



## Cyberbezpieczny Samorząd

### 1) Zakup serwerów z licencjami, macierzy pamięci masowej wraz z usługami

- 1) Urządzenia muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub wystawowych.
- 2) Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.
- 3) Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.
- 4) Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.
- 5) Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.
- 6) Urządzenia na etapie dostawy pomiędzy producentem, a zamawiającym nie mogą podlegać modyfikacjom.
- 7) Cały zaoferowany sprzęt (dwa serwery i macierz) musi posiadać jeden punkt świadczenia napraw gwarancyjnych

#### Dwa serwery o poniższej charakterystyce:

| Parametr     | Charakterystyka (wymagania minimalne)  |
|--------------|--|
| Obudowa      | <ul style="list-style-type: none"><li>Obudowa Rack o wysokości max 1U z możliwością instalacji min. 4 dysków 3.5"</li><li>Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.</li><li>Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne.</li></ul>      |
| Płyta główna | <ul style="list-style-type: none"><li>Płyta główna z możliwością zainstalowania do dwóch procesorów.</li><li>Obsługa procesorów 32 rdzeniowych.</li><li>Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.</li><li>Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.</li><li>Płyta główna powinna obsługiwać do 1TB pamięci RAM.</li></ul> |
| Chipset      | <ul style="list-style-type: none"><li>Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.</li></ul>   |
| Procesor     | <ul style="list-style-type: none"><li>Zainstalowany jeden procesor 16-rdzeniowy, min. 2.8 GHz (częstotliwość bazowa), klasy x86, dedykowany do pracy z zaoferowanym serwerem, umożliwiający</li></ul>  |





## Cyberbezpieczny Samorząd

|   |  |
|---|--|
|   | osiągnięcie wyniku min. 335 w teście SPECrte2017_int_base, dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> dla konfiguracji dwuprocesorowej.   |
| <b>RAM</b>  | <ul style="list-style-type: none"><li>Minimum 256GB DDR5 RDIMM 5600MT/s,</li></ul>   |
| <b>Gniazda PCI</b>                                | <ul style="list-style-type: none"><li>minimum jeden slot PCIe x16 generacji 4</li></ul>  |
| <b>Kontroler RAID</b>                             | <ul style="list-style-type: none"><li>Sprzętowy kontroler dyskowy, posiadający<ul style="list-style-type: none"><li>Możliwość konfiguracji poziomów RAID: 0, 1, 10.</li></ul></li></ul>  |
| <b>Dyski twarde</b>                               | <ul style="list-style-type: none"><li>Zainstalowane<ul style="list-style-type: none"><li>2 x dysk SSD SATA o pojemności min. 480 GB, 6Gb, 2,5" Hot-Plug.</li></ul></li><li>Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB z możliwością konfiguracji RAID 1.</li></ul>   |
| <b>Interfejsy sieciowe/FC/SAS</b>                 | <ul style="list-style-type: none"><li>Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT</li><li>Min. 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)</li><li>Min. 2 interfejsy sieciowa 25Gb Ethernet w standardzie SFP28</li><li>W zestawie z serwerem muszą znajdować się 2 kable DAC 10GbE SFP+/SFP+ min. 3m, dostarczone przez producenta serwera</li><li>W zestawie z serwerem wykonawca dostarczy 3 patchcordsy RJ-45 cat 6 o długości minimum 3m</li></ul> |
| <b>Elementy montażowe</b>                         | <ul style="list-style-type: none"><li>Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych</li></ul>  |
| <b>Wbudowane porty</b>                            | <ul style="list-style-type: none"><li>4 porty USB w tym min:<ul style="list-style-type: none"><li>1 port USB 3.0 z tyłu obudowy,</li><li>1 port micro USB z przodu obudowy</li></ul></li><li>2 port VGA z czego jeden z przodu obudowy</li></ul>   |
| <b>Video</b>                                      | <ul style="list-style-type: none"><li>Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200</li></ul>  |
| <b>Zasilacze</b>                                  | <ul style="list-style-type: none"><li>Redundantne, Hot-Plug min. 700W klasy Titanium</li></ul>   |
| <b>System operacyjny/dodatkowe oprogramowanie</b> | <ul style="list-style-type: none"><li>Fabrycznie zainstalowany Windows Server 2025 Standard z możliwością downgrade'u do wersji 2022.</li><li>Dołączony przez producenta serwera nośnik umożliwiający instalację wersji 2022 Standard oraz 2025 Standard</li><li>Licencja pokrywająca wszystkie fizyczne rdzenie w serwerze</li></ul>  |
| <b>Bezpieczeństwo</b>                             | <ul style="list-style-type: none"><li>Zatrask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.</li><li>Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</li><li>BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła</li><li>Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</li></ul>  |





## Cyberbezpieczny Samorząd

|                          |   |
|--------------------------|---|
|                          | <ul style="list-style-type: none"><li>• Moduł TPM 2.0</li><li>• Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera</li><li>• Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem</li><li>• Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).</li><li>• Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania.</li></ul>  |
| <b>Karta Zarządzania</b> | <ul style="list-style-type: none"><li>• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą:<ul style="list-style-type: none"><li>○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</li><li>○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);</li><li>○ szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;</li><li>○ możliwość podmontowania zdalnych wirtualnych napędów;</li><li>○ wirtualną konsolę z dostępem do myszy, klawiatury;</li><li>○ wsparcie dla IPv6;</li><li>○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;</li><li>○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;</li><li>○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;</li><li>○ integracja z Active Directory;</li><li>○ możliwość obsługi przez dwóch administratorów jednocześnie;</li><li>○ wsparcie dla automatycznej rejestracji DNS;</li><li>○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.</li><li>○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera</li><li>○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera</li></ul>oraz z możliwością rozszerzenia funkcjonalności o:<ul style="list-style-type: none"><li>○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej</li><li>○ Przesyłanie danych telemetrycznych w czasie rzeczywistym</li><li>○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze</li></ul></li></ul> |





## Cyberbezpieczny Samorząd

|                                      |  |
|--------------------------------------|--|
| <b>Oprogramowanie do zarządzania</b> | <ul style="list-style-type: none"><li>○ Automatyczna rejestracja certyfikatów (ACE)</li><li>● Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:<ul style="list-style-type: none"><li>○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych</li><li>○ integracja z Active Directory</li><li>○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta</li><li>○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish</li><li>○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram</li><li>○ Szczegółowy opis wykrytych systemów oraz ich komponentów</li><li>○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF</li><li>○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.</li><li>○ Grupowanie urządzeń w oparciu o kryteria użytkownika</li><li>○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji</li><li>○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach</li><li>○ Szybki podgląd stanu środowiska</li><li>○ Podsumowanie stanu dla każdego urządzenia</li><li>○ Szczegółowy status urządzenia/elementu/komponentu</li><li>○ Generowanie alertów przy zmianie stanu urządzenia.</li><li>○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń</li><li>○ Integracja z service desk producenta dostarczonej platformy sprzętowej</li><li>○ Możliwość przejęcia zdalnego pulpitu</li><li>○ Możliwość podmontowania wirtualnego napędu</li><li>○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów</li><li>○ Możliwość importu plików MIB</li><li>○ Przesyłanie alertów „as-is” do innych konsol firm trzecich</li><li>○ Możliwość definiowania ról administratorów</li><li>○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów</li><li>○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)</li><li>○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta</li><li>○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów</li><li>○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów,</li></ul></li></ul> |
|--------------------------------------|--|





## Cyberbezpieczny Samorząd

|                                 |  |
|---------------------------------|--|
|                                 | <p>MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.</p> <ul style="list-style-type: none"><li>Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.</li><li>Wdrażanie serwerów, rozwiązań modułowych oraz przełączników sieciowych w oparciu o profile</li><li>Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.</li><li>Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.</li><li>Zdalne uruchamianie diagnostyki serwera.</li><li>Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.</li><li>Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.</li></ul>   |
| <b>Certyfikaty</b>              | <ul style="list-style-type: none"><li>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001</li><li>Serwer musi posiadać deklaracja CE.</li><li>Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej <a href="http://www.epeat.net">www.epeat.net</a> potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - <b>Wykonawca złoży dokument potwierdzający spełnianie wymogu.</b></li><li>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Windows Server 2025.</li></ul> |
| <b>Dokumentacja użytkownika</b> | <ul style="list-style-type: none"><li>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</li><li>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</li></ul>  |
| <b>Warunki gwarancji</b>        | <ul style="list-style-type: none"><li>Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 7 lat.</li><li>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.</li></ul>   |





## Cyberbezpieczny Samorząd

- Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
- Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
- Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.
- Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
- Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.
- Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
- Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
  - Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
  - Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.
  - Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.
  - Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.
  - Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wystanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.
- Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.





## Cyberbezpieczny Samorząd

|  |   |
|--|---|
|  | <ul style="list-style-type: none"><li>Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.</li></ul> |
|--|---|

### Dodatkowe licencje:

- Serwery muszą zostać dostarczone z licencjami CAL dostarczonymi przez producenta oferowanych serwerów - łącznie 40 licencji na użytkownika Windows Server 2025/2022 (Windows Server 2025 User CAL)

### Macierz o poniższej charakterystyce:

| Element konfiguracji/cecha/funkcjonalność | Wymagania minimalne   |
|---|---|
| Typ obudowy                               | Macierz musi być przystosowana do montażu w szafie rack 19", o wysokość maksymalnie 2U z możliwością instalacji min. 24 dysków 2.5"   |
| Przestrzeń dyskowa                        | Zainstalowane:<br>3 x dysk SSD SAS o pojemności min. 1.92 TB, Hot-Plug, 1DWPD<br>5 x dysk HDD SAS 12Gbps o pojemności min. 2,4 TB, 10 tys. obr./min., 2,5", Hot-Plug  |
| Możliwość rozbudowy                       | Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych.   |
| Obsługa dysków                            | Macierz musi mieć możliwość obsługi dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej.   |
| Sposób zabezpieczenia danych              | Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).<br>Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID.<br>Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).<br>Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków. |
| Tryb pracy kontrolerów macierzowych       | Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.  |
| Pamięć cache                              | Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM.   |







## Cyberbezpieczny Samorząd

|   |   |
|---|---|
|   | <p>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.</p>   |
| Rozbudowa pamięci cache                               | <p>Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.</p> <p>Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.</p>   |
| Interfejsy  | <p>Macierz musi posiadać, co najmniej 8 portów 25Gb iSCSI w standardzie SFP28 (4 porty na kontroler).</p> <p>W zestawie muszą znajdować się 4 kable DAC 25GbE SFP28/SFP28 min. 3m, dostarczone przez producenta macierzy.</p>   |
| Zarządzanie   | <p>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.</p>  |
| Zarządzanie grupami dyskowymi oraz dyskami logicznymi | <p>Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej.</p> <p>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.</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>   |
| Thin Provisioning                                     | <p>Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.</p> <p>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).</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>              |
| Tiering   | <p>Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS.</p> <p>Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.</p> <p>Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.</p>  |
| Wewnętrzne kopie migawkowe                            | <p>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.</p> <p>Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p> |







## Cyberbezpieczny Samorząd

|  |   |
|--|---|
| Wewnętrzne kopie pełne                         | Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.<br>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.   |
| 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. 3 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 dostarczanego urządzenia. |
| Zdalna replikacja danych                       | Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy.<br>Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.   |
| Podłączanie zewnętrznych systemów operacyjnych | Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).<br>Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix.<br>Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.<br>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.  |
| 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.<br>Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.<br>Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.<br>Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.  |
| 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.  |





## Cyberbezpieczny Samorząd

|                          |  |
|--------------------------|--|
|                          | Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.  |
| Standardy bezpieczeństwa | Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International)  |
| Inne                     | <p>Urządzenie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanej macierzy, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.</p> <p>Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.</p> <p>Deklaracja zgodności CE.</p>  |
| Warunki gwarancji        | <ul style="list-style-type: none"><li>• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 7 lat.</li><li>• Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.</li><li>• Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.</li><li>• Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</li><li>• Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.</li><li>• Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</li><li>• Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.</li><li>• Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</li><li>• Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</li><li>• Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.</li></ul> |





## Cyberbezpieczny Samorząd

### Montaż, konfiguracja, uruchomienie:

- Usługa wdrożenia musi obejmować montaż i uruchomienie oferowanego sprzętu w siedzibie zamawiającego, a także odpowiednie redundantne połączenie serwerów z macierzą.
- Na oferowanych urządzeniach musi zostać przeprowadzona aktualizacja firmware'u. Urządzenia zostaną skonfigurowane zgodnie z najlepszymi praktykami (w tym zasób dyskowy na macierzy dla podłączonych serwerów), a na serwerach zainstalowane zostanie oprogramowanie do wirtualizacji (Windows Server Hyper-V) wraz z obsługą klastra.
- Przy wykorzystaniu zaoferowanych licencji Microsoft muszą zostać utworzone 2 nowe maszyny wirtualne z systemem Windows Server 2022 lub 2025 Standard. Maszyny należy uruchomić w ramach klastra.
- Wykonawca na jednej z utworzonych maszyn wirtualnych uruchomi usługę kontrolera domeny wraz z usługami wymaganymi do jej prawidłowego działania.
- Wykonawca musi utworzyć konta dla wszystkich użytkowników (maksymalnie 45 kont) oraz skonfigurować politykę domenową z uwzględnieniem wytycznych zamawiającego.
- Wszystkie komputery zamawiającego z systemem w wersji Professional (maksymalnie 45 urządzeń) zostaną przez wykonawcę podłączone do domeny, a na każdym komputerze przeprowadzona zostanie migracja profilu lokalnego do domenowego połączona z konfiguracją dla wybranych urządzeń profili mobilnych.
- Zamawiający zapewni pełen dostęp do komputerów na czas wykonywania prac.
- Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00).
- Podczas wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonych systemów.
- Wykonawca musi zaoferować usługę wsparcia technicznego minimum 10h pomocy technicznej do wykorzystania do 30.06.2026, świadczonej zdalnie, dla wdrożonych rozwiązań.



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA