wewnętrzny napęd RDX dedykowany do zainstalowania w jednym z oferowanych serwerów;
- gwarancja producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.
- Dopuszcza się dostarczenie zewnętrznego napędu RDX USB lub SAS w obudowie RACK, wraz z niezbędnymi akcesoriami i okablowaniem z gwarancją producenta w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia.

1. **Nośniki do napędu RDX**

- Nośniki o pojemności 1TB w ilości 6 szt. kompatybilne z oferowanym napędem RDX

E. Specjalistyczne oprogramowanie dla serwera – 1 szt.

Oprogramowania do zabezpieczania danych poprzez mechanizm kopi zapasowych dedykowane dla środowisk wirtualizacyjnych.

1. Oprogramowanie musi wspierać co najmniej systemy operacyjne:
    - Dla hosta:
        i. VMware ESX/ESX(i) 5.0, 5.1, 5.5, 6.0, 6.5, 6,7.
        ii. Hyper-V.
        iii. Citrix XenServer.
        iv. Red Hat Virtualization.
        v. Linux KVM.
        vi. Oracle VM Server.
    - Dla maszyn wirtualnych:
        i. Windows XP (SP3) i nowsze.
        ii. Windows Server 2003 i nowsze.
        iii. Windows SBS 2011/2008, 2003/2003R2.
        iv. Windows Storage Server 2012/2012R2, 2008R2/2008/2003.
        v. Windows MultiPoint Server 2012/2011/2010.
        vi. Linux OS.
        vii. macOS.

2. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:
    - Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www.
    - Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego).
    - Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych.
    - Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu).
    - Definiowanie uprawnień dla administratorów system kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.).
    - Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami.
    - Wsparcie dla Single Sign On dla logowania do systemu.
    - Zarządzanie procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT.

- Definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem).
- Tworzenie zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych.
- Zdalna instalacja agentów kopi zapasowych na maszynach z systemem operacyjnym Windows.
- Zdalne uaktualniania agentów kopi zapasowych.
- Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych.
- Możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej).
- Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych.
- Centralny katalog wszystkich danych zapisanych w kopiach zapasowych
- Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.

3. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:
    - Kopie zapasowe całych dysków i partycji.
    - Kopie zapasowe wybranych plików i folderów.
    - Technologia bezagentowego wykonywania kopii zapasowej dla maszyn wirtualnych (dotyczy Hyper-V i VMWare ESXi).
    - Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory)
    - Kopie zapasowe baz danych Oracle.
    - Kopie zapasowe hostów Hyper-V i VMWare ESXi.
    - Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych.
    - Zapis kopi zapasowych na udziały sieciowe.
    - Zapis kopi zapasowych na serwer SFTP..
    - Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana.
    - Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery).
    - Możliwość wyszukiwania plików w kopiach zapasowych.
    - Szyfrowanie plików kopi zapasowych.
    - Wsparcie dla technologii VSS.
    - Deduplikacja kopi zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć.
    - Kompresja plików kopi zapasowych.
    - Replikacja kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy).
    - Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.

4. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:
    - Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore

- Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową.
- Odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej platformie sprzętowej.
- Odtworzenie poszczególnych plików i folderów.
- Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowania maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania).
- Granularne odtwarzanie baz danych Microsoft Exchange.
- Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange.
- Wyszukiwanie i podgląd odtwarzanych wiadomości email.
- Granularne odtwarzanie baz danych Microsoft SQL.
- Granularne odtwarzanie witryn i plików Microsoft SharePoint.
- Odtwarzanie kontrolerów domeny Microsoft Active Directory.
- Granularne odtwarzanie baz danych Oracle.
- Dla hostów VMware ESXi i Hyper-V – uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej bez konieczności odtwarzania całej maszyny na hoście. Możliwość docelowego odtworzenia uruchomionej maszyny z pliku kopii zapasowej na wybranym hoście bez przerywania jej pracy.

5. Dodatkowe wymagania związane ochroną danych:
    - Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń

6. Wymagania co do modelu licencjonowania rozwiązania:
    - Możliwość zakupu licencji subskrypcyjnych w okresie 1/3/5 lat
    - Model licencjonowania oparty na maszynach fizycznych i hostach – brak limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji)

F. Specjalistyczne oprogramowanie uwierzytelnianie wieloskładnikowe - 10 szt.

1. Rozwiązanie musi posiadać wsparcie dla systemów z rodziny Microsoft Windows Se-rver: 2008 / 2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials.
2. Rozwiązanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016.
3. Rozwiązanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 /2019.
4. Rozwiązanie musi wspierać integrację z Microsoft Remote Desktop Web Access.
5. Rozwiązanie musi wspierać integrację z Microsoft Terminal Services Web Access.
6. Rozwiązanie musi integrację z Microsoft Remote Web Access.
7. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnia-nie użytkowników dla rozwiązań VPN, które wspierają technologię RADIUS.

8. Rozwiązanie musi integrować się z systemem Windows Server poprzez konsolę MMC(Microsoft Managment Console).
9. Moduł zarządzania uwierzytelnianiem się użytkowników musi integrować się z wbudowanym w systemie Windows Server modułem do zarządzania kontami użytkowników (ADUC) w postaci dodatkowej zakładki we właściwościach użytkownika.
10. Administrator musi mieć możliwość określenia z jakiej metody uwierzytelniania użytkownicy będą korzystać:

    • dwuskładnikowe uwierzytelnianie poprzez użycie aplikacji mobilnej zainstalowanej na urządzeniu mobilnym użytkownika,
    • dwuskładnikowe uwierzytelnianie poprzez wiadomości SMS wysyłane do użytkowników,
    • klasyczna uwierzytelnianie (przy użyciu nazwy użytkownika i hasła).
11. Administrator musi mieć możliwość wysłania w postaci wiadomości SMS odnośnika, za pomocą którego użytkownik może pobrać i zainstalować dedykowaną aplikację mobilną wspierającą systemy mobilne opisane w punkcie 28 niniejszej specyfikacji.
12. Rozwiązanie nie może wymagać od użytkownika instalacji aplikacji mobilnej w telefonie - wówczas jednorazowe hasła muszą być przesyłane do użytkownika w postaci wiadomości SMS.
13. Dodatek w module ADUC musi wyświetlać informację co najmniej o dniu i godzinie ostatniej próby logowania oraz ostatniej nieudanej próby logowania użytkownika.
14. Rozwiązanie musi posiadać mechanizm zabezpieczający przed atakiem typu brute-force, które po określonej liczbie prób nieudanego logowania musi automatycznie zablokować możliwość uwierzytelnienia się dla danego użytkownika.
15. Administrator musi mieć możliwość odblokowania konta użytkownika w celu umożliwienia ponownego dostępu.
16. Administrator musi mieć możliwość wymuszenia zabezpieczenia aplikacji mobilnej za pomocą kodu PIN lub za pomocą danych biometrycznych – wówczas każdy użytkownik instalujący aplikację mobilną bez nadania kodu PIN nie będzie mógł generować jednorazowych haseł (OTP).
17. Administrator musi mieć możliwość podglądu informacji na temat:
    - aktualnego stanu licencji,
    - ilości wykorzystanych licencji (użytkowników),
    - ilości pozostałych do wykorzystania wiadomości SMS.
18. Rozwiązanie przy użyciu serwera RADUIS musi umożliwiać dostęp do zabezpieczonych zasobów za pomocą klasycznej metody uwierzytelnienia (nazwa użytkownika i hasła).
19. Administrator musi mieć możliwość wyboru, którzy użytkownicy będą korzystać z dwuskładnikowego uwierzytelniania.
20. Administrator musi mieć możliwość ograniczenia dostępu przy uwierzytelnianiu metodą RADIUS do grupy użytkowników wskazanych w konfiguracji.
21. Jednorazowe hasło (OTP) generowane przez użytkowników, powinno być unikalne i może być użyte tylko raz – nie dopuszcza się wielokrotnego użycia tego samego OTP.

22. Do wysyłania wiadomości SMS nie może być wymagane posiadanie własnej bramy SMS i centrali GSM.
23. Wysyłanie wiadomości SMS z hasłami jednorazowymi musi odbywać się z infrastruktury producenta rozwiązania.
24. Wysyłanie wiadomości musi być możliwe w przypadku telefonów pracujących w roamingu.

API i SDK

25. Producent rozwiązania musi udostępnić API pozwalające programistom na zintegrowanie rozwiązania z serwisem web lub oprogramowaniem wykorzystującym uwierzytelnianie w oparciu o usługę Active Directory.
26. Producent rozwiązania musi udostępniać SDK w celu umożliwienia programistom implementacji dwuskładnikowego uwierzytelniania dla środowisk nie wykorzystujących usługi Active Directory do uwierzytelniania użytkowników (np.wykorzystujących własną bazę danych z użytkownikami).
27. SDK musi być dostarczone zarówno dla platformy Microsoft .NET jak i języków programowania PHP i Java.

Aplikacja mobilna

28. Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.1 lub wyższej), iOS (9 lub wyższej), Windows Phone 8.1, Windows Mobile 10.
29. Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.
30. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.
31. Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego użytkowników poprzez dwuskładnikowe uwierzytelnianie.
32. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

G. Szkolenia stacjonarne w zakresie zakupionego oprogramowania – 21 h

1. ESET Advanced Administration - warsztat praktyczny (1 d x 7 h (Łącznie 7 h)) – 1 osoba
2. ESET Enterprise Inspect - Administrator XDR (1 d x 7 h (Łącznie 7 h)) – 1 osoba
3. Acronis Cyber Backup - Zaawansowana konfiguracja rozwiązania (1 d x 7 h (razem7 h)) - 1 osoba

1. Szkolenia będą organizowane stacjonarnie w na terenie województwa śląskiego.

2. Szkolenie musi być certyfikowane. Wykonawca w ramach otrzymanego wynagrodzenia zapewni uczestnikom szkolenia imienne certyfikaty potwierdzające ukończenie szkolenia i jego zakres.

3. Certyfikat ISO, spełniamy wymagania PN-EN ISO 9001-2015 m.in. w zakresie szkoleń

4. Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika szkolenia, pozwalające na samodzielną edukację z zakresu objętego szkoleniem. Zamawiający dopuszcza

dostarczenie dla każdego uczestnika szkolenia kompletu materiałów w formie elektronicznej, np. dokumenty w formacie PDF, w miejsce materiałów papierowych.
5. Wykonawca dostarczy uczestnikom szkolenia wyżej wymienione materiały szkoleniowe najpóźniej w dniu rozpoczęcia szkolenia.

6. Wszelkie koszty opracowania materiałów szkoleniowych ponosi Wykonawca.

7. Po zakończeniu szkolenia, Wykonawca dokona ewaluacji zadowolenia uczestników oraz efektywności szkolenia.

8. Wykonawca umożliwi uczestnikom skorzystanie z konsultacji po ukończeniu szkolenia 14-dniowy kontakt z trenerem po szkoleniu.