Numer sprawy: **IGM.271.1.2026**

Szczegółowy Opis Przedmiotu Zamówienia

na Dostawę sprzętu i oprogramowania informatycznego związaną z realizacją projektu w ramach grantu Cyberbezpieczny Samorząd dla Gminy Łabiszyn i jej jednostek organizacyjnych

[zmiana z dnia 18.02.2026r. kolorem zielony zaznaczono wprowadzone zmiany w opisie]

[zmiana z dnia 24.02.2026r. kolorem fioletowym zaznaczono wprowadzone zmiany w opisie]

Spis treści

1. Zestawienie ilościowe.

Część nr 1 – Dostawa sprzętu i oprogramowania informatycznego.

Lp.	Nazwa	Ilość
1.	Zakup serwera TYP A	1 szt.
2.	Zakup serwera TYP B	4 szt.
3.	Zakup UPS	1 szt.
4.	Zakup NAS TYP A	2 szt.
5.	Zakup NAS TYP B	2 szt.
6.	Zakup przełącznika sieciowego	4 szt.
7.	Zakup UTM	1 szt.

Część nr 2 – Dostawa oprogramowania informatycznego.

Lp.	Nazwa	Ilość
1.	Zakup oprogramowania do agregacji logów	1 szt.
2.	Rozbudowa systemu backup	1 szt.

Część nr 3 – Rozbudowa oprogramowania antywirusowego

Lp.	Nazwa	Ilość
1.	Rozbudowa oprogramowania antywirusowego o funkcje XDR, szyfrowania danych, zarządzanie podatnościami	1 szt.

Część nr 4 – Dostawa oprogramowania do zarządzania bezpieczeństwem

Lp.	Nazwa	Ilość
1.	Zakup oprogramowania do zarządzania bezpieczeństwem IT (DLP, monitoring zasobów, zarządzanie dostępem)	1 szt.

2. Zasada równoważności rozwiązań i neutralności technologicznej.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań lub też stosowane jest w celu wskazania aktualnie użytkowanego środowiska Zamawiającego, z którym rozwiązanie równoważne powinno być kompatybilne.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.
5. Brak określenia „minimum" oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.
9. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia poprawności przeprowadzonych testów może wezwać

Wykonawcę do przedstawienia wskazanego przez Zamawiającego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.

10. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
11. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne

opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

3. Przedmiot zamówienia dla części nr 1.

3.1. Wymagania ogólne.

1. Dostarczony sprzęt i oprogramowanie muszą być wolne od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt i oprogramowanie muszą być fabrycznie nowe (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), muszą pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu i oprogramowania.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale", „end-of-support", „end-of-life" producenta lub innych listach prowadzonych przez producentów produktów świadczących o tym, że produkt został wycofany ze sprzedaży, wsparcie dla niego zostało zakończone lub producent zaprzestaje wydawania aktualizacji, poprawek bezpieczeństwa czy też napraw dla produktu.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów. Niedopuszczalna jest realizacja tylko części funkcji bądź wymaganych standardów zamiast innych określonych jako minimalne w niniejszym dokumencie. Wszystkie wymagania minimalne muszą zostać zapewnione przez dostarczane produkty bez konieczności zakupu żadnych dodatkowych elementów przez Zamawiającego, chyba że z niniejszego dokumentu wynika inaczej.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do wskazanej lokalizacji przez Zamawiającego, będą to następujące lokalizacje: Urząd Miejski w Łabiszynie, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Zakład Wodociągów i Kanalizacji w Łabiszynie, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Miejski Zespół Oświaty, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Miejski Ośrodek Pomocy Społecznej, ul. Szubińska 1, 89-210 Łabiszyn; Zespół Szkół w Łabiszynie, ul. Nadnotecka 2, 89-210 Łabiszyn.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzeń do działania, pozwalające na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
11. Dla dostaw sprzętu informatycznego z oprogramowaniem Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego

oprogramowania (w tym systemu operacyjnego) nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania (faktury, rachunki) w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

12. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia sprzętu i oprogramowania – wymagania minimalne:
    a. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego sprzętu i oprogramowania po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uwzględniające obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
        i. scenariusze testowe, procedury oraz wzory raportów testów,
        ii. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
        iii. opis koncepcji realizacji prac,
        iv. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
    b. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
        i. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 10 dni kalendarzowych od dnia zawarcia umowy,
        ii. Zamawiający w terminie nie dłuższym niż 5 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
        iii. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
        iv. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
        v. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
        vi. zatwierdzony projekt techniczny wraz procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
    c. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.

d. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
e. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
f. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery". Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.

13. Instruktaże w zakresie dostarczonego sprzętu i oprogramowania – wymagania minimalne.
    a. Instruktaże stanowiskowe będą prowadzone w języku polskim w siedzibie Zamawiającego i obejmą zakresem m.in.: użytkowane oprogramowanie; budowę, architekturę i konfigurację rozwiązania; administrowanie wdrożonym rozwiązaniem.
    b. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
    c. Instruktaże powinny trwać minimum 8 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób (maksymalnie 2 osoby).
    d. Zamawiający dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
    e. Administratorzy rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne, a także instalacji oprogramowania, znać i umieć realizować procedury backupu. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem rozwiązania, a także sposoby ich przeciwdziałania, wykrywania i usuwania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować wdrożone rozwiązanie, jak również znać jego wdrożoną konfigurację.
14. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi", „powinien", „możliwość" określając w ten sposób wymaganą funkcjonalność oprogramowania.

3.2. Zakup serwera TYP A (1 szt.).

Minimalne parametry techniczne serwera:

1. Obudowa typu RACK o wysokości maksymalnie 2U z możliwością instalacji min. 12 dysków 2.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych.
2. Płyta główna z możliwością zainstalowania dwóch procesorów.
3. Zainstalowane dwa procesory klasy x86 dedykowane do pracy z oferowanym serwerem, umożliwiające osiągnięcie przez serwer wyniku co najmniej 245 punktów w teście SPECrate2017_fp_base dla konfiguracji dwuprocesorowej według wyników publikowanych na stronie www.spec.org. Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie dla procesora dedykowanego do pracy z zaoferowanym serwerem żądanej przez Zamawiającego wydajności.
4. Pamięć RAM: zainstalowane min. 256 GB w najnowszej technologii oferowanej przez producenta, płyta główna musi obsługiwać do min. 1 TB pamięci RAM DDR5, co najmniej 12 slotów na pamięć wolnych w oferowanej konfiguracji.
5. Zabezpieczenia pamięci RAM: Memory Rank Sparing i/lub Memory Mirror i/lub Single Device Data Correction i/lub Memory Lockstep i/lub Chipkill i/lub Extended ECC i/lub Advanced Memory Device Correction i/lub AMD Memory Guard i/lub ECC i/lub Demand Scrubbing i/lub Patrol Scrubbing i/lub Permanent Fault Detection (PFD).
6. Zintegrowana karta graficzna ze złączem VGA.
7. Interfejsy sieciowe: Wbudowane co najmniej 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, co najmniej 2 interfejsy sieciowe 10Gb Ethernet w standardzie 10GBase-T, co najmniej 2 interfejsy w 10GbE w standardzie SFP+ z dedykowanymi wkładkami do każdego portu.
8. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 2 dyski twarde Hot-Plug SSD SATA o prędkości min. 6 Gb/s o pojemności co najmniej 480 GB każdy oraz 5 dysków twardych Hot-Plug SAS o prędkości min. 12 Gb/s o pojemności co najmniej 2,4 TB każdy. W przypadku uszkodzenia dysku w okresie gwarancji Zamawiający wymaga by uszkodzony dysk pozostał jego własnością.
9. Kontroler RAID: Sprzętowy kontroler dyskowy umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
10. Wsparcie dla dysków samoszyfrujących.
11. Wbudowane porty: min. 3 porty USB, w tym co najmniej 1 port USB musi być dostępny z przodu obudowy. Ilość dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera.
12. Wentylatory: typu Hot Plug.
13. Zasilacze: Redundantne typu Hot Plug o mocy nieprzekraczającej 700 W każdy.
14. Karta/moduł zarządzania: Niezależny od zainstalowanego na serwerze systemu operacyjnego posiadający dedykowane złącze umożliwiający zdalne zarządzanie:
    1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
    2) zdalne monitorowanie i informowanie o statusie serwera,
    3) szyfrowane połączenie oraz autentykacje i autoryzację użytkownika,
    4) możliwość podmontowania zdalnych wirtualnych napędów,

5) wirtualną konsolę z dostępem do myszy, klawiatury,
6) wsparcie dla IPv6,
7) wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,
8) integracja z Active Directory,
9) wsparcie dla dynamic DNS.

15. System bezpieczeństwa serwera realizowany poprzez następujące zabezpieczenia:
    1) wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera;
    2) blokada zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych;
    3) moduł TPM 2.0.
16. Serwer powinien posiadać funkcjonalność umożliwiającą konfigurację i monitoring kluczowych komponentów (takich jak CPU, RAM, dyski, temperatury, statusy wentylatorów) za pomocą aplikacji mobilnej. Aplikacja powinna być dostępna na urządzenia mobilne działające na systemach Android oraz iOS i umożliwiać dostęp do serwera za pomocą popularnych protokołów bezprzewodowych, takich jak BLE lub Wi-Fi.
17. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzenie serwerem klasy Microsoft Windows Serwer Standard 2025 wraz z 35 licencjami dostępowymi umożliwiającymi korzystanie przez 35 użytkowników z zasobów serwera lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności.
    Warunki równoważności dla dostawy oprogramowania Microsoft Windows Serwer Standard 2025 wraz z 35 licencjami dostępowymi Microsoft Windows Server 2025 CAL User:
    1) Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji oraz dostępu do serwerowego systemu operacyjnego dla minimum 35 użytkowników.
    2) Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 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.
    8) Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
    9) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
    10) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

11) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
12) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
13) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
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 2 języków poprzez wybór z listy dostępnych lokalizacji.
16) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
17) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
18) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
19) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
20) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

18. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
19. Jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub ISO 14001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, ze oferowany serwer spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany serwer i jego/ich producenta/producentów wymagań w zakresie określonym powyżej.
20. Gwarancja: min. 60 miesięcy gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dysków Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii w języku polskim poprzez ogólnopolską linię telefoniczną producenta oraz dedykowany portal techniczny producenta, dla obu kanałów w trybie ciągłym, tj. niezależnie od pory dnia, dni roboczych i dni wolnych od pracy. Zamawiający wymaga pojedynczego serwisowego punktu kontaktu dla całego rozwiązania Producenta (w tym także zaoferowanego oprogramowania) umożliwiającego komunikację w języku polskim. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocenę bezpieczeństwa cybernetycznego. Wszelkie naprawy mogą być realizowane przez

osoby certyfikowane przez producenta, które po diagnostyce muszą z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) rozpocząć naprawę w siedzibie Zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. W przypadku jeżeli serwis gwarancyjny urządzeń nie będzie realizowany bezpośrednio przez producenta urządzenia, wówczas firma serwisująca musi posiadać certyfikat ISO 9001 oraz ISO 27001 lub inny równoważny dokument poświadczający, że usługi serwisu świadczone będą zgodnie z zasadami wynikającymi z tych norm oraz firma serwisująca musi posiadać autoryzacje producenta urządzeń, w takim przypadku Wykonawca jest zobowiązany dostarczyć wraz z ofertą dokumenty potwierdzające spełnienie przez firmę serwisującą przedmiotowego wymogu. Możliwość przedłużenia gwarancji producenta do 72 miesięcy.

3.3. Zakup serwera TYP B (4 szt.).

Minimalne parametry techniczne serwera:

1. Obudowa typu RACK o wysokości maksymalnie 2U z możliwością instalacji min. 12 dysków 2.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych.
2. Płyta główna z możliwością zainstalowania dwóch procesorów.
3. Zainstalowany jeden procesor klasy x86 dedykowany do pracy z oferowanym serwerem, umożliwiający osiągnięcie przez serwer wyniku co najmniej 245 punktów w teście SPECrate2017_fp_base dla konfiguracji dwuprocesorowej według wyników publikowanych na stronie www.spec.org. Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie dla procesora dedykowanego do pracy z zaoferowanym serwerem żądanej przez Zamawiającego wydajności.
4. Pamięć RAM: zainstalowane min. 128 GB w najnowszej technologii oferowanej przez producenta, płyta główna musi obsługiwać do min. 1 TB pamięci RAM DDR5, co najmniej 12 slotów na pamięć wolnych w oferowanej konfiguracji.
5. Zabezpieczenia pamięci RAM: Memory Rank Sparing i/lub Memory Mirror i/lub Single Device Data Correction i/lub Memory Lockstep i/lub Chipkill i/lub Extended ECC i/lub Advanced Memory Device Correction i/lub AMD Memory Guard i/lub ECC i/lub Demand Scrubbing i/lub Patrol Scrubbing i/lub Permanent Fault Detection (PFD).
6. Zintegrowana karta graficzna ze złączem VGA.
7. Interfejsy sieciowe: Wbudowane co najmniej 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, co najmniej 2 interfejsy sieciowe 10Gb Ethernet w standardzie 10GBase-T.
8. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 5 dysków twardych Hot-Plug SAS o prędkości min. 12 Gb/s o pojemności co najmniej 2,4 TB każdy. W przypadku uszkodzenia dysku w okresie gwarancji Zamawiający wymaga by uszkodzony dysk pozostał jego własnością.
9. Kontroler RAID: Sprzętowy kontroler dyskowy umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
10. Wsparcie dla dysków samoszyfrujących.
11. Wbudowane porty: min. 3 porty USB, w tym co najmniej 1 port USB musi być dostępny z przodu obudowy. Ilość dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych

przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera.

12. Wentylatory: typu Hot Plug.
13. Zasilacze: Redundantne typu Hot Plug o mocy nieprzekraczającej 700 W każdy.
14. Karta/moduł zarządzania: Niezależny od zainstalowanego na serwerze systemu operacyjnego posiadający dedykowane złącze umożliwiający zdalne zarządzanie:
    1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
    2) zdalne monitorowanie i informowanie o statusie serwera,
    3) szyfrowane połączenie oraz autentykacje i autoryzację użytkownika,
    4) możliwość podmontowania zdalnych wirtualnych napędów,
    5) wirtualną konsolę z dostępem do myszy, klawiatury,
    6) wsparcie dla IPv6,
    7) wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,
    8) integracja z Active Directory,
    9) wsparcie dla dynamic DNS.
15. System bezpieczeństwa serwera realizowany poprzez następujące zabezpieczenia:
    1) wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera;
    2) blokada zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych;
    3) moduł TPM 2.0.
16. Serwer powinien posiadać funkcjonalność umożliwiającą konfigurację i monitoring kluczowych komponentów (takich jak CPU, RAM, dyski, temperatury, statusy wentylatorów) za pomocą aplikacji mobilnej. Aplikacja powinna być dostępna na urządzenia mobilne działające na systemach Android oraz iOS i umożliwiać dostęp do serwera za pomocą popularnych protokołów bezprzewodowych, takich jak BLE lub Wi-Fi.
17. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzenie serwerem klasy Microsoft Windows Serwer Standard 2025 wraz z:
    1) 15 licencjami dostępowymi umożliwiającymi korzystanie przez 15 użytkowników z zasobów serwera dla serwera użytkowanego w Zakładzie Wodociągów i Kanalizacji w Łabiszynie.
    2) 15 licencjami dostępowymi umożliwiającymi korzystanie przez 15 użytkowników z zasobów serwera dla serwera użytkowanego w Miejskim Zespole Oświaty w Łabiszynie.
    3) 20 licencjami dostępowymi umożliwiającymi korzystanie przez 20 użytkowników z zasobów serwera dla serwera użytkowanego w Miejskim Zespole Oświaty w Łabiszynie.
    4) 20 licencjami dostępowymi umożliwiającymi korzystanie przez 20 użytkowników z zasobów serwera dla serwera użytkowanego w Zespole Szkół w Łabiszynie.

    lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności.

Warunki równoważności dla dostawy oprogramowania Microsoft Windows Serwer Standard 2025 wraz z licencjami dostępowymi Microsoft Windows Server 2025 CAL User:

1) Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji oraz dostępu do serwerowego systemu operacyjnego.
2) Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 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.
8) Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
9) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
10) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
11) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
12) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
13) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
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 2 języków poprzez wybór z listy dostępnych lokalizacji.
16) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
17) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
18) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
19) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
20) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

18. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
19. Jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub ISO 14001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, ze oferowany serwer spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą

RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany serwer i jego/ich producenta/producentów wymagań w zakresie określonym powyżej.

20. Gwarancja: min. 60 miesięcy gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dysków Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii w języku polskim poprzez ogólnopolską linię telefoniczną producenta oraz dedykowany portal techniczny producenta, dla obu kanałów w trybie ciągłym, tj. niezależnie od pory dnia, dni roboczych i dni wolnych od pracy. Zamawiający wymaga pojedynczego serwisowego punktu kontaktu dla całego rozwiązania Producenta (w tym także zaoferowanego oprogramowania) umożliwiającego komunikację w języku polskim. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocenę bezpieczeństwa cybernetycznego. Wszelkie naprawy mogą być realizowane przez osoby certyfikowane przez producenta, które po diagnostyce muszą z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) rozpocząć naprawę w siedzibie Zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. W przypadku jeżeli serwis gwarancyjny urządzeń nie będzie realizowany bezpośrednio przez producenta urządzenia, wówczas firma serwisująca musi posiadać certyfikat ISO 9001 oraz ISO 27001 lub inny równoważny dokument poświadczający, że usługi serwisu świadczone będą zgodnie z zasadami wynikającymi z tych norm oraz firma serwisująca musi posiadać autoryzacje producenta urządzeń, w takim przypadku Wykonawca jest zobowiązany dostarczyć wraz z ofertą dokumenty potwierdzające spełnienie przez firmę serwisującą przedmiotowego wymogu. Możliwość przedłużenia gwarancji producenta do 72 miesięcy.

3.4. Zakup UPS (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Typ obudowy: umożliwiająca umieszczenie w szafie RACK a także zapewniająca ustawienie wolnostojące.
2. Moc pozorna: min. 2200 VA.
3. Moc rzeczywista: min. 2000 W.
4. Architektura UPSa: line-interactive lub online.
5. Typ przebiegu: sinusoidalny.
6. Liczba i rodzaj gniazdek z utrzymaniem zasilania: min. 8x IEC320 C13.
7. Typ gniazda wejściowego: C14 lub C20.
8. Czas podtrzymania dla obciążenia 100%: min. 3 min.
9. Czas podtrzymania przy obciążeniu 50%: min. 10 min.
10. Zabezpieczenia: przeciwprzepięciowe, przeciwzwarciowe, przeciwprzeciążeniowe.
11. Wyświetlacz LCD lub diody LED sygnalizujące stan pracy urządzenia.
12. Alarmy dźwiękowe urządzenia sygnalizujące stan pracy urządzenia w zakresie określonych przez producenta zdarzeń.
13. Interfejsy: min. 1 x USB, 1 x RJ45.

14. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany UPS spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta UPS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany UPS wymagań w zakresie określonym powyżej.
15. Gwarancja producenta: min. 24 miesiące.

3.5. Zakup NAS TYP A (2 szt.).

Minimalne parametry urządzenia:

1. Obudowa do szafy RACK.
2. Procesor wielordzeniowy osiągający w teście wydajności PassMark Performance Test co najmniej wynik 8 500 punktów, testy powinny być aktualne w okresie nie dłuższym niż 30 dni przed składaniem ofert. Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie przez oferowany procesor żądanej przez Zamawiającego wydajności.
3. Pamięć RAM: min. 32 GB.
4. Pamięć flash: min. 4 GB.
5. Funkcje: wsparcie dla wirtualizacji, scentralizowana pamięć masowa na dane, backup, udostępnianie i przywracanie systemu po awarii.
6. Możliwość zainstalowania łącznie 8 dysków 3,5 calowych SATA o prędkości min. 3 - 6 Gb/s.
7. Zainstalowane dyski: min. 8 x dysk 12 TB SATA 6 GB/s przeznaczonych dla systemów NAS pracujących w trybie ciągłym. dyski muszą być zgodne z urządzeniem NAS, tj. muszą znajdować się na liście zgodności prowadzonej przez producenta urządzenia NAS lub które zostały przetestowane pod kątem zgodności z produktami producenta urządzenia NAS.
8. Poziom RAID: 1,5,6.
9. Kompatybilność dysków: 3,5-calowe dyski twarde SATA; 2,5-calowe dyski twarde SATA; 2,5-calowe dyski SSD SATA.
10. Obsługa połączeń 10GbE SFP+ (co najmniej dwa porty) oraz 10 GbE RJ45 (co najmniej dwa porty) wraz z 2 wkładkami 10GbE SFP+ do NAS oraz niezbędnymi kablami do połączenia NAS z przełącznikiem za pomocą wszystkich interfejsów.
11. Porty USB: min. 2x USB 3.0.
12. Szyny do montażu w szafie RACK.
13. Dostawa oprogramowania do archiwizacji m.in. maszyn wirtualnych Hyper-V z możliwością automatycznego odtworzenia całej maszyny wirtualnej z kopii oraz z kopii już obecnie posiadanych maszyn wirtualnych.
14. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany NAS spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu

lub oświadczenia producenta NAS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany NAS wymagań w zakresie określonym powyżej.

15. Gwarancja producenta min. 24 miesiące realizowanej w miejscu instalacji sprzętu, z czasem naprawy do następnego dnia roboczego od przyjęcia zgłoszenia. Gwarancja musi obejmować także dyski. W przypadku awarii dyski twarde pozostają własnością Zamawiającego.

3.6. Zakup NAS TYP B (2 szt.).

Minimalne parametry techniczne urządzenia:

1. Obudowa wolnostojąca.
2. Procesor wielordzeniowy.
3. Pamięć RAM: min. 16 GB.
4. Oprogramowanie systemu operacyjnego umożliwiające minimum: zarządzanie i administrację urządzeniem, tworzenie kopii zapasowych z komputerów i serwerów, udostępnianie plików, zarządzanie przestrzenią dyskową, grupowanie dysków, zarządzanie dostępem i użytkownikami, wyszukiwanie plików, kompresowanie plików.
5. Możliwość zainstalowania łącznie 6 dysków 3,5-calowych.
6. Możliwość zainstalowania do dwóch dysków SSD w celu buforowania lub tworzenia dodatkowych pul pamięci.
7. Zainstalowane dyski: min. 6 x 4 TB, dyski muszą być zgodne z urządzeniem NAS, tj. które znajdują się na liście zgodności prowadzonej przez producenta urządzenia NAS lub które zostały przetestowane pod kątem zgodności z produktami producenta urządzenia NAS.
8. RAID 0, 1, 5, 6, 10.
9. Interfejsy sieciowe: 2 x Port Gigabit sieci Ethernet (RJ45).
10. Porty USB: min. 2 x USB3.2.
11. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany NAS spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta NAS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany NAS wymagań w zakresie określonym powyżej.
12. Co najmniej 24 miesiące gwarancji producenta.

3.7. Zakup przełącznika sieciowego (4 szt.).

Minimalne parametry techniczne urządzenia:

1. Rodzaj urządzenia: zarządzalny przełącznik L3.

2. Rodzaj obudowy: umożliwiający montaż w szafie RACK (wraz z kompletem szyn/wieszaków do montażu w szafie RACK).
3. Przepustowość routowania/przełączania: min. 200 Gbit/s.
4. Prędkość przekazywania: min. 150 Mpps.
5. Bufor pamięci dla pakietów: max. 3 MB.
6. Rozmiar tablicy MAC: min. 32 000 wpisów.
7. Dostępne interfejsy: min. 48 x 1000Base-T- RJ-45, min. 4 x 10GbE SFP+. Nie są dopuszczane porty SFP+ współdzielone z portami RJ45 (tzw. „combo"). Porty SFP/SFP+ muszą obsługiwać moduły o prędkości transmisji zarówno 1 Gbps jak i 10 Gbps.
8. Obsługiwane standardy komunikacyjne: 802.3i; 802.3u; 802.3z; 802.3ab; 802.3ae; 802.3ad; 802.3ah; 802.3az; 802.3x; 802.1ab; 802.1w; 802.1s; 802.1p; 802.1q.
9. Obsługiwane protokoły zarządzające: SNMPv1, SNMPv2, SNMPv3, OSPFv2, OSPFv3, RMON.
10. Obsługiwane protokoły sieciowe: IPv4, IPv6, LLDP, MSTP, RSTP, Telnet, TACACS, MLD, RIPv1, RIPv2, OSPFv2, OSPFv3, SSH.
11. Inne cechy: zarządzanie przez www, generowanie raportów zdarzeń systemowych, obsługa min. 4000 sieci VLAN, obsługa mulitcast, funkcję agregacji portów z wykorzystaniem protokołu LACP, uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia; obsługa list kontroli dostępu (ACL).
12. Możliwość łączenia urządzeń w stos min. 4.
13. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany przełącznik sieciowy spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta przełącznika sieciowego lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany przełącznik wymagań w zakresie określonym powyżej.
14. Co najmniej 60 miesięcy gwarancji producenta.

3.8. Zakup UTM (1 szt.).

W ramach działania przewiduje się zakup urządzenia UTM wraz z licencjami subskrypcyjnymi. Subskrypcja musi umożliwić Zamawiającemu korzystanie z aktualnych baz funkcji ochronnych producenta i serwisów oraz obejmować kontrolę aplikacji, IPS, antywirus, antyspam, web filtering. W ramach przedmiotu zamówienia Wykonawca musi zapewnić także wsparcie techniczne, które może być tylko realizowane przez producenta, dystrybutora, bądź oficjalnego partnera dystrybutora. Subskrypcja dla urządzenia UTM obejmująca wszystkie wymagania wskazane powyżej musi być dostarczona na okres do dnia 30.06.2026 r. niezależnie od oferowanych modeli licencjonowania producenta.

Minimalne wymagania techniczne urządzenia:

1. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych.
2. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trybów: Routera z funkcją NAT.
3. System musi wspierać IPv4 oraz IPv6 w zakresie: firewall, ochrony w warstwie aplikacji, protokołów routingu dynamicznego.
4. Redundancja, monitoring i wykrywanie awarii:
   a. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – system musi zapewniać możliwość łączenia w klaster Active-Passive. Musi być dostępna funkcja synchronizacji sesji firewall,
   b. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych,
   c. Monitoring stanu realizowanych połączeń VPN.
5. Interfejsy: co najmniej 5 x Ethernet 10/100/1000, obsługa połączeń WIFI 2.4GHz/5GHz (802.11 a/b/g/n/ac).
6. Wydajność:
   - Przepustowość firewall – co najmniej 10 Gbps,
   - Liczba równoległych sesji – co najmniej 0,7 mln.
   - Przepustowość IPS – co najmniej 1,4 Gbps.
   - Liczba jednoczesnych klientów SSL VPN – co najmniej 200.
7. Funkcje Systemu Bezpieczeństwa:
   - Kontrola Aplikacji,
   - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN,
   - Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS,
   - Ochrona przed atakami - Intrusion Prevention System,
   - Kontrola stron WWW,
   - Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3,
   - Zarządzanie pasmem (QoS, Traffic shaping),
   - Analiza ruchu szyfrowanego protokołem SSL.
8. Polityki firewall:
   - Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, IPS i aplikacje, reakcje zabezpieczeń, rejestrowanie zdarzeń,
   - System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz translację jeden do jeden oraz jeden do wielu,
   - W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
9. Połączenia VPN:
   - System musi umożliwiać konfigurację połączeń typu IPSec VPN,
   - System musi umożliwiać konfigurację połączeń typu SSL VPN.
10. Routing i obsługa łączy WAN:
    - W zakresie routingu rozwiązanie powinno zapewniać obsługę: routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu,

- System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia.

11. Kontrola antywirusowa:
    - Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji,
    - Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji,
    - Moduł kontroli antywirusowej ma mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze w celu rozpoznawania zagrożeń.
12. Ochrona przed atakami:
    - Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych,
    - Baza sygnatur ataków musi być aktualizowana automatycznie,
    - System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
13. Kontrola aplikacji:
    - Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie analizy pakietów,
    - Baza Kontroli Aplikacji musi być aktualizowana automatycznie,
    - Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
14. Kontrola WWW:
    - W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware, phishing, spam, proxy avoidance. Jako rozwiązanie równoważne dopuszcza się realizację zapewnienia bezpieczeństwa w tych kategoriach na poziomie firewalla,
    - Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard,
    - Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL,
    - Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
15. Uwierzytelnianie użytkowników w ramach sesji:
    - System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą co najmniej haseł statycznych,
    - Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory.
16. Zarządzanie:
    - Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego,
    - Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów,
    - Wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
17. Urządzenie powinno umożliwiać monitorowania logów ruchu, administracja urządzenia musi być możliwe poprzez graficzny interfejs zarządzania, rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub e-mail, urządzenie powinno mieć możliwość generowania raportów.

18. W ramach Zamówienia Wykonawca dostarczy licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować kontrolę aplikacji, IPS, antywirus, antyspam, web filtering na okres do dnia 30.06.2026 r.
19. Urządzenie musi być objęte serwisem gwarancyjnym producenta na okres do dnia 30.06.2026 r.

4. Opis przedmiotu zamówienia części nr 2, 3, 4.

4.1. Wymagania ogólne.

1. Dostarczone oprogramowanie musi być wolne od wad prawnych i fizycznych oraz nienoszące oznak użytkowania.
2. Dostarczone oprogramowanie musi być fabrycznie nowe, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego oprogramowania.
3. Niedopuszczalne są produkty prototypowe, oprogramowanie nie może znajdować się na liście „end-of-sale", „end-of-support", „end-of-life" producenta lub innych listach prowadzonych przez producentów produktów świadczących o tym, że produkt został wycofany ze sprzedaży, wsparcie dla niego zostało zakończone lub producent zaprzestaje wydawania aktualizacji, poprawek bezpieczeństwa czy też napraw dla produktu.
4. Wykonawca zapewni dostawę oprogramowania do wskazanej lokalizacji w siedzibie Zamawiającego.
5. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
6. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
7. Dla dostaw oprogramowania Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania, nieużywanego oraz nigdy wcześniej nieaktywowanego oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania posiadającego fizyczny nośnik naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
8. Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:
    a. Instalacja ma odbyć się na komputerach oraz serwerach wskazanych przez Zamawiającego, a w przypadku jeżeli dostarczone oprogramowanie działa w modelu rozwiązania chmurowego to Wykonawca jest zobligowany do konfiguracji oprogramowania w chmurze Wykonawcy bądź Producenta oferowanego oprogramowania.

b. Zamawiający dopuszcza instalację i wdrożenie zdalne przy wykorzystaniu narzędzia Wykonawcy, z zastrzeżeniem, że Wykonawca jest zobowiązany dostarczyć oprogramowanie do zdalnej pracy umożliwiające szyfrowanie połączeń oraz nagrywanie sesji serwisowych.
c. W przypadku jeżeli dotyczy, Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.
d. Wykonawca, pomimo zapewnienia serwisu producenta zobowiązany będzie do udzielania pomocy technicznej Zamawiającemu przez okres gwarancji.
e. Usługa wsparcia wdrożenia obejmuje:
    i. przeprowadzenie analizy przedwdrożeniowej,
    ii. pomoc przy instalacji silnika bazy danych – jeżeli będzie wymagana instalacja,
    iii. rejestracja produktu – jeżeli wymagana,
    iv. instalację oprogramowania: na stacji roboczej lub serwerze – jeżeli dotyczy,
    v. dystrybucję oprogramowania na wybranych stacjach roboczych – jeżeli dotyczy,
    vi. konfigurację oprogramowania,
    vii. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego,
    viii. szkolenie administratorów z zakresu pracy z programem,
    ix. w uzgodnionym terminie z Zamawiającym zostanie przeprowadzane kontrolne połącznie zdalne w celu weryfikacji ustawień oraz poprawienia konfiguracji.

9. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia oprogramowania – wymagania minimalne:
    a. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego oprogramowania, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uwzględniające obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
        i. scenariusze testowe, procedury oraz wzory raportów testów,
        ii. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
        iii. opis koncepcji realizacji prac,
        iv. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
    b. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
        i. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 10 dni roboczych od dnia zawarcia umowy,
        ii. Zamawiający w terminie nie dłuższym niż 5 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
        iii. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,

iv. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
v. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
vi. zatwierdzony projekt techniczny wraz procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.

c. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.
d. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
e. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
f. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery". Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.

10. Wymagania licencyjne dla dostarczonego oprogramowania:
    a. Licencjobiorcą licencji będą: Urząd Miejski w Łabiszynie, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Zakład Wodociągów i Kanalizacji w Łabiszynie, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Miejski Zespół Oświaty, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Miejski Ośrodek Pomocy Społecznej, ul. Szubińska 1, 89-210 Łabiszyn; Zespół Szkół w Łabiszynie, ul. Nadnotecka 2, 89-210 Łabiszyn zgodnie ze wskazaniem poniżej.
    b. Zamawiający dopuszcza udzielenie licencji w wersji papierowej i/lub elektronicznej. W przypadku jeżeli producent oprogramowania nie wystawia licencji w zakresie oferowanego oprogramowania Wykonawca powinien dostarczyć stosowne oświadczenie producenta oprogramowania bądź jego dystrybutora.
    c. Licencje muszą obowiązywać do dnia 30.06.2026 r. niezależnie od modeli dystrybucji poszczególnych producentów oferowanego oprogramowania.
    d. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
    e. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do przeniesienia oprogramowania na inny serwer/komputer.
    f. Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet). Użytkownik może pracować w dowolny dostępny technologicznie sposób.
    g. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.

h. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
i. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym urządzeniu klienckim (licencja nie może być przypisana do komputera/urządzenia).
j. Licencja oprogramowania nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji ze zgromadzonych danych.
k. Wykonawca zapewni gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.

11. Wymagania gwarancyjne i serwisowe dla dostarczonego oprogramowania w formie licencji czasowych lub subskrypcyjnych:
    a. Gwarancja producenta musi zostać zapewniona przez Wykonawcę na oferowane oprogramowanie do dnia 30.06.2026 r.
    b. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w oprogramowaniu do serwisu producenta lub jego dystrybutora.
    c. Serwis producenta musi zostać zapewniony przez Wykonawcę do dnia 30.06.2026 r.
    d. Serwis polega na świadczeniu usługi wsparcia technicznego udzielonego przez producenta lub autoryzowanego dystrybutora producenta w języku polskim i objąć musi minimum:
        i. dostęp do najnowszych wersji oprogramowania,
        ii. wsparcie telefoniczne w zakresie oferowanego oprogramowania zespołu inżynierów technicznych,
        iii. wsparcie w prawidłowym i zgodnym z wymaganiami producenta użytkowaniu oprogramowania,
        iv. przyjmowanie i realizacja zgłoszeń serwisowych,
        v. doradztwo techniczne w zakresie konfiguracji i optymalizacji oprogramowania,

        w przypadku jeżeli w dalszej części niniejszego dokumentu zdefiniowano wymogi serwisu lub gwarancji w innym zakresie powyższe wymogi są obowiązujące i należy potraktować jako podstawowe, precyzowane przez dodatkowe wymagania opisane w dalszej części dokumentu.

12. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi”, „powinien”, „możliwość” określając w ten sposób wymaganą funkcjonalność oprogramowania.

4.2. Zakup oprogramowania do agregacji logów (1 szt.) – Część 2.

<u>Minimalne parametry funkcjonalne oprogramowania do agregacji logów:</u>

1. System musi umożliwiać zbieranie logów z szerokiego spektrum źródeł, takich jak systemy operacyjne (Linux, Windows, macOS), aplikacje, urządzenia sieciowe, bazy danych, serwery webowe, oraz platformy chmurowe (np. AWS, Azure, Google Cloud), a także z innego oprogramowania do zbierania logów.
2. System musi wspierać zbieranie logów w różnych formatach, w tym min. syslog, plain text zapewniając możliwość monitorowania standardowych i niestandardowych źródeł danych.

3. System musi centralizować logi z wszystkich podłączonych źródeł umożliwiając ich łatwe zarządzanie i analizę w jednym miejscu.
4. System musi oferować zaawansowane funkcje filtracji i transformacji logów.
5. System musi posiadać funkcję normalizacji logów pochodzących z różnych źródeł umożliwiając standaryzację danych i ich późniejszą korelację.
6. System musi posiadać mechanizm korelacji zdarzeń, który umożliwia łączenie i analizowanie zdarzeń pochodzących z różnych źródeł w celu wykrywania bardziej złożonych zagrożeń.
7. System musi wspierać tworzenie i zarządzanie regułami korelacji, które mogą być dostosowywane do specyficznych potrzeb organizacji, a także grupowane według źródła logów, rodzaju zagrożenia lub poziomu krytyczności.
8. System musi umożliwiać hierarchizację reguł umożliwiając tworzenie bardziej zaawansowanych strategii wykrywania zagrożeń.
9. System musi posiadać silniki detekcji zagrożeń, które analizują logi w czasie rzeczywistym, identyfikując złośliwe działania, próby włamań, naruszenia polityk bezpieczeństwa oraz inne anomalie.
10. System musi wspierać wykrywanie zagrożeń opartych zarówno na sygnaturach, jak i na anomaliach umożliwiając szybkie reagowanie na nowe i nieznane wcześniej zagrożenia.
11. System musi posiadać funkcję wykrywania specyficznych rodzajów ataków, takich jak brute force, ataki DDoS, próby eskalacji uprawnień, ataki typu SQL injection, czy próby przejęcia kont użytkowników.
12. System musi umożliwiać dynamiczne przypisywanie poziomów krytyczności do wykrytych zdarzeń pozwalając na priorytetyzację incydentów bezpieczeństwa.
13. System musi generować alarmy w czasie rzeczywistym, z możliwością ich wysyłania przez e-mail, webhooki, do systemów SIEM lub innych systemów zarządzania incydentami.
14. System musi oferować możliwość korelacji i łączenia alarmów zapewniając pełny kontekst zdarzenia i redukcji liczbę fałszywych alarmów.
15. System musi umożliwiać archiwizację wszystkich zebranych logów z możliwością ich przeszukiwania w celu przeprowadzania analizy historycznej oraz audytów po incydencie.
16. System musi posiadać funkcję generowania raportów zgodności z regulacjami, takimi jak PCI DSS, GDPR oraz inne z możliwością dostosowywania tych raportów do specyficznych wymagań Zamawiającego.
17. System musi oferować możliwość tworzenia niestandardowych raportów, które mogą zawierać szczegółowe zestawienia zdarzeń, analizę trendów oraz ocenę skuteczności polityk bezpieczeństwa.
18. System musi posiadać wbudowaną integrację z Kibana umożliwiającą wizualizację danych logów, wykonywanie zapytań oraz przetwarzanie danych.
19. System musi udostępniać API RESTful pozwalające na integrację z zewnętrznymi systemami oraz automatyzację procesów związanych z analizą logów i zarządzaniem incydentami.
20. System musi oferować integrację z zewnętrznymi bazami danych zagrożeń, takimi jak VirusTotal, w celu automatycznego sprawdzania logów związanych z plikami pod kątem znanych zagrożeń.
21. System musi wspierać integrację z honeypotami pozwalając na wykrywanie i analizowanie prób ataków na pułapki umożliwiając lepsze zrozumienie działań atakujących.
22. System musi posiadać funkcję geolokalizacji IP w analizowanych logach umożliwiając identyfikowanie podejrzanych połączeń z nieautoryzowanych lokalizacji.

23. System musi oferować interaktywne dashboardy do monitorowania logów w czasie rzeczywistym z możliwością ich dostosowania do specyficznych potrzeb operacyjnych Zamawiającego.
24. System musi umożliwiać tworzenie spersonalizowanych widoków i filtrów, które pozwolą na szybką identyfikację incydentów i anomalii dostosowanych do potrzeb administratorów.
25. System musi posiadać mechanizmy autoryzacji i autentykacji użytkowników umożliwiając kontrolę dostępu do danych, konfiguracji oraz interfejsów zarządzających.
26. Zamawiający oczekuje dostawy oprogramowania na licencji typu „open source". Zamawiający dopuszcza licencje komercyjne, jednak w takim przypadku Zamawiający oczekuje dostawy licencji wieczystej, która nie będzie wymagała nigdy żadnych dodatkowych licencji w celu aktualizacji oprogramowania do najnowszej wersji.

<u>Wdrożenie oprogramowania do agregacji logów – minimalny zakres prac Wykonawcy:</u>

1. Wdrożenie powinno uwzględniać wszystkie funkcjonalności oprogramowania od zbierania logów po ich analizę, korelację i generowanie raportów.
2. Wdrożenie powinno odbyć się na rzecz i uwzględniając infrastrukturę poszczególnych jednostek biorących udział we wdrożeniu oprogramowania, tj. Urząd Miejski w Łabiszynie, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Miejski Ośrodek Pomocy Społecznej, ul. Szubińska 1, 89-210 Łabiszyn; Miejski Zespół Oświaty, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Zakład Wodociągów i Kanalizacji w Łabiszynie, ul. Plac 1000-lecia 1, 89-210 Łabiszyn.
3. W ramach wdrożenia należy przeprowadzić analizę wstępną, w ramach której:
    a. Należy przeprowadzić ocenę infrastruktury: Dokładnie zidentyfikować wszystkie urządzenia w sieci, w tym serwery, przełączniki, komputery, drukarki, routery, firewalle i inne urządzenia sieciowe. Wskazać, które z nich generują logi, które będą zbierane i analizowane przez oprogramowanie.
    b. Należy określić wymagania: Zidentyfikować specyficzne potrzeby i wymagania Zamawiającego, takie jak zgodność z regulacjami, kluczowe punkty monitorowania, typy zagrożeń, na które należy zwracać szczególną uwagę, oraz priorytety w zakresie analizy logów.
    c. Należy zaplanować odpowiedni sprzęt i zasoby: Ustalić odpowiednią infrastrukturę sprzętową i zasoby, które będą niezbędne do wdrożenia oprogramowania. Uwzględnić wymagania dotyczące serwera, pamięci masowej, sieci i innych zasobów, aby zapewnić wydajność systemu oraz odpowiednią konfigurację i wydajność maszyny wirtualnej.
4. Następnie prace wdrożeniowe obejmą przygotowanie środowiska, w ramach których:
    a. Należy zainstalować serwer centralny: Zainstalować i skonfigurować serwer centralny, który będzie odpowiedzialny za centralizację logów, ich przetwarzanie oraz zarządzanie oprogramowaniem. Serwer powinien mieć odpowiednią moc obliczeniową oraz wystarczającą przestrzeń dyskową do przechowywania zebranych logów – należy określić wszystkie niezbędne zasoby.
    b. Należy skonfigurować agentów na urządzeniach końcowych: Na wszystkich serwerach, komputerach oraz innych urządzeniach, które będą generować logi, zainstalować i skonfigurować agentów do zbierania danych. Agenci muszą być dostosowani do specyficznych systemów operacyjnych i urządzeń.
    c. Należy utworzyć połączenia sieciowe: Upewnić się, że wszyscy agenci są poprawnie połączeni z serwerem centralnym. Połączenia powinny być zabezpieczone, aby zapewnić integralność i poufność przesyłanych danych.

5. W następnym kroku prace wdrożeniowe powinny objąć konfigurację zbierania i przetwarzania logów, w ramach których:
    a. Należy skonfigurować zbieranie logów z różnych źródeł: Ustawić oprogramowanie tak, aby zbierało logi z serwerów, przełączników, routerów, firewalli oraz innych urządzeń sieciowych. Należy upewnić się, że logi są zbierane w czasie rzeczywistym, a system wspiera różnorodne formaty logów (np. syslog, JSON, plain text).
    b. Należy ustalić reguły filtracji i transformacji logów: Zdefiniować zasady filtracji, które określą, jakie logi mają być przechowywane i analizowane. Oprogramowanie powinno być skonfigurowany do transformacji logów, tak aby dane były normalizowane i wzbogacane o dodatkowe informacje, takie jak metadane czy lokalizacja geograficzna.
    c. Należy zaimplementować korektę i deduplikację logów: Zaimplementować mechanizmy deduplikacji, które będą eliminować powtarzające się zdarzenia, zapobiegając generowaniu zbędnych alarmów i umożliwiając bardziej efektywną analizę.
6. Następnie prace wdrożeniowe skupić się powinny na ustawieniu reguł korelacji i detekcji, w ramach których:
    a. Należy skonfigurować reguły korelacji: Ustawić reguły korelacji, które pozwolą na analizę logów pochodzących z różnych źródeł w celu wykrywania bardziej złożonych zagrożeń. Reguły te powinny być dostosowane do specyfiki sieci jednostek wdrażających oprogarmowanie.
    b. Należy zdefiniować sygnatury i anomalia: Zaimplementować reguły wykrywania zagrożeń zarówno na podstawie sygnatur, jak i anomalii. System powinien być w stanie identyfikować znane wzorce zagrożeń oraz odchylenia od normalnego zachowania systemu.
    c. Należy skonfigurować poziomy krytyczności: Określić poziomy krytyczności dla różnych rodzajów zdarzeń, aby umożliwić priorytetyzację alarmów. Dostosować poziomy krytyczności do wymagań Zamawiającego uwzględniając lokalne regulacje i polityki.
7. W ramach wdrożenia wymaganym od Wykonawcy jest implementacja mechanizmów alarmowania, w ramach których:
    a. Należy skonfigurować alerty w czasie rzeczywistym: Ustalić mechanizmy generowania alertów w czasie rzeczywistym, które będą informować administratorów o wykrytych zagrożeniach. Alerty powinny być wysyłane za pomocą e-maila.
    b. Należy ustawić logikę alarmów: Zdefiniować logikę, która będzie decydować, kiedy i w jaki sposób generowane są alarmy. Należy upewnić się, że alarmy są kontekstowe i że system łączy powiązane zdarzenia w celu zredukowania liczby fałszywych pozytywów.
8. W celu wdrożenia monitorowania i analizy historycznej:
    a. Należy skonfigurować dashboardy monitorujące: Utworzyć interaktywne dashboardy do monitorowania logów i alarmów w czasie rzeczywistym. Dashboardy powinny być dostosowane do potrzeb Zamawiającego umożliwiając łatwe śledzenie kluczowych wskaźników bezpieczeństwa.
    b. Należy skonfigurować mechanizmy archiwizacji i analizy logów: Skonfigurować mechanizmy archiwizacji logów, które pozwolą na ich długoterminowe przechowywanie i analizę historyczną. Należy zapewnić możliwość przeszukiwania archiwalnych logów w celu prowadzenia audytów i dochodzeń po incydentach.
    c. Należy zaimplementować generowanie raportów zgodności: Zaimplementować automatyczne generowanie raportów zgodności, które będą odzwierciedlać wymagania

regulacyjne, takie jak RODO, i które będą regularnie dostarczane do odpowiednich wydziałów urzędu.

9. Dodatkowo należy przygotować oprogramowanie do integracji z innymi systemami poprzez konfigurację integracji z Elastic Stack umożliwiając wizualizację danych logów w Kibana, wykonywanie zaawansowanych zapytań w Elasticsearch oraz przetwarzanie danych przez Logstash. Dodatkowo, należy Zaimplementować API RESTful, które umożliwi integrację oprogramowania z innymi systemami zarządzania incydentami oraz automatyzację procesów związanych z analizą logów.
10. W końcowej fazie wdrożenia przed uruchomieniem produkcyjnym oprogramowania należy przeprowadzić testowanie i optymalizację oprogramowania, tj.:
    a. Wykonać testy funkcjonalne, aby upewnić się, że wszystkie komponenty modułu działają poprawnie. Testy powinny obejmować zbieranie logów, ich analizę, generowanie alarmów oraz integrację z innymi systemami.
    b. Przeprowadzić testy obciążeniowe, aby sprawdzić, czy system działa wydajnie nawet przy dużej ilości generowanych logów. Należy upewnić się, że serwer centralny jest w stanie obsłużyć przewidywaną ilość danych.
    c. Na podstawie wyników testów dokonać niezbędnych optymalizacji, takich jak dostosowanie filtrów, reguł korelacji czy poziomów krytyczności, aby system dział zgodnie z oczekiwaniami Zamawiającego.
11. W ramach wdrożenia oprogramowania do agregacji logów należy przeprowadzić szkolenie administratorów odpowiedzialnych za obsługę oprogramowania obejmujące wszystkie aspekty jego konfiguracji, monitorowania i zarządzania incydentami oraz sporządzić szczegółową dokumentację konfiguracji modułu, w tym opis wszystkich zdefiniowanych reguł, schematów połączeń oraz procedur zarządzania systemem.

4.3. Rozbudowa systemu backup (1 szt.) – Część 2

Rozbudowa systemu backup składać się będzie z zapewnienia dla Miejskiego Ośrodka Pomocy Społecznej, ul. Szubińska 1, 89-210 Łabiszyn dwóch elementów:

1. Dostawa oprogramowania umożliwiającego backup w chmurze o parametrach minimum:
    a. Data obowiązywania licencji: 30 czerwca 2026 r.
    b. Ilość danych w chmurze: min. 5 TB.
    c. Brak kosztów transmisji danych.
    d. Szyfrowanie połączenia przesyłu i transferu danych.
    e. Dostępność danych na poziomie 99 % w danym roku.
    f. Do plików i folderów w usłudze chmury można uzyskać dostęp i nimi zarządzać poprzez witrynę www.
    g. Miejsce składowania danych na obszarze UE.

2. Aktualizacja posiadanego oprogramowania backup Ferro Backup System do najnowszej wersji oferowanej przez producenta w postaci licencji wieczystej umożliwiającej backup 20 stacji roboczych oraz jednego serwera fizycznego z maksymalnie 4 maszynami wirtualnymi wraz z zapewnieniem wsparcia producenta oprogramowania w okresie do 30.06.2026 r.
   lub dostawa równoważnej platformy oprogramowania backup zapewniającej wszystkie powyższe wymagania oraz poniżej wskazane kryteria równoważności:

1. System musi tworzyć „samowystarczalne” archiwa do odzyskania których nie jest wymagana osobna baza danych.
2. System musi mieć mechanizmy kompresji w celu zmniejszenia wielkości archiwów.
3. System musi zapewniać backup jednoprzebiegowy.
4. System musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania.
5. System musi mieć możliwość uruchamiania skryptów przed i po zadaniu backupowym.
6. System musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
7. System musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej.
8. System musi wspierać backup maszyn wirtualnych.
9. System powinien zapewniać wykonywanie kopii zapasowych plików przechowywanych na urządzeniach pracujących pod kontrolą systemów Windows i Linux.
10. System powinien mieć możliwość pracy w programie z dowolnego miejsca bez potrzeby korzystania z Pulpitu zdalnego, jednoczesnej pracy z danym serwerem przez kliku administratorów.
11. System powinien mieć wbudowane następujące funkcje:
    a. Możliwość wykonania backupu całego systemu operacyjnego, łącznie z zainstalowanymi programami, sterownikami i danymi użytkownika, tak aby w przypadku awarii możliwe było odzyskanie działającego systemu operacyjnego i wszystkich zainstalowanych komponentów.
    b. Zautomatyzowane przywracanie systemu operacyjnego z serwerów (prosty sposób przywracania systemu operacyjnego z serwera kopii zapasowych poprzez sieć do uszkodzonego komputera). Możliwość przywrócenia po awarii systemu operacyjnego wraz z wszystkimi zainstalowanymi programami (ang. bare-metal restore), tak aby uruchomić system operacyjny bez potrzeby ponownej instalacji i konfiguracji.
    c. Ochrona przed programami ransomware szyfrującymi pliki.
    d. Backup i odzyskiwanie maszyn wirtualnych Hyper-V oraz VMWare ESX, ESXi. Program powinien wykonywać kopie zapasowe zarówno zatrzymanych jak i uruchomionych maszyn wirtualnych.
    e. Certyfikaty SSL dla połączeń HTTPS – możliwość obsługi samopodpisanych certyfikatów oraz stosowania własnych certyfikatów SSL.
    f. Zabezpieczanie połączeń sieciowych w systemach archiwizacji danych - typu klient-serwer za pomocą reguł IPSec.
    g. Możliwość archiwizacja danych w chmurze.
    h. Backup plików PST (MS Outlook) - backup plików PST bez zamykania programu Outlook.
    i. Możliwość automatycznego backupu urządzenia przy zamykaniu systemu.
    j. Archiwizacja danych także na napędy taśmowe – możliwość replikacji na napędy taśmowe.
    k. Możliwość backupu na dysk sieciowy - składowanie kopii na urządzeniach typu NAS szybkim i wydajnym protokołem iSCSI.
    l. Możliwość instalacji serwera backupu pod systemem Linux i Mac OS.

m. Możliwość wydajnego i pewnego backupu baz danych i plików poczty (Microsoft SQL Server, Microsoft Exchange Server, Oracle, MySQL, InterBase, Firebird, Microsoft Access, dBase, Paradox oraz plików programów pocztowych: Microsoft Outlook, Outlook Express, Mozilla Thunderbird).
n. Możliwość archiwizacji otwartych i zablokowanych plików.
o. Możliwość szyfrowania archiwów (w tym AES 256).
p. Możliwość wykonywania archiwizacji pełnej i różnicowej, także różnicowej na poziomie fragmentów plików (archiwizowane są tylko te części plików, które zostały zmodyfikowane od czasu poprzednich archiwizacji a pozostałe są pomijane).
q. Możliwość generowania raportów i statystyk, które pomagają w analizie działania aplikacji (Raporty informujące o niewykonanych i opóźnionych zadaniach archiwizacji i statystyki zawierające informacje na temat szybkości i rozmiaru backupu z poszczególnych komputerów).
r. Możliwość wykonywania zadań archiwizacji w/g harmonogramu następującego typu: Na żądanie - zadanie archiwizacji będzie wykonywane tylko przez manualne uruchomienie zadania; Codziennie - zadanie archiwizacji będzie uruchamiane codziennie o wskazanej godzinie; Co określoną liczbę dni - zadanie archiwizacji będzie wykonywane automatycznie co określoną liczbę dni; Co określoną liczbę godzin - zadanie archiwizacji będzie wykonywane automatycznie co określoną liczbę godzin; Co określoną liczbę minut - zadanie archiwizacji będzie wykonywane automatycznie co określoną liczbę minut; W dni tygodnia - zadanie archiwizacji będzie wykonywane automatycznie w wybrane dni tygodnia; Czas rozpoczęcia - umożliwia ustalenie terminu rozpoczęcia zadania archiwizacji z dokładnością do jednej minuty; Następny termin - umożliwia ustalenie daty kolejnej archiwizacji; Zadania opóźnione mogą być pominięte i wykonane w następnym terminie, wykonane natychmiast po podłączeniu serwera; Przy zamykaniu systemu.
s. Dziennik zdarzeń służący do sprawdzania poprawności działania systemu i wyszukiwania przyczyn ewentualnych problemów – możliwość na bieżąco śledzenia generowanych zdarzeń, dotyczących działania całego systemu, takie jak: błędy, ostrzeżenia i informacje. Wszystkie zapisane zdarzenia można filtrować co najmniej według typu zdarzenia oraz nazwy komputera, którego dana informacja dotyczy.
t. Podczas wyboru plików i katalogów do archiwizacji pozwalać określić woluminy, maski lub pełne ścieżki do plików i katalogów, które mają być archiwizowane i te, które mają być wykluczone z archiwizacji.
u. Obsługę co najmniej następujących rodzajów archiwizacji: archiwizacja pełna; archiwizacja różnicowa; archiwizacja różnicowa na poziomie fragmentów plików.
v. Obsługę kopii rotacyjnych (wersjonowanie, retencja danych - pozwala określić, ile maksymalnie przechowywać archiwów na dysku, ile przechowywać kopii wstecz).
w. Obsługę replikacji archiwów - archiwa należące do wybranego zadania backupu mogą być powielane w inne miejsce, replikacja może być wykonywana na napędy dyskowe, optyczne i taśmowe.
x. Monitoring i kontrola pracy serwera backupu, powinna w łatwy i intuicyjny sposób umożliwić zatrzymanie i uruchomienie serwera backupu, możliwość wywołania wirtualnego wiersz poleceń na serwerze backupu i podłączonych stacjach roboczych.

y. Dziennik zdarzeń służy do sprawdzania poprawności działania Systemu i wyszukiwania przyczyn ewentualnych problemów. W zakładce Dziennik zdarzeń można na bieżąco śledzić wszystkie generowane zdarzenia dotyczące działania całego Systemu (serwera jak i stacji roboczych), takie jak: błędy, ostrzeżenia i informacje.
z. Wszystkie zapisane zdarzenia można filtrować według typu zdarzenia oraz nazwy urządzenia, którego dana informacja dotyczy.
aa. Wysyłanie alertów administracyjnych, zawierających raporty lub wybrane komunikaty z dziennika zdarzeń, wg ustalonego harmonogramu na wskazany adres e-mail lub np. do serwera syslog.
bb. Możliwy dostęp do zasobów sieciowych przez np. definiowanie ścieżki UNC, dyski sieciowe i dyski serwerów FTP, które mogą być wykorzystywane przez system jako: miejsce przechowywania archiwów, katalog docelowy replikacji, ścieżka zapisu alertów administracyjnych.
cc. Możliwe używania poleceń lokalnych, służących do rozszerzania funkcjonalności programu. Dzięki nim można automatycznie uruchamiać na serwerze backupu zewnętrzne programy, skrypty lub pliki wsadowe, wykonywać operacje na plikach, wykorzystywać komponenty ActiveX, sterować usługami Active Directory, itp.
dd. Program może być uruchamiany w trybie Usługi systemowej lub awaryjnie, także w trybie aplikacji użytkownika.
ee. Możliwe uruchomienie programu w trybie diagnostycznym oraz w trybie naprawy bazy danych.

4.4. Rozbudowa oprogramowania antywirusowego o funkcje XDR, szyfrowania danych, zarządzanie podatnościami (1 szt.) – Część 3

Rozbudowa oprogramowania antywirusowego będzie polegać na zapewnieniu najnowszej wersji licencji istniejącego oprogramowania w okresie do dnia 30.06.2026 r. oraz rozbudowę o dodatkowe moduły oprogramowania dla Urzędu Miejskiego w Łabiszynie, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Miejskiego Ośrodka Pomocy Społecznej, ul. Szubińska 1, 89-210 Łabiszyn; Miejskiego Zespołu Oświaty, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Zakładu Wodociągów i Kanalizacji w Łabiszynie, ul. Plac 1000-lecia 1, 89-210 Łabiszyn. Aktualnie poszczególne jednostki posiadają licencje oprogramowania antywirusowego ESET, a przedmiotem zamówienia jest rozbudowa licencji do wersji ESET PROTECT Elite ważnej w okresie do dnia 30.06.2026 r. ~~dla maksymalnie 120 użytkowników łącznie dla~~ **maksymalnie 100 użytkowników łącznie** oraz umożliwienie zarządzania wszystkimi użytkownikami/urządzeń końcowych z jednej konsoli chmurowej

lub dostawa równoważnej platformy bezpieczeństwa zgodnie z określonymi poniżej kryteriami równoważności.

Minimalne wymagania (kryteria równoważności) określone dla równoważnej platformy bezpieczeństwa:

Administracja zdalna w chmurze.

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.

2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

<u>Ochrona stacji roboczych.</u>

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    d. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
    a. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    b. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
    c. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,

d. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

<u>Ochrona serwera.</u>

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
   Dodatkowe wymagania dla ochrony serwerów Windows:
9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
    Dodatkowe wymagania dla ochrony serwerów Linux:
18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Szyfrowanie.

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10/11 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android.

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
    a. usunięcie zawartości urządzenia,
    b. przywrócenie urządzenie do ustawień fabrycznych,
    c. zablokowania urządzenia,
    d. uruchomienie sygnału dźwiękowego,
    e. lokalizację GPS.
    f. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
    g. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
    h. nazwę aplikacji,

i. nazwę pakietu,
j. kategorię sklepu Google Play,
k. uprawnienia aplikacji,
l. pochodzenie aplikacji z nieznanego źródła.

Ochrona serwera pocztowego MS Exchange.

1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.
2. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.
3. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
4. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
5. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
6. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
7. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
8. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
9. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
10. Rozwiązanie ma posiadać mechanizm greylisting (szara lista).
11. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

Sandbox w chmurze.

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.

11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
    a. Czysty,
    b. Podejrzany,
    c. Bardzo podejrzany,
    d. Szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

<u>Ochrona usługi Microsoft 365.</u>

1. Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams.
2. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Micosoft 365.
3. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.
4. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.
5. Rozwiązanie musi być dostępne w języku polskim.
6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:
    a. użytkowników, otrzymujących najwięcej spamu,
    b. użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
    c. użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
    d. kont użytkowników, które mogę być podejrzane.
7. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.
8. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:
    a. jaka ilość wiadomości została przeskanowania,
    b. wynik skanowania poszczególnej wiadomości,
    c. czynność podjęta przez rozwiązanie.
9. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o: zagrożeniach, które zostały wykryte,
    a. na jakim koncie zostały wykryte,
    b. jakie zagrożenie zostało wykryte,
    c. podjętą czynność.
10. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.
11. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.

12. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
13. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:
    a. wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
    b. wprowadzenia białych i czarnych list adresów ochrony Exchange'a Online,
    c. dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
14. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
15. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
16. Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
17. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
18. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.

<u>Moduł zarządzania podatnościami i aktualizacjami.</u>

1. Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.
2. Baza wykrywanych podatności musi zawierać minimum 35000 CVE.
3. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli ani innych dodatkowych komponentów na stacjach końcowych.
4. Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.
5. Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum:
    a. nazwę aplikacji lub systemu operacyjnego;
    b. punktacje CVSS;
    c. opis wykrytej podatności;
    d. wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta.
6. Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach.
7. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.
8. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
9. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
10. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.

11. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
12. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.
13. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.
14. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.

Moduł XDR.

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica".
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer musi posiadać minimum 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji

dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.

16. Konsola administracyjna musi mieć możliwość tagowania obiektów.
17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

Ochrona poprzez dwuskładnikowe uwierzytelnianie.

1. Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022.
2. Rozwiązanie musi wspierać system operacyjne Windows 10 / Windows 11.
3. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
4. Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019.
5. Oprogramowanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016.
6. Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 / 2019.
7. Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access.
8. Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web Access.
9. Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access.
10. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
11. Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).
12. Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji.
13. Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.
14. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.
15. Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS.
16. Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego.

Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego Wykonawca dostarcza i wdraża na swój koszt. Wykonawca przeprowadzi instruktaże stanowiskowe i będzie świadczył asystę techniczną w zakresie umożliwiającym pracownikom jednostki Zamawiającego płynną obsługę wymienianego oprogramowania. Wdrożenie rozwiązania równoważnego nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy i musi odbywać się zgodnie z wytycznymi wynikającymi z niniejszego dokumentu.

4.5. Zakup oprogramowania do zarządzania bezpieczeństwem IT (DLP, monitoring zasobów, zarządzanie dostępem) (1 szt.) – Część 4 [zmiana w dniu 18.02.2026r. kolorem zielony zaznaczono wprowadzone zmiany w opisie]

Przedmiotem zamówienia jest dostawa i wdrożenie oprogramowania w formie licencji wieczystej do zarządzania bezpieczeństwem IT umożliwiającego szereg funkcji podnoszących cyberbezpieczeństwo dla Urzędu Miejskiego w Łabiszynie, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Miejskiego Ośrodka Pomocy Społecznej, ul. Szubińska 1, 89-210 Łabiszyn; Miejskiego Zespołu Oświaty, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Zakładu Wodociągów i Kanalizacji w Łabiszynie, ul. Plac 1000-lecia 1, 89-210 Łabiszyn.

Wykonawca jest zobligowany wziąć pod uwagę zakres użytkowania oprogramowania obejmujący łącznie maksimum 60 urządzeń.

Minimalne wymagania funkcjonalne dla oprogramowania do zarządzania bezpieczeństwem IT:

1. Funkcjonalność agenta.
   a) System musi umożliwiać pełne zdalne zarządzanie agentami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania agenta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego.
   b) Agent musi mieć możliwość konfiguracji zakresu skanowania plików.
   c) Agent musi mieć możliwość wyświetlenia dowolnego komunikatu wysłanego z poziomu konsoli administracyjnej, a konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkowniku, który go wyświetlił.
   d) Agent musi mieć budowę modułową – uniemożliwienie pracy jednego z modułów (np. w wyniku niekompatybilnego systemu operacyjnego, pracy programów firm trzecich, awarii sprzętowej) nie może blokować pracy całego Agenta.
   e) Po wykryciu nieprawidłowości w pracy dowolnego z modułów Agent powinien podjąć samoczynną próbę jego naprawy i przywrócenia do działania.
2. Funkcjonalność konsoli administracyjnej.
   a) Konsola musi być w pełni polskojęzyczna.
   b) Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną.
   c) Konsola administracyjna musi posiadać dashboardy – dashboard użytkownika, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie.
   d) Dashboard użytkownika jest budowany samodzielnie przez użytkownika poprzez wybór szybkiego skrótu do dowolnego ekranu aplikacji lub wybór dowolnego widgetu.
   e) Dashboard prezentujący parametry sieci powinien zawierać widgety pogrupowane w kategorie.
   f) Konsola administracyjna musi być wyposażona w panel zawierający graficzne widgety prezentujące dane w postaci wykresu kołowego i/lub słupkowego i/lub w formie tabeli z danymi.
   g) Dane na widgetach muszą być aktualizowane automatycznie lub w każdym czasie na życzenia użytkownika.

h) Widgety muszą być skojarzone dziedzinowo ze wszystkimi obszarami zarządzania infrastrukturą.
i) System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widgety, ich konfigurację i kolejność).
j) Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu. Reguły muszą być zapamiętywane i dostępne w kolejnych sesjach oraz oparte co najmniej o: nazwę komputera, IP, rodzaj systemu operacyjnego, identyfikator agenta, strukturę organizacyjną, stan agenta (włączony/wyłączony), nazwę użytkownika zalogowanego, producenta sprzętu, dostawcę sprzętu, lokalizację komputera, dowolnie zdefiniowaną przez użytkownika wartość (np. kolor obudowy komputera).
k) System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, dodawanie, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.
l) Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie musi utracić prawa do korzystania z konsoli administracyjnej systemu.
m) Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja agenta, stanu agenta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera.
n) Konsola musi zawierać w sobie pełną dokumentację systemu, dokumentacja musi być na bieżąco aktualizowana poprzez automatyczne mechanizmy aktualizacji z serwera aktualizacji producenta.

3. Zarządzanie licencjami.
   a) System musi umożliwiać zarządzanie licencjami w ramach dowolnego elementu struktury organizacyjnej (dla wybranej struktury organizacyjnej pokazuje liczbę instalacji i liczbę licencji w danym modelu licencjonowania wraz z listą komputerów).
   b) System musi dawać możliwość wykonywania wielu audytów legalności i zapamiętywać wyniki tych audytów w odniesieniu do systemów operacyjnych jak i aplikacji/pakietów, z uwzględnieniem struktury organizacyjnej.
   c) System musi pozwalać na zdefiniowanie dowolnej ilości grup oprogramowania.
   d) System musi umożliwiać zdefiniowanie listy aplikacji zabronionych.
   e) System musi umożliwiać utworzenie zdefiniowanie oprogramowania zabronionego i w momencie pojawienia się do na komputerze oprogramowanie powinno przystąpić do automatycznego odinstalowania oprogramowania z listy.
   f) System musi umożliwiać automatyczne przypisanie kategorii do każdego uruchomionego procesu.
   g) System musi umożliwiać zbieranie szczegółowych informacji o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji).
   h) System musi umożliwiać odczytywanie identyfikatorów i kluczy produktowych dla systemu operacyjnego.

i) System powinien automatycznie klasyfikować licencje OEM dla systemów operacyjnych oraz licencje typu freeware dla aplikacji.
j) System musi informować administratora o wygasaniu licencji.
k) System musi umożliwiać wyróżnianie licencji zabezpieczonych kluczami sprzętowymi.
l) System musi automatycznie wskazywać liczbę posiadanych licencji oraz liczbę używanego oprogramowania.
m) System musi prezentować datę instalacji oprogramowania.
n) System musi umożliwiać prowadzenie ewidencji licencji (data zakupu, dostawca, nr faktury, typ licencji, klucz produktowy, identyfikator produktowy, data wygaśnięcia, nr dokumentu OT) poprzez rejestrację dokumentów źródłowych (faktur zakupu) z możliwością dołączenia dowolnych załączników z repozytorium.
o) System musi umożliwiać przypisanie licencji do użytkownika i/lub komputera oraz musi udostępniać informację o licencjach zarejestrowanych i nieprzypisanych.
p) System musi umożliwiać zbieranie informacji na temat uruchamianych aplikacji na inwentaryzowanych komputerach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji).
q) System musi udostępniać informację o uruchamianych aplikacjach w okresie 6 miesięcy oraz udostępniać datę ostatniego uruchomienia.
r) System musi umożliwiać podgląd historii zmian aplikacji i pakietów na komputerach.
s) System musi umożliwiać zdalne odinstalowanie oprogramowania na wybranych komputerach.

4. Inwentaryzacja sprzętu komputerowego.
   a) System musi umożliwiać automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną.
   b) System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation).
   c) System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny, numer części, rozmiar, częstotliwość, taktowanie.
   d) System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego.
   e) System musi umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu).
   f) System musi umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).
   g) System musi umożliwiać skanowanie uprawnień użytkowników oraz grup użytkowników wraz z informacją o uprawnieniach.
   h) System musi umożliwiać prowadzenie ewidencji zmian konfiguracji sprzętu.
   i) System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).
   j) System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium.
5. Inwentaryzacja urządzeń podłączanych do komputera.
   a) System musi automatycznie identyfikować i klasyfikować urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.).
   b) System musi pozwalać na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika.

c) System musi ewidencjonować historię podłączanych urządzeń zewnętrznych w zakresie minimum: komputer, data, godzina, użytkownik).

6. Inwentaryzacja urządzeń innych niż komputery.
   a) System musi umożliwiać inwentaryzację manualną (ewidencję) sprzętu innego niż komputery: np. drukarki, switche, routery, monitory, pamięci masowe itp.
   b) System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner. Skaner musi wykryć typ urządzenia na danym IP/porcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać c najmniej protokół SNMP w wersji 1/2c/3.
   c) Skaner musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.
   d) System musi zbierać informacje o jakości połączenia.
   e) System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają agenta, a w przypadku, gdy takiego agenta nie posiadają powinien umożliwić zdalną instalację agenta.
   f) System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci.
   g) System musi umożliwiać generowanie map według dowolnych filtrów użytkownika.
   h) System musi monitorować zmiany ewidencyjne i ruchy sprzętu.
   i) System musi umożliwiać przypisanie urządzenia do użytkownika, ewidencję napraw, gwarancji.
   j) System musi mieć możliwość przypominania o upływającym terminie gwarancji.
   k) System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu.
   l) System musi umożliwiać samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów oraz zapewniać automatyczną numerację tych dokumentów zapewniającą unikatowość.

7. Ochrona danych (DLP).

1) System musi automatycznie tworzyć listę podłączanych do komputerów urządzeń USB.
2) System musi automatycznie klasyfikować podłączane urządzenia (pamięć masowa, pendrive, aparat fotograficzny, urządzenie multimedialne itp.)
3) System musi umożliwiać uzyskanie informacji kto, kiedy i na jakim komputerze posługiwał się urządzeniem zewnętrznym, pozwalając na jego jednoznaczne zidentyfikowanie.
4) System musi umożliwiać utworzenie listy urządzeń USB dozwolonych do stosowania.
5) System musi mieć możliwość zidentyfikowania urządzenia USB i wprowadzenia go do systemu za pośrednictwem konsoli administracyjnej.
6) System musi umożliwiać zdefiniowanie reguł stanowiących podstawę użytkowania urządzeń USB (dozwolone/niedozwolone) na inwentaryzowanych komputerach.
7) System musi zapewniać ciągłą ochronę danych niezależnie od położenia komputera (w sieci lokalnej, sieci VPN, poza siecią).
8) System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez bieżące (w czasie rzeczywistym) monitorowanie działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa oraz reguł ich opisujących.

9) Obiekty docelowe reguł muszą być definiowalne za pomocą parametrów takich jak: nazwa komputera, adres IP, unikatowy identyfikator agenta, status podłączenia do systemu (online/offline), zainstalowany system operacyjny, nazwę zalogowanego użytkownika, model komputera, producent komputera, dostawca komputera, budżet, z którego zakupiony został komputer, strukturę organizacyjną. Przy definiowaniu obiektów docelowych dla reguł DLP można korzystać ze znaków wieloznacznych.
10) System musi posiadać funkcjonalności monitorowania, blokowania, powiadomieniu użytkownika o wystąpieniu naruszenia zdefiniowanej polityki oraz pełnego logowania zdarzeń dotyczących polityki dla celów administracyjnych (powiadomienie administratora systemu).
11) System musi mieć możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP. A także możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji.
12) Nowy komputer zgłaszający się do systemu po raz pierwszy musi bez dodatkowej ingerencji administratora automatycznie pobrać oraz wdrożyć (uruchomić) przeznaczoną dla niego politykę.
13) System musi mieć możliwość określenia ram czasowych działania danej reguły.
14) System musi dysponować mechanizmami dostępu do plików na poziomie jądra systemu operacyjnego MS Windows (32-bit i 64-bit), co uniemożliwia obejście zabezpieczeń nawet osobie z uprawnieniami administratora na poziomie systemu operacyjnego.
15) System powinien posiadać możliwość definiowania schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione.
16) System musi mieć możliwość reakcji i powiadamiania o przekroczeniu dozwolonego czasu pracy komputera
17) System powinien umożliwić wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku).
18) System musi w pełni wspierać polityki dotyczące kontroli i ochrony urządzeń:
    a) Blokowanie dostępu do wybranych typów urządzeń od strony sprzętowej. Wsparcie dla CD-ROM, portów USB, kart sieciowych, GPS, kart graficznych, modemów, klawiatur, czytników kart, drukarek, urządzeń Bluetooth i innych, monitorowanie podłączanych urządzeń.
    b) Blokowanie dostępu do urządzeń USB, tworzenie czarnych list urządzeń, monitorowane podłączanych urządzań USB.
    c) Zarządzanie dostępem do sieci społecznościowych, serwisów informacyjnych, blogów, bibliotek, forów dyskusyjnych oraz dowolnych stron www.
    d) Blokowanie sieci ze względu na zdefiniowany typ i maskę sieci WIFI. Polityka musi zapewniać blokowanie dostępu do sieci zarówno otwartych jak i zabezpieczonych.
19) System musi w pełni wspierać polityki dotyczące ochrony danych w użyciu takie jak:
    a) Podjęcie działania w momencie uruchomienia określonego procesu.
    b) Podjęcie działań monitorowania i blokowania operacji w momencie próby kopiowania tekstu, zdjęcia czy ścieżki plików do schowka.
    c) Monitorowanie wykonywanych zrzutów ekranu, blokowanie możliwości ich zapisania i wykorzystania.

d) Przechwytywanie zrzutów ekranu z komputerów użytkowników wyzwalany akcją użytkownika lub na życzenie administratora zgodnie z wcześniej ustawionym interwałem czasowym.

20) Przez dane w użyciu należy rozumieć dane, które są aktywnie przetwarzane przez dowolną aplikację i/lub punkt końcowy (komputer). Przykłady danych w użyciu: edycja dokumentu MS Word, Excel, PowerPoint, edycja pliku tekstowego CSV, TXT, tworzenie pliku, przechwytywanie ekranu (screenshot), kopiowanie / wklejanie danych.
21) System musi w pełni wspierać polityki dotyczące ochrony danych w ruchu z zakresu:
    a) monitorowania danych przesyłanych za pomocą poczty e-mail oraz blokowanie przesyłania plików określonych typów. Monitorowanie poczty e-mail co najmniej w zakresie: data, pracownik, komputer, adresaci, ilość, typ i rozmiar załączników.
    b) monitorowania danych przesyłanych do chmury oraz blokowanie synchronizacji plików określonych typów z wybraną chmurą.
    c) monitorowania i blokowania operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach

Przez dane w ruchu należy rozumieć dane, które są przesyłane, np. kopiowanie danych (plików) z dysku sieciowego na nośnik USB, kopiowanie danych (plików) z komputera na komputer, przesyłanie danych e-mailem w treści lub w postaci załącznika, pobieranie danych z serwera FTP, przesyłanie danych za pomocą komunikatora.

22) System musi w pełni wspierać następujące polityki dotyczące Klasyfikacji i ochrony dokumentów:
    a) oznaczanie na dowolnym komputerze (znakowanie przez agenta) określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami.
    b) znakowanie określonych plików przechowywanych w zasobach serwerów lub udostępnionych zasobach (np. samodzielna macierz dyskowa) wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami, z wykorzystaniem harmonogramu.

8. Zdalna administracja komputerami.
    a) System musi automatycznie wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika.
    b) System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym.
    c) System musi umożliwiać min. przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacja oprogramowania, poprawek i aktualizacji.
    d) System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem.
    e) System powinien być wyposażony w predefiniowane zadania w zakresie minimum: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory windows,

włączenie usługi Windows Update, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD).

f) Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania oraz udostępniać informację zwrotną o przebiegu wykonania.
g) System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, windows powershell.

9. Automatyzacja.
   a) System musi mieć możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące.
   b) Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania danej czynności (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych, a także zatrzymania/uruchomienia harmonogramu uruchomienia dla każdej z czynności.
   c) System musi mieć możliwość definiowania czynności wykonywanych automatycznie.
   d) System musi być wyposażony w następujące mechanizmy automatyzacji: wykonywanie kopii bezpieczeństwa bazy danych, identyfikacja aplikacji i pakietów, porządkowanie bazy danych / odbudowa indeksów, usuwanie nadmiarowych danych w bazie danych, usuwanie zewnętrznych plików (logów).
   e) System musi być wyposażony w mechanizmy informowania - wysyłania komunikatów (alerty) o: zasobach zakazanych (pliki erotyczne i pornograficzne), zasobach multimedialnych (pliki multimedialne), nowych komputerach w bazie danych, braku skanowania komputerów, brakach w licencjach, niewłaściwych datach systemowych komputerów, urządzeniach bez użytkowników, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www /aplikacjach, wygasaniu serwisu lub licencji, przekroczeniu wielkości bazy danych, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu sieci, nadmiernym obciążeniu sieci na komputerze, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku, upływającej gwarancji,
   f) System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.).
   g) System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)
   h) System musi umożliwiać tworzenie zadań cyklicznych dla komputerów.
10. Repozytorium.
   a) Konsola administracyjna musi być wyposażona w repozytorium dokumentów dowolnego typu.
   b) Repozytorium musi umożliwiać: dodawanie nowych dokumentów dowolnego typu, przeszukiwanie, oznaczanie dokumentów więcej niż jednym znacznikiem, podgląd dokumentów, dołączanie dokumentów z repozytorium w dowolnym miejscu systemu, uzyskanie informacji w jakich miejscach systemu dany dokument repozytorium występuje.
11. Monitorowanie drukarek sieciowych i wydruków.
   a) System musi posiadać możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa).
   b) Ewidencja wydruków musi obejmować minimum: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera, z którego dokonano

wydruku, format dokumentu, informację i jedno bądź dwustronnym wydruku, informację o wydruku mono/kolor.

c) System musi generować zestawienia pozwalające ustalić miejsca powstawania wydruków (komórki organizacyjne, użytkownicy) oraz stopień obciążenia poszczególnych urządzeń drukujących.

d) Dla każdej z drukarek SNMP system musi udostępniać informacje: nr seryjny, IP, MAC, bieżący status drukarki, całkowitą ilość wydrukowanych stron, ilość wydrukowanych stron od uruchomienia, błędy, alerty, dostępne porty, stan pokryw, interfejsów sieciowych, rodzaj i ilości pamięci całkowitej i wykorzystanej, informacje o poziomie materiałów eksploatacyjnych

12. Monitorowanie stron www.
    a) System musi posiadać możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej.
    b) Ewidencja otwieranych stron musi dotyczyć wielu jednocześnie otwartych zakładek.
    c) Ewidencja otwieranych stron musi działać również, gdy otwierana jest strona z połączeniem szyfrowanym (https).
    d) Ewidencja musi obejmować co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony, łączny czas korzystania, czas aktywności, czas pasywności.
13. Monitorowanie dziennika zdarzeń.
    a) System musi posiadać możliwość monitorowania dziennika zdarzeń wszystkich komputerów.
    b) Ewidencja zdarzeń musi następować w oparciu o definiowalną kategorię zdarzenia: critical, error, warning, info, audit failure, audit success, debug oraz typ dziennika: aplikacja, bezpieczeństwo, system.
    c) System musi pozwalać na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia.
    d) Ewidencja musi zawierać: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia.
    e) System musi umożliwiać monitorowanie komunikatów Syslog.
14. Monitorowanie pracy komputerów.
    a) System musi posiadać możliwość monitorowania daty włączenia i wyłączenia komputera niezależnie czy znajduje się w sieci lokalnej czy też poza nią i prezentować czas pracy komputera w układzie graficznym.
    b) System musi posiadać ewidencję daty i godziny przyłączenia i odłączenia komputera od systemu monitorującego.
    c) System musi ewidencjonować zdarzenia związane z logowaniem się użytkowników do danego komputera, również w przypadku podłączania się wielu użytkowników jednocześnie
15. Monitorowanie sesji zdalnych połączeń.
    d) System musi prowadzić ewidencję sesji zdalnych połączeń na każdym komputerze.
    e) Informacja o nawiązanej sesji musi zawierać co najmniej: nazwę i adres IP komputera, z którego nastąpiło połączenia, nazwę użytkownika nawiązującego połączenie, nazwę i adres IP komputera docelowego, adres portu połączenia.
16. Raportowanie i eksport danych.
    a) System musi mieć możliwość kategoryzowania raportów (spośród wszystkich raportów) oraz dodawania raportów użytkownika (zaprojektowanych przez użytkownika).
    b) System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów.

c) System musi umożliwiać eksport danych z raportu do formatów: PDF, XLS, DOC, RTF.
d) System musi posiadać grupę zdefiniowanych raportów dotyczących wszystkich obszarów funkcjonalnych.
e) System musi posiadać możliwość ustalenia harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu.

17. Powiadomienia.
    a) System musi umożliwiać generowanie powiadomienia w formie alertu w konsoli systemu, wiadomości email wysłanej na wybrane adresy oraz wiadomości SMS na wskazane numery telefonów.
    b) System musi umożliwiać tworzenie wybranych powiadomień wiele razy z określeniem innych grup obiorców.
    c) System musi umożliwiać edycję treści wysyłanych powiadomień i możliwość korzystania z danych umieszczonych w systemie w treści powiadomienia.
    d) System musi posiadać grupę zdefiniowanych powiadomień dotyczących obszarów funkcjonalnych.
18. Bezpieczeństwo.
    a) System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.
    b) Uwierzytelnianie do systemu musi być realizowane z wykorzystaniem imiennego konta użytkownika i hasła, z wykorzystaniem imiennego konta administratorów aplikacji i hasła, za pośrednictwem jednokrotnego uwierzytelniania poprzez Active Directory.
    c) Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej.
    d) Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków.
    e) System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie.
    f) System musi udostępniać historię korzystania z poszczególnych opcji przez wybranych użytkowników/administratorów.
    g) System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nieprzyrostowej oraz udostępniać informacje o rezultacie wykonania kopii.
    h) System musi być wyposażony w mechanizmy powtórnego załadowania danych historycznych pochodzących od agentów.
19. System musi w pełni wspierać następujące polityki ochrony danych:
    a) Zdefiniowanie schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione.
    b) Oznaczanie na dowolnym komputerze (znakowanie przez agenta) określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami będącymi alternatywnym strumieniem danych w pliku.

c) Znakowanie określonych plików przechowywanych w zasobach serwerów lub udostępnionych zasobach (np. samodzielna macierz dyskowa) wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami, z wykorzystaniem harmonogramu jako alternatywny strumień danych.
d) Kontrolowanie wykonywania przez użytkowników operacji zrzutu ekranu.
e) Generowanie automatycznych zrzutów ekranu komputera w ramach ustalonego interwału czasowego wyrażonego w sekundach.
f) Umożliwienie powiadamianie o przekroczeniu dozwolonego czasu pracy komputera.
g) Podjęcie działania w momencie uruchomienia określonego procesu.
h) Monitorowanie określonych typów urządzeń przenośnych.
i) Monitorowania i blokowania operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach.
j) Zarządzanie dostępem do sieci społecznościowych, serwisów informacyjnych, blogów, bibliotek, forów dyskusyjnych oraz dowolnych stron www.
k) Wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku).
l) Monitorowanie danych przesyłanych za pomocą poczty e-mail oraz blokowanie przesyłania plików określonych typów w lokalnej wersji poczty outlook.
m) Monitorowanie danych przesyłanych do chmury oraz blokowanie synchronizacji plików określonych typów z wybraną chmurą.
n) Blokowanie lub zezwalanie działania określonym typom urządzeń dostępnych w menedżerze urządzeń.
o) System musi pozwalać na zarzadzanie dostępem do telefonów komórkowych w trybie pamięci masowej, czytników kart pamięci i pendrive USB.
p) Podjęcie działań monitorowania i blokowania operacji w momencie próby kopiowania tekstu, zdjęcia czy ścieżki plików do schowka.
q) Blokowanie sieci ze względu na zdefiniowany typ i maskę sieci WIFI. Polityka musi zapewniać blokowanie dostępu do sieci zarówno otwartych jak i zabezpieczonych.

20. Monitorowanie i ochrona danych.
a) System musi wspierać definiowanie nieograniczonej liczby znaczników (ang. fingerprint) i umożliwiać użycie ich do znakowania danych (plików).
b) System musi umożliwiać zdefiniowania bądź wykluczenia maski plików do oznakowania z wykorzystaniem znaków wieloznacznych, w konkretnych lokalizacjach lokalnych bądź sieciowych.
c) Znacznik nie może naruszać struktury pliku, w szczególności sygnatury podpisu cyfrowego, wielkości pliku i musi być niewidoczny dla użytkownika.
d) Jeden plik może być oznaczony dowolną ilością znaczników.
e) Zdejmowanie znaczników może być prowadzone w sposób manualny zdalnie przez administratora lub automatycznie, gdy reguła ustali, że znacznik powinien być zdjęty (np. plik w wyniku prowadzonej przez użytkownika edycji nie posiada już danych osobowych).
f) System musi automatycznie znakować plików tworzone przez zdefiniowane procesy aplikacji, wybranych użytkowników.

g) System musi mieć możliwość automatycznego ustawiania / usuwania znaczników na plikach (np. txt, doc, docx, xls, xlsx, ppt, pptx) w oparciu o dowolnie zdefiniowaną zawartości (treści) pliku w postaci tekstu i wyrażenia regularnego.

21. Monitorowanie czasu pracy.
    a) System musi mieć możliwość zdefiniowania dowolnej ilości reguł dotyczących czasu pracy komputera.
    b) System musi mieć możliwość zdefiniowania zalecanego czasu pracy dla każdego komputera, przy czym czas pracy w każdym dniu tygodnia może być zdefiniowany inaczej.
    c) System musi mieć możliwość automatycznego dołączenia bieżącego zrzutu ekranu do każdego incydentu związanego z przekroczeniem zalecanego czasu pracy.
22. Zarządzanie politykami bezpieczeństwa.
    a) System musi mieć możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP.
    b) System musi mieć możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji.
    c) System musi mieć możliwość definiowania obiektów, na których działać będzie reguła w oparciu o parametry: nazwę komputera, adres IP, unikatowy identyfikator agenta, nazwę systemu operacyjnego, zalogowanego użytkownika, model komputera, strukturę organizacyjną, producenta komputera, dostawcę komputera, budżet z jakiego komputer został zakupiony.
    d) Nowy komputer zgłaszający się do systemu po raz pierwszy musi bez dodatkowej ingerencji administratora automatycznie pobrać oraz wdrożyć (uruchomić) przeznaczoną dla niego politykę.
    e) System musi mieć możliwość określenia ram czasowych działania danej reguły.