



Załącznik nr 1

Dotyczy postępowania o udzielenie zamówienia publicznego na:

**Dostawa serwerów z oprogramowaniem, urządzeń pamięci masowej,
urządzeń sieciowych i zasilaczy awaryjnych wraz z usługami wdrożenia, szkolenia i wsparcia
w ramach projektu „Cyberbezpieczny Samorząd”**

OPIS PRZEDMIOTU ZAMÓWIENIA

UWAGA!!!

wszystkie dokumenty sporządzone w języku obcym należy składać wraz z tłumaczeniem na język polski(może być tłumaczenie własne).

1. Zakup serwera z systemem operacyjnym

Obszar wymagań	Wymagania minimalne
Obudowa	Typu rack o wysokości maksymalnie 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli
Płyta główna	Płyta główna z możliwością instalacji dwóch fizycznych procesorów Możliwości rozbudowy: co najmniej jeden wolny slot PCIe x16 generacji co najmniej 4
Procesor	Zainstalowane dwa procesory ośmiordzeniowe klasy x86 dedykowane do pracy z oferowanym serwerem, umożliwiające osiągnięcie przez serwer wyniku co najmniej 125 punktów w teście SPECrate2017_int_base dla konfiguracji dwuprocesorowej według wyników publikowanych na stronie www.spec.org . Do oferty należy załączyć wydruk z ww. strony; wydruki w języku obcym należy złożyć wraz z tłumaczeniem na język polski (może być tłumaczenie własne);
Pamięć RAM	Zainstalowane co najmniej 128 GB DDR4. Płyta główna musi obsługiwać do 1TB pamięci RAM DDR4 lub więcej.
Grafika	Zintegrowana karta graficzna ze złączem VGA.
Sieć	Wbudowane co najmniej 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ Czteroportowa karta 12Gb SAS HBA do połączenia z oferowaną macierzą.
Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane: 2 dyski Hot-Plug SSD z interfejsem SATA 6Gb/s o pojemności co najmniej 480GB każdy, 3 dyski Hot-Plug SAS 12Gb/s o pojemności co najmniej 2,4TB każdy.

	Możliwość zainstalowania co najmniej dwóch dysków M.2 z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontrolery dyskowe	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60 Wsparcie dla dysków samoszyfrujących
Porty	Co najmniej 3 zewnętrzne porty USB, w tym co najmniej 1 port USB 3.x, co najmniej 1 port USB musi być dostępny z przodu obudowy Dodatkowo port dedykowany dla karty zarządzającej dostępny z przodu obudowy Co najmniej 1 port VGA Ilość dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących wymagany wolny slot PCI Express serwera.
Wentylacja	Redundantne wentylatory hotplug.
Zasilanie	Redundantne zasilacze hotplug o mocy nie większej niż 700W każdy.
Zarządzanie	Dedykowany moduł zdalnego zarządzania, diagnostyki i monitorowania pracy serwera, niezależny od systemu operacyjnego, posiadający dedykowany port RJ-45 GbE umożliwiający co najmniej: <ul style="list-style-type: none"> • zarządzanie poprzez graficzny interfejs, • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera), • szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika, • możliwość podmontowania zdalnych wirtualnych napędów, • wirtualną konsolę z dostępem do myszy, klawiatury, • integrację z Active Directory, • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej, • możliwość podłączenia lokalnego i bezpośredniego zarządzania poprzez złącze RS-232 lub USB lub microUSB, • automatyczne zgłaszanie alertów do centrum serwisowego producenta, • automatyczne update firmware dla wszystkich komponentów serwera, • możliwość przywrócenia poprzednich wersji firmware.
Bezpieczeństwo, diagnostyka	<ul style="list-style-type: none"> • Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera. • Blokada zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardej. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • Możliwość ustawienia w BIOS bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0. • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera. • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania



	serwerem.
System operacyjny	<p>System operacyjny kompatybilny z oferowanym serwerem, spełniający nw. wymagania minimalne:</p> <ol style="list-style-type: none"> 1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 4) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 6) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 7) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 8) Wbudowane wsparcie instalacji i pracy na wolumenach, które: <ol style="list-style-type: none"> 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). 9) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 10) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET 11) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 12) Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 13) Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ol style="list-style-type: none"> a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 14) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 15) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 16) Mechanizmy logowania w oparciu o: <ol style="list-style-type: none"> a) login i hasło, b) karty z certyfikatami (smartcard), c) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 17) 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



	<p>wykorzystywania szyfrowanych danych.</p> <p>18) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).</p> <p>19) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</p> <p>20) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.</p> <p>21) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).</p> <p>22) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</p> <p>23) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:</p> <ul style="list-style-type: none"> a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: <ul style="list-style-type: none"> i) Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii) Ustawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii) Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. iv) Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1 i wyższych. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej. e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: <ul style="list-style-type: none"> i) dystrybucję certyfikatów poprzez http, ii) konsolidację CA dla wielu lasów domeny, iii) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv) automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. <ul style="list-style-type: none"> i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie Nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone
--	---



	<p>między serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:</p> <ul style="list-style-type: none"> i) Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii) Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii) Obsługi 4-KB sektorów dysków iv) Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v) Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi) Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) <p>24) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.</p> <p>25) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).</p> <p>26) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</p> <p>27) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</p> <p>28) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</p> <p>29) Zorganizowany system szkoleń i dostępne materiały edukacyjne w języku polskim.</p> <p>Zaofertowana wraz z serwerem licencja na system operacyjny:</p> <ul style="list-style-type: none"> 1. musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta i pozwalała na legalne używanie na oferowanym serwerze, 2. musi obejmować najnowszą wersję systemu dostępną na dzień składania oferty oraz uprawniać do instalacji wersji poprzedniej (tzw. <i>downgrade</i>), 3. musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz umożliwiać zainstalowanie czterech instancji wirtualnych tego serwerowego systemu operacyjnego, 4. musi obejmować licencje dostępowe dla 25 użytkowników, jeśli takie licencje są wymagane przez producenta do dostępu do oprogramowania serwerowego. <p>Do oferty należy załączyć potwierdzenie kompatybilności serwera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego); wydruki w języku obcym należy złożyć wraz z tłumaczeniem na język polski (może być tłumaczenie własne);</p>
Wymagania środowiskowe	<p>Oferowany serwer musi być zgodny z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Do oferty należy załączyć deklarację zgodności z dyrektywą RoHS.</p>
Warunki gwarancyjne, wsparcie techniczne	<p>Co najmniej pięcioletnia gwarancja producenta, obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji. Warunki świadczenia serwisu gwarancyjnego:</p> <ul style="list-style-type: none"> • usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, • czas reakcji serwisu- do końca następnego dnia roboczego, • w przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. <p>Możliwość zgłaszania awarii 7 dni w tygodniu w języku polskim poprzez ogólnopolską linię telefoniczną producenta oraz dedykowany polskojęzyczny portal techniczny producenta.</p> <p>W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru</p>



	seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji. Usługa realizowana przez polskojęzyczny portal producenta.
--	--

2. Zakup macierzy dyskowej

Obszar wymagań	Wymagania minimalne
Obudowa	Typu rack o wysokości maksymalnie 2U z możliwością instalacji do 12 dysków 3.5" Hot-Plug
Dyski twarde	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. Macierz musi obsługiwać dyski 2,5" i 3,5". Zainstalowane: 8 dysków Hot-Plug SAS 12Gb/s o pojemności co najmniej 4TB każdy. Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 24 dysków twardych.
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). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. 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). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Kontrolery	Macierz musi posiadać co najmniej 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. 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 baterijnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Interfejsy	Macierz musi posiadać co najmniej 8 portów SAS 12Gb (4 porty na kontroler) Z macierzą należy dostarczyć 4 kable HD Mini-SAS 12Gb- Mini-SAS 6Gb umożliwiające połączenie z oferowanymi serwerami w klastrze
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z



	poziomu przeglądarki internetowej.
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.</p> <p>Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.</p>
Wewnętrzne kopie pełne	<p>Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>
Migracja danych w obrębie macierzy	<p>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.</p> <p>Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na co najmniej 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.</p>



Podłączanie zewnętrznych systemów operacyjnych	<p>Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).</p> <p>Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, VMWare.</p> <p>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.</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.</p>
Redundancja	<p>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.</p> <p>Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.</p> <p>Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.</p>
Warunki gwarancyjne, wsparcie techniczne	<p>Co najmniej pięcioletnia gwarancja producenta, obejmująca wszystkie komponenty macierzy wchodzące w skład oferowanej konfiguracji. Warunki świadczenia serwisu gwarancyjnego:</p> <ul style="list-style-type: none"> • usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, • czas reakcji serwisu- do końca następnego dnia roboczego, • w przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. <p>Możliwość zgłaszania awarii 7 dni w tygodniu w języku polskim poprzez ogólnopolską linię telefoniczną producenta oraz dedykowany polskojęzyczny portal techniczny producenta.</p> <p>W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji- na podstawie numeru seryjnego urządzenia- czasu obowiązywania i typ udzielonej gwarancji. Usługa realizowana przez polskojęzyczny portal producenta.</p>

3. Zakup NAS

Obszar wymagań	Wymagania minimalne
Budowa	<p>Obudowa do montażu w szafie rack o wysokości maksymalnie 2U, wymagane wyposażenie w szynę do szafy rack</p> <p>Redundantne wentylatory</p>
Procesor	<p>Wielordzeniowy procesor 64-bitowy, uzyskujący wynik co najmniej 6 200 punktów w teście PassMark- CPU Mark według wyników dostępnych na stronie http://www.cpubenchmark.net 30 dni przed terminem składania ofert lub później.</p> <p>Do oferty należy załączyć wydruk z ww. strony; wydruki w języku obcym należy złożyć wraz z tłumaczeniem na język polski (może być tłumaczenie własne);</p>
Pamięć RAM	Zainstalowane co najmniej 32 GB pamięci RAM.
Obsługa dysków	Ilość kieszeni dysków: co najmniej 12 (możliwość rozbudowy do 24 dysków z wykorzystaniem jednostki rozszerzającej lub równoważnie obudowa na 24 dysków).



	Obsługiwane typy dysków: 3,5" SATA HDD, 2,5" SATA SSD
Zamontowane dyski	Zamontowanych co najmniej 12 dysków o pojemności co najmniej 4 TB każdy, o prędkości interfejsu co najmniej 6Gbps i maksymalnej stałej prędkości przesyłu danych 200 MB/s lub większej. Oferowane dyski muszą znajdować się na liście kompatybilności producenta urządzenia dyskowego NAS.
RAID	Obsługa RAID co najmniej: Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6 i RAID 10. Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Funkcje i usługi	Wsparcie dla wirtualizacji Scentralizowana pamięć masowa na dane Kopia zapasowa Udostępnianie i przywracanie systemu po awarii Mechanizm szyfrowania sprzętowego Uprawnienia listy kontroli dostępu systemu Windows (ACL) Wymagana kompatybilność z usługą katalogową serwera Windows (możliwość logowania użytkowników domeny za pośrednictwem protokołów SMB/FTP/WebDAV/File Station).
Porty	Co najmniej 2 porty 1 GbE RJ-45 Co najmniej 1 porty 10 GbE RJ-45 Co najmniej 2 porty 10 GbE SFP+ z wkładkami Co najmniej 2 porty USB 3.x Co najmniej 1 port rozszerzenia mini-SAS HD
Zasilanie	Wbudowane redundantne zasilacze
Bezpieczeństwo	Obsługa WORM (Write Once Read Many- jeden zapis, wiele odczytów) dla folderów współdzielonych i migawek, zaporę sieciową, szyfrowanie folderu współdzielonego, szyfrowanie całego woluminu, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów HTTP, HTTPS, SMB, SSH, Telnet, rsync, FTP, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania), dwuetapowa weryfikacja logowania (2FA), adaptacyjna metoda logowania dla konta administratora (AMFA), możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2, U2F, grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail.
Oprogramowanie	<ul style="list-style-type: none"> • Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych • Wymaga się zapewnienia aplikacji do realizacji chmury prywatnej, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI, a także agenty na urządzeniach PC/MAC oraz aplikację mobilną na Android/iOS. Ww. usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ww. usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników. Usługa musi być dostępna bez dodatkowych opłat, co najmniej w okresie gwarancji na urządzenie. • Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych serwerów,



	<p>bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego.</p> <ul style="list-style-type: none"> • Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych i serwera rsync • Obsługa minimum 1024 migawek na folder współdzielony i minimum 65000 migawek na cały system • Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 40 jednoczesnych połączeń
Oprogramowanie do kopii zapasowej	<p>Zakup urządzenia musi uprawniać do instalacji i eksploatacji oprogramowania do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów. Minimalne wymagane funkcje oprogramowania do backupu:</p> <ul style="list-style-type: none"> • oprogramowanie musi być w pełni zgodne z oferowanym urządzeniem, • kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal, • kopia zapasowa maszyn wirtualnych (VMware, Hyper-V) • kopia zapasowa serwerów fizycznych (Windows, Linux) • obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania, • obsługa wielu wersji i retencji, • możliwość wyzwalania kopii zapasowej według harmonogramu, • obsługa klastra przełączania awaryjnego Microsoft Hyper-V, • centralne zarządzanie, • konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji, harmonogramu i woluminów objętych backupem dla poszczególnych zadań, • portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), • delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla użytkowników bez uprawnień administratora, • kopia zapasowa usług chmur publicznych Microsoft 365 i Google Workspace.
Gwarancja	Gwarancja producenta co najmniej 36 miesięcy obejmująca również dyski.

4. Zakup oprogramowania backup

Obszar wymagań	Wymagania minimalne
Licencja	Wymagane dostarczenie licencji wieczystych dla serwera będącego przedmiotem zamówienia (obejmujących 2 serwery fizyczne i zainstalowane na każdym z nich 4 maszyny wirtualne) oraz 5 stacji roboczych, uprawniającej do korzystania ze wsparcia producenta przez okres 12 miesięcy
Systemy operacyjne	<p>Program serwerowy kompatybilny z systemem operacyjnym dostarczonym wraz z serwerem będącym przedmiotem zamówienia</p> <p>Program kliencki kompatybilny z systemami: Microsoft Windows 10; Windows 11; Microsoft Windows Server 2025, Linux, QNAP, Synology</p>
Funkcjonalność	<ul style="list-style-type: none"> • Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów



	<p>klienckich</p> <ul style="list-style-type: none"> • Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików) • Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS) • Automatyczny backup przy wyłączaniu komputera • Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i ? • Backup całego systemu operacyjnego i zainstalowanych programów dla systemów Windows • Backup baz danych i plików poczty w trybie online i offline • Kopie rotacyjne (wersjonowanie) • Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi • Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore) • Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej • Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych • Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO • Kompresja po stronie stacji roboczej • Ochrona przed zapisem, usunięciem, modyfikacją pliku • Kopia bazy danych Microsoft SQL, PostgreSQL/MS SQL • Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP, • Replikacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO • Centralne sterowanie całym systemem z jednego miejsca • Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników • Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN • Wysyłanie alertów administracyjnych na e-mail • Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych • Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki • Automatyczna aktualizacja oprogramowania na komputerach zdalnych • Interfejs, instrukcja i pomoc techniczna w języku polskim
--	--

5. Zakup zarządzalnych przełączników sieciowych (typ 1)

Obszar wymagań	Wymagania minimalne
Porty	Co najmniej 24 sloty SFP+ 10 Gbps Co najmniej 4 sloty SFP28 25 Gbps
Wydajność	Przełączanie non-blocking Przepustowość odpowiednia dla środowisk AV over IP
Zasilanie	Wewnętrzny zasilacz AC 230V

	Obsługa zasilania redundantnego (1+1)
Chłodzenie	Aktywne chłodzenie z wentylatorami z możliwością pracy w trybie cichym
Zarządzanie i monitorowanie	Zarządzanie przez CLI, GUI, SSH, HTTP/HTTPS Obsługa SNMPv1/v2c/v3 Obsługa sFlow, RSPAN Możliwość integracji z rozwiązaniami do centralnego zarządzania
Protokoły i funkcje sieciowe	Obsługa funkcji L2 i L3 Routing statyczny i dynamiczny (m.in. OSPF) Obsługa IPv4 i IPv6 Link Aggregation (LACP, statyczny) STP/RSTP/MSTP Obsługa Jumbo Frames co najmniej 9000 bajtów
Bezpieczeństwo i dostęp	Obsługa IEEE 802.1X (Port/MAC-based Authentication) Dynamic VLAN Assignment ARP Inspection, IP Source Guard RADIUS, TACACS+
Obudowa	Obudowa do montażu w szafie rack, zajmująca nie więcej niż 1U
Wypożyczenie dodatkowe	Wkładki światłowodowe 10GBASE-X SFP+ 24 sztuki dla każdego z dwóch przełączników Kable światłowodowe SFP+ 10 Gbps: o długości 0,5 m – 8 sztuk dla każdego z dwóch przełączników, o długości 1 m – 4 sztuki dla każdego z dwóch przełączników, o długości 2 m – 8 sztuk dla każdego z dwóch przełączników, o długości 3 m – 4 sztuki dla każdego z dwóch przełączników, o długości 5 m – 4 sztuki dla każdego z dwóch przełączników. Wkładki światłowodowe 25GBASE-X SFP28 – 4 sztuki dla każdego z dwóch przełączników Kable światłowodowe SFP28 25 Gbps o długości 5 m – 2 sztuki dla każdego z dwóch przełączników.
Gwarancja	Gwarancja producenta co najmniej 36 miesięcy.

6. Zakup zarządzalnego przełącznika sieciowego (typ 2)

Obszar wymagań	Wymagania minimalne
Porty	48 portów 10/100/1000 Mbps RJ45 PoE+ 4 sloty SFP+ 10 Gbps
Wydajność	Przepustowość: co najmniej 176 Gb/s Szybkość przekierowywania pakietów: co najmniej 131 Mpps Bufor pamięci: co najmniej 12 MB
Zasilanie	Wewnętrzny zasilacz AC 100–240 V, 50/60 Hz Budżet mocy PoE: co najmniej 500 W (do 30 W na port)
Chłodzenie	Aktywne chłodzenie z trzema wentylatorami
Zarządzanie i monitorowanie	Zarządzanie przez CLI, GUI, SSH, Telnet SNMPv1/v2c/v3, RMON Możliwość zarządzania przy wykorzystaniu platformy zarządzającej, o której mowa w poz. 8



	Kontroler do zarządzania access-pointami
Protokoły i funkcje sieciowe	Obsługa funkcji L2 i L2+ Routing statyczny VLAN 802.1Q, STP/RSTP/MSTP Link Aggregation (LACP) IGMP Snooping, QoS, Port Mirroring Obsługa Jumbo Frames co najmniej 9000 bajtów
Bezpieczeństwo i dostęp	IEEE 802.1X (Port/MAC-based Authentication) ACL (L2–L4), IP-MAC-Port Binding, Port Security DHCP Snooping, Storm Control, DoS Defense
Obudowa	Obudowa do montażu w szafie rack 19", zajmująca nie więcej niż 1U
Wposażenie dodatkowe	Wkładki światłowodowe SFP+ 10 Gbps – 4 sztuki Kable sieciowe LAN RJ45: o długości 2 m – 16 sztuk, o długości 3 m – 16 sztuk, o długości 5 m – 16 sztuk.
Gwarancja	Gwarancja producenta co najmniej 36 miesięcy.

7. Zakup access pointów

Obszar wymagań	Wymagania minimalne
Standard Wi-Fi	IEEE 802.11a/b/g/n/ac/ax (Wi-Fi 6)
Maksymalne prędkości transmisji	2,4 GHz – co najmniej 570 Mb/s 5 GHz – co najmniej 2400 Mb/s
Porty	4 porty Ethernet 1 Gb/s 1 port FXS RJ11 1 port Ethernet z obsługą wyjścia PoE (802.3af/at)
Zasilanie	Zasilanie PoE 802.3af/at/bt lub 12V/1,5A DC
Pobór mocy	Maksymalnie 20 W (bez włączonego wyjścia PoE)
Anteny	Wewnętrzne, dookólne 2,4 GHz: 2× 5 dBi 5 GHz: 3× 4,7 dBi
Zasięg	Maksymalny deklarowany zasięg 140 m ² lub większy
Montaż	Biurkowy lub naścienny (zestaw montażowy w zestawie)
Funkcje sieciowe	Obsługa MU-MIMO, OFDMA, HE160, Beamforming Obsługa 250 jednoczesnych klientów Obsługa 16 SSID (8 na każde pasmo) Funkcja Mesh, płynny roaming, sieć dla gości, QoS (WMM), kontrola pasma, równoważenie obciążenia
Bezpieczeństwo	Uwierzytelnianie: 802.1X, MAC, strona powitalna Szyfrowanie: WPA3-Personal/Enterprise, WPA2, WPA Izolacja klientów, kontrola dostępu, filtrowanie MAC, VLAN, wykrywanie nieautoryzowanych AP

Zarządzanie	Kompatybilność z oferowanym kontrolerem do zarządzania access-pointami Możliwość zarządzania przy wykorzystaniu platformy zarządzającej, o której mowa w poz. 8 Kontroler do zarządzania access-pointami
Gwarancja	Gwarancja producenta co najmniej 36 miesięcy.

8. Kontroler do zarządzania access-pointami

Parametr	Wymagania minimalne
Porty	2 porty Ethernet 10/100/1000 Mb/s 1 port USB 3.0
Zasilanie	Zasilanie AC 100–240 V, 50/60 Hz
Platforma zarządzająca	Platforma do zarządzania siecią oparta na architekturze SDN (Software Defined Networking) umożliwiająca scentralizowane zarządzanie oferowanymi przełącznikami sieciowymi oraz access-pointami poprzez wspólny interfejs zarządzania. Rozwiązanie musi zapewniać możliwość konfiguracji, monitorowania i aktualizacji urządzeń zarówno lokalnie, jak i zdalnie, za pośrednictwem chmury, bez konieczności stosowania dodatkowych licencji. System musi zapewniać funkcje automatycznego wykrywania urządzeń, grupowego wdrażania ustawień i aktualizacji oprogramowania, a także zaawansowane monitorowanie stanu sieci, wykrywanie anomalii oraz zarządzanie dostępem użytkowników.
Zarządzanie i monitorowanie	Centralne zarządzanie do 500 punktów dostępowych, przełączników i routerów Obsługa do 15 000 klientów Zarządzanie lokalne i zdalne przez aplikację lub interfejs webowy Dostęp do chmury bez opłat licencyjnych
Funkcje sieciowe	Automatyczne wykrywanie urządzeń Konfiguracje grupowe Grupowe aktualizacje firmware'ów Monitorowanie stanu sieci, ostrzeżenia, harmonogram restartów Ujednolicony proces konfiguracji Spersonalizowana strona logowania do sieci
Obudowa	Metalowa obudowa z możliwością montażu w szafie rack lub na blacie
Wypożyczenie dodatkowe	Zestaw do montażu w szafie rack Kabel Ethernet Przewód zasilający Instrukcja szybkiej konfiguracji
Gwarancja	Gwarancja producenta co najmniej 36 miesięcy.

9. Zakup oprogramowania EDR

Obszar wymagań	Wymagania minimalne
Licencja	Licencja bezterminowa na 25 urządzeń końcowych
Wymagania wstępne	Oprogramowanie EDR powinno zapewniać pełną ochronę punktów końcowych bez



	konieczności stosowania agentów o wysokim zużyciu zasobów systemowych. Rozwiązanie powinno być skalowalne i umożliwiać późniejszą rozbudowę o dodatkowe moduły analityczne lub funkcje ochrony.
Funkcjonalność wykrywania i ochrony przed zagrożeniami	Monitorowanie i analiza aktywności procesów, aplikacji oraz plików w czasie rzeczywistym. Wykrywanie anomalii behawioralnych mogących świadczyć o występowaniu zagrożenia. Identyfikacja i blokowanie nieautoryzowanych działań na poziomie systemu operacyjnego. Wykrywanie i neutralizowanie ataków typu ransomware, malware, exploit. Obsługa analizy działań użytkowników w celu wykrywania zachowań nietypowych lub niebezpiecznych.
Funkcjonalność reakcji na incydenty (Response)	Automatyczna izolacja urządzenia w przypadku wykrycia zagrożenia (separacja sieciowa). Możliwość zakończenia lub zablokowania procesu lub aplikacji wykrytej jako zagrożenie. Możliwość ręcznego lub automatycznego usuwania plików i rejestrów powiązanych ze złośliwą aktywnością. Generowanie alertów i powiadomień dla administratora o incydentach bezpieczeństwa.
Analiza zagrożeń i logowanie zdarzeń	Zbieranie pełnych danych o zdarzeniach systemowych, procesach, plikach i ruchu sieciowym. Tworzenie dzienników aktywności urządzeń końcowych (logi systemowe i użytkownika). Możliwość korelacji zdarzeń i analizy przyczyn incydentów (root cause analysis). Eksport danych o zdarzeniach do zewnętrznych systemów analizy (np. SIEM) poprzez standardowe formaty. Obsługa tworzenia i przeglądania szczegółowych raportów dotyczących zdarzeń bezpieczeństwa.
Zarządzanie i administracja	Centralna konsola administracyjna do zarządzania wszystkimi agentami EDR. Możliwość tworzenia i wdrażania polityk bezpieczeństwa na urządzeniach końcowych. Zarządzanie aktualizacjami agentów oraz aktualizacjami baz sygnatur. Definiowanie różnych poziomów uprawnień dla administratorów i operatorów bezpieczeństwa. Funkcjonalność filtrowania zdarzeń, urządzeń i użytkowników w konsoli zarządzającej.
Inne funkcjonalności	Obsługa dynamicznego monitorowania procesów w systemie operacyjnym bez istotnego wpływu na wydajność urządzeń. Mechanizmy automatycznego klasyfikowania i oceny wykrytych zagrożeń według poziomu ryzyka. Możliwość przeprowadzenia ręcznej analizy podejrzanych plików bezpośrednio z konsoli zarządzania. Opcjonalna integracja z usługami analizy zagrożeń w chmurze. Funkcja automatycznego aktualizowania polityk zabezpieczeń bez konieczności restartu urządzeń.
Współpraca i kompatybilność	Możliwość pracy w środowiskach lokalnych, hybrydowych oraz zdalnych. Obsługa urządzeń końcowych opartych na systemach Windows 10 i nowszych. Integracja z rozwiązaniami bezpieczeństwa, takimi jak oprogramowanie antywirusowe i zapory sieciowe. Możliwość pracy w środowiskach z domenami Active Directory oraz niezależnych sieciach.

10. Zakup oprogramowania do szyfrowania plików

Obszar wymagań	Wymagania minimalne
----------------	---------------------



Licencja	Licencja bezterminowa na 25 urzędzeń końcowych
Szyfrowanie danych	Możliwość szyfrowania plików i folderów na komputerach użytkowników oraz serwerach. Możliwość szyfrowania całych dysków systemowych i danych. Obsługa szyfrowania nośników wymiennych, takich jak pamięci USB, dyski zewnętrzne i karty SD. Możliwość szyfrowania plików i załączników wysyłanych pocztą elektroniczną. Obsługa szyfrowania lokalnego oraz w środowisku domenowym. Możliwość tworzenia zaszyfrowanych archiwów danych.
Zarządzanie dostępem i bezpieczeństwo	Wsparcie dla uwierzytelniania dwuskładnikowego przy dostępie do danych zaszyfrowanych. Automatyczne blokowanie dostępu do danych po upływie czasu bezczynności użytkownika. Możliwość blokowania kopiowania danych z zaszyfrowanych lokalizacji na niezabezpieczone nośniki. Automatyczne wymuszanie szyfrowania danych zapisywanych na nośnikach wymiennych. Możliwość odzyskiwania danych w przypadku utraty klucza lub hasła przez użytkownika (recovery mechanism). Szyfrowanie danych przy zachowaniu zgodności z powszechnie uznawanymi standardami kryptograficznymi (np. AES-256).
Obsługa użytkownika końcowego	Intuicyjny interfejs użytkownika umożliwiający samodzielne szyfrowanie i odszyfrowywanie danych. Możliwość szyfrowania pojedynczych plików, katalogów lub nośników jednym kliknięciem. Możliwość definiowania domyślnych akcji (np. automatyczne szyfrowanie nowych plików w folderze). Dostępność funkcji deszyfrowania offline z mechanizmami bezpieczeństwa.
Pozostałe wymagania funkcjonalne	Możliwość przesyłania szyfrowanych plików z opcją czasowego dostępu. Obsługa wymuszonego szyfrowania danych przed ich zapisem na określonych typach lokalizacji (np. dysk zewnętrzny, chmura).
Kompatybilność	Wsparcie dla systemów operacyjnych Microsoft Windows 10 i nowszych.

11. Zakup oprogramowania menadżera logów

Obszar wymagań	Wymagania minimalne
Licencja	Oprogramowanie open source lub bezterminowa licencja na oprogramowanie komercyjne, umożliwiająca wdrożenie i użytkowanie rozwiązania na infrastrukturze objętej wdrożeniem zgodnie z dalszymi wymaganiami
Oprogramowanie	Platformą sprzętowa dla rozwiązania centralnego składowania dzienników będzie wirtualna maszyna w środowisku Hyper-V, uruchomiona przez Wykonawcę na platformie sprzętowej będącej przedmiotem zamówienia. Tworzenie użytkowników w systemie centralnego składowania logów może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu. System centralnego składowania dzienników zdarzeń powinien mieć możliwość zdefiniowania dowolnie wielu i dowolnie skonfigurowanych źródeł danych, wśród których znajdują się m.in.: Syslog UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP.



	<p>Konfiguracja źródeł danych powinna pozwalać na zdefiniowanie dowolnego portu komunikacji, np. Syslog UDP 514 lub/i Syslog UDP 10514.</p> <p>System centralnego składowania dzienników zdarzeń powinien mieć możliwość ekstrakcji fragmentów wpisów logów z możliwością wykorzystania ich do filtrowania danych, budowania zapytań dla powiadomień i alarmów czy widoków w ramach dashboardów oraz ich import jak i eksport.</p> <p>System centralnego składowania dzienników zdarzeń powinien udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trybie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV czy urządzeniach z dowolną przeglądarką WWW.</p> <p>System centralnego składowania dzienników zdarzeń powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego.</p> <p>System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów).</p>
Wdrożenie	<p>Instalacja systemu operacyjnego na maszynie wirtualnej przygotowanej przez Wykonawcę na platformie sprzętowej będącej przedmiotem zamówienia.</p> <p>Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca proponuje rozwiązanie pozwalające na uspoźnienie zegarów czasów sieci Zamawiającego.</p> <p>Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracją parametrów podstawowej pracy, w tym polityki dostępu dla administratorów IT Zamawiającego.</p> <p>Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktów prawnych i dobrych praktyk występujących w środowisku Zamawiającego.</p> <p>Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły:</p> <p>serwery wraz z maszynami wirtualnymi będącymi przedmiotem zamówienia oraz posiadane już przez Zamawiającego 2 serwery fizyczne (5 serwerów wirtualnych),</p> <p>przełączniki sieciowe będące przedmiotem zamówienia oraz przełączniki sieciowe w infrastrukturze zamawiającego,</p> <p>stacje robocze Windows 10 i 11 (25 szt.),</p> <p>firewall.</p> <p>Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającą odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.</p> <p>Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.</p> <p>Automatyzacja analizy napływających logów poprzez zbudowanie dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.</p> <p>Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.</p> <p>Konfiguracja wysyłania powiadomień poprzez e-mail w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.</p> <p>Wprowadzenie administratorów IT do obsługi wdrożonego systemu.</p>
Gwarancja i asysta	Zamawiający wymaga, aby Wykonawca w czasie od dnia odbioru do 30.06.2026 r. zapewnił



techniczna	wsparcie techniczne polegające na: zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu, asysty w zakresie aktualizacji zarówno systemu, jak i jego komponentów. Zamawiający wymaga aby ww. usługi były świadczone w godzinach pracy Zamawiającego. Wykonawca wskaże kanał komunikacji elektronicznej (np. e-mail lub dedykowany system zgłoszeń) przeznaczony do zgłaszania potrzeby skorzystania z wsparcia technicznego.
------------	--

14. Zakup UPS serwerowych

Obszar wymagań	Wymagania minimalne
Typ urządzenia	Zasilacz awaryjny w obudowie tower z możliwością montażu w szafie RACK, zajmujący maksymalnie 2U
Moc	Co najmniej 2700 W, moc pozorna co najmniej 3000 VA
Topologia	Online
Typ przebiegu	Sinusoida
Czas podtrzymania	Co najmniej 2 min. przy obciążeniu 100 % Co najmniej 8 min. przy obciążeniu 50 %
Gniazda	Co najmniej 6 gniazd IEC 320 C13 Złącze dla dodatkowych baterii
Komunikacja	Porty: 1 x USB lub 1x Ethernet
Zabezpieczenia	Przeciwprzepięciowe, przeciwzwarciovowe, przeciwprzeciążeniowe
Sygnalizacja	Wyświetlacz LCD lub diody LED, alarm dźwiękowy
Gwarancja	Co najmniej 24 miesiące.

12. Zakup usług wdrożenia zakupionych rozwiązań wraz z usługami wsparcia w okresie realizacji projektu

- Urządzenia przeznaczone do montażu w szafie rack Wykonawca zainstaluje w szafach wskazanych przez Zamawiającego, uruchomi je i skonfiguruje w porozumieniu z Zamawiającym. Wykonawca musi uwzględnić w cenie oferty, a następnie dostarczyć i zamontować wszelkie okablowanie, elementy rozszerzające, akcesoria montażowe umożliwiające instalację urządzeń w szafach i ich uruchomienie.
- Wykonawca zobowiązany jest do wdrożenia dostarczonego sprzętu i oprogramowania w następującym zakresie:

Serwery:

 - Instalacja i konfiguracja systemów operacyjnych na dostarczonych serwerach.
 - Konfiguracja sieci oraz podłączenie serwerów do infrastruktury LAN i SAN.
 - Instalacja środowisk wirtualizacji oraz utworzenie klastra serwerów.
 - Konfiguracja środowisk wirtualnych, przestrzeni dyskowej oraz testy poprawności działania.

Macierz dyskowa:

 - Instalacja i konfiguracja macierzy dyskowej.
 - Konfiguracja przestrzeni dyskowej oraz przyłączenie do środowiska serwerowego.
 - Testy funkcjonalne działania macierzy i dostępności danych.

Serwer NAS:

 - Instalacja i konfiguracja serwera NAS.



- 9) Konfiguracja przestrzeni dyskowej i integracja z siecią.
- 10) Testy funkcjonalne dostępu do zasobów NAS.
Oprogramowanie do backupu:
 - 11) Instalacja oprogramowania do backupu na każdym wskazanym systemie.
 - 12) Konfiguracja polityk backupu oraz harmonogramów kopii zapasowych.
 - 13) Testowe wykonanie kopii zapasowej i pełnego przywrócenia urządzeń do sprawności działania.
 - 14) Opracowanie dokumentacji dotyczącej konfiguracji systemu backupu.*Przełączniki sieciowe typ 1 i typ 2:*
 - 15) Montaż w szafach rack.
 - 16) Konfiguracja sieci VLAN, agregacji łączy oraz protokołów redundancji na dostarczonych przełącznikach, istniejących w sieci LAN i firewallu zamawiającego.
 - 17) Testy funkcjonalne transmisji danych i konfiguracji sieciowej.*Access Pointy i kontroler:*
 - 18) Montaż i konfiguracja punktów dostępowych.
 - 19) Instalacja i konfiguracja kontrolera do zarządzania access pointami.
 - 20) Konfiguracja sieci bezprzewodowej według wskazań Zamawiającego.
 - 21) Testy funkcjonalne działania sieci Wi-Fi.*Oprogramowanie EDR:*
 - 22) Instalacja agentów EDR na wskazanych urządzeniach.
 - 23) Konfiguracja polityk bezpieczeństwa i testy wykrywania zagrożeń.*Oprogramowanie do szyfrowania plików:*
 - 24) Instalacja oprogramowania na wskazanych stacjach roboczych i serwerach.
 - 25) Konfiguracja zasad szyfrowania oraz testy poprawności działania.*Menadżer logów:*
 - 26) Instalacja i konfiguracja menadżera logów.
 - 27) Integracja z urządzeniami i systemami Zamawiającego.
 - 28) Testy zbierania i analizy logów oraz konfiguracja polityk retencji danych.*UPS serwerowe:*
 - 29) Instalacja i uruchomienie zasilaczy UPS w szafach rack.
 - 30) Testy poprawności działania zasilania awaryjnego oraz konfiguracja powiadomień.
3. Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu lub – jeśli są one udostępniane przez producenta w formie elektronicznej – prześle adresy WWW, pod którymi można je pobrać.
4. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji właściwemu dla danej części Zamawiającego lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.
5. Wykonawca jest zobowiązany do świadczenia usług wsparcia technicznego dla sprzętu i oprogramowania polegających na aktualizacji oprogramowania, sterowników, na udzielaniu konsultacji i wskazówek dotyczących dostarczonego sprzętu i oprogramowania na każdorazowe żądanie Zamawiającego. Usługi wsparcia muszą być dostępne co najmniej w godzinach pracy Zamawiającego przez okres 9 miesięcy od dnia odbioru w wymiarze co najmniej 4 godzin miesięcznie (do czego nie wlicza się czasu przeznaczonego na aktualizację oprogramowania i sterowników). Usługi będą obejmować w szczególności wsparcie wyznaczonych przedstawicieli Zamawiającego (administratorów IT) w zakresie administrowania rozwiązaniami, doskonalenia środowiska sieciowego, rozwijania kompetencji administratorów IT Zamawiającego oraz wsparcia w obsłudze incydentów. Dopuszcza się świadczenie usług przez Wykonawcę z wykorzystaniem środków komunikacji elektronicznej, jednak wykorzystanie środków komunikacji elektronicznej nie może wiązać się z dodatkowymi kosztami dla Zamawiającego, w szczególności nie może on być zobowiązany do nabywania dodatkowych usług, licencji na oprogramowanie itd.

13. Zakup usług szkolenia administratora IT

Na zakończenie prac wdrożeniowych wykonawca przeprowadzi cykl szkoleń dla administratora IT z zakresu wdrażanych rozwiązań.

Szkolenia muszą mieć formę praktycznych warsztatów na wdrożonym sprzęcie i oprogramowaniu oraz demonstracji na rzeczywistych konfiguracjach.

W ramach szkoleń należy przewidzieć sesje Q&A (pytania i odpowiedzi) po każdym bloku tematycznym.

Wykonawca przekaże administratorowi odpowiednie materiały szkoleniowe w formie elektronicznej (PDF/manuale).

Czas trwania szkolenia: łącznie 24 godziny.

Ramowy program szkolenia:

1. Serwery z systemem operacyjnym
 - 1) Instalacja, podstawowa konfiguracja i zabezpieczenie serwerowego systemu operacyjnego.
 - 2) Zarządzanie rolami i funkcjami serwera.
 - 3) Konfiguracja i zarządzanie lokalną zaporą systemową (Firewall) – tworzenie bezpiecznych reguł dostępu.
 - 4) Konfiguracja polityk silnych haseł, blokady konta po błędnych logowaniach.
 - 5) Wyłączenie niepotrzebnych usług (np. Telnet, SMBv1).
 - 6) Wdrażanie aktualizacji bezpieczeństwa systemu operacyjnego.
 - 7) Konfiguracja audytowania dostępu do plików i logowań.
 - 8) Zarządzanie uprawnieniami użytkowników według zasady minimalnych przywilejów.
 - 9) Szyfrowanie dysków systemowych (np. BitLocker lub równoważny).
 - 10) Konfiguracja zasad automatycznego wylogowania użytkowników.
 - 11) Monitorowanie dzienników zdarzeń systemowych.
2. Macierz dyskowa i serwer NAS
 - 1) Konfiguracja przestrzeni dyskowej (tworzenie wolumenów, LUN).
 - 2) Definiowanie uprawnień dostępu do zasobów macierzy i NAS.
 - 3) Konfiguracja systemu plików i udziałów sieciowych.
 - 4) Integracja NAS z domeną Active Directory.
 - 5) Testy wydajności i funkcjonalności przestrzeni dyskowej.
3. Oprogramowanie do backupu
 - 1) Instalacja i konfiguracja systemu backupu.
 - 2) Definiowanie polityk kopii zapasowych (pełnych, przyrostowych, różnicowych).
 - 3) Harmonogramowanie backupów i zarządzanie przestrzenią dyskową backupu.
 - 4) Konfiguracja szyfrowania kopii zapasowych.
 - 5) Testowe odtwarzanie danych.
 - 6) Konfiguracja systemu powiadomień o błędach backupu.
4. Zarządzalne przełączniki sieciowe (typ 1 i typ 2)
 - 1) Instalacja i podstawowa konfiguracja przełączników.
 - 2) Konfiguracja VLAN-ów – segmentacja sieci użytkowników, serwerów, firewall i Wi-Fi.
 - 3) Konfiguracja agregacji łączy (LACP) oraz protokołów redundancji (RSTP).
 - 4) Konfiguracja bezpiecznego dostępu administracyjnego (SSH, zmiana portów dostępu).
 - 5) Konfiguracja list kontroli dostępu (ACL) na portach.
 - 6) Włączenie funkcji port security – ograniczenie liczby urządzeń na porcie.
 - 7) Monitorowanie urządzeń podłączonych do przełączników.
5. Access Pointy i kontroler do zarządzania Access Pointami



- 1) Instalacja i podstawowa konfiguracja access pointów i kontrolera.
- 2) Definiowanie sieci SSID dla pracowników i gości.
- 3) Konfiguracja uwierzytelnienia WPA2/WPA3 Enterprise.
- 4) Ograniczenie dostępu do sieci Wi-Fi przez ukrywanie SSID lub filtrowanie MAC.
- 5) Monitorowanie i zarządzanie urządzeniami w sieci Wi-Fi.
6. Oprogramowanie EDR
 - 1) Instalacja agentów EDR na urządzeniach końcowych.
 - 2) Konfiguracja zasad bezpieczeństwa EDR: monitorowanie procesów, plików i sieci.
 - 3) Ustawienie automatycznych reakcji na wykryte zagrożenia (np. izolacja urządzenia).
 - 4) Analiza alertów bezpieczeństwa.
 - 5) Generowanie raportów zdarzeń i incydentów.
7. Oprogramowanie do szyfrowania plików
 - 1) Instalacja i konfiguracja systemu szyfrowania plików.
 - 2) Definiowanie zasad szyfrowania plików, folderów oraz nośników USB.
 - 3) Zarządzanie kluczami szyfrowania i procedurami odzyskiwania danych.
 - 4) Automatyczne szyfrowanie nowo utworzonych plików i folderów.
 - 5) Blokowanie nieautoryzowanego przesyłania danych.
8. Oprogramowanie menadżera logów
 - 1) Instalacja i konfiguracja systemu zbierania logów.
 - 2) Integracja logów z serwerów, przełączników, systemów bezpieczeństwa i aplikacji.
 - 3) Korelacja zdarzeń i analiza bezpieczeństwa.
 - 4) Definiowanie alertów i raportów z nietypowych zdarzeń.
9. UPS serwerowe
 - 1) Instalacja i konfiguracja zasilaczy awaryjnych UPS.
 - 2) Integracja UPS z serwerami – konfiguracja procedury bezpiecznego zamknięcia systemu.
 - 3) Monitoring stanu zasilania i powiadamianie o zdarzeniach awaryjnych.
 - 4) Testy wyłączeń awaryjnych i odzyskiwania zasilania.