Załącznik nr 2

Obszar techniczny - zakup sprzętu, usług i oprogramowania podnoszącego poziom Planowany jest zakup sprzętu, który zapewni wyższy poziom cyberbezpieczeństwa. Projekt zakłada również zakup, wdrożenie, konfigurację i utrzymanie następującego oprogramowania: serwerowego systemu operacyjnego, wirtualizacyjnego, pozwalającego na tworzenie i zarządzanie kopiami zapasowymi, pobierania i ewidencji wybranych logów, ostrzeganie i powiadamianie o zagrożeniach i podatnościach.

I.	Klaster WIRTUALIZACYJNY HA

1.	Serwer Gwarancja 3 lata, w miejscu eksploatacji, z pozostawieniem dysku w przypadku awarii	2	szt

L.p.	Cecha	Wymagania minimalne
1	**Obudowa**	Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi) Możliwość wyposażenia serwera w ramię do prowadzenia kabli. Serwer wyposażenia w zamykany, zdejmowany panel przedni chroniący przed nieuprawionym dostępem do dysków Możliwość wyposażenia serwera w czujniki otwarcia obudowy współpracującego z BIOS/UEFI. Serwer wyposażony moduł TPM 2.0.
2	**Procesor**	Jeden procesor 16-rdzeniowy, x86 - 64 bity, Intel Xeon Gold 6426Y (2.5GHz/16-core/185W) lub równoważny procesor 16-rdzeniowy, osiągający w testach SPECrate2017_int_base powyżej 329 punktów w konfiguracji dwuprocesorowej. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org. Płyta główna wspierająca zastosowanie procesorów od 8 do 60 rdzeniowych, mocy do min. 350W i taktowaniu CPU do min. 3.6GHz.
	Liczba procesorów	Min. 1 procesor z możliwością instalacji drugiego procesora
	Pamięć operacyjna	256 GB RDIMM DDR5 4800 MT/s w modułach o pojemności 32GB każdy. Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 6TB.
	Sloty rozszerzeń	2 aktywne gniazda PCI-Express generacji 5, w tym min. 1 slot x16 (szybkość slotu – bus width) pełnej wysokości (full height). Możliwość rozbudowy do 3 slotów PCI-Express generacji 5.
	Dysk twardy	Zatoki dyskowe na 8 dysków SFF typu Hot Swap, NVMe/SAS/SATA/SSD, 2,5” i opcja rozbudowy/rekonfiguracji o dodatkowe 2 dyski typu Hot Swap, NVMe/SAS/SATA/SSD, 2,5”.. Zainstalowane dwa dyski M.2 NVMe 480GB SSD każdy, zestawione w sprzętowy RAID1, niezajmujące kieszeni na dyski 2,5”.

	Kontroler	Możliwość wyposażenia serwera w kontroler sprzętowy z min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 16 napędów dyskowych NVMe/SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie
	Karta HBA	Zainstalowana dwu-portowa karta HBA SAS12G
	Interfejsy sieciowe	Minimum 4 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.
	Karta graficzna	Zintegrowana karta graficzna
	Porty	5 x USB (w tym 1 port wewnętrzny USB 3.2 Gen1, 2 porty USB 3.2 Gen1 z tyłu serwera oraz 1 port USB 3.2 Gen1 z przodu serwera) 1x VGA Możliwość rozbudowy o: - dodatkowy port typu DisplayPort dostępny z przodu serwera - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45
	Napęd	Możliwość instalacji wewnętrznego napędu DVD-ROM lub DVD-RW
	Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1000W.
	Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia mininmalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego

		• obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB i i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power caping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającejj (DNS/DHCP)
	Diagnostyka	Elektroniczny panel diagnostyczny dostępny z przodu serwera pozwalający uzyskać informacje o stanie: procesora, pamięci, wentylatorów, kary sieciowej, zasilaczy, kartach rozszerzeń, temperaturze.
	Wsparcie techniczne	3-letnia gwarancja producenta w miejscu instalacji z czasem reakcji w miejscu instalacji w ciągu następnego dnia roboczego od zgłoszenia usterki. Możliwość zgłaszania awarii w trybie 24x7. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera.

	Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
1.1	**Prace instalacyjne i konfiguracyjne**	1 **szt**
	Migracja danych	Zamawiający wymaga przeniesienia środowisk, systemów dziedzinowych firmy REKORD, a także plików i danych z obecnie wykorzystywanych serwerów na nowe, dostarczone serwery. Środowiska wymagane do przeniesienia, w których działają systemy dziedzinowe, obejmują: PostgreSQL, MySQL oraz Firebird. Proces przenoszenia systemów nie może powodować zakłóceń w bieżącej pracy użytkowników systemów dziedzinowych. Po zakończeniu przeniesienia Zamawiający wymaga przeprowadzenia testów weryfikujących poprawność działania całego środowiska oraz wszystkich systemów dziedzinowych.

2.	Macierz Gwarancja 3 lata, w miejscu eksploatacji, z pozostawieniem dysku w przypadku awarii	1	szt

L.p.	Cecha	Wymagania minimalne
1.	**Typ obudowy**	Przystosowana do montażu w szafie rack 19”.
2.	**Przestrzeń dyskowa**	Macierz musi być wyposażona w minimum 10 dysków SAS SSD o pojemności minimum 1,92 TB każdy.
3.	**Możliwość rozbudowy**	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 240 dysków twardych.
4.	**Obsługa dysków**	Macierz musi obsługiwać dyski SSD, SAS i NL SAS. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. Komunikacja z dyskami 12Gb SAS.
5.	**Sposób zabezpieczenia danych**	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5, RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych (tzw. wide-striping). Macierz musi umożliwiać utworzenie pojedynczej grupy RAID zabezpieczonej podwójną parzystością stworzonej ze 128 dysków. Konfiguracja takiej grupy RAID musi umożliwiać zmianę rozmiaru takie grupy poprzez dodawanie i odejmowanie pojedynczych dysków w trybie online bez konieczności przerywania dostępu do danych.
6.	**Tryb pracy kontrolerów macierzowych**	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe w SAS 12Gb. Kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów FC i LAN.
7.	**Pamięć cache**	Każdy kontroler macierzowy musi być wyposażony w minimum 12GB pamięci Cache, 24 GB sumarycznie w macierzy. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
8.	**Rozbudowa pamięci cache**	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.
9.	**Interfejsy do hostów**	Macierz musi posiadać, co najmniej 8 portów SAS 12Gb
10.	**Zarządzanie**	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. Wymagana możliwość autentykacji poprzez LDAP oraz funkcjonalność role-based access control.

		Wymaga się możliwości definiowania przynajmniej następujących poziomów dostępu do macierzy: • administrator – pełen dostęp, • monitor – możliwość odczytu konfiguracji.
11.	**Kreator konfiguracji**	System zarzadzania powinien posiadać funkcjonalność kreatora konfiguracji uruchamianego w przypadku braku zdefiniowanych pul dyskowych i wolumenów, w przypadku braku zdefiniowanych powiadomień oraz braku wykrycia jakichkolwiek zadań wykonywanych na macierzy.
12.	**Zarządzanie grupami dyskowymi oraz dyskami logicznymi**	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Możliwość tworzenia wolumenów logicznych o pojemności maksymalnej co najmniej 140TB. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.
13.	**Thin Provisioning**	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
14.	**Wewnętrzne kopie migawkowe**	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
15.	**Wewnętrzne kopie pełne**	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
16.	**Migracja danych w obrębie macierzy**	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 2 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy

		ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
17.	**Redundancja**	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
18.	**Dodatkowe wymagania**	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.
19.	**Inne**	Wraz z macierzą należy dostarczyć 4 szt. kabli HPE External 2.0m (6ft) Mini-SAS HD 4x to Mini-SAS HD 4x Cable
20.	**Gwarancja**	3-letnia gwarancja producenta w miejscu instalacji z czasem reakcji na następny dzień roboczy do zgłoszenia. Serwis realizowany przez polski oddział serwisu producenta. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy.

3.	**System operacyjny z obsługą wirtualizacji bez limitu maszyn wirtualnych** Subskrypcja 3 lata	1	szt

2 x Windows Datacenter 2025 lub równoważny

1	Serwerowy system operacyjny Microsoft Windows Serwer w najnowszej dostępnej wersji, minimum 2025 lub równoważny (kryteria równoważności zgodnie z pkt VIII).
2	Licencja serwerowego systemu operacyjnego musi uwzględniać wszystkie rdzenie procesorów zainstalowanych w serwerze.
3	Licencja serwerowego systemu operacyjnego musi uprawniać do uruchamiania nieograniczonej ilości serwerowych systemów operacyjnych w środowisku wirtualnym.
4	Wraz z serwerowym systemem operacyjnym należy dostarczyć 30 licencji (dotyczy łącznej ilość wymaganych licencji dostarczonych z serwerami) dostępowych dające użytkownikom prawo korzystania z usług udostępnianych przez serwer oraz umożliwiające korzystanie z jego zasobów.
5	Licencje serwerowego systemu operacyjnego nie mogą być ograniczone czasowo.

II.	INFRASTRUKTURA

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.
W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa.
W ramach rozbudowy istniejącego systemu, której celem jest rozszerzenie mechanizmów bezpieczeństwa o warstwę dostępową, wymaganym jest dostarczenie przełączników oraz innych elementów funkcjonalnych, współpracujących z istniejącym rozwiązaniem,

1.	**Przełącznik serwerownia: 24x 10GBase-T slots and 2 x 100GE** Gwarancja / wsparcie 3 lata	1	szt

L.p.	Cecha	Wymagania minimalne
1.	**Typ obudowy**	Przystosowana do montażu w szafie rack 19”.
2.	**Interfejsy sieciowe**	Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: • 24 porty 10G BASE-T • 2 porty 100G QSFP28
3.	**Zarządzanie**	• Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania. • Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. • Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). • Wsparcie dla SNMP w wersjach 1-3. • Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. • Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. • Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. • Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). • Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. • Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. • Automatycznie wykonywane rewizje konfiguracji.
4.	**Parametry wydajnościowe**	• Przepustowość urządzenia - min. 880 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 1300 Mpps. • Tablica adresów MAC o pojemności co najmniej 64 k wpisów.

		• Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
5.	**Wymagane funkcje**	• Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. • Obsługa Jumbo Frames. • Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). • Agregacja portów zgodna ze standardem 802.3ad. • Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. • Obsługa routingu statycznego. • Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP. • Port-mirroring. • Uwierzytelnianie 802.1x na poziomie portu. • Uwierzytelnianie 802.1x w oparciu o adres MAC. • W ramach 802.1x wsparcie dla dedykowanego VLANu dla gości (guest VLAN). • W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. • W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. • Obsługa protokołu sFlow.
6.	**Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC**	1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: • Centralne zarządzanie konfiguracją urządzenia. • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania. • Centralne zarządzanie sieciami VLAN. • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u. • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. • Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. • Automatyczna detekcja i rekomendacje konfiguracji. • Przesyłanie logów na zewnętrzny serwer syslog.

		• Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. • Obsługa białych i czarnych list adresów MAC. • Wykrywanie aplikacji komunikujących się w sieci. 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
7.	**Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa**	1. System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. 2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
8.	**Gwarancja oraz wsparcie**	System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne
9.	**Dodatkowe wymagania**	Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

2.	**Przełącznik dla urządzeń 48 x GE port + 4SFP** Gwarancja / wsparcie 3 lata	4	szt

L.p.	Cecha	Wymagania minimalne
1.	**Typ obudowy**	Przystosowana do montażu w szafie rack 19”.
2.	**Zasilanie**	• Zasilanie AC 230V. • Maksymalny pobór mocy: 60 W.
3.	**Interfejsy sieciowe**	Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: • 48 porty 10Ge BASE-T • 4 porty 10GE SFP+
4.	**Zarządzanie**	• Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). • Wsparcie dla SNMP w wersjach 1-3 • Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. • Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. • Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. • Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). • Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. • Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. • Automatycznie wykonywane rewizje konfiguracji.
5.	**Parametry wydajnościowe**	• Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. • Tablica adresów MAC o pojemności co najmniej 32k wpisów. • Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
6.	**Wymagane funkcje**	• Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. • Obsługa Jumbo Frames. • Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). • Agregacja portów zgodna ze standardem 802.3ad. • Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.

		• Obsługa routingu statycznego. • Port-mirroring. • Uwierzytelnianie 802.1x na poziomie portu. • Uwierzytelnianie 802.1x w oparciu o adres MAC. • W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). • W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. • W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. • Obsługa protokołu sFlow.
7.	**Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC**	1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: • Centralne zarządzanie konfiguracją urządzenia • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania • Centralne zarządzanie sieciami VLAN. • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. • Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. • Automatyczna detekcja i rekomendacje konfiguracji. • Przesyłanie logów na zewnętrzny serwer syslog. • Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. • Obsługa białych i czarnych list adresów MAC. • Wykrywanie aplikacji komunikujących się w sieci. 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

8.	**Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa**	1. System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. 2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
9.	**Gwarancja oraz wsparcie**	System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne
10.	**Dodatkowe wymagania**	Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

III.	KOPIE ZAPASOWE

1.	**Oprogramowanie do wykonywania kopii zapasowych wraz z menedżerem backupu** Wsparcie 3 lata	5	szt

L.p.	Cecha	Wymagania minimalne
1.	Ogólne	Rozwiązanie musi pozwalać na instalację na następujących platformach: - RedHat Enterprise Linus 8.x/9.x (wymagana licencja) - CentOS Linux Stream 8/9 - Rocky Linux 8.x/9.x - Alma Linux 8.x/9.x - Oracle Linux 8.x/9.x - SUSE Linux Enterprise Server 15 - Debian 12.5 - Ubuntu Server 22.04
		Rozwiązanie musi mieć możliwość konfigurowania liczby równoległych wątków wykonujących zadania tworzenia kopii zapasowej i odtwarzania
		Rozwiązanie musi umożliwiać bezagentowe (bez konieczności instalowania agenta w zabezpieczanym systemie operacyjnym)
		Mechanizm tworzenia oraz odtwarzania maszyn wirtualnych musi być spójny dla wszystkich wymienionych platform wirtualizacyjnych pod kątem konfiguracji.
		Architektura rozwiązania powinna umożliwiać skalowanie horyzontalne (ang. scale-out) komponentów realizujących proces kopii zapasowej (ang. data-mover)
		System powinien przechowywać wszystkie metadane kopii zapasowych w relacyjnej bazie danych
		System powinien umożliwiać konfigurację w klastrze active-passive (komponent zarządzający rozwiązaniem)
		System powinien umożliwiać pracę w trybie autonomicznym (bez konieczności instalowania innych systemów backupów)
		Rozwiązanie musi umożliwić zarówno ręczne odtworzenie pojedynczej maszyny wirtualnej jak I zaplanowanie masowego odtworzenia wielu maszyn wirtualnych do wskazanego z góry środowiska (na żądanie oraz cyklicznie z opcją nadpisania istniejących maszyn wirtualnych)
		Rozwiązanie musi umożliwiać składowanie kopii zapasowej maszyn wirtualnych w 2 lokalizacjach
		Rozwiązanie musi umożliwiać definiowanie ustawień retencji bezpośrednio w polityce backupu dla maszyn wirtualnych, aplikacji i instancji pamięci masowej, tak żeby różne ich grupy instancji mogły używać innych ustawień retencji
		Rozwiązanie musi umożliwiać wysyłanie powiadomień w przypadku niepowodzenia operacji wykonania kopi zapasowej lub jej odtworzenia, powiadomienia powinny być dostępne w formie wiadomości e-mail, Slack, własnego serwisu REST API (pod wskazany endpoint POST)

		Rozwiązanie powinno umożliwiać automatyczne wysyłanie raportów do centralnej bazy producenta (opcjonalnie z zawartością logów) w celu usprawnienia diagnostyki i świadczenia wsparcia przez producenta

2.	Wirtualizacja Hyper-V	Obsługa Hyper-V w wersji: 20H2, 21H2, 22H2, 23H2
		Wykonywanie przyrostowych kopii zapasowych w oparciu o technologie RCT.
		Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji
		Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej
		Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI.
		Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej
		Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki)
		Możliwość tworzenia pełnych kopii zapasowych maszyn wirtualnych w oparciu o migawki (ang. snapshot)
		Możliwość automatycznego wykonania polecenia na maszynie wirtualnej (której kopia zapasowa jest wykonywana) bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej.
		Możliwość wykonywania cyklicznie migawek maszyny wirtualnej bez eksportu danych i ich automatyczna rotacja (usuwanie najstarszych – polityka powinna umożliwiać wskazanie liczby migawek i okres przez jaki powinny być przetrzymywane)
		Możliwość automatycznego uruchomienia maszyny wirtualnej po zakończonym procesie odtworzenia.
		Możliwość zrównoleglania transferu pojedynczego dysku podczas wykonywania kopii zapasowej jak i odtworzenia
		Rozwiązanie musi umożliwiać podpięcie interfejsów sieciowych maszyny wirtualnej do wybranych sieci w docelowym środowisku
		Rozwiązanie musi umożliwiać natychmiastowe odtworzenie z dostępem do zasobów maszyny wirtualnej (bez konieczności kopiowania danych do docelowego środowiska przed pierwszym uruchomieniem) i w razie potrzeby zainicjować migrację danych z rozwiązania kopii zapasowej do pamięci masowej środowiska docelowego
		Rozwiązanie musi umożliwiać bezpośredni transfer danych do Dell Data Domain z użyciem DD Boost API
3.	Vmware vSphere/ESXi	Obsługa Vmware vSphere/ESXi w wersji: 6.5, 6.7, 7.0, 8.0
		Wykonywanie kopii zapasowych w oparciu o technologie NBD & HotAdd.
		Wykonywanie przyrostowych kopii zapasowych z wykorzystaniem mechanizmu CBT.
		Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji
		Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej
		Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI.
		Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej

		Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki)
		Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o przypisane w środowisku tagi.
		Możliwość automatycznego wykonania polecenia na maszynie wirtualnej (której kopia zapasowa jest wykonywana) bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej.
		Możliwość wykonywania cyklicznie migawek maszyny wirtualnej bez eksportu danych i ich automatyczna rotacja (usuwanie najstarszych – polityka powinna umożliwiać wskazanie liczby migawek i okres przez jaki powinny być przetrzymywane)
		Możliwość użycia migawek spójnych na poziomie aplikacji (ang. quiesced snapshot) przy wykonywaniu kopii zapasowej
		Rozwiązanie musi umożliwiać podpięcie interfejsów sieciowych maszyny wirtualnej do wybranych sieci w docelowym środowisku
		Możliwość odtworzenia maszyn wirtualnych z wykorzystaniem mechanizmu natychmiastowego odtworzenia (Instant restore)
		Wsparcie dla migracji „na żywo” przestrzeni dyskowej dla odtwarzanych maszyn wirtualnych (storage live migration)
		Możliwość automatycznego uruchomienia maszyny wirtualnej po zakończonym procesie odtwarzania.
		Rozwiązanie musi wspierać technologię Distributed Virtual Switch
4.	Nutanix AHV	Obsługa Nutanix Acropolis opartych o wirtualizatora AHV w wersji: 5.5, 5.6, 5.8, 5.9, 5.10, 5.11, 5.15, 5.16, 5.17, 5,18, 5.19, 5.20, 6.0, 6.1, 6.5, 6.6, 6.7, 6.8
		Możliwość wykonania przyrostowych kopii zapasowej w oparciu o mechanizm CBT.
		Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji
		Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej
		Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI.
		Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej
		Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki
		Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o przypisane w środowisku tagi (gdy używamy Prism Central).
		Możliwość tworzenia pełnych kopii zapasowych maszyn wirtualnych w oparciu o migawki (ang. snapshot)
		Możliwość użycia migawek spójnych na poziomie aplikacji (ang. application-consistent snapshot) przy wykonywaniu kopii zapasowej)
		Możliwość automatycznego wykonania polecenia na maszynie wirtualnej (której kopia zapasowa jest wykonywana) bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej.

		Możliwość wykonywania cyklicznie migawek maszyny wirtualnej bez eksportu danych i ich automatyczna rotacja (usuwanie najstarszych – polityka powinna umożliwiać wskazanie liczby migawek i okres przez jaki powinny być przetrzymywane)
		Rozwiązanie musi umożliwiać podpięcie interfejsów sieciowych maszyny wirtualnej do wybranych sieci w docelowym środowisku
		Możliwość automatycznego uruchomienia maszyny wirtualnej po zakończonym procesie odtwarzania.
5.	Kubernetes	Obsługa Kubernetes od wersji 1.19.
		Możliwość tworzenia pełnych kopii zapasowych wdrożeń (deployments) w oparciu o migawki (ang. snapshot), gdy wolumeny (ang. Persistent Volumes) używają jest Ceph RBD oraz plikowego backupu (bez użycia migawek), gdy wolumeny (ang. Persistent Volumes) używają NFS
		Możliwość wykonania przyrostowych kopii zapasowej, gdy wolumeny (ang. Persistent Volumes) używają jest Ceph RBD
		Możliwość odtworzenia całego wdrożenia (deployment) na środowisko wirtualizacji
		Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej, gdy wolumeny (ang. Persistent Volumes) używają jest Ceph RBD.
		Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI, gdy wolumeny (ang. Persistent Volumes) używają jest Ceph RBD.
		Możliwość pominięcia wybranych dysków wdrożenia z kopii zapasowej
		Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki)
		Możliwość automatycznego przypisywania polityk do wdrożeń w oparciu o przypisane w środowisku etykiety (ang. label).
		Możliwość automatycznego wykonania polecenia wewnątrz wdrożenia (którego kopia zapasowa jest wykonywana) bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej.
		Rozwiązanie powinno umożliwiać zabezpieczenie bazy danych metadanych środowiska (etcd)
		Możliwość tworzenia pełnych kopii zapasowych wdrożeń w oparciu o migawki (ang. snapshot), gdy wolumeny (ang. Persistent Volumes) używają jest Ceph RBD oraz plikowego backupu (bez użycia migawek), gdy wolumeny (ang. Persistent Volumes) używają NFS
6.	Red Hat OpenShift	Obsługa Red Hat OpenShift od wersji 4.3.
		Możliwość tworzenia pełnych kopii zapasowych wdrożeń/konfiguracji wdrożeń (deployments/deployments config) w oparciu o migawki (ang. snapshot), gdy wolumeny (ang. Persistent Volumes) używają jest Ceph RBD oraz plikowego backupu (bez użycia migawek), gdy wolumeny (ang. Persistent Volumes) używają NFS
		Możliwość wykonania przyrostowych kopii zapasowej, gdy wolumeny (ang. Persistent Volumes) używają jest Ceph RBD

		Możliwość odtworzenia całego wdrożenia/konfiguracji wdrożenia na środowisko wirtualizacji
		Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej, gdy wolumeny (ang. Persistent Volumes) używają jest Ceph RBD.
		Możliwość udostępnienia dysków wdrożeń/konfiguracji wdrożeń w kopii zapasowej do innych systemów poprzez protokół iSCSI, gdy wolumeny (ang. Persistent Volumes) używają jest Ceph RBD.
		Możliwość pominięcia wybranych dysków wdrożenia/konfiguracji wdrożenia z kopii zapasowej
		Możliwość automatycznego przypisywania polityk do wdrożeń/konfiguracji wdrożeń w oparciu o reguły nazewnictwa (np. wdrożenia/konfiguracje o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki)
		Rozwiązanie powinno umożliwiać zabezpieczenie bazy danych metadanych środowiska (etcd)
		Możliwość automatycznego przypisywania polityk do wdrożeń/konfiguracji wdrożeń w oparciu o przypisane w środowisku etykiety (ang. label).
		Możliwość automatycznego wykonania polecenia wewnątrz wdrożenia (którego kopia zapasowa jest wykonywana) bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej.
		Wsparcie dla interfaceu OpenShift API for Data Protection (OADP).
7.	OpenShift Virtualization	Obsługa OpenShift Virtuzlization od wersji 4.11
		Możliwość tworzenia pełnych kopii zapasowych maszyn wirtualnych w oparciu o migawki (ang. snapshot), wolumeny (ang. Persistent Volumes) opartych o system plików lub urządzenia blokowe
		Możliwość tworzenia przyrostowych kopii zapasowych maszyn wirtualnych w oparciu o migawki (ang. snapshot), wolumeny (ang. Persistent Volumes) opartych o system plików lub urządzenia blokowe
		Możliwość tworzenia przyrostowych kopii zapasowych dla serwera wirtualizacji nieposiadającego własnego rozwiązania CBT API
		Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji
		Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej
		Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI.
		Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej
		Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki)
		Rozwiązanie powinno mieć możliwość wykonania kopii zapasowej bazy metadanych środowiska
		Rozwiązanie musi posiadać możliwość automatycznego przypisywania polityk do środowisk wirtualnych na podstawie etykiet przypisanych w konsoli środowiska.
		Możliwość automatycznego wykonania polecenia na maszynie wirtualnej (której kopia zapasowa jest wykonywana) bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej.

		Wsparcie dla interfaceu OpenShift API for Data Protection (OADP) do pobierania metadanych dla maszyn wirtualnych
8.	Azure Cloud	Możliwość tworzenia pełnych kopii zapasowych maszyn wirtualnych w oparciu o migawki (ang. snapshot)
		Możliwość wykonania przyrostowych kopii zapasowej w oparciu o mechanizm CBT
		Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji
		Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej
		Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI.
		Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej
		Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki)
		Rozwiązanie musi posiadać możliwość dostosowania przestrzeni dyskowej podczas przywracania maszyn wirtualnych (lokalizacja i opcja wykluczenia dysku)
9.	Azure Stack HCI	Obsługa Azure Stack HCI w wersji: 20H2, 21H2, 22H2, 23H2
		Wykonywanie przyrostowych kopii zapasowych w oparciu o technologie RCT.
		Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji
		Możliwość tworzenia przyrostowych kopii zapasowych dla serwera wirtualizacji nieposiadającego własnego rozwiązania CBT API
		Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej
		Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI.
		Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej
		Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki)
		Możliwość tworzenia pełnych kopii zapasowych maszyn wirtualnych w oparciu o migawki (ang. snapshot)
		Możliwość automatycznego wykonania polecenia na maszynie wirtualnej (której kopia zapasowa jest wykonywana) bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej.
		Możliwość wykonywania cyklicznie migawek maszyny wirtualnej bez eksportu danych i ich automatyczna rotacja (usuwanie najstarszych – polityka powinna umożliwiać wskazanie liczby migawek i okres przez jaki powinny być przetrzymywane)
		Możliwość automatycznego uruchomienia maszyny wirtualnej po zakończonym procesie odtworzenia.
		Możliwość zrównoleglania transferu pojedynczego dysku podczas wykonywania kopii zapasowej jak i odtworzenia
		Rozwiązanie musi umożliwiać podpięcie interfejsów sieciowych maszyny wirtualnej do wybranych sieci w docelowym środowisku
		Rozwiązanie musi umożliwiać natychmiastowe odtworzenie z dostępem do zasobów maszyny wirtualnej (bez konieczności kopiowania danych do docelowego środowiska

		przed pierwszym uruchomieniem) i w razie potrzeby zainicjować migrację danych z rozwiązania kopii zapasowej do pamięci masowej środowiska docelowego
10.	Google Cloud Platform	Możliwość tworzenia pełnych kopii zapasowych maszyn wirtualnych w oparciu o migawki (ang. snapshot)
		Możliwość wykonania przyrostowych kopii zapasowej w oparciu o mechanizm CBT
		Możliwość tworzenia przyrostowych kopii zapasowych dla serwera wirtualizacji nieposiadającego własnego rozwiązania CBT API
		Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji
		Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej
		Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI.
		Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej
		Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki)
		Możliwość automatycznego wykonania polecenia na maszynie wirtualnej (której kopia zapasowa jest wykonywana) bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej.
		Możliwość wykonywania cyklicznie migawek maszyny wirtualnej bez eksportu danych i ich automatyczna rotacja (usuwanie najstarszych – polityka powinna umożliwiać wskazanie liczby migawek i okres przez jaki powinny być przetrzymywane)
		Rozwiązanie musi posiadać możliwość dostosowania przestrzeni dyskowej podczas przywracania maszyn wirtualnych (lokalizacja i opcja wykluczenia dysku)

11.	Aplikacje	Rozwiązanie musi umożliwiać wykonanie kopii zapasowej przy użyciu natywnych poleceń zabezpieczanej aplikacji (wykonujących np. spójną kopię zapasową bazy danych) na zdalnych maszynach oraz poprzez opracowane dedykowane skrypty administracyjne bez konieczności wykonania obrazu całej maszyny wirtualnej lub instancji pamięci masowej (wolumenu lub systemu plików)
		Rozwiązanie musi umożliwiać zdefiniowanie w jaki sposób kopia zapasowa będzie wykonana (jakie polecenie, jakie parametry, gdzie znajdują się pliki do zabezpieczenia) a następnie umożliwiać wielokrotne przypisanie takiej konfiguracji do wielu instancji aplikacji z różnymi wartościami parametrów, tak aby nie było konieczności wielokrotnego podawania argumentów polecenia dla każdej z aplikacji z osobna
		Rozwiązanie musi umożliwiać wykonywanie skryptów i poleceń zarówno poprzez SSH/WinRM (zdalnie) jak i z maszyny, na której jest zainstalowane rozwiązanie producenta (tak, żeby nie było konieczności uruchamiania usług zdalnych takich jak SSH w celu wykonania kopii zapasowej)
		Rozwiązanie powinno umożliwiać wkopiowanie danych backupu do innego systemu z użyciem SSH lub WinRM – np. transfer danych kopii zapasowej z aplikacji produkcyjnej na środowisko aplikacji testowej

12.	Systemy plików	Możliwość wykonywania kopii zapasowych systemu plików podłączonego do rozwiązania (katalogi, pliki zwykłe, dowiązania symboliczne)
		Możliwość wykonania kopii zapasowej pełnej.
		Możliwość wykonania kopii zapasowej przyrostowej.
		Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej
		Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI (jako urządzenie blokowe z pojedynczym systemem plików XFS).
13.	Nutanix Files (AFS)	Możliwość wykonywania kopii zapasowych zasobów NFS/SMB udostępnionych przez Nutanix Files (AFS)
		Możliwość wykonania kopii zapasowej pełnej.
		Możliwość wykonania kopii zapasowej przyrostowej z wykorzystaniem mechanizmu śledzenia zmienionych plików (CFT).
		Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej
		Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI (jako urządzenie blokowe z pojedynczym systemem plików XFS).
14.	Nutanix Volume Groups	Możliwość wykonywania kopii zapasowych zasobów NFS/SMB udostępnionych przez Nutanix Files (AFS)
		Możliwość wykonania kopii zapasowej pełnej.
		Możliwość wykonania kopii zapasowej przyrostowej z wykorzystaniem mechanizmu śledzenia zmienionych bloków (CBT).
		Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej
		Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI

15.	Składowanie danych kopii zapasowych	Rozwiązanie musi umożliwiać wykonanie polecenia/skryptu administracyjnego przed i po dostępie do pamięci masowej – np. w celu wywołania mechanizmów replikacji danych lub wysyłania powiadomień
		Rozwiązanie musi umożliwiać synchronizację obecności kopii zapasowej w danej lokalizacji składowania z wewnętrzna bazą danych, np. gdyby ręcznie kopie zostały usunięte, nie powinny widnieć w interfejsie użytkownika; analogicznie, gdyby ponownie były dostępne, np. po tymczasowej awarii systemu plików, powinny ponownie zostać zaznaczone jako dostępne
16.		Rozwiązanie musi umożliwiać składowanie kopii zapasowej na lokalnych lub zdalnych zasobach dyskowych podmontowanych do rozwiązania jako systemy plików
		Rozwiązanie musi umożliwiać kontrolę retencji składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii)
		Rozwiązanie musi oferować deduplikację danych
		Rozwiązanie musi oferować szyfrowanie danych kluczem generowanym przez rozwiązanie
		Rozwiązanie powinno umożliwiać wykorzystanie mechanizmu ochrony przed nadpisaniem zabezpieczonych kopii zapasowych (ang. retention lock), gdy używany jest Dell PowerProtect Data Manager (DataDomain)

17.		Rozwiązanie musi umożliwiać składowanie kopii zapasowej na lokalnych lub zdalnych zasobach dyskowych podmontowanych do rozwiązania jako systemy plików
		Rozwiązanie musi umożliwiać kontrolę retencji składowania kopii zapasowych (liczba wersji, liczba dni)
		Rozwiązanie musi umożliwiać składować dane w postaci syntetycznej bez konieczności scalania przyrostowych kopii zapasowych w trakcie odtwarzania
		Rozwiązanie powinno umożliwiać wykorzystanie mechanizmu ochrony przed nadpisaniem zabezpieczonych kopii zapasowych (ang. retention lock), gdy używany jest Dell PowerProtect Data Manager (DataDomain)
18.		Rozwiązanie musi umożliwiać operacje składowania i odtwarzania kopii zapasowych na i z napędów taśmowych
		Rozwiązanie powinno korzystać z rodzajowego sterownika SCSI bibliotek taśmowych (ang. Generic SCSI Tape Driver) do zapisu danych
		Rozwiązanie musi umożliwiać definiowanie pul taśm z określonym napędem i zestawem taśm
		Rozwiązanie musi pozwalać na użycie wielu napędów taśmowych per pula (tape pool)
		Rozwiązanie musi zapewniać kompresję gzip2

	Immutable backup destination	Rozwiązanie powinno umożliwiać tworzenie niemodyfikowalnej (ang. Immutable) przestrzeni zapisu kopii zapasowych w oparciu o NFS 4.2/XFS
	Air gap backup destination	rozwiązanie powinno umożliwiać tworzenie izolowanej (ang. air gaped) przestrzeni zapisu kopii zapasowych w oparciu o zautomatyzowane połączenie do izolowanej maszyny używając NFS 4.2
	Retentio Lock for Data Domain	Rozwiązanie powinno umożliwiać zarządzenia funkcją retention lock dla przestrzeni zapisu danych kopii zapasowej opartej na Dell EMC Data Domain
	Single Sign-On	Rozwiązanie powinno być w stanie zapewnić mechanizm SSO oparty na integracji z serwerem Keycloak
	Uwierzytelniania wieloskładnikowe	Rozwiązanie musi wspierać mechanizm uwierzytelniania wieloskładnikowego (MFA)
	Szyfrowanie	Rozwiązanie musi obsługiwać algorytmy szyfrowania danych zgodne ze standardami FIPS 140-2.
	Inne	Rozwiązanie musi pozwalać na ukrycie adresów IP instancji w raportach email

	Administracja i zarządzanie	Rozwiązanie musi oferować możliwość dostępu administracyjnego za pośrednictwem interfejsu webowego (przeglądarka internetowa), tekstowego (CLI) oraz RestAPI
		Interfejsy powinny umożliwiać administratorom logowanie z użyciem poświadczeń Active Directory lub LDAP
		System powinien umożliwiać nadawanie uprawnień i dostępów administratorom do na podstawie definiowalnych ról (ang. RBAC) na poziomie globalnym systemu (sekcji interfejsu użytkownika) oraz do poszczególnych instancji środowisk wirtualnych, aplikacji i instancji pamięci masowych (wolumenów lub systemów plików)
	Interfejs webowy	Interfejs musi umożliwiać wyświetlenie podstawowych statystyk, czy dane środowisko wirtualne lub aplikacja jest zabezpieczona
		Interfejs musi umożliwiać wyświetlenie statystyk prędkości wykonywania kopii (ilość danych w jednostce czasu) i czasu trwania, czy dane środowisko wirtualne lub aplikacja jest zabezpieczona z podziałem na fazy wykonywania zadań kopii zapasowych (eksport danych ze środowiska i zapis w miejscu składowania danych)
		Interfejs musi umożliwiać zarządzanie bieżącymi zadaniami wykonywanymi na wszystkich węzłach (ang. data-movers) w rozwiązaniu
		Interfejs musi umożliwiać konfigurację cyklicznie przesyłanych raportów ze statusem ostatnio wykonanych kopii zapasowych
		Interfejs musi umożliwiać konfigurację cyklicznie przesyłanych raportów ze statusem kopii zapasowych, które nie powiodły się w ostatnim czasie – np. w ciągu ostatnich kilkunastu minut, niedostępności komponentu wykonującego kopie zapasowe (ang. data-mover)
		Interfejs musi umożliwiać wyświetlenie statystyk takich jak rozmiar kopii zapasowej oraz czas potrzebny na wykonanie kopii zapasowej

		lub odtworzenia w perspektywie czasu, np. w celu analizy przyrostu rozmiarów backupu lub czasu jego wykonywania
		Interfejs powinien umożliwiać raportowanie zajętość przestrzeni dyskowej w miejscach składowania danych z podziałem na środowiska wirtualne, polityki, maszyny wirtualne, instancje pamięci masowej
		Interfejs musi umożliwiać centralne zarządzanie konfiguracją komponentów realizujących proces kopii zapasowej (ang. data-mover), danych dostępowych i metod wykonywania kopii zapasowych wirtualizatorów oraz konfiguracji miejsc składowania danych
		Interfejs musi umożliwiać wykonanie na żądanie kopii zapasowej wskazanego środowiska, aplikacji lub instancji pamięci masowej (systemu plików lub wolumenu)
		Interfejs musi umożliwiać wykonanie odtworzenia kopii zapasowej wskazanego środowiska lub instancji pamięci masowej (systemu plików lub wolumenu)
		Interfejs musi umożliwiać wykonanie operacji montowania kopii zapasowej w celu dostępu do pojedynczych plików (jeśli wspierane dla danego wirtualizatora) – odtworzenie plików lub folderów musi również odbywać się za pośrednictwem interfejsu web'owego
		Interfejs musi umożliwiać konfigurację cyklicznego wykonywania kopii zapasowej wskazanych środowisk wirtualnych, aplikacji, instancji pamięci masowej (systemu plików lub wolumenu), migawek środowisk wirtualnych oraz okresowego przywracania wskazanych maszyn wirtualnych
		Harmonogramy cyklicznego wykonywania kopii zapasowych, migawek i przywracania środowisk wirtualnych powinny umożliwiać wskazywanie: godziny rozpoczęcia, dni tygodnia oraz ich kolejne wystąpienie w miesiącu (np. drugi wtorek miesiąca), miesiące
		Harmonogramy cyklicznego wykonywania kopii zapasowych, migawek i przywracania środowisk wirtualnych powinny umożliwiać interwałowe wykonywania zadania - wskazywanie: godziny rozpoczęcia, i godziny zakończenia i odstępu
		Interfejs musi umożliwiać monitorowanie na żywo postępu i ewentualne anulowanie zadań wykonywanych przez rozwiązanie
		Interfejs musi umożliwiać szybkie wyszukiwanie elementów konfiguracji, środowisk wirtualnych, aplikacji i instancji pamięci masowej (systemu plików lub wolumenu)
		Interfejs musi udostępniać kreatora konfiguracji podstawowych elementów rozwiązania takich jak dodanie środowiska wirtualnego, rozwiązań pamięci masowych, polityk i harmonogramów
		Interfejs musi umożliwiać definiowanie ról i nadawanie uprawnień grupom użytkownikom do poszczególnych sekcji interfejsu graficznego oraz granularnie na poziomie pojedynczej zabezpieczanej instancji (RBAC)
		Interfejs powinien umożliwiać wykonanie testu połączenia ze środowiskiem zabezpieczanym oraz miejsca składowania kopii zapasowych
		Rozwiązanie powinno posiadać interface zarządzania przez WWW w języku polskim

	Interfejs tekstowy	Interfejs musi umożliwiać wyświetlenie podstawowych statystyk, czy dane środowisko wirtualne lub aplikacja jest zabezpieczona
		Interfejs musi umożliwiać wykonanie na żądanie kopii zapasowej wskazanego środowiska, aplikacji, lub instancji pamięci masowej (systemu plików lub wolumenu)
		Interfejs musi umożliwiać wykonanie na odtworzenia kopii zapasowej wskazanego środowiska lub instancji pamięci masowej (systemu plików lub wolumenu)
		Interfejs musi umożliwiać wykonanie operacji montowania kopii zapasowej w celu dostępu do pojedynczych plików (jeśli wspierane dla danego wirtualizatora) – odtworzenie plików lub folderów musi wówczas odbywać się bezpośrednio ze wskazanej ścieżki na systemie rozwiązania
		Interfejs musi umożliwiać konfigurację cyklicznego wykonywania kopii zapasowej wskazanych środowisk wirtualnych lub aplikacji, migawek środowisk wirtualnych oraz okresowego przywracania wskazanych maszyn wirtualnych
		Interfejs musi umożliwiać monitorowanie postępu i ewentualne anulowanie zadań wykonywanych przez rozwiązanie
		Interfejs musi mieć funkcję uzupełniania poleceń
		Interfejs musi mieć możliwość pracy w trybie interaktywnym
		Interfejs tekstowy musi być umożliwiać wykonywanie poleceń w trybie nie-interakcyjnym (z poziomu skryptu)
	Interfejs programistyczny (API)	Rozwiązanie musi umożliwiać pełną konfigurację, wykonywanie wszystkich operacji oraz odczyt wszystkich dostępnych statystyk z poziomu API
		Rozwiązanie musi udostępniać wszystkie API z użyciem technologii REST i JSON

2.	**Urządzenie backup** Gwarancja 3 lata	1	szt

LP		**Wymagane minimalne parametry**
1	**Typ obudowy**	Przystosowana do montażu w szafie rack 19”.
2	Przestrzeń dyskowa	• Możliwość instalacji dysków 3,5” typu Hot-Plug • Minimum 8 dysków HDD 12TB 7,2 rpm SATA III, zgodnych z systemami NAS • Możliwość rozbudowy przestrzeni użytkowej do minimum 100 TB • Możliwość instalacji dysków twardych SATA/SAS (HDD/SSD) • RAID: 0, 1, 5, 6, 10, 50, 60
3	Procesor	wielordzeniowy osiągający w teście PassMark CPU Mark wynik minimum 13.500 pkt według danych ze strony https://www.cpubenchmark.net/cpu_list.php
4	Pamięć RAM	• Zainstalowana minimum 16 GB • Możliwość rozbudowy pamięci do minimum 64 GB
5	Interfejsy	• Minimum 2 porty USB w tym co najmniej dwa w wersji 3.0 lub nowszej • Porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń. • Zamawiający dopuszcza w serwerach stosowanie dodatkowych portów z wykorzystaniem certyfikowanych modułów rozszerzeń obudowy pod warunkiem ich dostarczenia. Porty nie mogą zostać osiągnięte poprzez zewnętrzne adaptery i przejściówki, nie mogą również zajmować slotów kart rozszerzeń PCI-E oraz wnęk na dyski.
6	Interfejsy sieciowe	• Minimum dwa interfejsy sieciowe 2,5 Gb Ethernet Base-T.
7	Zasilanie	• Zasilacze redundantne Hot Plug, każdy o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia o sprawności minimum 92% każdy przy 50% obciążeniu, pracujące w sieci 230V 50/60Hz prądu zmiennego.

IV.	ZASILANIE AWARYJNE

1.	**Zasilacz awaryjny dla serwerów** Gwarancja 3 lata	1	szt

LP	Cecha	Wymagane minimalne parametry
1	Obudowa	typu RACK o wysokości maksymalnej 4U
2	Technologia	UPS liniowa interaktywna
3	Napięcie wejściowe	AC 230 V
4	Częstotliwość wyjściowa	47 - 63 Hz
5	Zakres napięcia wyjściowego	AC 140 - 280 V
6	Złącza wejściowe:	1 x zasilanie IEC 60320 C20
7	Złącza wyjściowych zasilania	Min. 8 x power IEC 60320 C13 2 x zworka IEC min. 2 x zasilanie IEC 60320 C19
8	Napięcie wyjściowe	AC 230 V 47 - 63 Hz
9	Zasilanie	2700 wat / 3000 VA
10	Kształt fali wyjściowej:	Sinusoida
11	Eliminowanie zakłóceń:	Tak
12	Klasyfikacja energetyczna	645 dżule
13	Zabezpieczenie obwodu:	Odcięcie obwodu
14	Wydajność:	98.5%
15	Bateria	• Ilość: 1 • Technologia Kwasowo-ołowiowy • Czas pracy (do):minimum 6.3 min przy pełnym obciążeniu Czas ładowania 3 godziny
16	Interfejsy	• 1 x USB 1 x RS-232 1 x EPO (emergency power off)
20	Gniazda rozszerzeń:	1 (całkowity) / 1 (wolna)
21	Emisja dźwięku	Max 55dB
22	Zarządzanie	Alarm dźwiękowy, wyświetlacz LCD, ochrona przed przeciążeniem, oprogramowanie do zarządzania

23	Zgodność z normami	CSA, C-Tick, GOST, UL 1449, UL 1778, VDE, IEC 60950, EN 50091-2, IRAM, RoHS, EN 50091-1, FCC Part 15 A, REACH

V. OPROGRAMOWANIE I USŁUGI

V.1. OPROGRAMOWANIE do jednolitego uwierzytelniania użytkowników logujących się do aplikacji dziedzinowych Urzędu

Dostarczenie i wdrożenie aplikacji zgodnej z funkcjonującymi systemami dziedzinowymi Zamawiającego. Dostarczona aplikacja będzie zainstalowana wewnątrz infrastruktury zamawiającego. Podstawową i bazową funkcjonalnością aplikacji jest zapewnienie jednolitego systemu logowania do aplikacji dziedzinowych funkcjonujących w UG Psary. Oprogramowanie musi być zintegrowane z logowaniem domenowym. Aplikacja musi ewidencjonować operację logowania użytkowników do systemów dziedzinowych oraz zapewnić pełną rozliczalność operacji administracyjnych. (zmiana parametrów i ustawień programowania).

Oprogramowanie musi zapewniać:

- wydzielony moduł do uwierzytelniania,
- wydzielony panel administracyjny pozwalający na instalację w sieci niedostępnej dla zwykłych użytkowników,
- osobną tożsamość użytkowników, niezależną od tożsamości bazodanowej,
- jednolite zarządzanie danymi identyfikacyjnymi użytkowników – loginy, hasła, uprawnienia do aplikacji – lista użytkowników w wydzielonej bazie danych,
- możliwość zdefiniowania wzorca danych przy tworzeniu użytkowników,
- możliwość grupowego zakładania użytkowników na podstawie danych zewnętrznych (np. z systemu kadrowego, pliku XLSX),
- możliwość zdefiniowania dowolnej ilości profili i haseł,
- możliwość przypisania profilu haseł do użytkownika,
- możliwość wskazania czasu ważności konta dla użytkownika
- możliwość wymuszania zmiany hasła przy pierwszym (kolejnym) zalogowaniu do systemu,
- możliwość ustawiania losowego hasła z powiadomieniem użytkownika przez email,
- możliwość wymuszania zmiany hasła zgodnie ze zdefiniowaną częstotliwością,
- możliwość zdefiniowana ograniczenia ilości zmian hasła przez użytkownika w okresie 30 dni,
- możliwość blokowania i odblokowywania konta użytkownika,
- możliwość określenia liczby nieudanych prób logowania, po których użytkownik zostanie zablokowany,
- możliwość wyszukiwania użytkowników,
- własny mechanizm uwierzytelniania oparty na protokole np. OpenID Connect,
- uwierzytelnianie poświadczeniami domenowymi (np. integracja z Microsoft Active Directory)
- uwierzytelnianie poświadczeniami Windows,
- obsługę Single Sing-ON (jednokrotne logowanie do wielu aplikacji),
- uwierzytelnianie oparte o tokeny,
- obsługę centralnej struktury organizacyjnej z pełną historią zmian i możliwością sprawdzania stanu na dany dzień,

- możliwość obsługi wielu organizacji z osobnymi strukturami komórek organizacyjnych,
- możliwość obsługi jednostek jako wydzielonych organizacji i jako wyróżnionych komórek
- możliwość importu danych struktury organizacyjnej z Microsoft Active Directory
- możliwość importu i synchronizacji struktury organizacyjnej i użytkowników z więcej niż jednej domeny AD
- możliwość sterowania dostępem do instancji aplikacji na poziomie organizacji
- możliwość dodania lub usunięcia pracownika w organizacji / komórce organizacyjnej,
- możliwość obsługi grup użytkowników,
- komórki organizacyjne stają się automatycznie grupami użytkowników,
- obsługę listy dostępnych instancji aplikacji,
- możliwość zdefiniowania ram czasowych dla przypisania użytkownika do aplikacji
- identyfikację instancji aplikacji poprzez identyfikatory, dozwolone adresy URL i obsługiwaną metodę uwierzytelniania,
- uwierzytelnianie instancji modułów aplikacji poprzez dedykowane identyfikatory i klucze,
- mechanizm ról do obsługi uprawnień,
- obsługiwanie ról na poziomie organizacji:
    a) Administrator – pełne uprawnienia administracyjne,
    b) Członek organizacji,
- Obsługiwane ról na poziomie aplikacji:
    a) Użytkownik instancji aplikacji – może pracować na instancji aplikacji w kontekście organizacji,
    b) Administrator instancji aplikacji – administruje całą instancją aplikacji,
    c) Administrator instancji aplikacji dla organizacji – administruje instancją aplikacji wieloorganizacyjnej w kontekście organizacji,
- pulpit administratora z obsługą:
    a) informacji o stanie kopii zapasowych
    b) informacja o stanie zdrowia usług
    c) możliwość wysyłania wiadomości i powiadomień do użytkowników
    d) możliwość stworzenia własnych linków do systemu
    e) szybkie wylogowywanie użytkowników z aplikacji przez administratora
    f) szybkie blokowanie dostępu użytkowników do aplikacji przez administratora
- Historię operacji związanej z aktywnością użytkownika:
    a) Wylogowanie,
    b) Autoryzacja,
    c) Uwierzytelnienie,
    d) Błąd uwierzytelniania,
    e) Błąd autoryzacji,
    f) Zablokowanie użytkownika,
    g) Zablokowanie z powodu osiągnięcia limitu nieudanych prób logowania,
    h) Odblokowanie użytkownika
    i) Autoryzacja dla zmiany hasła,
    j) Aktywność użytkownika,
    k) Brak autoryzacji z powodu zablokowania
- Historię operacji wykonanych przez administratora:
    a) dodanie, edycja, usuniecie komórki organizacyjnej,
    b) dodanie, edycja, usuniecie organizacji,

c) dodanie, edycja, usuniecie użytkownika,
d) edycja grupy użytkowników,
e) nadanie profilu haseł użytkownikowi,
f) nadanie użytkownikowi roli w organizacji,
g) odblokowanie użytkownika,
h) przeniesienie komórki organizacyjnej,
i) przeniesienie organizacji,
j) przypisanie użytkownika do grupy użytkowników,
k) przypisanie użytkownika do komórki organizacyjnej,
l) trwałe zablokowanie użytkownika,
m) usunięcie grupy użytkowników,
n) usunięcie komórki organizacyjnej,
o) usunięcie profilu haseł użytkownikowi,
p) usunięcie przypisania aplikacji do organizacji,
q) usunięcie użytkownika,
r) usunięcie użytkownika z grupy użytkowników,
s) usunięcie użytkownika z komórki organizacyjnej,
t) usunięcie użytkownikowi roli w organizacji,
u) utworzenie grupy użytkowników,
v) wygenerowanie i zmiana hasła użytkownika,
w) zablokowanie użytkownika,
x) zamknięcie komórki organizacyjnej,
y) zamknięcie organizacji,
z) zmiana hasła użytkownika,
aa) zmiana loginu użytkownika,
bb) zmiana ustawień globalnych.

V.2. Menadżer audytu systemowego szt.3

W ramach zadania należy dostarczyć usługę, która powinna umożliwiać prowadzenie okresowych przeglądów funkcjonowania systemu zarządzania bezpieczeństwem informacji (SZBI), a także dokumentowanie decyzji i wniosków zapadających podczas tych przeglądów. Na tej podstawie możliwe będzie planowanie działań doskonalących.

Wymagane rejestry:

- RC – Rejestr audytów / przeglądów
- RC – Rejestr działań korygujących i plan postępowania z ryzykiem
- RC – Rejestr planowania
- RC – Rejestr umów związanych z bezpieczeństwem
- RC – Dziennik administratora
- RC – Przegląd / konserwacja systemu informatycznego

V.3. Menadżer audytu danych osobowych szt.3

W ramach zadania należy dostarczyć usługę, która powinna wspierać działania związane z przetwarzaniem danych osobowych oraz zgodnością z przepisami RODO i ustawą o ochronie danych osobowych. Umożliwia prowadzenie zgłoszeń, przeglądów uprawnień oraz rejestrację zdarzeń związanych z przetwarzaniem danych.

Wymagane rejestry:

- RC – Incydenty i niezgodności
- RC – Formularz zgłoszeń
- RC – Rejestr zdarzeń bezpieczeństwa
- RC – Rejestr zgłoszeń i ewidencji usterek
- RC – Ocena dostawców
- RC – Rejestr udostępnienia danych
- RC – Rejestr uprawnień – definicje
- RC – Rejestr uprawnień – pracownicy
- RC – Rejestr wejść do serwerowni
- RC – Rejestr szkoleń
- RC – Oceny szkoleń
- RC – Słownik definicji
- RC – Normy ISO

V.4. Menadżer podatności technicznych szt.3

W ramach zadania należy dostarczyć usługę chmurową, która powinna zapewniać możliwość inwentaryzacji i nadzorowania aktywów informacyjnych, zarządzania konfiguracją i dokumentowania zasobów IT. Obejmuje również możliwość oceny wybranych aspektów bezpieczeństwa informacji oraz zgodności z KRI i innymi standardami.

Wymagane rejestry:

- RC – Rejestr aktywów
- RC – Rejestr inwentarza
- RC – Obrót pozycjami
- RC – Rejestr serwerów
- RC – Rejestr komputerów
- RC – Rejestr tabletów
- RC – Rejestr licencji / oprogramowania
- RC – Rejestr podpisów elektronicznych
- RC – Rejestr baz danych
- RC – Rejestr kopii zapasowych
- RC – Rejestr haseł i ustawień
- RC – Rejestr nośników komputerowych
- RC – Rejestr kluczy kryptograficznych
- RC – Rejestr usług systemowych
- RC – Rejestr wypożyczeń sprzętu
- RC – Rejestr podmiotów
- RC – Deklaracja stosowania (ISO 27001:2017)
- RC – Ocena wybranych aspektów bezpieczeństwa
- RC – Ocena zgodności z CERT
- RC – Ocena zgodności z KRI
- RC – Rejestr ocen zgodności z KRI / KSC
- RC – Rejestr procedur bezpieczeństwa
- RC – Standardy Cyberbezpieczeństwa
- RC – Kampanie edukacyjne