Załącznik nr 1

do Specyfikacji Warunków Zamówienia w postępowaniu Nr IR.271.1.5.2025

OPIS PRZEDMIOTU ZAMÓWIENIA

Zamówienie – dostarczenie kompleksowego i całościowego rozwiązania IT w celu polepszenia cyberbezpieczeństwa.

W ramach tego rozwiązania dostarczone zostanie rozwiązanie IT w postaci systemu zabezpieczenia danych, urządzenia do tworzenia kopii bezpieczeństwa, oprogramowania do tworzenia kopii bezpieczeństwa, systemu redundancji danych w chmurze, serwerów fizycznych, macierzy dyskowej, serwerowych systemów operacyjne i oprogramowanie bezpieczeństwa, jak też zasilanie awaryjne w postaci UPSów, systemu ochrony stacji.

Przeprowadzone zostanie również w ramach zamówienia szkolenie specjalistyczne w zakresie dostarczanych i wdrażanych rozwiązań IT.

Celem zamówienia jest zwiększenie poziomu cyberbezpieczeństwa u Zamawiającego, poprzez wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych. Celem jest wdrożenia mechanizmów i środków zwiększających na ataki z cyberprzestrzeni.

W wyniku podjętych działań przyczyniających się do sprawnego i bezpiecznego działania systemów informatycznych, podniesie się poziom cyberbezpieczeństwa.

W celu wzmocnienia odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych konieczny jest zakup sprzętu, oprogramowania i usług informatycznych w obszarze cyberbezpieczeństwa jako kompleksowego i efektywnego rozwiązania.

Skutkiem realizacji będzie skuteczne zabezpieczenie systemów informatycznych przed cyberprzestępczością w kontekście: ochrony danych osobowych (RODO), potencjalnej utraty danych, ujawnienia wrażliwych danych osobom nieuprawnionym albo umożliwienia atakującym zniszczenia dokumentów lub danych, co zapewni ciągłość pracy oraz zwiększy poczucie bezpieczeństwa.

Przedmiot obejmuje kompleksowe rozwiązanie:

1. System zabezpieczeń danych - Backup środowiska wraz z oprogramowaniem.
2. System redundancji danych w chmurze – usługa na okres do 30 czerwca 2026 r. dla 4.8 TB danych.
3. Serwer fizyczny – 2 szt. serwer fizyczny typ 1; 1 szt. serwer fizyczny typ 2.
4. Macierze dyskowe – 1 szt. macierz

5. Serwerowe systemy operacyjne i oprogramowanie bezpieczeństwa – licencje na oprogramowania pokrywające zapotrzebowanie licencyjne dostarczonych serwerów oraz 70 szt. licencji CAL.
6. Zasilanie awaryjne – 1 szt. UPS dedykowany do serwerowni, 50 szt. UPS stanowiskowych.
7. System zabezpieczeń danych.
8. Szkolenie specjalistyczne dotyczące rozwiązań wykorzystywanych w zakresie cyberbezpieczeństwa.

[System zabezpieczenia danych]

Zarządzanie i magazyny

1. Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2024 r.
2. System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu.
3. Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe:
    a. Obudowa rack rozmiar: 1u
    b. Pamięć RAM: 16 GB
    c. Przestrzeń dostępna na przechowywanie danych:minimum 24TB
    d. Osobne dyski SSD M.2 nVME działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego,
    e. Redundantne zasilanie,

       Interfejsy sieciowe: 2szt 1 Gb oraz 2 szt. 10Gb.
    f. Gwarancja NBD on-premise o czasie trwania analogicznym do trwania wsparcia technicznego.
4. Produkt dostępny w polskiej wersji językowej.
5. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
6. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków
7. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów
8. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych
9. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
10. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
11. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe
12. System zarządzania nie może być oparty o relacyjne bazy danych.

13. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
14. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
15. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
16. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.
17. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
18. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
19. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.
20. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
21. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
22. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
23. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych
24. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.
25. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
26. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
27. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
28. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało

zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.

29. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,
30. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
31. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.
32. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).
33. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.
34. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
35. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych
36. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.
37. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
38. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.
39. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
40. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
41. System musi pozwalać na automatyczne aktualizacje oprogramowania.
42. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
43. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia.
44. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.

45. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
46. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.
47. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
48. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.
49. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
50. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.
51. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
52. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
53. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
54. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental,
55. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
56. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3 oraz dedykowana chmura producenta appliance'u
57. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb,S3, nfs, iscsi, katalog lokalny
58. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).
59. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.

60. Możliwość generowania raportów dobowych w oparciu o harmonogram
61. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter powinno być zlokalizowane na terenie Polski)
62. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)
63. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.
64. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu)

Wspierane systemy

Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:

Alpine 3.10+,

Debian: 9+,

Ubuntu: 16.04+,

Fedora: 29+,

centOS: 7+,

RHEL: 6+,

openSUSE: 15+,

SUSE Enterprise Linux(SLES): 12 SP2+,

macOS: 10.13+,

Windows: 7, 8.1, 10(1607+),

Windows Server: 2008 R2+,

Środowisk wirtualnych:

Hyper-V 2016+,

VMware: 6.7+.

Środowiska fizyczne i bazy danych

1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.

2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.
3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.
4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.
5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.
6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych.
7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.
8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.
9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.
11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.
12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).
13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.
14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).

Środowiska wirtualne

1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.

2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.
3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.
4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.
5. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.
6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.
8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.

Aplikacje SaaS

1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.
2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji)
3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.
4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi
5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.
6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.
7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.
8. System musi umożliwiać zabezpieczenie środowisk Jira
9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.

Licencjonowanie i wsparcie techniczne

1. Wszystkie linie supportu muszą być obsługiwane w języku polskim.
2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta przez minimum 24 miesiące.
3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.
4. Wsparcie techniczne musi być świadczone w modelu 24/7.
5. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)
6. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.
7. W ramach wsparcia technicznego Zamawiający musi mieć dostęp do tzw. Dedicated Customer Success Managera, tj. osoby po stronie Dostawcy dedykowanej do obsługi zgłoszeń technicznych, doraźnej pomocy i bieżącej pomocy w utrzymania infrastruktury Zamawiającego.
8. W ramach dokumentacji posprzedażowej Dostawca musi dostarczyć bezpośredni numer telefonu oraz adres e-mail do Dedicated Customer Success Managera.
9. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych.
10. Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu.
11. Licencja umożliwia przechowywanie danych w chmurze dostarczonej bezpośrednio przez producenta w pakiecie przestrzeni 4.8TB na czas trwania wsparcia technicznego.

Anty-ransomware i bezpieczeństwo

1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").
2. System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System
3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.
4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent,

którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.

System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczanym urządzeniu.

[System redundancji danych w chmurze]

2 szt. licencji pozwalających na przechowywanie kopii danych w chmurze, spełniających poniższe parametry:

Element konfiguracji	**Wymagania minimalne**
Liczba procesorów	Min. 18 vCPU
Pamięć operacyjna	Min. 60GB RAM
Przestrzeń dyskowa	Min. 4.8TB SSD
Interfejsy sieciowe	Min. 1 szt. 1 Gbit/s
Transfer	Min. 30 TB z serwera Nielimitowany do serwer
Lokalizacja	W obszarze UE

Usługa powinna być świadczona na okres do 30.06.2026r.

[Serwery]

2 x serwer fizyczny typ1

Nazwa elementu, parametru lub cechy	**Opis wymagań Serwerów**
Obudowa	Do instalacji w szafie Rack 19”, wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych oraz organizatorem kabli. Zainstalowana maskownica z przodu obudowy uniemożliwiająca bezpośredni dostęp do dysków, zamykana na kluczyk. Obudowa powinna umożliwiać instalację do 10 dysków 2,5”
Procesor	Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – 12. Minimalna częstotliwość pracy procesora 2 GHz. Wynik wydajności procesora

	zainstalowanego w oferowanym serwerze nie powinien być nizszy niż 216 punktów base w teście SPECrate 2017 Integer w konfiguracji dwuprocesorowej, opublikowanym przez SPEC.org (www.spec.org). Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org.
Liczba zainstalowanych procesorów	2
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje
Pamięć operacyjna	Zainstalowane minimum 512GB pamięci RAM o częstotliwości 4800MHz. Pamięć zainstalowana w kościach maksymalnie 32GB. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.
Zabezpieczenie pamięci	Memory mirroring, ECC, SDDC, ADDDC, Bounded Fault detection / correction
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. 1 port VGA na tylnym panelu. Możliwość zainstalowania drugiego portu VGA na przednim panelu serwera.
Dyski/Rozbudowa dysków	W chwili dostawy serwer musi posiadać zainstalowane minimum 2 sztuki dysków M.2 NVMe o pojemności min. 960GB. Dyski powinny być skonfigurowane w grupę RAID 1. Minimalne parametry dysków: 1 DWPD MTBF: 2mln godzin IOPS dla odczytu (4kb bloki): 550.000 IOPS dla zapisu (4kb bloki): 60.000 Oraz minimum 6 dysków 1.92TB SSD typu HotPlug Wymagany jest wewnętrzny slot na kartę Micro SD.
Kontroler dyskowy	Możliwość rozbudowy o sprzętowy kontroler dyskowy. Kontroler powinien posiadać poziomy zabezpieczeń typu RAID 0, 1, 10, 5. Wymaga się obsługi globalnych dysków hot-spare.

Zasilacz	Minimum dwa zasilacze o mocy minimum 1100W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
Interfejsy sieciowe	Zainstalowana dwuportowa karta 10Gb Base-T. Karta nie może zajmować żadnego ze slotów PCIe. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
Sloty I/O PCIe	Serwer powinien posiadać przynajmniej 3 sloty PCIe x16 generacji 5. Poza gniazdami PCIe dodatkowy slot OCP 3.0 PCIe 5.0 x16.
Dodatkowe porty	• z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem). Dedykowany port do diagnostyki dostępny z przodu serwera. Możliwość instalacji portu VGA. • z tyłu obudowy: 2x USB 3.2, 1x USB 2.0 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9. • wewnątrz obudowy: 1x USB 3.2 Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera.
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, posiadające redundantne wirniki w każdym wentylatorze. Gwarancja poprawnego działania serwera w temperaturze 30 st. Celsjusza.
Zarządzanie	Wymaga się aby serwer posiadał diody sygnalizującę awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu. Wymaga się aby serwer posiadał port diagnostyczny z przodu obudowy umożliwiający podłączenie zewnętrznego panelu diagnostycznego LCD umożlwiającego detekcję usterek. Panel powinien umożliwiać wyświetlenie poniższych informacji: • aktywne ostrzeżenia • Status serwera • Typ oraz model serwera, numer seryjny • Wersje oprogramowania UEFI oraz modułu zarządzania • Informacje nt modułu zarządzania: nazwa hosta, adres MAC, adres IP, adres DNS

	• Dane środowiskowe: temperaturę procesora, poziom napięcia wejściowego, poziom zużycia energii • Aktywne sesje połączeniowe do interfejsu zarządzania Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe Porty). Płytka I/O musi posiadać swój własny min. 2 rdzeniowy procesor o taktowaniu min. 1.2GHz. Wymagane funkcjonalności kontrolera zdalnego zarządzania: • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna • Pozyskanie 13ostępne13cych informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarzadzajacej, utylizacja cpu, utylizacja pamięci oraz komponentow I/O, lokalizacja • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. • Wysylanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zapis video zdalnych sesji • Podmontowanie lokalnych 13ostęp z wykorzystaniem Java client • Przekierowanie kosnoli szeregowej przez IPMI • Zrzut ekranu w momencie zawieszenia systemu • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera

	• Możliwość mapowania obrazów ISO z lokalnego dysku operatora • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS • Możliwość zamontowania minimum 4 obraów ISO jednocześnie w czasie jednej sesji • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę • Możliwość zdefiniowania minimum 12 użytkowników lokalnych na karcie zarządzającej • wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API • Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. • Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. • Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. • Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. • Możliwość monitorowania i zarządzania grupą serwerwów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200. Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: - zarzadzanie infrastruktura serwerówi storage bez udziału dedykowanego agenta - przedstawianie graficznej reprezentacji zarządzanych urządzeń

	- możliwość skalowania do minimum 1000 urządzeń - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2 - wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych - udostępnianie szybkiego podgląd stanu środowiska - udostępnianie podsumowania stanu dla każdego urządzenia - tworzenie alertów przy zmianie stanu urządzenia - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, - konsola zarzadzania oparta o HTML 5 - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne 15ostępne na stronie producenta oferowanego rozwiązania - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań - definiowanie roli użytkowników oprogramowania - obsługa REST API oraz Windows PowerShell - obsługa SNMP, SYSLOG, Email Forwarding - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML - obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami - przedstawianie historycznych aktywności użytkowników -blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń bedacych w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv - Obsluga NTP

	- przesyłanie alertów do konsoli firm trzecich - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń) - instalowanie systemów operacyjnych oraz wirtualizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesylem plików diagnostycznych, Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: Vmware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk. Jeżeli oprogramowanie wymaga dodatkowej licencji, powinna zostać ona dostarczona wraz z serwerem. Jeżeli licencja jest ograniczona czasowo, okres powinien pokrywać długość gwarancji serwera.
Funkcje zabezpieczeń	Zainstalowany czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0. Zainstalowany przedni panel zabezpieczający, zamykany na klucz. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Możliwość włączania i wyłączania portów USB na obudowie z poziomu UEFI. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji
Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.
Obsługa	Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów

	dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych.
Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu odbywa się poprzez dedykowany port USB na froncie serwera.
Systemy operacyjne	Microsoft Windows Server 2019, 2022, 2025; Red Hat Enterprise Linux 8.6, 8.7, 9.0, 9.1, SUSE Linux Enterprise Server 15 SP4 oraz 15 Xen SP4; Vmware vSphere (ESXi) 7.0 U3, ESXI 8.x; Ubuntu 22.04 LTS
Waga	maximum: 21 kg
Gwarancja	Gwarancja producenta w trybie 24x7 z 4-godzinnym czasem naprawy po diagnozie problemu. Możliwość rozszerzenia gwarancji o gwarantowany czas naprawy w ciągu 6 godzin od zgłoszenia usterki. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: - Wykrywanie usterek sprzętowych z predykcją awarii. - Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.

1 x serwer fizyczny typ2

Nazwa elementu, parametru lub cechy	Opis wymagań Serwerów
Obudowa	Do instalacji w szafie Rack 19”, wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych oraz organizatorem kabli. Zainstalowana maskownica z przodu obudowy uniemożliwiająca bezpośredni dostęp do dysków, zamykana na kluczyk. Obudowa powinna umożliwiać instalację do 10 dysków 2,5”
Procesor	Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – 12. Minimalna częstotliwość pracy procesora 2 GHz. Wynik wydajności procesora zainstalowanego w oferowanym serwerze nie powinien być nizszy niż 216 punktów base w teście SPECrate 2017 Integer w konfiguracji

	dwuprocesorowej, opublikowanym przez SPEC.org (www.spec.org). Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org.
Liczba zainstalowanych procesorów	2
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje
Pamięć operacyjna	Zainstalowane minimum 128GB pamięci RAM o częstotliwości 4800MHz. Pamięć zainstalowana w kościach maksymalnie 32GB. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.
Zabezpieczenie pamięci	Memory mirroring, ECC, SDDC, ADDDC, Bounded Fault detection / correction
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. 1 port VGA na tylnym panelu. Możliwość zainstalowania drugiego portu VGA na przednim panelu serwera.
Dyski/Rozbudowa dysków	W chwili dostawy serwer musi posiadać zainstalowane minimum 2 sztuki dysków M.2 NVMe o pojemności min. 960GB. Dyski powinny być skonfigurowane w grupę RAID 1. Minimalne parametry dysków: 1 DWPD MTBF: 2mln godzin IOPS dla odczytu (4kb bloki): 550.000 IOPS dla zapisu (4kb bloki): 60.000 Oraz minimum 6 dysków 1.92TB SSD typu HotPlug Wymagany jest wewnętrzny slot na kartę Micro SD.
Kontroler dyskowy	Możliwość rozbudowy o sprzętowy kontroler dyskowy. Kontroler powinien posiadać poziomy zabezpieczeń typu RAID 0, 1, 10, 5. Wymaga się obsługi globalnych dysków hot-spare.

Zasilacz	Minimum dwa zasilacze o mocy minimum 1100W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
Interfejsy sieciowe	Zainstalowana dwuportowa karta 10Gb Base-T. Karta nie może zajmować żadnego ze slotów PCIe. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
Sloty I/O PCIe	Serwer powinien posiadać przynajmniej 3 sloty PCIe x16 generacji 5. Poza gniazdami PCIe dodatkowy slot OCP 3.0 PCIe 5.0 x16.
Dodatkowe porty	• z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem). Dedykowany port do diagnostyki dostępny z przodu serwera. Możliwość instalacji portu VGA. • z tyłu obudowy: 2x USB 3.2, 1x USB 2.0 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9. • wewnątrz obudowy: 1x USB 3.2 Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera.
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, posiadające redundantne wirniki w każdym wentylatorze. Gwarancja poprawnego działania serwera w temperaturze 30 st. Celsjusza.
Zarządzanie	Wymaga się aby serwer posiadał diody sygnalizującę awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu. Wymaga się aby serwer posiadał port diagnostyczny z przodu obudowy umożliwiający podłączenie zewnętrznego panelu diagnostycznego LCD umożlwiającego detekcję usterek. Panel powinien umożliwiać wyświetlenie poniższych informacji: • aktywne ostrzeżenia • Status serwera • Typ oraz model serwera, numer seryjny • Wersje oprogramowania UEFI oraz modułu zarządzania • Informacje nt modułu zarządzania: nazwa hosta, adres MAC, adres IP, adres DNS

	• Dane środowiskowe: temperaturę procesora, poziom napięcia wejściowego, poziom zużycia energii • Aktywne sesje połączeniowe do interfejsu zarządzania Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe Porty). Płytka I/O musi posiadać swój własny min. 2 rdzeniowy procesor o taktowaniu min. 1.2GHz. Wymagane funkcjonalności kontrolera zdalnego zarządzania: • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna • Pozyskanie nastepujacych informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarzadzajacej, utylizacja cpu, utylizacja pamięci oraz komponentow I/O, lokalizacja • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. • Wysylanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zapis video zdalnych sesji • Podmontowanie lokalnych mediow z wykorzystaniem Java client • Przekierowanie kosnoli szeregowej przez IPMI • Zrzut ekranu w momencie zawieszenia systemu • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera

	• Możliwość mapowania obrazów ISO z lokalnego dysku operatora • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS • Możliwość zamontowania minimum 4 obraów ISO jednocześnie w czasie jednej sesji • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę • Możliwość zdefiniowania minimum 12 użytkowników lokalnych na karcie zarządzającej • wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API • Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. • Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. • Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. • Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. • Możliwość monitorowania i zarządzania grupą serwerwów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200. Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: - zarzadzanie infrastruktura serwerówi storage bez udziału dedykowanego agenta - przedstawianie graficznej reprezentacji zarządzanych urządzeń

	- możliwość skalowania do minimum 1000 urządzeń - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2 - wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych - udostępnianie szybkiego podgląd stanu środowiska - udostępnianie podsumowania stanu dla każdego urządzenia - tworzenie alertów przy zmianie stanu urządzenia - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, - konsola zarzadzania oparta o HTML 5 - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostepne na stronie producenta oferowanego rozwiązania - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań - definiowanie roli użytkowników oprogramowania - obsługa REST API oraz Windows PowerShell - obsługa SNMP, SYSLOG, Email Forwarding - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML - obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami - przedstawianie historycznych aktywności użytkowników -blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń bedacych w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv - Obsluga NTP

	- przesyłanie alertów do konsoli firm trzecich - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń) - instalowanie systemów operacyjnych oraz wirtualizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesylem plików diagnostycznych, Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk. Jeżeli oprogramowanie wymaga dodatkowej licencji, powinna zostać ona dostarczona wraz z serwerem. Jeżeli licencja jest ograniczona czasowo, okres powinien pokrywać długość gwarancji serwera.
Funkcje zabezpieczeń	Zainstalowany czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0. Zainstalowany przedni panel zabezpieczający, zamykany na klucz. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Możliwość włączania i wyłączania portów USB na obudowie z poziomu UEFI. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji
Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.
Obsługa	Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów

	dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych.
Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu odbywa się poprzez dedykowany port USB na froncie serwera.
Systemy operacyjne	Microsoft Windows Server 2019, 2022, 2025; Red Hat Enterprise Linux 8.6, 8.7, 9.0, 9.1, SUSE Linux Enterprise Server 15 SP4 oraz 15 Xen SP4; VMware vSphere (ESXi) 7.0 U3, ESXI 8.x; Ubuntu 22.04 LTS
Waga	maximum: 21 kg
Gwarancja	Gwarancja producenta w trybie 24x7 z 4-godzinnym czasem naprawy po diagnozie problemu. Możliwość rozszerzenia gwarancji o gwarantowany czas naprawy w ciągu 6 godzin od zgłoszenia usterki. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: - Wykrywanie usterek sprzętowych z predykcją awarii. - Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.

[Macierz dyskowa]

1 sztuka macierzy dyskowej

Minimalne wymaganie dotyczące jednej sztuki macierzy.

LP	CECHA	OPIS WYMAGAŃ
1)	Obudowa	Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Maksymalna wyskość obudowy to 2U.
2)	Kontrolery dyskowe	Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active-active. Kontrolery nie mogą pracować w trybie active-passive. Macierz musi umożliwiać rozbudowę do co najmniej 4 kontrolerów. Wszystkie kontrolery muszą być zarządzane z jednego interfejsu graficznego. Nie dopuszcza się zastosowania wirtualizatora do połączenia 4 kontrolerów.
3)	Zasilanie	Oferowane urządzenie musi być przystosowane do zasilania z sieci AC oraz wyposażone w kable zasilające PDU. Macierz musi być

LP	CECHA	OPIS WYMAGAŃ
		wyposażona w zdublowany, redundantny system zasilania, umożliwiający prawidłową, nieprzerwaną pracę urządzenia w przypadku awarii dowolnego pojedynczego źródła zasilania.
4)	Redundancja	Macierz nie może posiadać pojedynczego punktu awarii (SPOF), który powodowałby brak dostępu do danych. Wszystkie krytyczne komponenty takie jak kontrolery dyskowe, pamięć, zasilacze i wentylatory muszą być zaprojektowane nadmiarowo.
5)	Wymagana przestrzeń	Fizyczna przestrzeń dyskowa zbudowana tylko i wyłącznie za pomocą SSD SAS. Przestrzeń użytkowa po zbudowaniu grupy RAID 6 z 1 dyskiem hot-spare lub przestrzenią hot-spare równą pojemności 1 dysku musi wynosić min 44 TB. Ze względów wydajnościowych oraz niezawodnościowych całej macierzy pojemność RAW pojedynczego dysku nie może być większa niż 4 TB. Wymagana pojemność użytkowa rozumiana jest jako pojemność dostępna po konfiguracji RAID i odliczeniu rezerwy na dyski/przestrzeń *spare* i dostępna dla hostów bez uwzględnienia jakichkolwiek mechanizmów kompresji, czy deduplikacji. Oferowana macierz musi umożliwiać rozbudowę do min 100 dysków tego samego typu, czyli SSD SAS bez konieczności klastrowania oferowanej macierzy z dodatkowymi kontrolerami. Nie dopuszcza zastosowania się chipsetu QLC w dyskach SSD SAS. Macierz nie może obsługiwać dysków HDD.
6)	Zabezpieczenia dyskami SPARE	Możliwość definiowania przez administratora dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.
7)	Pamięć Cache	Co najmniej 128GB pamięci cache na całą macierz (dwa kontrolery). Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin.
8)	Dostępne interfejsy front-end	Razem kontrolery muszą udostępnić minimum 8 portów 1G Eth RJ45 oraz min 8 portów 10Gb Eth z wkładkami optycznymi. Wymagana możliwość rozbudowy o 8 portów 25G Eth tylko poprzez dodanie nowych kart sieciowych.
9)	Obsługiwane protokoły	Wymagane wsparcie dla NFS, CIFS. Nie dopuszcza się spełnienia wymogu poprzez zastosowanie główki/gateway NAS.
10)	Obsługiwane typy zabezpieczenia RAID	Kontrolery wyposażone w funkcjonalność konfiguracji poziomu RAID 6 lub równoważnego tolerującego jednoczesną awarię 2 dysków.

LP	CECHA	OPIS WYMAGAŃ
11)	Thin Provisioning	Wymagana funkcjonalność tworzenia file system'ów o pojemności większej niż zajmowana fizyczna przestrzeń dyskowa (ang. ThinProvisioning). Wymagana możliwość zwiększania pojemności file system'ów w sposób online.
12)	Multi-tenancy	Wymagana możliwość logicznego podziału macierzy na wiele wirtualnych/logicznych systemów z dedykowanymi portami logicznymi, użytkownikami oraz uprawnieniami. Użytkownik danego wirtualnego/logicznego systemu nie może mieć dostępu do file system'u z innego wirtualnego/logicznego systemu.
13)	Zarządzanie	Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagany także dostęp do CLI. Zarządzanie poprzez min 2 porty 1Gb Eth typu management. Wymagane jest stałe monitorowanie stanu macierzy w tym monitorowanie wydajności obiektów takich jak: - cała macierz - kontrolery - porty front-end - porty logiczne - dyski - file systemy - hosty - CPU Pod kątem parametrów takich jak: - operacje wejścia/wyjścia IOPS - przepustowość (KB/s lub MB/s) - czas odpowiedzi (latency) - średnie użycie CPU w % dla kontrolerów Wymagana możliwość monitorowania stanu żywotności dysków SSD SAS. Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI macierzy do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych w formie wykresów graficznych. Wymagana możliwość konfigurowania zasobów macierzy. Wymagana możliwość tworzenia polityk logowania. Wymagane wsparcie multi-factor authentication do logowania się do macierzy.
14)	Kopie wewnątrz macierzy	Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych. Snapshoty muszą być wykonywanie w technologii ROW

LP	CECHA	OPIS WYMAGAŃ
		(Redirect On Write). Macierz musi umożliwiać utworzenie min 4000 snapshotów. Wymagana możliwość prezentacji folderu ze snapshotami w ramach udziału CIFS pod kątem przywracania pojedynczych plików. Wymagana możliwość przywrócenia pojedynczego pliku ze snapshota do file system'u w ramach operacji macierzy na poziomie CLI. Wymagana możliwość tworzenia harmonogramu wykonywania snapshotów. Wymagana możliwość zabezpieczenia snapshotów przed modyfikacją lub usunięciem przez wybrany okres czasu pod kątem szybkiego przywrócenia danych w przypadku ataku ransomware.
15)	Replikacja file system'ów	Możliwość zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym z wykorzystaniem portów IP. Funkcjonalność ta nie może wpływać na obciążenie serwerów podłączonych do macierzy. Macierz musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60min) lub konkretnych okien czasowych (np. w każdą sobotę o godz 20:00).
16)	Kontrola zasobów plikowych	Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni. Wymagana możliwość skonfigurowania polityki filtrowania zapisywanych plików na wystawionych udziałach CIFS/NFS poprzez wykluczenie ich konkretnych rozszerzeń. Wymagana także możliwość wskazania rozszerzeń które mogą być zapisywane. Wymagana możliwość nadawania uprawnień do określonych operacji dla wybranych użytkowników na udziałach CIFS/NFS. Wymagana możliwość ograniczenia dostępu do udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp.
17)	Ochrona zasobów plikowych	Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem na poziomie całego file system'u (WORM). Wymagana możliwość podłączenia serwera z oprogramowaniem antywirusowym celem skanowania plików wykorzystywanych przez użytkowników na zasobach wystawionych przez macierz protokołem CIFS.

LP	CECHA	OPIS WYMAGAŃ
18)	Wydajność	Model macierzy w oferowanej konfiguracji w teście wydajnościowym musi osiągnąć min 1800 MB/s przy następujących parametrach: - Zapełnienie macierzy – powyżej 70% fizycznej pojemności, - Protokół: NFSv3, - Porty: 10G, - Read: 70%, - Write: 30%, - typ workloadu: Random, - wielkość plików: 64KB, - Latency: <3ms, - RAID 6 lub równoważny
19)	Serwisowalność	Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych. Macierz przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączania. Macierz musi umożliwiać zdalne zarządzanie. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z legalnego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub partnera serwisowego lub wykonawcy. Wymagana gwarancja na w trybie 9x5 NBD onsite.

[Serwerowe systemy operacyjne i oprogramowanie bezpieczeństwa]

Zamawiający aktualnie korzysta z oprogramowania typu Microsoft Windows Server 2012 R2 i wymaga dostarczenia licencji na oprogramowanie Microsoft Windows Server 2022 Standard 64-bit PL lub nowszy w ilości umożliwiającej pokrycie zapotrzebowania licencyjnego dostarczonych serwerów + 70 licencji CAL User lub równoważny serwerowy system operacyjny.

Opis równoważności oprogramowania

Przez oprogramowanie równoważne Zamawiający rozumie oprogramowanie spełniające następujące warunki poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Wszystkie elementy systemu oraz jego licencja pochodzą od tego samego producenta.
2. Wymaga się dostarczenia odpowiedniej liczby licencji dla serwerów, 2 i 1- procesorowych, posiadających min 12 rdzeni,
3. Jeżeli wymagane jest posiadanie licencji dostępowych, należy dostarczyć licencję dla odpowiedniej liczby użytkowników.

4. Licencja na SSO zapewnia uruchomienie systemu operacyjnego w środowisku fizycznym i min. 2 w środowisku wirtualnym za pomocą wbudowanego mechanizmu wirtualizacji, bez konieczności zakupu dodatkowych licencji.
5. SSO posiada graficzny interfejs użytkownika umożliwiający jego obsługę przy pomocy klawiatury i myszy.
6. Obsługa do 48 TB RAM
7. SSO musi posiadać obsługę zdalnego pulpitu zgodnego z protokołem RDP
8. Możliwość uruchomienia posiadanego, skonfigurowanego i używanego przez Zamawiającego oprogramowania do backupu, aktualnie zainstalowanego na systemie operacyjnym Windows.
9. Pełna współpraca z procesorami o architekturze 64 bit
10. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym
11. SSO zapewniający natywne wsparcie dla środowiska .NET Framework 4.x
12. System operacyjny musi wspierać pracę domenową.
13. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory
14. Zawarta możliwość uruchomienia roli serwera DNS
15. Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory
16. Posiada wbudowaną zaporę sieciową (firewall) dla połączeń przychodzących i wychodzących z systemu.
17. Interfejsy użytkownika dostępne w wielu językach do wyboru - w tym polskim i angielskim,
18. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
19. Możliwość dokonywania bezpłatnych aktualizacji i poprawek
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
21. Zabezpieczenie hasłem dostępu do systemu, konta i profilu użytkowników,
22. Mechanizmy logowania w oparciu o login i hasło,
23. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości współbieżnej (ang. Simultaneous Multi-Threading, SMT).
24. 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).

25. 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.
26. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
27. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
28. 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).
    c. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie minimum 2 aktywnych środowisk wirtualnych systemów operacyjnych.
29. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
30. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
31. Dostarczone oprogramowanie musi być fabrycznie nowe.

Ogólne zasady oceny równoważności

1. W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne (dotyczy równoważności we wszystkich wskazanych powyżej przypadkach) nie będzie poprawnie współpracować z oprogramowaniem lub sprzętem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu rozwiązania.
2. Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązań opisanych, jako rozwiązania referencyjne, po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.
3. Wykonawca zobowiązany jest podać w ofercie co najmniej nazwę producenta, nazwę oferowanego Oprogramowania, identyfikator Oprogramowania nadawany przez jego producenta, rodzaj licencji (według oznaczenia producenta), w sposób umożliwiający Zamawiającemu jednoznaczną identyfikację i weryfikację zaoferowanego Oprogramowania oraz udowodnić, że oferowane rozwiązanie spełnia wskazane przez Zamawiającego kryteria stosowane w celu oceny równoważności.

4. Zamawiający nie dopuszcza dostarczenia licencji dla produktów równoważnych w formie upgradu czy licencji czasowej.
5. Zamawiający nie dopuszcza zaoferowania subskrypcji licencyjnej opartej o rozwiązania chmurowe.
6. W przypadku błędnego działania środowiska lub wykrytych niezgodności pod kątem spełnienia warunków OPZ po instalacji oprogramowania równoważnego Zamawiający ma prawo odstąpić od umowy.

[Zasilanie awaryjne]

1 x UPS dedykowany do serwerowni o minimalnych wymaganiach:

Moc		20 kVA 18 kW
Klasyfikacja (PN-EN IEC 62040-3)		On-Line, podwójna konwersja, VFI
Normy		PN-EN IEC 62040-1 PN-EN IEC 62040-2 PN-EN IEC 62040-3 Lub równoważne
Typ zabudowy		Tower
Wejście - zasilanie	Liczba faz	3
	Napięcie znamionowe	360 / 380 / 400 / 415 V
	Zakres napięcia	277 ÷ 485 V
	Częstotliwość znamionowa	50 / 60 Hz (autodetekcja)
	Zakres częstotliwości	40 ÷ 70 Hz
	Współczynnik mocy (PF)	≥ 0,99
	Zniekształcenia harmoniczne (THDi)	< 5 %
	Zgodność z systemem zasilania	TN
	Sposób podłączenia	3P + N + PE (listwa zaciskowa)
Wejście - (bypass)	Liczba faz	3
	Napięcie znamionowe	360 / 380 / 400 / 415 V
	Zakres napięcia	-40 / 15 %
	Częstotliwość znamionowa	50 / 60 Hz
	Zdolność przeciążeniowa bypass	102 ÷ 125 % do 20 min

		125 ÷ 150 % do 2 min > 150 % do 1 s
	Sposób podłączenia	3P + N (listwa zaciskowa)
Akumulatory	Technologia akumulatorów	VRLA / AGM
	Napięcie nominalne łańcucha akumulatorów	± 240 V DC
	Opcjonalne napięcie łańcucha akumulatorów	± 168 / 192 / 216 / 240 V DC
	Napięcie nominalne pojedynczego akumulatora	12 V DC
	Opcjonalne napięcie pojedynczego akumulatora	2÷12 V DC
	Ilość akumulatorów wewnętrznych nominalna	40 szt.
	Obsługiwane ilości akumulatorów wewnętrznych	20 ÷ 60 szt.
	Pojemność wewnętrznych akumulatorów	7 / 9 / 10 Ah
	Pojemność zewnętrznych akumulatorów	7 ÷ 250 Ah
	Montaż akumulatorów zewnętrznych	dedykowane obudowy EBM dostosowane do akumulatorów 7 / 9 / 10 Ah otwarte stojaki STB dla akumulatorów o większych pojemnościach
	Czas pracy z akumulatorów dla obciążenia 18 kW	zależny od zastosowanych akumulatorów wewnętrznych lub zewnętrznych w EBM / STB
	Prąd ładowania nominalny	3,5 ÷ 14 A
	Możliwość podłączenia zewnętrznych akumulatorów EBM / STB	tak (wyposażenie opcjonalne)
	Sposób podłączenia akumulatorów	+ / N / - oraz PE (listwa zaciskowa)
Wyjście	Liczba faz	3
	Napięcie wyjściowe	360 / 380 / 400 / 415 V (konfigurowalne)
	Tolerancja napięcia w trybie pracy z sieci	± 1 %
	Częstotliwość dla pracy z sieci	synchronizowana
	Częstotliwość dla pracy z akumulatorów	50 / 60 Hz
	Dokładność częstotliwości dla pracy z akumulatorów	± 0,1 %
	Przebieg napięcia	fala sinusoidalna
	Współczynnik mocy (PF)	0,9
	Współczynnik szczytu (CF)	3:1

	Zniekształcenia harmoniczne (THDu)	≤ 2 % (obciążenie liniowe) ≤ 5 % (obciążenie nieliniowe)
	Zdolność przeciążeniowa	102 ÷ 125 % do 10 min 125 ÷ 150 % do 1 min > 150 % do 0,5 s
	Sposób podłączenia	3P + N + PE (listwa zaciskowa)
System	Sprawność w trybie sieci	≥ 93 %
	Sprawność w trybie ECO	≥ 98 %
	Czas przełączenia	przełączenie zsynchronizowane: 0 ms
	Funkcje rozruchu	Zimny start (COLD START) Miękki start (SOFT START)
	Interfejs użytkownika	5” kolorowy ekran LCD dotykowy, graficzny z obsługą w języku polskim dwukolorowy LED sygnalizujący stan pracy
	Złącze EPO	tak
	Zabezpieczenia	zwarciowe przeciążeniowe temperaturowe
	Filtr przeciwzakłóceniowy	RFI EMI
	Alarmy	przeciążenie praca z akumulatorów niskie napięcie akumulatorów awaria wentylatorów
	Praca w trybie konwersji	CVCF
	Praca równoległa	do 6 jednostek
	EMI	PN-EN IEC 62040-2
	EMS	PN-EN 61000-4-2 PN-EN IEC 61000-4-3 PN-EN 61000-4-4

		PN-EN 61000-4-5 lub równoważne
Komunikacja	Interfejsy standardowe	USB (typ B) RS232 2 x złącze kart rozszerzeń
	Interfejsy opcjonalne	karty rozszerzeń: WEB / SNMP RS485 / MODBUS styki bezpotencjałowe
	Obsługa systemów operacyjnych	MS Windows / Linux / Unix / MacOS
Cechy	Wymiary (szer. x wys. x gł.)	350 x 1085 x 785 mm
	Waga bez akumulatorów	80 kg
	Kolor obudowy	czarny
	Temperatura pracy	0 °C ÷ 40 °C
	Wilgotność	0 ÷ 95 % (bez kondensacji)
	Głośność (@ 1 m)	65 dB
	Stopień ochrony (PN-EN 60529:2003)	IP 20
	Montaż zasilacza	pionowy, wolnostojący
	Wysokość robocza bez obniżenia mocy	0 ÷ 1000 m n.p.m.
	Wysokość robocza z obniżeniem mocy	obniżenie mocy o 1 % co 100 m w zakresie 1000 ÷ 3000 m n.p.m.

50 x UPS stanowiskowy

Minimalne wymagania techniczne dla jednostki UPS:

- Moc znamionowa 1000 VA / 600 W;

- Zasilanie 1 fazowe / wyjście 1 fazowe;

- Rodzaj obudowy zasilacza – stojący „tower”;

- Rodzaj pracy: Line Interactive z AVR i filtrami EMI.

Odbiorniki są zasilane ze źródła zasilania UPS poprzez interaktywny stabilizator napięcia AVR w celu stabilizacji skoków i zaników napięcia. Ponadto zastosowanie filtrów zakłóceń EMI pozwala na jeszcze lepsze zapewnienie bezprzerwowej pracy zasilacza. Gdy nastąpi awaria zasilania, odbiorniki

są zasilane przez falownik napięciem o charakterystyce pseudosinusoidalnej przez czas wystarczający na bezpieczne wyłączenie za pośrednictwem oprogramowania producenta.

- Czas podtrzymania: 5 minut dla 70% obciążenia;
- Typ baterii wewnętrznych: szczelne, bezobsługowe, kwasowo-ołowiowe VRLA AGM;
- Wysoka niezawodność dzięki automatycznym testom baterii;
- Częstotliwość wejściowa: 50 / 60 Hz z automatycznym wyborem;
- Napięcie wejściowe: 1 x 220 / 230 / 240 V;
- Tolerancja napięcia wejściowego :230 V ±25%;
- Napięcie wyjściowe przy pracy z sieci: 230 V (-8%/+10%);
- Napięcie na wyjściu w pracy z baterii: 230 V (±5%);
- Częstotliwość na wyjściu podczas pracy z baterii: 50 lub 60 Hz (±0,5%);
- Przebieg na wyjściu: pseudosinusoidalny;
- Sposoby komunikacji w standardzie: USB, RS232;
- Sposoby komunikacji dostępne opcjonalnie: karta SNMP;
- Gniazda wyjściowe: 4x IEC 320 C13 (10 A);
- Zabezpieczenia: zwarciowe – przeciwprzepięciowe – przeciw nadmiernemu wyczerpaniu baterii;
- Rozruch zasilacza z baterii bez obecnej sieci - tzw. „zimny start”;
- Zasilacz UPS uruchomi się automatyczne po powrocie zasilania i wyczerpaniu baterii;
- Spełnienie standardy: dyrektywy europejskie: LV 2014/35/UE dyrektywa niskonapięciowa EMC 2014/30/UE Kompatybilność elektromagnetyczna, dyrektywa Bezpieczeństwo IEC EN 62040-1, EMC IEC EN 62040-2; Zgodność z RoHS
- Wymiary zasilacza UPS z bateriami wewnętrznymi nieprzekraczające: dł. 146 mm x gł. 350 mm x wys. 160m;
- Masa zasilacza UPS z bateriami wewnętrznymi – nieprzekraczająca: 8kg;
- Wyposażanie dostarczone wraz z zasilaczem: 2 przewody do podłączenia odbiorników;
- Deklaracja zgodności CE dla oferowanego zasilacza UPS potwierdzająca zgodność wyrobu z wymaganymi dyrektywami Unii Europejskiej.

[Ochrona stacji, serwerów i poczty z XDR]

70 x licencji na oprogramowanie ESET PROTECT Enterprise ON-PREM lub dostawa licencji na oprogramowanie równoważne.

Liczba chronionych stacji roboczych, urządzeń mobilnych i serwerów łącznie: 70 szt.

Zamawiający posiada obecnie licencje ESET PROTECT Essential; klucz publiczny: 33C-S5S-DVX

Obecnie posiadana licencja jest ważna do: 2025-05-23

Licencja na oprogramowanie zostanie udzielona na okres do 30.06.2026r.

Kryteria równoważności

Oprogramowanie zaoferowane przez wykonawcę musi posiadać funkcjonalności opisane poniżej. Zamawiający dopuszcza oprogramowanie oferujące rozwiązania bardziej rozbudowane aniżeli te wskazane na poniższej liście przedstawiającej i opisującej kryteria równoważności. Dostarczone oprogramowanie musi być w pełni kompatybilne z wykorzystywanymi przez zamawiającego urządzeniami tj. : min.: Windows Serwer 2012 R2, Windows 10 Professional, Windows 11 Professional.

Kryteria równoważności (wymagane funkcjonalności):

1. Dostarczona na oprogramowanie licencja musi umożliwiać co najmniej:

1.1. Dostęp do subskrypcji aktualnych baz sygnatur.

1.2. Dostęp do najnowszej wersji oprogramowania.

1.3. Wsparcia technicznego producenta lub dystrybutora oprogramowania.

2. Parametry i funkcjonalności dostarczonego oprogramowania, nie mogą być gorsze niż wskazane poniżej:

1. System musi zapewniać ochronę antywirusową:

a) serwera plików,

b) stacji roboczych,

c) urządzeń przenośnych (smartfony, tablety).

2. Dla stacji roboczych system musi zapewniać ponadto: ochronę dostępu do sieci (firewall), zapewniać kontrolę podłączanych urządzeń (np. pamięci USB, zewnętrzne napędy, itp.).

3. Konfiguracja, nadzór nad pracą poszczególnych modułów oraz instalacja musi być wykonywana z centralnej konsoli zarządzającej (Zamawiający posiada już konsolę do zarządzania dla oprogramowania ESET PROTECT Essential ON-PREM).

4. Wsparcie techniczne musi odbywać się w języku polskim przez cały czas trwania umowy w trybie zgłoszeniowym w Dni Robocze (tj. od poniedziałku do piątku z wyłączeniem sobót, świąt i dni wolnych od pracy) na adres e-mail w godzinach od 8.00 do 16.00.

5. Zamawiający wymaga rozwiązania zgłoszonego problemu dotyczącego eksploatacji oprogramowania w ciągu 5 Dni Roboczych.

6. Moduł ochrony antywirusowej i antispyware musi poprawnie współpracować

z następującymi systemami operacyjnymi wykorzystywanymi przez Zamawiającego: Microsoft Windows (10 lub wyższą), Microsoft Windows Server (2012 R2 lub wyższą).

7. Moduł ochrony stacji roboczych musi posiadać polskojęzyczny interfejs.

8. Moduł antywirusowej i antispyware powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hackerskich, oprogramowania typu spyware

i adware, rootkit, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.

9. Moduł ochrony antywirusowej.

9.1. Ochrona antywirusowa musi być realizowana na podstawie:

a) sygnatur,

b) heurystyki (z możliwością jej wyłączenia),

c) na bieżąco weryfikowanej informacji o nowych zagrożeniach w bazie producenta dostępnej przez Internet.

9.2. Moduł musi mieć możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony.

9.3. Moduł musi umożliwiać skanowanie antywirusowe w chwili dostępu (real time), na żądanie i według harmonogramu z następującymi warunkami:

a) skanowanie na żądanie i wg harmonogramu musi mieć możliwość przerwania

w dowolnym momencie,

b) skanowanie na żądanie musi mieć możliwość wstrzymania w przypadku wykrycia pracy na baterii,
c) skanowanie na żądanie musi mieć możliwość wstrzymania w przypadku wykrycia pracy w trybie pełnoekranowym (np. prezentacja).

9.4. Moduł musi wykrywać zagrożenia: na dyskach, w plikach w tym archiwach plikowych, na stronach web, w przesyłkach email w tym w załącznikach, na podłączanych nośnikach przenośnych.

9.5. Moduł musi zapewniać ochronę komunikacji przy wykorzystaniu protokołów POP3, SMTP, IMAP w czasie rzeczywistym niezależnie od klienta pocztowego.

9.6. Moduł musi zapewniać ochronę komunikacji przy wykorzystaniu protokołu HTTP

w czasie rzeczywistym niezależnie od przeglądarki.

9.7. Moduł musi zawierać warstwę ochronną przeglądarki działającą na stacjach użytkowników i ostrzegające ich o złośliwej zawartości strony internetowej wraz

z możliwością aktywnego blokowania dostępu do wybranych stron internetowych, określonych centralnie przez administratora systemu. Rozwiązanie musi realizować także możliwość określenia blokowanych stron web na podstawie kategorii strony (np. pornografia, strony społecznościowe, itp.).

9.8. Moduł musi umożliwiać ustawienia priorytetu procesu skanowania.

9.9. Aktualizacja wzorców wirusów musi odbywać się co najmniej raz dziennie.

9.10. Moduł musi umożliwiać aktualizację wzorców wirusów z archiwum internetowego lub z centralnego punktu dystrybucji wzorców wirusów.

9.11. Moduł musi umożliwiać pobieranie aktualizacji za pośrednictwem serwera Proxy.

9.12. Po wykryciu zagrożenia musi istnieć możliwość oczyszczenia zainfekowanego pliku a jeśli nie jest to możliwe – usunięcia bądź umieszczenia go w lokalnej kwarantannie.

9.13. W przypadku zainstalowania na urządzeniach przenośnych musi nastąpić automatyczna zmiana punktu dystrybucji wzorców na archiwum internetowe bez konieczności ingerencji użytkownika.

9.14. Moduł musi umożliwiać konfigurowanie dostępności i zakresu ingerencji użytkownika w proces skanowania.

[Szkolenia specjalistyczne]

Zamówienie obejmuje szkolenia z wdrażanych rozwiązań w ramach zamówienia

1. Zamawiający wymaga aby Wykonawca zorganizował i przeprowadził szkolenie w siedzibie Zamawiającego.
2. Szkolenie ma obejmować dostarczane oprogramowania i urządzenia.
3. Warsztaty mają odbyć się w formie stacjonarnej u Zamawiającego.
4. Zamawiający wymaga aby usługa została zrealizowana w terminie realizacji zamówienia po dostarczeniu i wdrożeniu urządzeń oraz oprogramowania. Dokładny termin zostanie ustalony zgodnie z procedurą przewidzianą we wzorcu umowy.
5. Zamawiający wymaga przeszkolenia w formie warsztatów 1 uczestnika, z tym że ilość jest szacunkowa, co nie powinno wpływać na koszty.
6. Zamawiający wymaga aby w trakcie warsztatów realizowane były ćwiczenia opisujące codzienną pracę administracyjną z wdrożonym rozwiązaniem, rozwiązywaniem problemów, procedurę aktualizacji rozwiązania oraz rozbudowy o dodatkowe widoki i kanały napływu danych.
7. Zamawiający wymaga aby warsztaty zamykały się w ramach czasowych 2 dni roboczych (2x 7 godz.)
8. Zamawiający wymaga aby warsztaty kończyły się potwierdzeniem uczestnictwa w formie certyfikatu potwierdzającego odbyte szkolenie.