**Załącznik nr 2 – Szczegółowy opis przedmiotu zamówienia**

Szczegółowy opis przedmiotu zamówienia

do zapytania ofertowego nr B/2026

Przedmiotem zamówienia jest pakiet 8 części realizujących podniesienie funkcjonalne systemów posiadanych przez Zamawiającego oraz zwiększających poziom bezpieczeństwa sieciowego jednostki. Oferujący może składać ofertę na pojedynczą część lub na kilka części jednocześnie.

Zakres przedmiotowy zamówienia:

[I. Część 1 – Dostawa oraz wdrożenie systemu PAM wraz z licencjami, niezbędnym sprzętem oraz usługa wsparcia 2](#_Toc222495411)

[II. Część 2 – Dostawa systemu ochrony przed wyciekiem informacji DLP wraz z kompletem niezbędnych licencji oraz zapewnieniem wsparcia technicznego i serwisu dla zaoferowanego systemu 8](#_Toc222495412)

[III. Część 3 – Dostarczenie oraz wdrożenie systemu klasy NDR, w tym system aplikacyjny i sprzętowy 13](#_Toc222495413)

[IV. Część 4 – Zakup systemu kopii zapasowej wraz z oprogramowaniem systemowym oraz zakupem zapasowych dysków serwerowych 17](#_Toc222495414)

[V. Część 5 – Zakup sprzętu komputerowego na stanowiska medyczne wraz z systemem operacyjnym oraz zakup licencji domenowych 22](#_Toc222495415)

[VI. Część 6 – Zakup i dostawa sprzętu serwerowego pod system wirtualizacyjny 27](#_Toc222495416)

[VII. Część 7 – Zakup i dostawa licencji na system wirtualizacyjny wraz z subskrypcją 29](#_Toc222495417)

[VIII. Część 8 – Audyt końcowy w obszarze cyberbezpieczeństwa. 31](#_Toc222495418)

## Część 1 – Dostawa oraz wdrożenie systemu PAM wraz z licencjami, niezbędnym sprzętem oraz usługa wsparcia

Przedmiotem zamówienia jest dostawa oraz wdrożenie systemu PAM (Privileged Access Manager) wraz z licencjami i koniecznymi systemami sprzętowymi a w szczególności:

* wykonanie Analizy Przedwdrożeniowej
* dostawa Systemu PAM w najnowszej dostępnej wersji spełniającego wymagania określone w Opisie przedmiotu zamówienia
* udzielenie licencji/subskrypcji dla Systemu PAM na warunkach producenta Systemu PAM, w liczbie zapewniającej spełnienie wszystkich wymagań Zamawiającego
* udzielenie licencji/subskrypcji dla Systemu PAM na warunkach producenta Systemu PAM
* sporządzenie i dostarczenie Zamawiającemu Dokumentacji Powykonawczej
* Wymagana ilość licencji 10 szt.

Przedmiot zamówienia obejmuje także udzielenie gwarancji na dostarczony i wdrożony System PAM, zapewnienie świadczenia usługi wsparcia technicznego przez producenta Systemu PAM oraz świadczenie usługi wsparcia technicznego Wykonawcy - przez okres min. 36 miesięcy, licząc od dnia podpisania umowy.

### Ogólne wymagania

1. Zamawiający wymaga, aby System PAM został wdrożony i zintegrowany z system SIEM, który posiada Zamawiający
2. Zamawiający wymaga, aby Wykonawca przeprowadził Analizę Przedwdrożeniową z zakresu:

* Systemu Informatycznego Zamawiającego
* kont uprzywilejowanych w Systemie Informatycznym Zamawiającego

1. Zamawiający wymaga implementację Systemu PAM w posiadanej przez Zamawiającego infrastrukturze wirtualnej (VMware lub Proxmox)
2. Zamawiający wymaga, aby Wykonawca w ramach wdrożenia wykonał:

* instalację, konfigurację i integrację Systemu PAM z Systemem Informatycznym Zamawiającego
* konfiguracja Systemu PAM musi uwzględniać:
  + Utworzenie kont użytkowników i grup Systemu PAM zgodnie z wymaganiami Zamawiającego
  + Integracja uwierzytelniania i autoryzacji użytkowników Systemu PAM z Active Directory
  + Utworzenie kont systemów docelowych w Systemie PAM
  + Utworzenie polityk związanych ze złożonością hasła
  + Utworzenie harmonogramów zmiany hasła
  + Utworzenie schematów wnioskowania o dostęp do hasła i/lub sesji
* Hardening Systemu PAM

1. Wdrożenie najlepszych praktyk bezpiecznego i optymalnego działania Systemu PAM
2. Całe rozwiązanie będzie działać na jednej maszynie wirtualnej
3. Wymagane jest dostarczenie przez Wykonawcę Projektu Technicznego Systemu PAM oraz Dokumentację Powykonawczą w formie elektronicznej (PDF i DOCX)
4. Zawartość merytoryczna Dokumentacji powykonawczej musi obejmować:

* Schemat infrastruktury i architekturę rozwiązania Systemu PAM wraz z opisem
* Zasady licencjonowania dostarczonego Systemu PAM
* Konfigurację sprzętową i logiczną elementów infrastruktury Systemu PAM
* Procedurę instalacji i konfiguracji wszystkich elementów Systemu PAM „krok po kroku”
* Procedury uruchamiania, zatrzymywania Systemu PAM oraz elementów infrastruktury
* Procedury konfiguracji kont systemu docelowego w Systemie PAM
* Procedury wykonywania kopii i odtworzenia Systemu PAM z kopii zapasowej
* Procedury uruchamiania Systemu PAM w przypadku awarii
* Procedury opisujące standardowe działania administracyjne
* Procedury odzyskania Systemu PAM po awarii
* Procedury awaryjne umożliwiające dostęp do infrastruktury w przypadku awarii Systemu PAM
* Dobre praktyki dla administratorów

1. Przeprowadzenie przez Wykonawcę testów odbiorczych z zakresu:

* Uruchamianie i zatrzymywanie Systemu PAM
* Weryfikacja procesu zarządzania hasłami na kontach systemów docelowych
* Weryfikacja procesu zarządzania sesjami
* Weryfikacja poprawności działania procedur
* Symulację awarii Systemu PAM

1. Wdrożenie całego systemu nie może negatywnie wpłynąć na działanie innych systemów
2. Dostarczone oprogramowanie musi pochodzić z oficjalnego kanału dystrybucji producenta zapewniając realizację zapisów gwarancyjnych

### Ogólne - architektura

1. System PAM musi być rozwiązaniem bezagentowym tj. umożliwiającym nawiązywanie sesji z

wykorzystaniem serwerów proxy bez potrzeby instalacji oprogramowania (agenta) na systemie, do

którego będzie nawiązywana sesja, umożliwiającym uwierzytelnianie wieloskładnikowe i obsługujące wiele platform i systemów operacyjnych. System PAM ma zabezpieczać dostęp do maszyn fizycznych, maszyn wirtualnych, sprzętu sieciowego m.in. routery, przełączniki, zapory sieciowe, aplikacje, bazy danych itp.

1. System musi być dostarczany w formie zamkniętej platformy wirtualnej przygotowanej do implementacji w infrastrukturze VMware lub ProxMox . Przez zamkniętą platformę rozumiemy wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizująca wszystkie funkcjonalności systemu.
2. Rozwiązanie nie może wymagać wdrożenia kolejnych komponentów jako osobne maszyny wirtualne lub fizyczne. Do prawidłowego działania wszystkich dostępnych funkcjonalności wymagane jest posiadanie tylko jednej maszyny wirtualnej
3. Rozwiązanie musi oferować wdrożenie drugiej instancji i konfiguracji klastra typu active-active

Licencjonowanie

1. System PAM musi zostać dostarczony z kompletem licencji dla 10 użytkowników, którzy będą korzystali z Systemu PAM, minimum dla następującej liczby funkcjonalności:

* Ochrona kont uprzywilejowanych
* Ochrona kluczy SSH
* Zarządzanie i monitorowanie sesji uprzywilejowanych
* Rejestrowanie sesji uprzywilejowanych
* Raportowanie wykorzystania kont uprzywilejowanych

1. Dostarczone licencje na System PAM do ochrony kont uprzywilejowanych nie mogą mieć ograniczeń czasowych. Dostarczone licencje będą udzielone bezterminowo
2. Dostarczone licencje na system PAM nie mogą w żaden sposób limitować ilości chronionych systemów docelowych
3. System powinien być dostarczony wraz z rocznym/trzyletnim serwisem umożliwiającym korzystanie ze wsparcia producenta oraz dystrybutora oraz pobieranie aktualizacji przygotowanych przez producenta
4. W ramach zakupionych licencji użytkownicy systemu muszą posiadać możliwość skorzystania z mechanizmu prywatnego sejfu

### Funkcjonalności

1. System PAM musi zapewniać możliwość zarządzania (w szczególności):

* Użytkownikami na systemach operacyjnych: Windows, Unix/Linux
* Kontami domenowymi: MS Active Directory
* Kontami lokalnymi: VMware ESX/ESXi
* Kontami na urządzeniach m.in.: Cisco, Aruba, Alcatel, CheckPoint, Fortigate, Huawei, IBM AIX,Brocade, UNIFI
* Kontami baz danych: Microsoft SQL, Oracle, MySQL, PostgreSQL
* Kontami do zarządzania i monitorowania serwerów: m.in. iLO, iDRAC
* Kontami w innych nie wymienionych systemach/urządzeniach do których dostęp odbywa się po protokołach: SSH, RDP,VNC, TELNET, HTTP/HTTPS
* Kluczami SSH

1. System PAM musi umożliwiać utworzenie poświadczeń typu Just-in-Time (JIT), które będą tworzone lub aktywowane na czas trwania sesji
2. System PAM musi umożliwiać usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych oraz użytkowników zewnętrznych, rejestrując obsługiwane sesje, oraz obsługując minimum następujące protokoły: SSH, RDP,VNC, TELNET, HTTP/HTTPS, X11
3. System PAM musi wspierać również protokoły bez rejestracji sesji: Cassandra, Elasticsearch, LDAP, LDAPS, MongoDB, MySQL, Oracle, PostgreSQL, Redis, Solr, SQL Server, RDS Sybase, Windows RM, Windows RPC, Windows SMB
4. System PAM musi umożliwiać dostęp użytkowników do systemu docelowego następującymi narzędziami:

* przeglądarka internetowa
* klient RDP
* klient protokołu SSH/Telnet (np. putty)
* klient serwerów bazodanowych m.in. DBeaver

1. System PAM musi wspierać minimum następujące mechanizmy uwierzytelniania: LDAP, RADIUS, Tacacs Active Directory, OpenID, SAML
2. System PAM musi zapewniać możliwość dwuskładnikowego uwierzytelniania
3. System PAM musi wspierać integrację z rozwiązaniami dwuskładnikowego uwierzytelnienia takimi jak Google Authenticator i Microsoft Authenticator
4. System PAM musi obsługiwać monitorowanie i ochronę kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego, do różnych systemów poprzez wiele lub jedno konto uprzywilejowane
5. System PAM musi ograniczać administratorowi możliwość dostępu do haseł lub ograniczać podgląd do haseł uprzywilejowanych
6. System PAM musi umożliwiać budowanie polityk kontroli dostępu w oparciu o role, np. na podstawie przynależności do grup AD/LDAP
7. System PAM musi umożliwiać budowanie polityk kontroli dostępu wymuszającej:

* podanie powodu rozpoczęcia sesji
* podanie powodu podglądu hasła
* konieczność akceptacji rozpoczęcia sesji przez innego administratora/ów
* konieczność akceptacji podglądu hasła przez innego administratora/ów
* zakresu godzin, dni oraz dat kiedy użytkownik systemu będzie miał dostęp do poświadczeń.

1. System PAM musi umożliwiać udostępnienie poświadczenia do użytku dla użytkownika poza polityką dostępową, która jest do niego przypisana. Udostępnienie musi dawać możliwość wyboru długości trwania takiego dostępu
2. System PAM musi posiadać log dla wszystkich zdarzeń systemowych
3. System PAM musi umożliwiać wskazanie kont użytkowników, które realizowały logowanie do stacji/serwera
4. System PAM musi umożliwiać raportowanie wszystkich zmian wprowadzonych przez administratorów
5. System PAM musi umożliwiać raportowanie wszystkich logowań do systemu
6. System PAM musi umożliwiać raportowanie oparte na nietypowym źródle, czasie i długości połączenia do systemu docelowego
7. Rozwiązanie musi posiadać graficzną wizualizację przedstawiającą status bezpieczeństwa aktywnych oraz historycznych sesji do systemów zdalnych
8. System PAM musi umożliwiać ograniczenie dostępu do raportów dla wskazanej grupy użytkowników lub administratorów
9. System PAM musi mieć możliwość zmiany wartości hasła na systemie docelowym zgodnie z ustawioną polityką m.in.:

* umożliwiać zdefiniowanie wymagań na: długość hasła, znaki w haśle (małe i duże litery, cyfry, znaki specjalne)
* generować automatycznie hasła kont systemów docelowych w sposób pseudolosowy
* generować unikalne hasła dla konta systemów docelowych
* wymuszać automatyczną zmianę hasła po jego podglądzie

1. System PAM musi umożliwiać transparentne połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego
2. System PAM musi umożliwiać podgląd zestawionej sesji w czasie rzeczywistym
3. System PAM musi umożliwiać przerwanie i/lub zawieszenie trwającej sesji
4. System PAM musi posiadać menu pozwalające na zawieszenie lub przerwanie wszystkich sieci oraz zablokowanie dostępu do samego rozwiązania w przypadku sytuacji krytycznej
5. System PAM musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie białych i czarnych list poleceń wykonywanych w systemie docelowym (audyt poleceń)
6. Audyt poleceń musi umożliwiać podjęcie co najmniej akcji, zablokuj polecenie i rozłącz sesję po wykryciu audytowanego polecenia a także automatyczne umieszczenie na liście blokowanych użytkowników użytkownika, który próbował wykonać blokowane polecenie
7. Nagrywanie sesji nie może mieć żadnego wpływu na wydajność systemu docelowego
8. System PAM musi umożliwiać konfigurację parametrów nagrań, w tym:

* ilości klatek na sekundę
* jakości pojedynczej klatki
* formatu pojedynczej klatki: jpg lub png
* długości przechowywania nagrań

1. System PAM musi rejestrować znaki wprowadzone z klawiatury przez użytkownika co najmniej dla sesji SSH i RDP oraz umożliwiać szybkie przeszukiwanie zapisanych danych pod kątem występowania wskazanych słów kluczowych
2. System PAM musi umożliwiać utworzenie oddzielnego zestawu ustawień w oparciu o:

* politykę dostępową
* urządzenie docelowe
* poświadczenie
* adresu źródłowego

1. System PAM musi umożliwiać odtworzenie i pobranie zarejestrowanych nagrań sesji
2. Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie producenta na terenie Polski
3. System PAM musi być kompletny i pozwalać na uruchomienie minimum następujących funkcjonalności:

* zarządzać kontami uprzywilejowanymi w ramach organizacji
* monitorować wykorzystanie kont uprzywilejowanych
* nagrywać i archiwizować sesje zdalne
* gwarantować skalowalność rozwiązania w przypadku dodawania nowych zasobów oraz nowych usług

1. System PAM musi umożliwiać personalizację wyglądu aplikacji co najmniej poprzez umieszczenie logo zamawiającego w głównym oknie aplikacji

### Integracje

1. System musi umożliwiać integrację z systemami SIEM w celu wysyłania informacji o zarejestrowanych zdarzeniach w ramach monitorowanych sesji. Musi istnieć możliwość zdefiniowania typu zdarzeń, które powinny być wysłane do systemu SIEM
2. System musi umożliwiać integrację z mechanizmami wykorzystywanymi do uwierzytelniania użytkowników, minimum hasła, LDAP, Windows NTLM, klucze SSH, RADIUS

### Szkolenia

1. Szkolenia z Systemu PAM dla co najmniej 4 administratorów, które odbędzie się w siedzibie Zamawiającego, dopuszczona jest forma zdalna szkolenia
2. Szkolenie musi być przeprowadzone w dni robocze (od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy)
3. Szkolenie będzie składać się z dwóch części: teoretycznej oraz warsztatowej
4. Zakres szkolenia:

* Ogólną architekturę Systemu PAM
* Bezpieczeństwo Systemu PAM
* Konfiguracje kont systemów docelowych w Systemie PAM
* Zarządzanie użytkownikami w Systemie PAM i integracja z innymi mechanizmami uwierzytelnienia i autoryzacji
* Polityki złożoności hasła, harmonogram zmian haseł, walidacja poprawności zmiany hasła
* Zarządzanie sesjami w Systemie PAM
* Zarządzanie schematami wnioskowania i akceptacji dostępu hasła i/lub sesji w Systemie PAM
* Audyt i raportowanie w Systemie PAM
* Procedurę aktualizacji systemu PAM
* Rozwiązywanie problemów (troubleshooting).

Przedmiot zamówienia musi pochodzić z autoryzowanego kanału dystrybucji producenta.

**Termin realizacji przedmiotu zamówienia**

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie do dnia 15.05.2026.

**Dostawa**

Klucz licencyjny/certyfikat mają być dostarczony drogą elektroniczną na adres e-mail: [przedmiot.zamowienia@ecz-otwock.pl](mailto:przedmiot.zamowienia@ecz-otwock.pl)

Wymagana jest dostawa sprzętu na adres wskazany przez Zamawiającego.

Adres dostawy: Otwock (05-400).

Dokładny adres zostanie ustalony w formie kontaktu roboczego.

Dostawa przedmiotu zamówienia potwierdzona będzie protokołem odbioru.

**Płatność**

Faktura VAT wystawiona po realizacji zamówienia rozumianego jako podpisanie protokołu odbioru zgodnie z Umową z odroczoną datą płatności 14 dni.

## Część 2 – Dostawa systemu ochrony przed wyciekiem informacji DLP wraz z kompletem niezbędnych licencji oraz zapewnieniem wsparcia technicznego i serwisu dla zaoferowanego systemu

Przedmiotem zamówienia jest dostawa systemu ochrony przed wyciekiem informacji DLP (Data Loss Prevention) wraz z kompletem niezbędnych licencji oraz zapewnieniem wsparcia technicznego i serwisu dla zaoferowanego systemu na okres 36 miesięcy od dnia podpisania umowy.

### Przedmiot zamówienia obejmuje

1. Dostawę niezbędnych licencji i oprogramowania Systemu DLP dla 300 użytkowników w ramach zamówienia podstawowego na okres 36 miesięcy, licząc od dnia podpisania umowy
2. Świadczenie serwisu i wsparcia technicznego Wykonawcy przez okres obowiązywania umowy:

* dostęp do wsparcia i pomocy technicznej Wykonawcy w dni robocze przez okres trwania umowy
* usuwanie usterek i błędów
* zapewnienie dostępu do konta wsparcia Systemu DLP, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta
* zapewnienie dostępu do poprawek i nowych wersji Systemu DLP
* zapewnienie dostępu do dokumentacji technicznej Systemu DLP, dostępnej co najmniej w języku angielskim
* Wymagana ilość licencji 300 szt.

1. Realizacje Dokumentacji Powykonawczej w formie elektronicznej (PDF i DOCX):

* opis zastosowanego oprogramowania
* aktywacji licencji potrzebnych do funkcjonowania wdrażanego systemu
* opis struktury i konfiguracji Systemu, w tym pliki konfiguracyjne
* procedury przeglądów logów wraz z procedurami kontrolnymi
* procedury uruchamiania, zatrzymywania Systemu DLP oraz elementów infrastruktury
* procedury wykonywania kopii i odtworzenia Systemu DLP z kopii zapasowej
* procedury uruchamiania Systemu DLP w przypadku awarii
* procedury opisujące standardowe działania administracyjne
* procedury odzyskania Systemu DLP po awarii
* wytyczne (dobre praktyki) dla administratorów

### Wymagania serwera administracyjnego

1. System operacyjny:
   * Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
   * Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
2. Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 (64-bit) i nowszych
3. Serwer administracyjny musi obsługiwać bazy danych: a. MS SQL Server 2016 lub nowsze, b. MS SQL Express, c. AzureSQL S3 lub nowsze
4. Pomoc i dokumentacja programu dostępne w języku polskim lub angielskim
5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim
6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta
7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych
8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym
9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia
10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli
11. System musi posiadać mechanizm usuwający najstarsze informacje, gdy rozmiar bazy osiągnie domyślny limit
12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania
13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu
14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu)
15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory
16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym
17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa
18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości e-mail oraz czynności na plikach
19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików
20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych
21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email
22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu
23. Serwer administracyjny musi posiadać możliwość połączenia z serwerem SMTP udostępnianym przez producenta
24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików
25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku
26. Administrator musi mieć możliwość tworzenia kategorii danych dla plików zaszyfrowanych lub dla takich gdzie zawartość pliku jest niemożliwa do odczytania
27. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
28. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, numer REGON, NIP, wyrażenia regularne, określone ciągi znaków i numer IBAN
29. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym
30. Administrator musi mieć możliwość wyszukiwania danych wrażliwych w zasobach lokalnych
31. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM
32. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP
33. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania
34. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.
35. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams
36. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach
37. System musi umożliwiać synchronizacji grup bezpieczeństwa z Active Directory na potrzeby logowania do konsoli zarządzającej
38. System musi umożliwiać administratorowi nadanie użytkownikowi uprzywilejowanego dostępu, przez co nie będzie obejmowany politykami przez określony czas – 1 godzinę, 6 godzin lub do końca dnia
39. System musi posiadać możliwość tworzenia polityk dynamicznych, pozwalających na dostosowywanie się akcji (takich jak zapisywanie logu, powiadomienie użytkownika, blokowanie lub blokowanie z możliwością zastąpienia przez użytkownika) w zależności od profilu pracy użytkownika wykonującego daną czynność, gdzie akcja dobierana jest w zależności od wyniku systemu uczenia maszynowego
40. System musi umożliwiać dostosowanie polityk dynamicznych do dwóch trybów: standardowy oraz łagodny. Możliwość taka musi istnieć per użytkownik
41. System musi umożliwiać tworzenie raportów na podstawie logów zebranych w układach danych z możliwością dostosowania filtrów, użytkowników oraz zakresu czasu objętych raportowaniem
42. System musi umożliwiać utworzenie raportu, który będzie zawierał podsumowanie stanu zabezpieczenia danych wraz z rekomendacjami w formie cyklicznej
43. System musi zbierać informacje na temat podłączanych urządzeń do komputera, odwiedzanych domen internetowych, ścieżek sieciowych, drukarek lokalnych oraz sieciowych, umożliwiając jednocześnie przypisanie takowych wpisów do bezpiecznych lub niezaufanych lokalizacji bez potrzeby manualnego wpisywania ścieżek lub numerów seryjnych urządzeń
44. Dla każdej z wyżej wymienionych lokalizacji system powinien umożliwiać przypisanie indywidualnej polityki dostępu – np. umożliwiając przesyłanie danych do lokalizacji oznaczonej jako bezpieczna, jednocześnie blokując wysyłkę do lokalizacji oznaczonej jako niezaufana lub nieprzypisana
45. System musi umożliwiać audyt operacji wykonywanych przez administratora w obszarze konsoli DLP
46. System musi umożliwiać podłączenie archiwa logów w formacie plików o rozszerzeniu mdf

Przedmiot zamówienia musi pochodzić z autoryzowanego kanału dystrybucji producenta.

**Termin realizacji przedmiotu zamówienia**

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie do dnia 15.05.2026.

**Dostawa**

Klucz licencyjny/certyfikat mają być dostarczony drogą elektroniczną na adres e-mail: [przedmiot.zamowienia@ecz-otwock.pl](mailto:przedmiot.zamowienia@ecz-otwock.pl)

Wymagana jest dostawa sprzętu na adres wskazany przez Zamawiającego.

Adres dostawy: Otwock (05-400).

Dokładny adres zostanie ustalony w formie kontaktu roboczego.

Dostawa przedmiotu zamówienia potwierdzona będzie protokołem odbioru.

**Gwarancja i wsparcie**

Nie mniej niż 36 miesięcy.

**Wdrożenie**

Wdrożenie, instalacja, konfiguracja realizowane jest przez Wykonawcę.

**Szkolenia**

Szkolenia dla co najmniej 4 administratorów, które odbędzie się w siedzibie Zamawiającego, dopuszczona jest forma zdalna szkolenia.

## Część 3 – Dostarczenie oraz wdrożenie systemu klasy NDR, w tym system aplikacyjny i sprzętowy

Przedmiotem zamówienia jest dostarczenie oraz wdrożenie systemu klasy NDR (Network Detection and Response)

1. W składa systemu NDR musi wchodzić sprzęt fizyczny jak również oprogramowanie wraz z niezbędnymi licencjami.
2. Wykonanie analizy przedwdrożeniowej.
3. Całość musi zostać dostarczona i wdrożona w infrastrukturze Zamawiającego.
4. System NDR musi realizować swoje funkcje lokalnie On-Premise
5. Dostarczony System NDR musi być licencjonowany na okres trzech lat z możliwością zakupu dodatkowych licencji
6. Wsparcie techniczne musi być zapewnione na okres trzech lat od momentu podpisania umowy.
7. Sprzęt dostarczony w ramach umowy musi być objęty gwarancją na okres nie krótszy niż 24 miesiące
8. W skład systemu będą wchodzić:

* fizyczne sądy monitorujące
* fizyczne urządzenie zarządzające
* oprogramowanie instalowane na sondach oraz urządzeniu zarządzającym

1. Sondy służące do monitorowania muszą:

* na dedykowanych portach sondy muszą rejestrować kopię ruchu sieciowego
* podczas pierwszej analizy ruch sieciowy musi być przeszukiwany pod kątem podatności, analiza powinna obywać się za pośrednictwem traffic payloads.
* przetworzony strumień musi być przekazywany do urządzenia nadrzędnego
* pliki muszą być w standardzie pcap
* w przypadku wykrycia anomalii muszą być generowane alarmy o zdarzeniach
* do urządzenia nadrzędnego sona musi generować powiadomienia o jej działaniu

1. Urządzenie fizyczne musi:

* zarządzać wszystkimi sondami, weryfikować ich stan
* na urządzeniu musi odbywać się analiza shellcodes
* musi odbywać się analiza w oparciu o inżynierię wsteczną
* ROP (Return Oriented Programming)
* heurystyka
* JOP (Jump Oriented Programming)
* statyczne silniki malware
* w systemie muszą być dostępne wyniki przeprowadzonych analiz
* System musi posiadać moduł do przechowywania metadanych na potrzeby kolejnych analiz
* System musi mieć możliwość wysyłki logów syslog do systemów klasy SIEM z którego korzysta Zamawiający
* Obsługa nie mniej niż 2000 zdarzeń na sekundę
* Wolumen odbieranego ruchu sieciowego nie mniejszy niż 400 Mbps

1. Komunikacja pomiędzy sondami a urządzeniem administrującym musi odbywać się za pośrednictwem sieci IP
2. Do urządzenie musi mieć możliwość podłączenia wielu sond
3. System musi zapewnić bezpieczne (szyfrowane) połączenia pomiędzy sondami a urządzeniem administrującym
4. Sondy muszą wspierać protokoły IPv4, IPv6 i 802.1Q
5. Sonda musi być odporna na zakłócenia komunikacji z urządzeniem administrującym (dane zebrane podczas braku połączenia muszą być przesłane po odzyskaniu komunikacji)
6. Urządzenia fizyczne muszą posiadać redundantne zasilanie
7. posiadać technologię hot-swap oraz hot-plug
8. System NDR musi posiadać narzędzia do definiowania zasad detekcji oraz zakresów sieci na podstawie adresacji IP oraz VLAN
9. System NDR musi mieć możliwość obsługi protokołów takich jak DCE-RPC, DHCP, DNP3, DNS\_udp, DNS\_tcp, ENIP, FTP, HTTP, HTTP/2, IKEv2, Kerberos (KRB5), MQTT, NFS, RDP, RFB, SIP, SMB, SMTP, SNMP, SSH, TFTP, TLS.
10. System NDR musi wykrywać i obsłużyć nie mniej niż 500 unikatowych adresów IP
11. Dostęp do konsoli/konsol administracyjnych powinien odbywać się poprzez zabezpieczone połączenie HTTPS w przeglądarce
12. Każda z sond musi posiadać: architekturę modułową co pozwoli na ewentualną rozbudowę urządzenia za pośrednictwem kart rozszerzeń, minimum 4 porty monitorujące (możliwość rozszerzenia o kolejne), wybór standardu połączenia (kabel sieciowy lub kabel światłowodowy SFP lub SFP+), konfiguracja RAID 1 lub RAID 5 (do wyboru)
13. Standard odczytu plików pcap
14. Możliwość zaimplementowania sondy jako maszyny wirtualnej
15. W konsoli NDR muszą znaleźć się informacje związane z detekcjami oraz informacje takie jak adres IP, adres MAC, porty sieciowe, wyniki skanów, protokoły sieciowe, silnik detekcji który wykrył zagrożenie, sygnatury czasowe
16. Konsola NDR musi również zawierać podgląd zdarzeń, szacowany poziom ryzyka dla wykrytych zagrożeń, mapowania zagrożeń w odniesieniu do przynajmniej jednego framework-a np. MITRE
17. W konsoli NDR musi być możliwość dodania tagów jak również opisu lub notatek do zdarzenia
18. Konsola administracyjna musi posiadać funkcjonalności takie jak: kontrola stanu urządzeń, ilości wykorzystanych zasobów, dane diagnostyczne
19. Z konsoli administracyjnej musi być możliwość eksportu danych
20. W konsoli administracyjnej musi być możliwość konfiguracji ustawień komponentu uczenia maszynowego, antymalware, analizy ruchu sieciowego, jego modyfikacji, dodawania źródeł definicji reguł, konfiguracja komponentu analizy ruchu sieciowego oraz jego modyfikację, dodawanie źródeł definicji reguł
21. Konsola administracyjna musi umożliwiać zarządzanie kontami użytkowników
22. W konsoli administracyjnej musi odbywać się korelacja danych na podstawie wprowadzonych filtrów
23. System NDR musi obsługiwać silniki detekcji takie jak

* antymalware (skan plików w ruchu sieciowym aby zidentyfikować szkodliwe oprogramowanie),
* silniki skanowania w poszukiwaniu zagrożeń typu malware powinny obsługiwać również mechanizm skanowania plików sklasyfikowanych jako podejrzane, z użyciem nowych sygnatur po aktualizacji silnika detekcji na poziomie minimum 10 plików na sekundę
* analiza shellcode i powershell – detekcja technik wykorzystywanych przez cyberprzestępców w postaci specyficznego kodu służącego do wykrywania podatności oprogramowania zainstalowanego na stacjach roboczych czy serwerach
* analiza ruchu w oparciu o definicje zagrożeń – analiza całego ruchu sieciowego w oparciu o dostarczone reguły opisujące charakter niebezpiecznych połączeń, musi umożliwiać dodawanie i modyfikowani dodawanie własnych sygnatur ataków
* domain generation algorithm (DGA) – wykrywanie losowego generowanie domen, które są używane do okresowego generowania dużej liczby nazw domen, które mogą być używane jako odnośniki do połączeniami z serwerami C&C (Command and Control)

1. Aktualizacja komponentów oprogramowania narzędziowego musi być wykonywana manualnie przez administratora systemu
2. Aktualizacja sygnatur musi odbywać się metodą online, manualnie lub lokalnie (lokalne repozytorium)
3. System musi dawać możliwość wykonania kopii zapasowej ustawień systemu
4. System musi zapewnić retencję logów
5. W systemie musi być możliwość zdefiniowania uprawnień do dostępu do danych dla przynajmniej trzech poziomów: administrator, użytkownik uprzywilejowany oraz operator
6. W systemie musi być odnotowane każde logowanie użytkownika.
7. Wykonawca zrealizuje Dokumentację Powykonawczą w formie elektronicznej (PDF i DOCX):

* opis zastosowanego oprogramowania i sprzętu,
* aktywacji licencji potrzebnych do funkcjonowania wdrażanego systemu,
* opis struktury i konfiguracji Systemu,
* procedury przeglądów logów wraz z procedurami kontrolnymi,
* procedury uruchamiania, zatrzymywania Systemu oraz elementów infrastruktury,
* procedury wykonywania kopii i odtworzenia Systemu z kopii zapasowej,
* procedury uruchamiania Systemu w przypadku awarii,
* procedury opisujące standardowe działania administracyjne,
* procedury odzyskania Systemu po awarii,
* wytyczne (dobre praktyki) dla administratorów.

Przedmiot zamówienia musi pochodzić z autoryzowanego kanału dystrybucji producenta.

**Termin realizacji przedmiotu zamówienia**

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie do dnia 15.05.2026.

**Dostawa**

Klucz licencyjny/certyfikat mają być dostarczony drogą elektroniczną na adres e-mail: [przedmiot.zamowienia@ecz-otwock.pl](mailto:przedmiot.zamowienia@ecz-otwock.pl)

Dostawa przedmiotu zamówienia potwierdzona będzie protokołem odbioru.

**Gwarancja**

Nie mniej niż 36 miesiące.

**Wdrożenie**

Wdrożenie, instalacja, konfiguracja realizowane jest przez Wykonawcę przy współpracy z działem informatycznym Zamawiającego.

**Szkolenia**

Szkolenia dla co najmniej 4 administratorów, które odbędzie się w siedzibie Zamawiającego, dopuszczona jest forma zdalna szkolenia.

## Część 4 – Zakup systemu kopii zapasowej wraz z oprogramowaniem systemowym oraz zakupem zapasowych dysków serwerowych

Zamówienie składa się z dwóch zadań. Obejmuje zakup systemu kopii zapasowej wraz z oprogramowaniem systemowym oraz zakupem zapasowych dysków serwerowych.

### Zadanie A - sprzęt i zintegrowane oprogramowanie

|  |  |  |
| --- | --- | --- |
|  | **SPRZĘT KOMPUTEROWY I ZINTEGROWANE OPROGRAMOWANIE** | **szt.** |
| Zadanie A | Zakup systemu do realizacji zabezpieczonej kopii zapasowej | 1 |

Wymagania dotyczące oferowanego przedmiotu zamówienia:

1. oferowane urządzenie muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta oraz musi reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń po zwrocie, odnawianych, demonstracyjnych lub powystawowych;
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 objęte gwarancją producenta;
4. urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta;

Przedmiot zamówienia musi pochodzić z autoryzowanego kanału dystrybucji producenta.

**Termin realizacji przedmiotu zamówienia**

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie do 45 dni

kalendarzowych od daty zawarcia umowy.

**Dostawa**

W pełni kompletny serwer zostanie dostarczony na wskazany przez Zamawiającego adres.

Adres dostawy: Borowa 14/18, 05-400 Otwock.

Dokładny adres zostanie ustalony w formie kontaktu roboczego.

**Płatność**

Faktura VAT wystawiona po realizacji zamówienia rozumianego jako podpisanie protokołu odbioru zgodnie z Umową z odroczoną datą płatności 14 dni.

**Gwarancja**

1. Wykonawca w ramach realizacji Przedmiotu Zamówienia udzieli Zamawiającemu gwarancji zgodnie z wymaganiami opisanymi dla pozycji w poniższym rozdziale.
2. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem podpisania Protokołu Odbioru przez Zamawiającego.
3. Naprawy gwarancyjne muszą być realizowane przez serwis producenta lub autoryzowanego partnera serwisowego producenta.

**Szczegóły przedmiotu zamówienia**

Wymagane jest dostarczenie sprzętu z wbudowanym systemem/oprogramowaniem do realizacji i zarządzania kopiami zapasowymi. Oferowany przedmiot musi spełniać poniższe minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Komponentu** | **Wymagane parametry techniczne** |
| **Obudowa** | 2U |
| **Procesor** | Procesor osiągający w teście CPU Benchmarks, w kategorii CPU Mark (higher is better) wynik co najmniej **25000** pkt. według wyników opublikowanych na stronie  <http://www.cpubenchmark.net/cpu_list.php>.  Zamawiający zweryfikuje wydajność zaoferowanego procesora według wyników testów procesorów opublikowanych na stronie: <http://www.cpubenchmark.net/cpu_list.php> - należy załączyć do oferty dokument potwierdzający spełnianie wymogu w postaci wydruku ze strony [http://www.cpubenchmark.net/cpu\_list.php](http://www.cpubenchmark.net/cpu_list.phpw). |
| **Pamięć** | Min. 64GB  Pamięć musi być w 100% kompatybilna z wymogami producenta.  Listę zgodności sprzętowej producent musi prezentować na swojej stronie internetowej. |
| **Pamięć masowa** | Min. 2 dyski SSD 4 TB każdy;  Min. 10 dysków 20 TB każdy;  Dyski muszą być w 100% kompatybilne z wymogami producenta;  Listę zgodności sprzętowej producent musi prezentować na swojej stronie internetowej. |
| **Zabezpieczenie przed awarią dysków** | Minimalna obsługa systemów RAID 1, 5, 6 lub kompatybilnych  Obsługa systemu plików Btrfs |
| **Interfejsy** | Oddzielny port zarządzający: min. 1 port 1GbE RJ-45  Przesył danych: min. 2 porty 10GbE RJ-45  Przesył danych: min. 1 port 25GbE SFP28 |
| **Zasilanie** | Dwa gniazda zasilania |
| **Akcesoria** | Wysuwane szyny montażowe do szafy RACK |
| **Właściwości systemu/oprogramowania** | System posiada konsole zarządzającą;  Musi realizować kopię zapasową, przywracać, deduplikować,  replikować i zarządzać kopiami;  System musi być chroniony przed nieautoryzowanym dostępem do interfejsu za pomocą oddzielnego interfejsu zarządzającego;  Dostęp do interfejsu jest z realizowany minimum z poziomu protokołu https z konfigurowalną obsługą podwójnej autoryzacji MFA;  System posiada wbudowany, konfigurowalny firewall;  System obsługuje realizacje kopii zapasowe i przywracania dla:   * systemów PC z systemem Windows i Mac, * bezagentowa kopia systemów maszyn wirtualnych VMware/Hyper-V, * serwerów Windows/Linux, * kopii danych bazodanowych: Oracle i Microsoft SQL.   Posiada tworzenie planów kopii zapasowych;  Posiada funkcjonalność okresowego wyłączenia serwera kopii zapasowej poprzez wyłączenie np. kart sieciowych lub samego serwera;  Posiada funkcję szyfrowania kopii;  Transmisja przesyłu danych może być szyfrowana;  Blokowe przesyłanie pakietów danych dla zoptymalizowania wydajności tworzenia kopii;  Posiada funkcjonalność WORM (Write-Once-Read-Many);  Posiada własny system wirtualizacji w którym można szybko uruchomić kopie zwirtualizowanej maszyny;  Może realizować testowe odzyskiwanie po awarii w środowisku „piaskownicy”  Odzyskiwać można całe urządzenie lub pliki;  Monitorowanie stanu całego systemu jest realizowane w czasie rzeczywistym;  System może zarządzać kopiami zapasowymi innych serwerów backupowych; |
| **Gwarancja** | 5 lat |

### Zadanie B - zakup dysków

|  |  |  |
| --- | --- | --- |
|  | **Nazwa licencji** | **szt.** |
| Zadanie B | Dyski do systemu kopii zapasowej, zapas | 12 |

Wymagania dotyczące oferowanego przedmiotu zamówienia:

1. oferowane dyski muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta oraz musi reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń po zwrocie, odnawianych, demonstracyjnych lub powystawowych;
2. nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta;
3. sprzęt musi być objęty gwarancją producenta;
4. dyski muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta;

Przedmiot zamówienia musi pochodzić z autoryzowanego kanału dystrybucji producenta.

**Termin realizacji przedmiotu zamówienia**

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie do 45 dni kalendarzowych od daty zawarcia umowy.

**Dostawa**

Dyski zostaną dostarczone na wskazany przez Zamawiającego adres.

Adres dostawy: Borowa 14/18, 05-400 Otwock.

Dokładny adres zostanie ustalony w formie kontaktu roboczego.

**Płatność**

Faktura VAT wystawiona po realizacji zamówienia rozumianego jako podpisanie protokołu odbioru zgodnie z Umową z odroczoną datą płatności 14 dni.

**Gwarancja**

1. Wykonawca w ramach realizacji Przedmiotu Zamówienia udzieli Zamawiającemu gwarancji zgodnie z wymaganiami opisanymi dla pozycji w poniższym rozdziale.
2. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem podpisania Protokołu Odbioru przez Zamawiającego.
3. Naprawy gwarancyjne muszą być realizowane przez serwis producenta lub autoryzowanego partnera serwisowego producenta.

**Szczegóły przedmiotu zamówienia**

Oferowany przedmiot musi spełniać poniższe minimalne parametry funkcjonalne:

|  |  |
| --- | --- |
| **Komponentu** | **Wymagane parametry techniczne** |
| **Pamięć masowa** | 12 sztuk dysków HDD 20 TB każdy  Dyski muszą być w 100% kompatybilne z wymogami producenta dla systemu kopi zapasowej z punktu A - sprzęt i zintegrowane oprogramowanie |
| **Gwarancja** | 5 lat |

## Część 5 – Zakup sprzętu komputerowego na stanowiska medyczne wraz z systemem operacyjnym oraz zakup licencji domenowych

Zamówienie składa się z dwóch zadań. Obejmuje zakup sprzętu komputerowego na stanowiska medyczne wraz z systemem operacyjnym oraz zakup licencji domenowych.

### Zadanie A - sprzęt i system operacyjny

|  |  |  |
| --- | --- | --- |
|  | **SPRZĘT KOMPUTEROWY Z OPROGRAMOWANIEM** | **sztuk** |
| Zadanie A | Komputer stacjonarny typu All In One z systemem operacyjnym Microsoft Windows 11 Pro. | 70 |

Wymagania dotyczące oferowanych komputerów:

* oferowane urządzenia muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta oraz muszą reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń po zwrocie, odnawianych, demonstracyjnych lub powystawowych;
* nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta;
* elementy, z których zbudowane są urządzenia muszą być objęte gwarancją producenta;
* urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.

Przedmiot zamówienia musi pochodzić z autoryzowanego kanału dystrybucji producenta.

**Termin realizacji przedmiotu zamówienia**

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie do 45 dni

kalendarzowych od daty zawarcia umowy.

**Dostawa**

Dyski zostaną dostarczone na wskazany przez Zamawiającego adres.

Adres dostawy: Borowa 14/18, 05-400 Otwock.

Dokładny adres zostanie ustalony w formie kontaktu roboczego.

Odbiór przedmiotu zamówienia potwierdzony będzie protokołem odbioru.

**Płatność**

Faktura VAT wystawiona po realizacji zamówienia rozumianego jako podpisanie protokołu odbioru zgodnie z Umową z odroczoną datą płatności 14 dni.

**Gwarancja**

1. Wykonawca w ramach realizacji Przedmiotu Zamówienia udzieli Zamawiającemu gwarancji zgodnie z wymaganiami opisanymi dla pozycji w poniższym rozdziale.
2. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem podpisania Protokołu Odbioru przez Zamawiającego.
3. Naprawy gwarancyjne muszą być realizowane przez serwis producenta lub autoryzowanego partnera serwisowego producenta.

**Szczegółowy przedmiot zamówienia**

Wymagane jest dostarczenie 70 szt. komputerów stacjonarnych typu All in One wraz z systemem operacyjnym spełniających opisane poniżej minimalne parametry funkcjonalne:

|  |  |  |
| --- | --- | --- |
| **Komponentu** | **Wymagane parametry techniczne komputerów** | |
| **Typ** | Komputer stacjonarny – All in One (AiO) | |
| **Zastosowanie** | Komputer będzie wykorzystywany jako stacja pielęgniarska, lekarska do obsługi oprogramowania medycznego | |
| **Obudowa** | Typu All-in-One zintegrowana z monitorem min. 23.8”.  Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej  Monitor musi mieć możliwość obracania monitora w osi pionowej i poziomej bez obracania podstawy stopy monitora.  Monitor musi mieć możliwość regulacji monitora na stopie monitora.  Monitor musi posiadać systemu montażowy VESA 100. | |
| **Typowe**  **parametry**  **wyświetlacza** | Rozmiar i typ matrycy | min. 23,8” |
| Rozdzielczość | min. FHD (1920x1080) |
| Częstotliwość odświeżania | min. 60 Hz |
| Rodzaj matrycy | Matowa IPS |
| **Płyta główna** | Płyta główna wyposażona w  min. 2 złącza SO - DIMM z obsługą do 64GB DDR5 pamięci RAM, min. 1 złącze M.2 dla dysku oraz 1 złącze M.2 karty WiFi. | |
| **Procesor** | Procesor osiągający w teście CPU Benchmarks, w kategorii CPU Mark (higher is better) wynik co najmniej 40000 pkt. według wyników opublikowanych na stronie  <http://www.cpubenchmark.net/cpu_list.php>.  Zamawiający zweryfikuje wydajność zaoferowanego procesora według wyników testów procesorów opublikowanych na stronie: <http://www.cpubenchmark.net/cpu_list.php> - należy załączyć do oferty dokument potwierdzający spełnianie wymogu w postaci wydruku ze strony [http://www.cpubenchmark.net/cpu\_list.php](http://www.cpubenchmark.net/cpu_list.phpw). | |
| **Pamięć RAM** | Min. 16GB DDR5 4800 MT/s.  Jeden slot pozostaje wolny. | |
| **Pamięć masowa** | Dysk M.2 SSD min. 512GB PCIe NVMe | |
| **Grafika** | Zintegrowana | |
| **Komunikacja** | Karta sieciowa 1000 zintegrowana z płytą główną, wspierająca obsługę WoL  Karta Wi-Fi 6E AX z Bluetooth 5.3 (lub nowsze) | |
| **Wyposażenie**  **multimedialne** | Karta dźwiękowa zintegrowana z płytą główną, wbudowane min. dwa głośniki o mocy min. 2W każdy.  Wbudowana w obudowę kamera Full HD mechanicznie chowana w obudowie (nie dopuszcza się kamer przekręcanych i wystających poza obrys obudowy).  Wbudowane w obudowę dwa mikrofony. | |
| **Bezpieczeństwo i zdalne zarządzanie** | Wbudowana w płytę główną technologia zdalnego monitorowania i zarządzania komputerem na poziomie sprzętowym (out-of-band) działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC.  Wymagana jest obsługa funkcji zdalnego zarządzania przez wbudowane w komputer porty zarówno sieci przewodowej LAN, jak i bezprzewodowej WLAN, z wykorzystaniem protokołów TCP/IP wraz z szyfracją komunikacji zarządzania z silnym protokołem minimum TLS 1.2.  Musi obsługiwać funkcje minimum:   * zdalny odczyt konfiguracji, * kontrole stanu zasilania, * TPM minimum w wersji 2.0 * zdalną konfigurację ustawień przez interfejs BIOS, * zdalne przejęcie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) na poziomie sprzętowym bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego, * przekierowanie procesu ładowania systemu operacyjnego z wirtualnego nośnika CDROM/DVD/Boot USB storage w formie pliku obrazu bootującego takiego nośnika z serwera zarządzającego technologią zdalnego zarządzania sprzętowego w celu reinstalacji OS. * dostęp pracowników działu IT do konsoli serwera zarządzania zdalnego tą technologią powinien obsługiwać funkcję szyfrowania oraz co najmniej autentykację poświadczeń z wykorzystaniem własnej bazy użytkowników lub MS Active Directory. | |
| **System operacyjny** | Zainstalowany system operacyjny Microsoft Windows 11 Pro PL.Klucz licencyjny musi być zapisany trwale w BIOS i umożliwiać reinstalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. | |
| **Wymagania**  **dodatkowe** | Klawiatura USB w układzie US international (qwerty)  Mysz optyczna USB z co najmniej dwoma przyciskami oraz rolką (scroll). | |
| **Warunki gwarancji** | Firma serwisująca posiada status autoryzowanego przedstawiciela sprzętu, które stanowią przedmiot oferty.  Czas trwania wsparcia technicznego producenta wynosi 36 miesięcy. | |

|  |  |
| --- | --- |
| **Zdalne zarządzanie - konsola zarządzania** | Wszystkie dostarczone komputery muszą być obsługiwane przez jedno narzędzie/konsole.  Dostawca musi dostarczyć narzędzia i oprogramowanie służące do konfiguracji ustawień konfiguracji tej technologii zdalnego zarządzania na poziomie sprzętowym oraz do samego zdalnego zarządzania zgodnie z wymogami funkcji wymienionym w pkt **Bezpieczeństwo i zdalne zarządzanie**. Przez dostarczenie rozumie się również wskazania adresu strony WWW gdzie zamawiający może pobrać bezpłatnie takie narzędzia i oprogramowanie.  Narzędzia i oprogramowanie muszą posiadać walidację i wsparcie dla zastosowań produkcyjnych dla przewidywanej przez zamawiającego całkowitej łącznej ilości zarządzanych komputerów. Musi też mieć możliwość obsługi w przyszłości kolejnych stacji komputerowych zamawiającego. |

### Zadanie B - zakup licencji domenowych

|  |  |  |
| --- | --- | --- |
|  | **Nazwa licencji** | **szt.** |
| Zadanie B | Microsoft Windows Server 2025 - 1 Device CAL, licencja wieczysta | 16 |

Przedmiot zamówienia musi pochodzić z autoryzowanego kanału dystrybucji producenta.

**Zamówienie licencji**

Licencja będzie przypisana programy licencjonowania Microsoft: CSP Perpetual na email: [informatyka@eczotwockzoo.onmicrosoft.com](mailto:informatyka@eczotwockzoo.onmicrosoft.com)

Po zrealizowaniu zamówienia licencje będą dostępne w portalu Klienta Microsoft 365 Admin Center (MAC). Po zalogowaniu na portalu [https://admin.microsoft.com](https://admin.microsoft.com/) będzie można zweryfikować ilość zakupionych licencji (Rozliczenia/Twoje produkty).

**Termin realizacji przedmiotu zamówienia**

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie do 14 dni kalendarzowych od daty zawarcia umowy.

**Odbiór**

Odbiór przedmiotu zamówienia potwierdzony będzie protokołem odbioru.

**Płatność**

Faktura VAT wystawiona po realizacji zamówienia zgodnie z Umową z odroczoną datą płatności 14 dni.

## Część 6 – Zakup i dostawa sprzętu serwerowego pod system wirtualizacyjny

1. Parametry techniczne wymaganego serwera:

* serwer 2U Rack 19 cali wraz z akcesoriami do podłączenia w szafie RACK
* obudowa wyposażenia w zamykany, zdejmowany panel przedni chroniący przed nieuprawionym dostępem do dysków
* obudowa wyposażona w panel informacyjny, trwale zintegrowany z frontem obudowy, pokazujący mapę komponentów serwera, w tym realizuje identyfikacji usterki podzespołu   
  lub panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera
* możliwość wyposażenia serwera w czujniki otwarcia obudowy współpracującego z BIOS/UEFI.
* zainstalowany moduł TPM 2.0
* jeden procesor Intel Xeon Gold 5520+ 52.5M Cache, 2.20 GHz 28-rdzeniowy lub równoważny procesor minimum 28-rdzeniowy, osiągający w testach Multithread Rating nie mniej niż 60000 punktów /www.cpubenchmark.net/
* wyposażony w pamięci nie mniej niż 256GB /np. 2x128GB/
* zatoki dyskowe 12 dysków typu Hot Swap SAS/SATA/SSD 2.5’’ w tym startowo:
  + 3 dysków nie mniejszych niż 960GB 6G Mixed Use SFF BC Multi Vendor SSD,
  + 7 dysków nie mniejszych niż 1.92TB NVMe Gen4 U.3 SSD.
* kontroler sprzętowy z obsługa RAID 0/1/10/5/50/6/60 /praca z dyskami w trybach RAID i JBOD jednocześnie/ oraz z podtrzymywaniem zawartości pamięci cache minimum 8GB + zestaw bateryjny
* minimum 2 porty 10GbE SFP+
* minimum 2 porty 10GbE RJ-45
* 2 szt. modułów 10Gb SFP+ SR Transceiver
* 2 szt. zasilacza minimum 1000W
* karta zarządzająca dedykowana poprzez port RJ45 z obsługą serwisową rozszerzoną na 3 lata
* wbudowane w serwer oprogramowanie konfigurująco-monitorujące podzespoły serwera w czasie rzeczywistym w wersji rozszerzonej /Advanced/, posiadające minimalne funkcje:
  + dostęp zdalny do graficznego interfejsu zarządzającego poprzez interfejs web: https
  + zarządzanie dostępem do interfejsu dla użytkowników
  + dostęp do log systemu
  + pełna obsługa konsoli HTML5
  + możliwość montowania plików ISO z poziomu URL
  + możliwość aktualizacja firmware, bios, komponentów sprzętowych przez cały okres trwania wsparcia serwisowego z poziomu oprogramowania konfigurująco-monitorującego
  + zainstalowana wersja firmware nie starsza niż 01.08.2025 dla data publikacji
  + monitorowanie stanu pracy sprzętu, w tym zainstalowanych wszystkich dysków
  + możliwość eksportu/importu konfiguracji systemu konfigurująco-monitorującego
  + obsługa alertów dla błędnie działających komponentów poprzez email z obsługą SMTP SSL/TLS i SMTP Authentication
  + obsługa Syslog
  + wsparcie dla IPMI 2.0, SNMP v3, VLAN tagging, SSH
* urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta
* wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001 lub normami równoważnymi
* deklaracja zgodności CE
* Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet
* Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Przedmiot zamówienia musi pochodzić z autoryzowanego kanału dystrybucji producenta.

**Wdrożenie**

Zamawiający nie wymaga wdrożenia.

**Termin realizacji przedmiotu zamówienia**

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie do 70 dni kalendarzowych od daty zawarcia umowy.

**Gwarancja i wsparcie**

Nie mniej niż 3-letni okres wsparcia serwisowego

Nie mniej niż 3-letnia gwarancja producenta w miejscu instalacji

**Szkolenia**

Zamawiający nie wymaga szkoleń w zakresie instalacji czy obsługi.

**Dostawa**

W pełni kompletny serwer zostanie dostarczony na wskazany adres Zamawiającego wraz z załączonymi instrukcjami, licencjami producenta.

Adres dostawy: Borowa 14/18, 05-400 Otwock.

Dokładny adres zostanie ustalony w formie kontaktu roboczego.

Odbiór przedmiotu zamówienia potwierdzony będzie protokołem odbioru.

## Część 7 – Zakup i dostawa licencji na system wirtualizacyjny wraz z subskrypcją

System wirtualizacyjny będzie zainstalowany na serwerze z zapytania ofertowego Część 6.

System wirtualizujący Proxmox VE z obsługą serwisową na minimum 3 lata lub system wirtualizacyjny równoważny.

Zamawiający uzna za równoważny system wirtualizacyjny spełniający co najmniej poniższe wymagania techniczne:

* 1. oferowane oprogramowanie wirtualizacyjne musi stanowić autonomiczny system operacyjny dedykowany wyłącznie do zadań wirtualizacji;
  2. zarządzanie poprzez zintegrowany interfejs graficzny WEB-GUI, który pozwala na monitorowanie i zarządzanie wszystkimi zasobami z jednego miejsca;
  3. posiada funkcję: live migration, storage live migration, snapshot, replikację oraz wbudowane narzędzia do backupu;
  4. wspiera różne metod uwierzytelniania, jak np. Microsoft Active Directory, Linux PAM oraz podwójną autoryzację do logowania
  5. realizacja połączenia z serwerem backupowym na poziome tokenu autoryzującego i szyfrowaniem;
  6. system kopii zapasowej posiada kompresję, szyfrowanie danych dla transmisji oraz szyfrowanie danych kopii, deduplikację danych w obrębie backupu, przesyłanie danych różnicowych, możliwość przywrócenia całej maszyny a także pojedynczych plików/katalogów;
  7. obsługa LVM, ZFS, SMB, iSCSI, NFS;
  8. posiada wbudowany, konfigurowalny firewall;
  9. funkcja sieciowa BOND i VLAN;
  10. subskrypcja obsługi serwisowej na minimum 3 lata która obejmuje minimum:
      + wsparcie przez Portal Klienta
      + zdalne wsparcie (SSH)
      + licencje do obsługi serwisowej zakupione są na procesor lub odpowiednią ilość rdzeni, którą posiada serwer z zapytania ofertowego Część nr 4.

Przedmiot zamówienia musi pochodzić z autoryzowanego kanału dystrybucji producenta.

**Wdrożenie**

Zamawiający nie wymaga wdrożenia.

**Termin realizacji przedmiotu zamówienia**

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie do 14 dni kalendarzowych od daty zawarcia umowy.

**Szkolenia**

Zamawiający nie wymaga szkoleń w zakresie instalacji czy obsługi.

**Dostawa**

Klucz licencyjny/certyfikat mają być dostarczony drogą elektroniczną na adres e-mail: [przedmiot.zamowienia@ecz-otwock.pl](mailto:przedmiot.zamowienia@ecz-otwock.pl)

Dostawa przedmiotu zamówienia potwierdzona będzie protokołem odbioru.

## Część 8 – Audyt końcowy w obszarze cyberbezpieczeństwa.

Przedmiotem zamówienia jest usługa realizująca audyt w zakresie cyberbezpieczeństwa w ramach inwestycji D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia”.

Audyt będzie realizować zakres:

1. Analiza końcowa stanu bezpieczeństwa informacji w jednostce szpitalnej Zamawiającego
2. Zebranie końcowych odpowiedzi i dowodów audytowych
3. Opracowanie raportu z audytu wskazującego wykryte podatności oraz błędy wraz z rekomendacjami działań naprawczych i korygujących
4. Uzupełnienie “Ankiety weryfikacji dojrzałości w zakresie cyberbezpieczeństwa”, która stanowi Załącznik nr 9 do niniejszego Zapytania ofertowego (wyciąg z Załącznika nr 4 do Regulaminu wyboru przedsięwzięcia w trybie konkurencyjnym dla inwestycji D1.1.2).
5. Audyt będzie obejmować obszary, w których przetwarzane są dane osobowe wrażliwe, w tym kluczowe systemy informacji medycznej oraz infrastrukturę urządzeń medycznych. Audyt będzie obejmować niezbędną infrastrukturę teleinformatyczną podmiotu, w tym przynajmniej bezpieczeństwo takich elementów jak:

* Kanały komunikacji jak np. poczta
* Sieciowe urządzenia brzegowe wraz z zasadami segmentacji oraz przepływów
* Kontrolery domeny
* Platforma wirtualizacyjna
* System zarządzania kopiami zapasowymi
* Poprawność konfiguracji stacji roboczych oraz serwerów
* Sposoby uwierzytelniania się użytkowników do systemów medycznych

Zamawiający wymaga złożenia przez Oferenta wraz z ofertą wypełnionej ankiety dla podmiotu przetwarzającego dane osobowe, stanowiącej Załącznik nr 7 do niniejszego Zapytania ofertowego.

Zamawiający wymaga realizacji przedmiotu zamówienia w siedzibie Zamawiającego. Zamawiający nie dopuszcza możliwości realizacji przedmiotu zamówienia w sposób zdalny.

Zamawiający nie dopuszcza wykonywanie audytu przez podwykonawców.

**Termin realizacji przedmiotu zamówienia**

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie do dnia 30.05.2026.

**Płatność**

Faktura VAT wystawiona po realizacji zamówienia rozumianego jako podpisanie protokołu odbioru zgodnie z Umową z odroczoną datą płatności 14 dni.