***Załącznik nr 1 do SWZ***

|  |  |
| --- | --- |
| Numer sprawy: **FZK.271.13.2024** | Działdowo, dnia 11.10.2024r. |
| Szczegółowy Opis Przedmiotu Zamówienia  na dostawy i usługi związane z realizacją projektu  „Cyberbezpieczny Samorząd” | |

Spis treści

[1. Zestawienie ilościowe. 3](#_Toc177503826)

[2. Opis przedmiotu zamówienia dla części nr 1. 4](#_Toc177503827)

[2.1. Wymagania ogólne w zakresie dostawy sprzętu i oprogramowania. 4](#_Toc177503828)

[2.2. Zasada równoważności rozwiązań i neutralności technologicznej. 5](#_Toc177503829)

[2.3. Zakup serwera TYP A (1 szt.). 7](#_Toc177503830)

[2.4. Zakup serwera TYP B (1 szt.). 10](#_Toc177503831)

[2.5. Zakup macierzy (1 szt.). 13](#_Toc177503832)

[2.6. Zakup UPS (2 szt.). 16](#_Toc177503833)

[2.7. Zakup NAS TYP A (1 szt.). 16](#_Toc177503834)

[2.8. Zakup NAS TYP B (2 szt.). 17](#_Toc177503835)

[2.9. Zakup przełącznika sieciowego TYP A (1 szt.). 18](#_Toc177503836)

[2.10. Zakup przełącznika sieciowego TYP B (1 szt.). 18](#_Toc177503837)

[2.11. Rozbudowa istniejącej infrastruktury macierzy - zakup dysków twardych (4 szt.). 19](#_Toc177503838)

[2.12. Rozbudowa istniejącej infrastruktury UTM (1 szt.). 19](#_Toc177503839)

[3. Opis przedmiotu zamówienia dla części nr 2. 32](#_Toc177503840)

[3.1. Wymagania ogólne w zakresie dostawy oprogramowania. 32](#_Toc177503841)

[3.2. Zasada równoważności rozwiązań i neutralności technologicznej. 36](#_Toc177503842)

[3.3. Oprogramowanie do agregacji logów (3 szt.). 38](#_Toc177503843)

[3.4. Rozbudowa oprogramowania antywirusowego o funkcje XDR, szyfrowania danych, zarządzanie podatnościami (1 szt.). 39](#_Toc177503844)

[3.5. Zakup oprogramowania do zarządzania bezpieczeństwem IT (DLP, monitoring zasobów, zarządzanie dostępem) (1 szt.). 48](#_Toc177503845)

[4. Opis przedmiotu zamówienia dla Części nr 3. 53](#_Toc177503846)

[4.1. Wymagania ogólne. 53](#_Toc177503847)

[4.2. Zakup usług aktualizacji i wdrożenia SZBI. 55](#_Toc177503848)

[4.3. Zakup usług przeprowadzenia audytu zgodności KRI. 60](#_Toc177503849)

[4.4. Równoważność rozwiązań. 64](#_Toc177503850)

# 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 | 1 szt. |
| 3. | Zakup macierzy | 1 szt. |
| 4. | Zakup UPS | 2 szt. |
| 5. | Zakup NAS TYP A | 1 szt. |
| 6. | Zakup NAS TYP B | 2 szt. |
| 7. | Zakup przełącznika sieciowego TYP A | 1 szt. |
| 8. | Zakup przełącznika sieciowego TYP B | 1 szt. |
| 9. | Rozbudowa istniejącej infrastruktury macierzy - zakup dysków twardych | 4 szt. |
| 10. | Rozbudowa istniejącej infrastruktury UTM | 1 szt. |

Część nr 2 – Dostawa oprogramowania informatycznego.

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa | Ilość |
| 1. | Oprogramowanie do agregacji logów | 3 szt. |
| 2. | Rozbudowa oprogramowania antywirusowego o funkcje XDR, szyfrowania danych, zarządzanie podatnościami | 1 szt. |
| 3. | Zakup oprogramowania do zarządzania bezpieczeństwem IT (DLP, monitoring zasobów, zarządzanie dostępem) | 1 szt. |

Część nr 3 – Przeprowadzenie audytu KRI oraz aktualizacja i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji dla urzędu i jego jednostek organizacyjnych.

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa | Ilość |
| 1. | Zakup usług aktualizacji i wdrożenia SZBI | 1 szt. |
| 2. | Zakup usług przeprowadzenia audytu zgodności KRI | 3 szt. |

# Opis przedmiotu zamówienia dla części nr 1.

# Wymagania ogólne w zakresie dostawy sprzętu i oprogramowania.

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.
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.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do każdej wskazanej przez Zamawiającego lokalizacji.
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. W ramach prac konfiguracyjnych serwerów, macierzy dyskowej, przełączników, UPS, urządzeń NAS i UTM Zamawiający wymaga: zaprojektowania schematu logicznego LAN dla dostarczanej infrastruktury wraz z uwzględnieniem istniejącej infrastruktury; opracowania założeń optymalizacji ruchu i zapewnienia bezpieczeństwa implementacji i separacji sieci; instalacji urządzeń w szafie RACK; podłączenia urządzeń kablami zasilającymi do gniazd sieci zasilającej, połączenia dostarczanej infrastruktury ze sobą przy wykorzystaniu portów 10GbE SFP+ za pomocą kabli światłowodowych i wkładek SFP+, wykonania aktualizacji oprogramowania i firmware’ów na urządzeniach; skonfigurowania połączeń sieciowych na urządzeniach zgodnie z wcześniej zaprojektowanym schematem logicznym; przeprowadzenie konfiguracji i udostępnienia zasobów dyskowych urządzenia NAS przez utworzenie puli dyskowej udostępniającej przestrzeń dyskową przeznaczoną na kopie bezpieczeństwa; wykonanie testów akceptacyjnych polegających na weryfikacji poprawności pracy dostarczonych urządzeń; opracowanie i przekazanie Zamawiającemu dokumentacji powykonawczej zainstalowanych urządzeń oraz wykonanych prac instalacyjno-konfiguracyjnych.
11. 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.
12. 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.

# 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.

# Zakup serwera TYP A (1 szt.).

Minimalne parametry techniczne serwera TYP A:

1. Obudowa typu RACK o wysokości maksymalnie 2U z możliwością instalacji do 8 dysków 3.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
2. Płyta główna z możliwością zainstalowania dwóch procesorów.
3. Zainstalowane dwa procesory szesnastordzeniowe klasy x86 dedykowane do pracy z oferowanym serwerem, umożliwiające osiągnięcie przez serwer wyniku co najmniej 280 punktów w teście SPECrate2017\_int\_base dla konfiguracji dwuprocesorowej według wyników publikowanych na stronie [www.spec.org](http://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, płyta główna musi obsługiwać do min. 1 TB pamięci RAM DDR5.
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.
6. Co najmniej jeden wolny slot PCIe x8 generacji 4 w celu możliwości rozbudowy serwera.
7. Zintegrowana karta graficzna ze złączem VGA.
8. Interfejsy sieciowe: Wbudowane co najmniej 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 8 interfejsów sieciowych 10/25GbE Ethernet w standardzie SFP28, (karty dual port). Dodatkowo wkładki optyczne SFP28 25 Gb/s dedykowane do dostarczonego urządzenia w ilości 8 sztuk.
9. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 6 dysków twardych Hot-Plug SSD SAS o prędkości min. 12 Gb/s o pojemności co najmniej 1,92 TB każdy. W przypadku uszkodzenia dysku w okresie gwarancji Zamawiający wymaga by uszkodzony dysk pozostał jego własnością.
10. Możliwość zainstalowania co najmniej dwóch dysków M.2 SATA z możliwością konfiguracji RAID 1.
11. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w co najmniej dwa nośniki typu flash z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
12. Kontroler RAID: Sprzętowy kontroler dyskowy, umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
13. Wsparcie dla dysków samoszyfrujących.
14. Wbudowane porty: min. 3 zewnętrzne porty USB, w tym co najmniej 1 port USB 3.x, co najmniej 1 port USB musi być dostępny z przodu obudowy. Dodatkowo min. jeden port dedykowany dla karty zarządzającej 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.
15. Wentylatory: Redundantne typu Hot Plug.
16. Zasilacze: Redundantne typu Hot Plug o mocy nieprzekraczającej 1100 W każdy.
17. Karta zarządzania: Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:
    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.
18. 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;
    4. możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera;
    5. możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.
19. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzenie serwerem klasy Microsoft Windows Serwer Standard w najnowszej wersji oferowanej przez producenta na dzień składania ofert wraz z 20 licencjami dostępowymi umożliwiającymi korzystanie przez 20 użytkowników lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności.

Warunki równoważności dla dostawy oprogramowania klasy Microsoft Windows Serwer Standard:

* 1. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
  2. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
  3. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64 TB przez każdy wirtualny serwerowy system operacyjny.
  4. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
  5. 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.
  6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
  7. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
  8. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
  9. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
  10. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
  11. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
  12. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
  13. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
  14. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
  15. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
  16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
  17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
  18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
  19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
  20. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
  21. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
  22. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
  23. O ile to konieczne ze względu na licencjonowanie producenta oferowanego serwerowego systemu operacyjnego Zamawiający wymaga dostarczenia licencji dostępowych dla 20 użytkowników.

1. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
2. 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 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; Certyfikat NIST SP 800-193 lub inny równoważny dokument potwierdzający, że serwer spełnia wymagania normy NIST SP 800-193 ochrony przed cyberatakami. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany serwer i jego/ich producenta/producentów w zakresie określonym powyżej.
3. 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 dyski Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji przez portal producenta serwera.

# Zakup serwera TYP B (1 szt.).

Minimalne parametry techniczne serwera TYP A:

1. Obudowa typu RACK o wysokości maksymalnie 2U z możliwością instalacji do 8 dysków 3.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
2. Płyta główna z możliwością zainstalowania dwóch procesorów.
3. Zainstalowane dwa procesory szesnastordzeniowe klasy x86 dedykowane do pracy z oferowanym serwerem, umożliwiające osiągnięcie przez serwer wyniku co najmniej 280 punktów w teście SPECrate2017\_int\_base dla konfiguracji dwuprocesorowej według wyników publikowanych na stronie [www.spec.org](http://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, płyta główna musi obsługiwać do min. 1 TB pamięci RAM DDR5.
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.
6. Co najmniej jeden wolny slot PCIe x8 generacji 4 w celu możliwości rozbudowy serwera.
7. Zintegrowana karta graficzna ze złączem VGA.
8. Interfejsy sieciowe: Wbudowane co najmniej 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 8 interfejsów sieciowych 10/25GbE Ethernet w standardzie SFP28 (karty dual port). Dodatkowo dedykowane do dostarczonego urządzenia wkładki optyczne SFP28 25 Gb/s w ilości 8 sztuk.
9. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 6 dysków twardych Hot-Plug SSD SAS o prędkości min. 24 Gb/s o pojemności co najmniej 1,92 TB każdy. W przypadku uszkodzenia dysku w okresie gwarancji Zamawiający wymaga by uszkodzony dysk pozostał jego własnością.
10. Możliwość zainstalowania co najmniej dwóch dysków M.2 SATA z możliwością konfiguracji RAID 1.
11. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w co najmniej dwa nośniki typu flash z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
12. Kontroler RAID: Sprzętowy kontroler dyskowy, obsługujący interfejs SAS 24Gb/s umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
13. Wsparcie dla dysków samoszyfrujących.
14. Wbudowane porty: min. 3 zewnętrzne porty USB, w tym co najmniej 1 port USB 3.x, co najmniej 1 port USB musi być dostępny z przodu obudowy. Dodatkowo min. jeden port dedykowany dla karty zarządzającej 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.
15. Wentylatory: Redundantne typu Hot Plug.
16. Zasilacze: Redundantne typu Hot Plug o mocy nieprzekraczającej 1100 W każdy.
17. Karta zarządzania: Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:
    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.
18. 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;
    4. możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera;
    5. możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.
19. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzenie serwerem klasy Microsoft Windows Serwer Standard w najnowszej wersji na dzień składania ofert wraz z 50 licencjami dostępowymi umożliwiającymi korzystanie przez 50 użytkowników lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności.

Warunki równoważności dla dostawy oprogramowania klasy Microsoft Windows Serwer Standard:

* 1. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
  2. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
  3. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64 TB przez każdy wirtualny serwerowy system operacyjny.
  4. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
  5. 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.
  6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
  7. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
  8. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
  9. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
  10. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
  11. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
  12. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
  13. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
  14. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
  15. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
  16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
  17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
  18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
  19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
  20. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
  21. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
  22. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
  23. O ile to konieczne ze względu na licencjonowanie producenta oferowanego serwerowego systemu operacyjnego Zamawiający wymaga dostarczenia licencji dostępowych dla 50 użytkowników.

1. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
2. 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 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; Certyfikat NIST SP 800-193 lub inny równoważny dokument potwierdzający, że serwer spełnia wymagania normy NIST SP 800-193 ochrony przed cyberatakami. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany serwer i jego/ich producenta/producentów w zakresie określonym powyżej.
3. 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 dyski Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji przez portal producenta serwera.

# Zakup macierzy (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Obudowa typu RACK o wysokości maksymalnie 2U z możliwością instalacji do 12 dysków 3.5" Hot-Plug.
2. Macierz musi posiadać co najmniej 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
3. Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.

Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” i 3,5”. Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 24 dysków twardych.

1. Macierz musi posiadać co najmniej 8 portów iSCSI SFP+/SFP28 25Gb/s(4 porty na kontroler). Dodatkowo dedykowane do dostarczonego urządzenia wkładki optyczne SFP28 25 Gb/s (8 sztuk) oraz patchcordy światłowodowe SFP+ z wtyczkami i osłonkami o długości 2 m (8 szt.).
2. Zainstalowane min. 12 dysków Hot-Plug SAS SSD min. 24Gb/s o pojemności co najmniej 1,92TB każdy.
3. Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).
4. Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID.
5. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).
6. Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
7. Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).
8. Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.
9. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
10. Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.
11. Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.
12. Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na co najmniej 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
13. Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).
14. Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, VMWare. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.
15. Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
16. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje Wykonawca jest je zobowiązany dostarczyć w ramach niniejszego postępowania.
17. Jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent macierzy opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub inny równoważny dokument poświadczający, że producent macierzy posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, ze oferowana macierz 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 macierzy 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 oferowaną macierz i jego/ich producenta/producentów w zakresie określonym powyżej.
18. Gwarancja: min. 60 miesięcy gwarancji producenta obejmująca wszystkie komponenty macierzy wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dyski Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej macierzy, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji przez portal producenta macierzy.

# Zakup UPS (2 szt.).

Minimalne parametry techniczne urządzenia:

1. Typ obudowy: RACK, max 2U, Wykonawca jest zobowiązany dostarczyć szyny do montażu UPS w szafie RACK.
2. Moc pozorna: min. 2200 VA.
3. Moc rzeczywista: min. 2200 W.
4. Architektura UPSa: line-interactive lub online.
5. Typ przebiegu: sinusoidalny.
6. Liczba i rodzaj gniazdek z utrzymaniem zasilania: 2x IEC320 C19; 8x IEC320 C13. Dodatkowe złącze dla dodatkowych baterii.
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 (karta sieciowa)
14. Czujnik monitorujący temperaturę i wilgotność dedykowany do dostarczonego urządzenia
15. Gwarancja producenta: min. 24 miesiące.

# Zakup NAS TYP A (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Obudowa typu RACK. Wykonawca jest zobowiązany dostarczyć szyny do montażu NAS w szafie RACK.
2. Procesor wielordzeniowy osiągający w teście wydajności CPU PassMark Performance Test (https://www.cpubenchmark.net) z wynikiem aktualnym w okresie 30 dni przed terminem składania ofert co najmniej wynik 8600 punktów. Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie przez oferowany procesor żądanej przez Zamawiającego wydajności.
3. Pamięć RAM: min. 8 GB, możliwość rozbudowy i obsługi pamięci do 64 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 8 dysków. Obsługiwane typy dysków: 3,5” SATA HDD, 2,5” SATA SSD, M.2 2280 NVMe SSD. Dyski z możliwością wymiany podczas pracy (hot-swap).
6. Obsługiwane dyski twarde: 3.5" SATA HDD; 2.5" SATA SSD.
7. Zainstalowane dyski: 8 x 8 TB, Interfejs: SATA min. 6 Gb/s, prędkość obrotowa min. 7200 obr/min; rozmiar buforu min. 256 MB; z deklarowanym przez producenta średnim czasem bezawaryjnej pracy co najmniej 1 mln godzin. Dyski muszą być zgodne z urządzeniem NAS, tj. znajdować się na liście zgodności prowadzonej przez producenta urządzenia NAS.
8. Wymaganie poziomy RAID: JBOD, RAID 0, RAID 1, RAID 5, RAID 6 i RAID 10.
9. Interfejsy sieciowy: co najmniej 2 porty 2,5GbE RJ-45
10. Porty USB: min. 3 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 oferowane urządzenie NAS i jego/ich producenta/producentów w zakresie określonym powyżej.
12. Co najmniej 36 miesięcy gwarancji producenta.

# Zakup NAS TYP B (2 szt.).

Minimalne parametry techniczne urządzenia:

1. Obudowa typu RACK. Wykonawca jest zobowiązany dostarczyć szyny do montażu NAS w szafie RACK.
2. Procesor wielordzeniowy osiągający w teście wydajności CPU PassMark Performance Test (https://www.cpubenchmark.net) z wynikiem aktualnym w okresie 30 dni przed terminem składania ofert co najmniej wynik 17000 punktów. Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie przez oferowany procesor żądanej przez Zamawiającego wydajności.
3. Pamięć RAM: min. 8 GB, możliwość rozbudowy i obsługi pamięci do 64 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 8 dysków. Obsługiwane typy dysków: 3,5” SATA HDD, 2,5” SATA SSD, M.2 2280 NVMe SSD. Dyski z możliwością wymiany podczas pracy (hot-swap).
6. Obsługiwane dyski twarde: 3.5" SATA HDD; 2.5" SATA SSD.
7. Zainstalowane dyski: 8 x 10 TB, Interfejs: SATA min. 6 Gb/s, prędkość obrotowa min. 7200 obr/min; rozmiar buforu min. 256 MB; z deklarowanym przez producenta średnim czasem bezawaryjnej pracy co najmniej 1 mln godzin. Dyski muszą być zgodne z urządzeniem NAS, tj. znajdować się na liście zgodności prowadzonej przez producenta urządzenia NAS.
8. Wymaganie poziomy RAID: JBOD, RAID 0, RAID 1, RAID 5, RAID 6 i RAID 10.
9. Interfejsy sieciowy: co najmniej 2 porty 1GbE RJ-45 oraz co najmniej 2 porty 10GbE SFP+.
10. Porty USB: min. 3 x USB3.2.
11. Redundantne zasilanie.
12. 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 oferowane urządzenie NAS i jego/ich producenta/producentów w zakresie określonym powyżej.
13. Co najmniej 36 miesięcy gwarancji producenta.

# Zakup przełącznika sieciowego TYP A (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Rodzaj urządzenia: zarządzany 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. 480 Gbps.
4. Prędkość przekazywania: min. 240 Mpps.
5. Rozmiar tablicy MAC: min. 16 000 wpisów.
6. Bufor pamięci min. 3 MB.
7. Dostępne interfejsy: min. 24 sloty SFP+ 10G. Dodatkowo w zestawie dedykowane do dostarczonego urządzenia: moduły światłowodowe SFP+ 10 Gbps (12 szt.) wraz z patchcordami światłowodowymi SFP+ z wtyczkami i osłonkami o długości 3 m (12 szt.) oraz kable DAC SFP+ 10Gb/s o długości 3 m (12 szt.)
8. Złącza dodatkowe: min. 1 x USB.
9. Obsługiwane standardy komunikacyjne: IEEE 802.3, IEEE 802.3 u, IEEE 802.3 x, IEEE 802.3 z, IEEE 802.3 ab, IEEE 802.3 ad, IEEE 802.3 ae, IEEE 802.3 az, IEEE 802.1 AB, IEEE 802.1 d, IEEE 802.1 p, IEEE 802.1 s, IEEE 802.1 w, IEEE 802.1 Q, IEEE 802.1 x.
10. Dodatkowo obsługa: QoS, VLAN, ACL, DHCP, IPv4, IPv6, Telnet, SNMP v1/v2c/v3, Http/Https, TFTP, SSL, SSHv1/SSHv2, RADIUS/TACACS+.
11. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany przełącznik 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 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 i jego producenta w zakresie określonym powyżej.
12. Co najmniej 24 miesiące gwarancji producenta.

# Zakup przełącznika sieciowego TYP B (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Rodzaj urządzenia: zarządzany 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. 170 Gbps.
4. Prędkość przekazywania: min. 130 Mpps.
5. Rozmiar tablicy MAC: min. 16 000 wpisów.
6. Bufor pamięci min. 1,5 MB.
7. Dostępne interfejsy: min. 48 x RJ45 10/100/1000 Mbps; 4 x sloty SFP+ 10G. Dodatkowo w zestawie dedykowane do dostarczonego urządzenia moduły światłowodowe SFP+ 10 Gbps (4 szt.) oraz patchcordy światłowodowe SFP+ z wtyczkami i osłonkami o długości 3 m (4 szt.).
8. Złącza dodatkowe: min. 1 x USB.
9. Obsługiwane standardy komunikacyjne: IEEE 802.3, IEEE 802.3 u, IEEE 802.3 x, IEEE 802.3 z, IEEE 802.3 ab, IEEE 802.3 ad, IEEE 802.3 ae, IEEE 802.3 an, IEEE 802.3 az, IEEE 802.1 AB, IEEE 802.1 d, IEEE 802.1 p, IEEE 802.1 s, IEEE 802.1 w, IEEE 802.1 Q, IEEE 802.1 x.
10. Dodatkowo obsługa: QoS, VLAN, ACL, DHCP, IPv4, IPv6, Telnet, SNMP v1/v2c/v3, Http/Https, TFTP, SSL, SSHv1/SSHv2, RADIUS/TACACS+.
11. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany przełącznik 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 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 i jego producenta w zakresie określonym powyżej.
12. Co najmniej 24 miesiące gwarancji producenta.

# Rozbudowa istniejącej infrastruktury macierzy - zakup dysków twardych (4 szt.).

W ramach zamówienia przewiduje się zakup oraz montaż dysków do posiadanej przez Zamawiającego macierzy Dell EMC PowerVault ME4012 Hot-Plug SAS 12Gb/s o pojemności co najmniej 2,4 TB każdy dysk z gwarancją co najmniej 24 miesiące z prędkością obrotową nie niższą niż 10000 obr./min. Dostarczone dyski muszą być kompatybilne z posiadaną macierzą dyskową.

# Rozbudowa istniejącej infrastruktury UTM (1 szt.).

Rozbudowa istniejącej infrastruktury UTM składa się z:

1. Wymianę istniejącego urządzenia UTM dla Urzędu Gminy w Działdowie wraz z przeniesieniem istniejących licencji subskrypcyjnych.
2. Wymianę istniejącego urządzenia UTM dla Gminnego Ośrodka Pomocy Społecznej w Działdowie wraz z zakupem licencji subskrypcyjnych do dnia 25.03.2026 r.
3. Zakup licencji subskrypcyjnych do istniejącego urządzenia UTM dla Gminnego Zakładu Usług Komunalnych w Uzdowie do dnia 25.03.2026 r.

Wymiana istniejącego urządzenia UTM dla Urzędu Gminy w Działdowie wraz z przeniesieniem istniejących licencji subskrypcyjnych.

Przedmiotem zamówienia jest wymiana posiadanego przez Urząd Gminy w Działdowie urządzenia UTM Fortinet FG 60E na urządzenie o minimalnych poniższych parametrach wraz z przeniesieniem istniejącej licencji.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i  bezpieczeństwa niezależnie od dostawcy łącza.

System realizujący funkcję firewall musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

* + - 1. System musi wspierać IPv4 oraz IPv6 w zakresie:

1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.
   * + 1. Dla funkcji: firewall, IPSec, kontrola aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster active-active lub active-passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
       2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
       3. Monitoring stanu realizowanych połączeń VPN.
       4. System realizujący funkcję firewall musi dysponować minimum 7 portami Gigabit Ethernet RJ-45.
       5. System firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
       6. W ramach systemu firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
       7. W zakresie frewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
       8. Przepustowość stateful firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
       9. Przepustowość firewall z włączoną funkcją kontroli aplikacji: nie mniej niż 1.7 Gbps.
       10. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.
       11. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
       12. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, kontrola aplikacji, antywirus - minimum 700 Mbps.
       13. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

Kontrola Aplikacji.

Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, 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).

Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.

Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

Polityki firewall.

Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: Translację jeden do jeden oraz jeden do wielu i dedykowany ALG (Application Level Gateway) dla protokołu SIP.

W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hashe złośliwych plików.

Połączenia VPN.

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
2. Wsparcie dla IKE v1 oraz v2.
3. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
4. Obsługa protokołu Diffie-Hellman grup 19 i 20.
5. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
6. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
7. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
8. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
9. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
10. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
11. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
12. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
13. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
14. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN.

W zakresie routingu rozwiązanie powinno zapewniać obsługę: Routingu statycznego, Policy Based Routingu, Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN.

* + - 1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
      2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem.

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware.

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami.

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji.

1. Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
3. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
4. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW.

1. Moduł kontroli WWW musi korzystać z bazy adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji.

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie.

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie.

1. W ramach logowania system pełniący funkcję firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
3. Musi istnieć możliwość logowania do serwera SYSLOG.

Wymiana istniejącego urządzenia UTM dla Gminnego Ośrodka Pomocy Społecznej w Działdowie.

Przedmiotem zamówienia jest wymiana posiadanego przez Gminny Ośrodek Pomocy Społecznej w Działdowie urządzenia UTM Fortinet FG 60E na urządzenie o minimalnych poniższych parametrach wraz z zakupem licencji subskrypcyjnych do dnia 25.03.2026r.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i  bezpieczeństwa niezależnie od dostawcy łącza.

System realizujący funkcję firewall musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

* + - 1. System musi wspierać IPv4 oraz IPv6 w zakresie:

1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.
   * + 1. Dla funkcji: firewall, IPSec, kontrola aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster active-active lub active-passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
       2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
       3. Monitoring stanu realizowanych połączeń VPN.
       4. System realizujący funkcję firewall musi dysponować minimum 7 portami Gigabit Ethernet RJ-45.
       5. System firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
       6. W ramach systemu firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
       7. W zakresie frewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
       8. Przepustowość stateful firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
       9. Przepustowość firewall z włączoną funkcją kontroli aplikacji: nie mniej niż 1.7 Gbps.
       10. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.
       11. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
       12. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, kontrola aplikacji, antywirus - minimum 700 Mbps.
       13. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

Kontrola Aplikacji.

Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, 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).

Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.

Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

Polityki firewall.

Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: Translację jeden do jeden oraz jeden do wielu i dedykowany ALG (Application Level Gateway) dla protokołu SIP.

W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hashe złośliwych plików.

Połączenia VPN.

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
2. Wsparcie dla IKE v1 oraz v2.
3. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
4. Obsługa protokołu Diffie-Hellman grup 19 i 20.
5. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
6. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
7. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
8. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
9. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
10. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
11. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
12. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
13. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
14. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN.

W zakresie routingu rozwiązanie powinno zapewniać obsługę: Routingu statycznego, Policy Based Routingu, Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN.

* + - 1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
      2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem.

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware.

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami.

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji.

1. Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
3. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
4. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW.

1. Moduł kontroli WWW musi korzystać z bazy adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji.

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie.

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie.

1. W ramach logowania system pełniący funkcję firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
3. Musi istnieć możliwość logowania do serwera SYSLOG.

Zakup licencji subskrypcyjnych do istniejącego urządzenia UTM dla Gminnego Zakładu Usług Komunalnych w Uzdowie.

W ramach działania przewiduje się zakup usług subskrypcji na istniejące urządzenie Fortigate FG-40F. 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 do dnia 25.03.2026 r.

Zamawiający dopuszcza rozwiązanie równoważne w postaci dostawy innego urządzenia lub platformy bezpieczeństwa spełniających poniższe kryteria równoważności funkcjonalnej.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS.

System musi wspierać IPv4 oraz IPv6 w zakresie:

1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.

Minimalne parametry techniczne urządzenia:

1. Przepustowość Firewall: min. 5 Gbps.
2. Musi obsługiwać min. 700 000 jednoczesnych połączeń.
3. Musi obsługiwać co najmniej 200 połączeń VPN.
4. Wydajność IPsec VPN min. 4 Gbps.
5. Wydajność SSL VPN: min. 450 Mbps.
6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 0,6 Gbps.
8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.
9. Automatyczna aktualizacja plików sygnatur antywirusowych.
10. Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji.
11. Możliwość wsparcia IPS z poziomu urządzenia poprzez dodatkowe subskrypcje.
12. Automatyczna aktualizacja sygnatur IPS.
13. IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy.
14. Wsparcie dla wszystkich głównych protokołów: HTTP, FTP, SMTP, POP3.
15. Ilość interfejsów sieciowych: minimum 3 porty Gigabit Ethernet RJ-45.
16. Wsparcie VLAN: Musi posiadać minimum 200 sieci VLAN.
17. Administracja urządzenia musi być możliwa poprzez graficzny interfejs zarządzania.
18. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
19. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
20. Kontrola Aplikacji.
21. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
22. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS oparta o mechanizmy sztucznej inteligecji.
23. Ochrona przed atakami - Intrusion Prevention System.
24. Kontrola stron WWW.
25. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
26. Zarządzanie pasmem (QoS, Traffic shaping).
27. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
28. Analiza ruchu szyfrowanego protokołem SSL.
29. Analiza ruchu szyfrowanego protokołem SSH.
30. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
31. Zapewnienie obsługi Routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
32. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
33. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
34. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
35. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
36. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
37. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
38. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
39. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
40. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
41. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
42. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
43. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
44. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
45. Rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
46. Urządzenie powinno mieć możliwość generowania raportów.
47. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
48. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
49. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
50. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
51. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
52. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
53. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować następujące elementy: Kontrola Aplikacji, IPS, Antywirus, Antyspam, Antymalware, Web Filtering w okresie do dnia 25.03.2026 r.
54. Gwarancja producenta do dnia 25.03.2026 r. Gwarancja powinna obejmować również możliwość wymiany urządzenia na nowe w przypadku wady urządzenia UTM.
55. W przypadku zaoferowania rozwiązania równoważnego Wykonawca jest zobligowany do instalacji, wdrożenia oraz migracji konfiguracji istniejącego urządzenia UTM oraz przeprowadzenia szkolenia dla administratora w zakresie konfiguracji i eksploatacji na podstawie wcześniej zaakceptowanego przez Zamawiającego zakresu merytorycznego szkolenia.

# Opis przedmiotu zamówienia dla części nr 2.

# Wymagania ogólne w zakresie dostawy oprogramowania.

1. Dostarczone oprogramowanie musi być wolne od wad prawnych i fizycznych oraz wcześniej nieużytkowane.
2. Dostarczone oprogramowanie musi być fabrycznie nowe, musi pochodzić z oficjalnego kanału sprzedaży producenta, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta oferowanego oprogramowania.
3. Niedopuszczalne są produkty prototypowe oraz pochodzących z programów wyprzedażowych producenta. Oferowane oprogramowanie nie może znajdować się na liście „end-of-sale”, „end-of-life” oraz „end-of-support” producenta.
4. Wykonawca zapewni dostawę oprogramowania do wskazanej lokalizacji w siedzibie Zamawiającego.
5. Wykonawca jest odpowiedzialny za skonfigurowanie w porozumieniu z Zamawiającym oprogramowania w celu przygotowania zamawianego oprogramowania do działania.
6. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
7. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji oprogramowania.
8. 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.
9. Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:
10. 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.
11. 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.
12. W przypadku, jeżeli dotyczy, Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.
13. Wykonawca, pomimo zapewnienia serwisu producenta zobowiązany będzie do udzielania pomocy technicznej Zamawiającemu przez okres gwarancji.
14. Usługa wsparcia wdrożenia obejmuje:
15. przeprowadzenie analizy przedwdrożeniowej,
16. pomoc przy instalacji silnika bazy danych – jeżeli będzie wymagana instalacja,
17. rejestracja produktu – jeżeli wymagana,
18. instalację oprogramowania: na stacji roboczej lub serwerze – jeżeli dotyczy,
19. dystrybucję oprogramowania na wybranych stacjach roboczych – jeżeli dotyczy,
20. konfigurację oprogramowania,
21. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego,
22. szkolenie administratorów z zakresu pracy z programem,
23. w uzgodnionym terminie z Zamawiającym zostanie przeprowadzane kontrolne połącznie zdalne w celu weryfikacji ustawień oraz poprawienia konfiguracji.
24. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia oprogramowania – wymagania minimalne:
25. 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:
26. scenariusze testowe, procedury oraz wzory raportów testów,
27. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
28. opis koncepcji realizacji prac,
29. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
30. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
31. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 30 dni kalendarzowych od dnia zawarcia umowy,
32. Zamawiający w terminie nie dłuższym niż 7 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
33. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
34. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
35. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
36. zatwierdzony projekt techniczny wraz procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
37. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.
38. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
39. 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.
40. 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.
41. Instruktaże w zakresie dostarczonego oprogramowania – wymagania minimalne.
42. 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.
43. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
44. Instruktaże powinny trwać minimum 8 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób (maksymalnie 4 osoby).
45. Zamawiający nie dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
46. 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.
47. Wymagania licencyjne dla dostarczonego oprogramowania:
48. Licencjobiorcą wszystkich licencji będzie Gmina Działdowo. Zamawiający zastrzega, że oprogramowanie będzie wykorzystywane przez jednostki organizacyjne Zamawiającego, tj. Gminny Ośrodek Pomocy Społecznej oraz Gminny Zakład Usług Kompunalnych.
49. 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.
50. Licencje muszą zostać wystawione na czas do dnia 25.03.2026 r. niezależnie od modeli dystrybucji poszczególnych producentów oferowanego oprogramowania.
51. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
52. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do przeniesienia oprogramowania na inny serwer/komputer.
53. 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.
54. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
55. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
56. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym urządzeniu klienckim (licencja nie może być przypisana do komputera/urządzenia).
57. Licencja oprogramowania nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji ze zgromadzonych danych.
58. Wykonawca zapewni gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.
59. Wymagania gwarancyjne i serwisowe dla dostarczonego oprogramowania:
    1. Gwarancja producenta musi zostać zapewniona przez Wykonawcę na oferowane oprogramowanie do dnia 25.03.2026 r.
    2. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w oprogramowaniu do serwisu producenta lub jego dystrybutora.
    3. Serwis producenta musi zostać zapewniony przez Wykonawcę do dnia 25.03.2026 r.
    4. Serwis polega na świadczeniu usługi wsparcia technicznego udzielonego przez producenta lub autoryzowanego dystrybutora producenta w języku polskim i objąć musi minimum:
       1. dostęp do najnowszych wersji oprogramowania,
       2. wsparcie telefoniczne w zakresie oferowanego oprogramowania zespołu inżynierów technicznych,
       3. wsparcie w prawidłowym i zgodnym z wymaganiami producenta użytkowaniu oprogramowania,
       4. przyjmowanie i realizacja zgłoszeń serwisowych,
       5. 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.

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

# 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. 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.

# Oprogramowanie do agregacji logów (3 szt.).

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Minimalne parametry funkcjonalne oprogramowania:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3TB.
2. System musi być w stanie przyjmować minimum 5 GB logów na dzień.
3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.
4. Podgląd logowanych zdarzeń w czasie rzeczywistym.
5. Możliwość przeglądania logów historycznych z funkcją filtrowania.
6. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
   1. Listę najczęściej wykrywanych ataków.
   2. Listę najbardziej aktywnych użytkowników.
   3. Listę najczęściej wykorzystywanych aplikacji.
   4. Listę najczęściej odwiedzanych stron www.
   5. Listę krajów , do których nawiązywane są połączenia.
   6. Listę najczęściej wykorzystywanych polityk Firewall.
   7. Informacje o realizowanych połączeniach IPSec.
7. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
8. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
9. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: Malware, Aplikacje sieciowe, Email, IPS, Traffic, Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.
5. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
6. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
7. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

# Rozbudowa oprogramowania antywirusowego o funkcje XDR, szyfrowania danych, zarządzanie podatnościami (1 szt.).

Aktualnie Zamawiający posiada następujące licencje oprogramowania antywirusowego:

* Urząd Gminy Działdowo - ESET PROTECT Essential Plus On-Prem; liczba posiadanych licencji: 53.
* Gminny Ośrodek Pomocy Społecznej - ESET PROTECT Essential – liczba posiadanych licencji: 20.

Przedmiotem zamówienia jest rozbudowa oprogramowania do wersji ESET PROTECT Elite w okresie do dnia 25.03.2026 r. obejmująca licencje powyżej określone oraz wdrożenie jednolitej platformy ESET PROTECT Elite dla 10 użytkowników w Gminnym Zakładzie Usług Komunalnych w Uzdowie lub dostawa równoważnej platformy bezpieczeństwa zgodnie z funkcjonalnymi kryteriami równoważności określonymi poniżej.

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.

Ochrona stacji roboczych.

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:
    1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    4. 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,
    5. 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:
    1. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
    3. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
    4. 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.

Ochrona serwera.

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:

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. 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.
6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
4. 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 7/8/8.1/10 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:
   1. usunięcie zawartości urządzenia,
   2. przywrócenie urządzenie do ustawień fabrycznych,
   3. zablokowania urządzenia,
   4. uruchomienie sygnału dźwiękowego,
   5. lokalizację GPS.
   6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
   7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
   8. nazwę aplikacji,
   9. nazwę pakietu,
   10. kategorię sklepu Google Play,
   11. uprawnienia aplikacji,
   12. 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:
    1. Czysty,
    2. Podejrzany,
    3. Bardzo podejrzany,
    4. 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.

Ochrona usługi Microsoft 365.

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 dostępny w języku polskim.
6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:
   1. użytkowników, otrzymujących najwięcej spamu,
   2. użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
   3. użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
   4. 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:
   1. jaka ilość wiadomości została przeskanowania,
   2. wynik skanowania poszczególnej wiadomości,
   3. czynność podjęta przez rozwiązanie.
9. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o: zagrożeniach, które zostały wykryte,
   1. na jakim koncie zostały wykryte,
   2. jakie zagrożenie zostało wykryte,
   3. 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:
    1. wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
    2. wprowadzenia białych i czarnych list adresów ochrony Exchange’a Online,
    3. 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.

Moduł zarządzania podatnościami i aktualizacjami.

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:
   1. nazwę aplikacji lub systemu operacyjnego;
   2. punktacje CVSS;
   3. opis wykrytej podatności;
   4. 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 i wyłącznie 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: 2008 / 2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022.
2. Rozwiązanie musi wspierać system operacyjne Windows 7 / Windows 8 / Windows 8.1 / 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.

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

Przedmiotem zamówienia jest dostawa oprogramowania do zarządzania bezpieczeństwem IT umożliwiającego szereg funkcji podnoszących cyberbezpieczeństwo w Urzędzie Gminy Działdowo, a także jego jednostkach organizacyjnych. Wykonawca jest zobligowany wziąć pod uwagę zakres użytkowania oprogramowania dla Urzędu Gminy Działdowo - 50 urządzeń końcowych, Gminny Ośrodek Pomocy Społecznej w Działdowie - 20 urządzeń końcowych, Gminny Zakład Usług Komunalnych w Uzdowie - 10 urządzeń końcowych.

Minimalne wymagania funkcjonalne dla oprogramowania do zarządzania bezpieczeństwem IT:

1. Oprogramowanie musi składać się serwera zarządzającego, zdalnych konsoli oraz Agentów.
2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana powinna być przy użyciu szyfrowanego protokołu TLS 1.2.
3. Oprogramowanie musi umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych.
4. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych Administratorów - nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do grup urządzeń, jak i użytkowników.
5. Oprogramowanie musi posiadać funkcjonalność monitorowania infrastruktury serwerowej i sieciowej w zakresie:
   1. wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping),
   2. wizualizacji stanu urządzeń w postaci ikon urządzeń na mapach sieci,
   3. wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie.
   4. serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów,
   5. serwerów pocztowych: - monitorowanie serwisu odbierającego, jak i wysyłającego pocztę, - możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), - możliwość wykonywania operacji testowych, - możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa,
   6. monitorowania serwerów WWW i adresów URL,
   7. obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.
   8. obsługi komunikatów syslog i pułapek SNMP.
   9. monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych, - ruchu sieciowego, - podłączonych stacji roboczych- ruchu generowanego przez podłączone stacje robocze,
   10. kontroli nad monitorem usług Windows,
   11. monitorowania wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.
6. Oprogramowanie musi umożliwiać automatyczne gromadzenie danych o sprzęcie i oprogramowaniu na stacjach roboczych w zakresie:
   1. informacji dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.;
   2. zestawienia posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade;
   3. informacji o zainstalowanych aplikacjach oraz aktualizacjach Windows, umożliwiających audytowanie i weryfikację użytkowania licencji w organizacji;
   4. informacji o wszystkich zmianach przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.;
   5. możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera;
   6. możliwość odczytania numeru seryjnego (klucze licencyjne);
   7. możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych;
   8. możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
7. Oprogramowanie musi mieć możliwość prowadzenia bazy ewidencji majątku IT w zakresie:
   1. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji;
   2. definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz, możliwość importu danych z zewnętrznego źródła np. (.CSV);
   3. generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania;
   4. archiwizacji i porównywania audytów środków trwałych;
   5. tworzenia kodów kreskowych w Środkach Trwałych;
   6. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy;
   7. inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej co najmniej na system Android;
   8. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji dodatkowego oprogramowania poprzez manualne wykonanie skanów inwentaryzacji offline).
8. Oprogramowanie musi zapewniać funkcjonalność w zakresie monitorowania aktywności użytkowników na stacjach roboczych w zakresie:
   1. faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy);
   2. monitorowania procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika);
   3. użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona);
   4. informacji o edytowanych przez użytkownika dokumentach;
   5. historii pracy (cykliczne zrzuty ekranowe);
   6. listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),
   7. transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
   8. wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek.
9. Oprogramowanie musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
   1. skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie, archiwów ZIP;
   2. zarządzanie posiadanymi licencjami;
   3. audyt legalności oprogramowania oraz powiadamianie w razie przekroczenia liczby posiadanych licencji;
   4. zarządzanie posiadanymi licencjami: raport zgodności licencji;
   5. możliwość przypisania do programów numerów seryjnych, wartości itp.
10. Oprogramowanie musi zapewniać integrację z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.
11. W zakresie pomocy technicznej system musi umożliwiać:
    1. tworzenie zgłoszeń serwisowych i zarządzanie nimi (przypisywanie do administratorów);
    2. załączanie komentarzy, zrzutów ekranów i załączników w zgłoszeniach;
    3. konfigurowanie pól niestandardowych, powiązanych w wybraną kategorią zgłoszenia;
    4. przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o Sygnalistach”);
    5. dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę;
    6. planowanie zastępstw w przydzielaniu zgłoszeń;
    7. funkcję rozbudowanych raportów;
    8. powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistym;
    9. baza zgłoszeń z rozbudowaną wyszukiwarką;
    10. przejrzysty i intuicyjny interfejs webowy;
    11. wewnętrzny komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowych;
    12. komunikaty wysyłane do użytkowników/komputerów z możliwym/obowiązkowym potwierdzeniem odczytu;
    13. zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury;
    14. dwukierunkowa wymiana plików;
    15. zarządzanie procesami Windows z poziomu okna informacji o urządzeniu;
    16. zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania);
    17. procesowanie zgłoszeń z wiadomości e-mail;
    18. integracja bazy użytkowników z Active Directory;
    19. zarządzanie kontami lokalnych użytkowników Windows (tworzenie, usuwanie, edycja, reset hasła, eskalacja/deeskalacja uprawnień oraz włączanie/wyłączanie kont).
12. W zakresie kontroli dostępu do danych system musi umożliwiać:
    1. automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa;
    2. ograniczenie ryzyka wycieku strategicznych danych za pośrednictwem przenośnych pamięci masowych oraz urządzeń mobilnych;
    3. zabezpieczenie sieci firmowej przed wirusami instalującymi się automatycznie z pendrive'ów lub dysków zewnętrznych;
    4. integracja z Windows Defender: zarządzanie ustawieniami wbudowanego antywirusa wraz z możliwością alarmowania o wykrytych problemach oraz wynikach skanowania;
    5. integracja z Windows Firewall: włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych;
    6. możliwość usuwania nieistniejących/zutylizowanych nośników danych (np. USB);
    7. alarmy o podłączonym urządzeniu obcym (nieposiadającym atrybutu „nośnik zaufany”);
    8. integracja z Windows Bitlocker: odczyt stanu modułu TPM oraz zaszyfrowania woluminów
    9. zdefiniowanie polityki przenoszenia danych firmowych przez pracowników wraz z odpowiednimi uprawnieniami;
    10. informacje o urządzeniach podłączonych do danego komputera;
    11. lista wszystkich urządzeń podłączonych do komputerów w sieci;
    12. audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych;
    13. zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników;
    14. centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory.

# Opis przedmiotu zamówienia dla Części nr 3.

# Wymagania ogólne.

1. Zamówienie będzie realizowane na rzecz Urzędu Gminy Działdowo oraz jego następujących jednostkach organizacyjnych:
   1. Gminnego Ośrodka Pomocy Społecznej w Działdowie
   2. Gminny Zakład Usług Komunalnych w Uzdowie
2. Wykonawca jest zobowiązany do przeprowadzenia w poszczególnych latach realizacji projektu pn. „Cyberbezpieczny Samorząd” współfinansowanego w ramach środków Unii Europejskiej i budżetu państwa w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Priorytetu II: Zaawansowane usługi cyfrowe, Działania 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa , tj. w roku 2024, 2025 i 2026 audytu systemu zarządzania bezpieczeństwem informacji w związku z zapisami w § 19 ust. 2 pkt 14 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773), zwanego dalej „audytem KRI” dla Zamawiającego.
3. Wykonawca jest odpowiedzialny za przeprowadzenie aktualizacji i wdrożenie kompletnego Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwany: SZBI) dla Zamawiającego.
4. Zakres audytu systemu bezpieczeństwa informacji każdorazowo obejmie zgodność z kryteriami zawartymi w § 19 ust. 2 ww. rozporządzenia KRI oraz zgodność z wymaganiami normy **PN-EN ISO/IEC 27001:2023** dla Zamawiającego.
5. Raport z audytu KRI zostanie każdorazowo podpisany przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczony do Zamawiającego w formie elektronicznej.
6. Audyt KRI oraz aktualizacja i wdrożenie SZBI dla Zamawiającego muszą zostać przeprowadzone przez:
   1. audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) lub;
   2. audytora wewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy **PN-EN ISO/IEC 27001:2023.**
7. Wykonawca w trakcie realizacji zamówienia jest zobowiązany do zapoznania się z częściowo wypełnioną ankietą dojrzałości cyberbezpieczeństwa w zakresie wskazanym przez Zamawiającego oraz uwzględnić w ramach aktualizacji i wdrożenia SZBI planowany w ramach realizacji projektu zakres usprawnień SZBI.
8. Wykonawca po wykonaniu ostatniego audytu KRI jest zobowiązany do uzupełnienia ankiety dojrzałości cyberbezpieczeństwa. Ankietę dojrzałości cyberbezpieczeństwa należy wypełnić w oparciu o aktualny na dzień wypełnienia ankiety wzór ankiety opublikowany na stronie: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad (załącznik nr 6 - Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego i Jednostkach Podległych).
9. Wypełnienie ankiety dojrzałości cyberbezpieczeństwa polegać będzie na wypełnieniu przez Wykonawcę kolumn H, I z arkusza „Ankieta” dla Zamawiającego na podstawie zebranych przez Wykonawcę danych. Zamawiający nie dopuszcza pozostawienia pustych pól dla określonych powyżej kolumn, w przypadku jeżeli w polu opisowym nie przewiduje się zmian wówczas należy zamieścić odpowiednią informację. Ankieta dojrzałości cyberbezpieczeństwa zostanie podpisana przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczona do Zamawiającego w formie elektronicznej.
10. Jednostki samorządu terytorialnego oraz jego jednostki podległe, które biorą udział w projekcie „Cyberbezpieczny Samorząd” są zobowiązane do przesłania do NASK raportu z audytu KRI oraz wypełnionej ankiety dojrzałości cyberbezpieczeństwa. Niezwłocznie po ich przekazaniu przez Wykonawcę dokumenty te zostaną przekazane przez Zamawiającego do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) za pośrednictwem platformy ePUAP. Dane z tej dokumentacji przekazane przez JST do NASK posłużą do opracowania raportu na temat stanu bezpieczeństwa systemów jednostek samorządowych. Wykonawca jest zobowiązany mieć na uwadze także powyżej wskazany cel przeprowadzenia zamówienia i jego przeznaczenie.
11. Wykonawca przy świadczeniu usług jest zobowiązany uwzględnić i zastosować wymagania Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) oraz akty wykonawcze wydane do niej. W przypadku jeżeli w okresie realizacji zamówienia zostanie przyjęta ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw bądź inne przepisy implementujące Dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) w polski system prawny Wykonawca ma obowiązek uwzględnić wszystkie ich wymagania przy świadczeniu usług objętych niniejszym zamówieniem zarówno w trakcie realizacji zamówienia jak i w trakcie okresu gwarancji.
12. Wykonawca zrealizuje zamówienie w oparciu o dokumentację, którą Zamawiający dysponuje niezależnie od realizacji przedmiotu umowy i o wyjaśnienia udzielane przez Zamawiającego. W szczególności realizacja przedmiotu umowy przez Wykonawcę nie może być uwarunkowana wytwarzaniem lub uzupełnianiem dokumentów i opracowań przez Zamawiającego w związku z realizacją przedmiotu umowy, tj. Zamawiający nie może być zobowiązany do wypełniania ankiet, kwestionariuszy, sporządzania notatek itp., a informacje niezbędne Wykonawcy do wykonania przedmiotu umowy mogą być pozyskiwane wyłącznie w postaci materiałów źródłowych i wywiadu bezpośredniego.
13. Zamawiający dopuszcza prowadzenie prac związanych z: analizą dokumentacji, opracowaniem dokumentacji i polityk, opracowania raportów poza siedzibą Zamawiającego. Zamawiający nie dopuszcza prowadzenia instruktaży, konsultacji, audytów, analiz stanu istniejącego i określenie stanu faktycznego zabezpieczeń technicznych w formule zdalnej, tj. w postaci on-line lub innej poza siedzibą Zamawiającego.
14. Zamawiający nie dopuszcza, żeby poszczególne etapy realizacji usługi aktualizacji i wdrożenia SZBI wskazane w dalszej części dokumentu realizowane były w dniach następujących po sobie, Zamawiający zakłada co najmniej 7 dni roboczych przerw pomiędzy etapami. Wymóg dotyczy urzędu i jednostek organizacyjnych biorących udział w projekcie.
15. Zamawiający wymaga, żeby każdy etap (lub jego część) realizacji usługi aktualizacji i wdrożenia SZBI wskazany w dalszej części dokumentu był realizowany w siedzibie Urzędu i jednostkach organizacyjnych w czasie nie krótszym niż jeden dzień roboczy odrębnie dla Urzędu i jednostek organizacyjnych biorących udział w projekcie.
16. Zamawiający wymaga, żeby każdy audyt był realizowany w siedzibie Urzędu i jednostkach organizacyjnych w czasie nie krótszym niż jeden dzień roboczy odrębnie dla Urzędu i jednostek organizacyjnych biorących udział w projekcie.
17. Na wszystkie usługi Wykonawca udzieli gwarancji nie dłużej niż do dnia 25.03.2026 r. polegającej na wprowadzaniu niezbędnych zmian w dokumentacji i aktualizacji na podstawie stwierdzonych przez Zamawiającego niezgodności dokumentacji z bieżącym stanem w okresie gwarancji.

# Zakup usług aktualizacji i wdrożenia SZBI.

Celem usługi w ramach działania będzie aktualizacja i wdrożenie procedur systemu zarządzania bezpieczeństwem informacji wdrożonych u Zamawiającego z uwzględnieniem uwarunkowań i specyfiki projektu oraz specyfiki jednostek. Analiza zostanie przeprowadzona zgodnie z wymogami ISO/IEC 19011:2002. W efekcie zostanie zaktualizowana także polityka bezpieczeństwa w zakresie ochrony danych osobowych. Usługa obejmuje również aktualizację dokumentów opisujących zbiory danych i ich zgodność z wymogami prawnymi oraz aktualizację dokumentów opisujących miejsca i sposoby przetwarzania danych osobowych.

Na usługę aktualizacji, opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji składają się co najmniej:

1. Wykonanie oceny obecnej dostępnej dokumentacji.
2. Określenie stanu faktycznego zabezpieczeń danych w systemach informatycznych poprzez przeprowadzenie audytu zabezpieczeń dostępu do danych oraz przygotowanie raportu wraz z zaleceniami i projektem zmian spełnienie wymagań normy **PN-EN ISO/IEC 27001:2023** i zaleceń norm pokrewnych, oraz wymagań prawnych nałożonych na organizację, między innymi dotyczących ochrony danych osobowych.
3. Przeprowadzenie instruktażu wprowadzającego dla pracowników w zakresie ochrony informacji, inwentaryzacji aktywów informacyjnych oraz oceny ryzyka.
4. Aktualizacja/opracowanie Polityki Bezpieczeństwa zgodnej z wymaganiami normy **PN-EN ISO/IEC 27001:2023** i zaleceń norm pokrewnych, oraz wymagań prawnych nałożonych na organizację, między innymi dotyczących ochrony danych osobowych w zakresie:
5. organizacja systemu bezpieczeństwa informacji;
6. zarządzanie aktywami;
7. zarządzanie zasobami ludzkimi;
8. organizacja bezpieczeństwa fizycznego i środowiskowego;
9. zarządzanie komunikacją i eksploatacją;
10. rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania;
11. kontrola dostępu, zarządzania hasłami, stosowania zabezpieczeń kryptograficznych, czystego biurka i czystego ekranu, usuwania i niszczenia informacji, pracy w strefach bezpieczeństwa;
12. akwizycja, rozwój i utrzymanie systemu;
13. zarządzanie incydentami związanymi z bezpieczeństwem informacji;
14. zarządzanie ciągłością działania;
15. zarządzania kopiami zapasowymi;
16. zarządzania monitoringiem;
17. zobowiązanie do zachowania poufności, stosowania polityk i procedur SZBI;
18. używania urządzeń komputerowych;
19. metoda szacowania i postępowania z ryzykiem;
20. deklaracja stosowania
21. Wdrożenie Polityki Bezpieczeństwa Informacji. Poprzez wdrożenie należy rozumieć także aktualizację/utworzenie odpowiednich dokumentów po konsultacjach z pracownikami Zamawiającego, zatwierdzenie dokumentacji przez Kierownictwo Zamawiającego oraz przeprowadzenie instruktażu pracowników w zakresie wykonywania obowiązków zgodnie z opracowanym sposobem postępowania w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Ponad to:

1. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje procedury bezpieczeństwa fizycznego obejmujące obowiązek wyznaczania osoby odpowiedzialnej za bezpieczeństwo fizyczne.
2. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje zasady odpowiedzialności za cyberbezpieczeństwo wraz ze wskazaniem obowiązku wyznaczania osoby odpowiedzialnej za cyberbezpieczeństwo.
3. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę szkoleń z zakresu cyberbezpieczeństwa wraz z wprowadzeniem obowiązku regularnego, corocznego prowadzenia szkoleń.
4. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje treść zarządzenia wdrażającego SZBI dla Zamawiającego.
5. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan postępowania z ryzkiem obejmujący systematyczne tworzenie raportów oceny ryzyka w Jednostce oraz konieczność cyklicznego przeglądu tego raportu przez Kierownika JST.
6. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje szczegółowy sposób realizacji celów oraz we współpracy z Zamawiającym przypisze odpowiedzialności za ich realizację.
7. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje procedurę wprowadzającą obowiązek regularnego, corocznego przeglądu PBI jednostki.
8. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę szkoleń obejmującą obowiązek informowania o zmianach w PBI w toku okresowych szkoleń stanowiskowych.
9. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kluczowe aktywa informacyjne Jednostki (zbiory danych/systemy/usługi).
10. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje rejestr ryzyk uwzględniający aktywa Jednostki.
11. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje zagrożenia związane z cyberbezpieczeństwem w ramach procesów zarządczych oraz zarządzania ryzykiem.
12. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan postępowania z ryzkiem związanym z zagrożeniami bezpieczeństwa informacji.
13. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą obowiązek używania do określenia w Jednostce zagrożeń, podatności, prawdopodobieństwa ich wystąpienia i skutków.
14. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą obowiązek identyfikacji i priorytetyzacji odpowiedzi na ryzyka.
15. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą system oceny ryzyka.
16. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem cyberbezpieczeństwa uwzględniającą identyfikowane, ustanawiane i oceniane ryzyka.
17. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania danymi uwzględniającą polityki ich niszczenia, plan backup, plany reagowania i odtwarzania danych.
18. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan zarządzania podatnościami.
19. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania zapisami zdarzeń / logów/ inspekcji.
20. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę użytkowania dostępu do odczytu lub zapisu danych z zewnętrznych nośników danych.
21. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów.
22. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan zarządzania podatnościami uwzględniający obowiązek dokumentowania ryzyka z nimi związanego.
23. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów i ich aktualizacji w obszarze doświadczeń i wniosków z wykrytych i obsłużonych incydentów.
24. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów wraz z obowiązkiem ich aktualizacji.
25. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę planów odtwarzania uwzględniającą obowiązek ich aktualizacji w obszarze doświadczeń i wniosków z prowadzonych procesów odtwarzania.

Poszczególne etapy realizacji usługi.

Etap I. Audyt zerowy.

1. Określenie stanu spełnienia wymagań prawnych nałożonych na organizację w zakresie ochrony informacji.
2. Sprawdzenie spełnienia wymagań i zaleceń w ramach standardów **PN-EN ISO/IEC 27001:2023** i norm pokrewnych.
3. Inwentaryzacja aktywów informacyjnych i ocena ryzyka.
4. Ocena zabezpieczeń technicznych, organizacyjnych oraz fizycznych.
5. Analiza dokumentacji Polityki Bezpieczeństwa Informacji.
6. Analiza dokumentacji Polityki Bezpieczeństwa Danych Osobowych.
7. Opracowanie raportu z audytu zerowego zawierającego analizę bezpieczeństwa i adekwatności zabezpieczeń stosowanych przez Zamawiającego w odniesieniu do sieci i systemów informatycznych oraz rodzaju danych w nich przetwarzanych, z uwzględnieniem obowiązujących przepisów prawa, zasad wiedzy technicznej, wymagań normy **PN-EN ISO/IEC 27001:2023** i zaleceń norm pokrewnych.

Etap II. Zastosowanie zabezpieczeń na podstawie zaleceń poaudytowych.

1. Konsultacje przy wdrożeniu zabezpieczeń w infrastrukturze systemu informatycznego;
2. Konsultacje przy wdrożeniu zabezpieczeń organizacyjnych – polityki bezpieczeństwa danych osobowych, zapisów w umowach z dostawcami itp.

Etap III. Planowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

1. Przeprowadzenie instruktażu dla kadry zarządzającej z zasad bezpieczeństwa informacji.
2. Zakres SZBI:
3. określenie rodzaju działalności organizacji, jej lokalizacji, rodzajów aktywów i wykorzystywanych technologii;
4. określenie zasięgu organizacji;
5. badanie środowiska zewnętrznego, powiązań z innymi organizacjami, systemami oraz dostawcami.
6. Zdefiniowanie wymaganych polityk SZBI:
7. uwzględnienie rodzaju działalności organizacji, jej lokalizacji, rodzajów aktywów i wykorzystywanych technologii;
8. analiza wymagań prawnych oraz wymagań wynikających z umów;
9. uwzględnienie sposobu ustalania celów oraz wyznaczania kierunków działań w ramach systemu.
10. Szacowanie ryzyka:
11. wybór metody szacowania ryzyka;
12. określenie kryteriów akceptowalności ryzyk i identyfikacji akceptowalnych poziomów ryzyk;
13. zdefiniowanie obszarów zabezpieczeń objętych analizą ryzyka.
14. Wybór celów zabezpieczeń:
15. zdefiniowanie celów zabezpieczeń na podstawie listy zawartej w załączniku A normy **PN-EN ISO/IEC 27001:2023**;
16. zdefiniowanie własnych celów zabezpieczania i zabezpieczeń;
17. uwzględnienie wyników procesu szacowania ryzyka i określenie postępowania z ryzykiem;
18. określenie środków ochrony.

Etap IV. Inwentaryzacja i szacowanie ryzyka SZBI.

1. Przeprowadzenie instruktaży dla pracowników oraz kadry zarządzającej z metody inwentaryzacji i klasyfikacji aktywów informacyjnych.
2. Wykonanie wraz z pracownikami inwentaryzacji i klasyfikacji aktywów informacyjnych.
3. Zdefiniowanie planu postępowania z ryzykiem:
4. przeprowadzenie instruktaży dla kadry zarządzającej z wybranej metody oceny ryzyka;
5. szacowanie i ocena ryzyka – zaktualizowanie wartości ryzyka wynikające z audytu zerowego;
6. zdefiniowanie planu postępowania z ryzykiem;
7. określenie planu zarządzania zidentyfikowanymi i oszacowanymi ryzykami;
8. określenie zadań do realizacji, zdefiniowanie odpowiedzialności i ram czasowych.
9. Opracowanie raportu z oceny ryzyka.

Etap V. Opracowanie niezbędnej dokumentacji SZBI.

1. Opracowanie wspólnie z pracownikami Zamawiającego wymaganych procedur i instrukcji:
2. opracowanie Polityki Bezpieczeństwa Informacji;
3. opracowanie Instrukcji Zarządzania Systemem Informatycznym;
4. opracowanie procedur i instrukcji wymaganych przez normę **PN-EN ISO/IEC 27001:2023**;
5. opracowanie procedur i instrukcji dopasowanych do specyfiki działalności organizacji;
6. opracowanie Instrukcji postępowania na wypadek wykrycia incydentu naruszenia bezpieczeństwa;
7. opracowanie procedury audytu wewnętrznego;
8. opracowanie procedury nadzoru nad dokumentacją;
9. opracowanie procedury działań korygujących i zapobiegawczych;
10. opracowanie procedury zachowania ciągłości działania;
11. opracowanie wraz z pracownikami Zamawiającego planów ciągłości działania.
12. Wykonanie projektu zabezpieczeń - opracowanie projektu zabezpieczeń i konsultacje przy wdrożeniu odpowiednio skutecznych zabezpieczeń zgodnych z celami zabezpieczeń.
13. Opracowanie programu uświadamiania i szkolenia.
14. Przeprowadzenie instruktaży dla pracowników z dokumentacji ochrony informacji.
15. Przeprowadzenie instruktaży dla kadry zarządzającej z dokumentacji ochrony informacji.

Etap VI. Weryfikacja i monitorowanie SZBI.

1. Przeprowadzenie wraz z pracownikami organizacji audytu wewnętrznego.
2. Opracowanie raportu z audytu wewnętrznego.
3. Przeprowadzenie wraz z pracownikami organizacji przeglądu systemu SZBI:
4. przegląd zagrożeń;
5. przegląd podatności;
6. określenie i weryfikacja ryzyk;
7. weryfikacja planu postępowania z ryzykiem;
8. sprawdzenie zabezpieczeń i celów zabezpieczeń;
9. określenie zgodności zakresu SZBI;
10. weryfikacja zgodności z politykami i celami zabezpieczeń;
11. przegląd i ocena skuteczności zabezpieczeń;
12. weryfikacja zgodności wykorzystywania procedur;
13. weryfikacja zgodności obowiązków i uprawnień w ramach SZBI;
14. analiza audytów bezpieczeństwa;
15. weryfikacja dokumentacji i sposobu postępowania z incydentami;
16. weryfikacja sugestii oraz informacji zwrotnych od zainteresowanych stron;
17. sprawdzenie aktualności procedur ciągłości działania.
18. Opracowanie raportu z przeglądu.

# Zakup usług przeprowadzenia audytu zgodności KRI.

Zakres audytu systemu bezpieczeństwa informacji (zwany na potrzeby przedmiotowego postepowania audytem zgodności KRI, audytem KRI) obejmie zgodność z kryteriami zawartymi w Rozporządzeniu KRI oraz zgodność z wymaganiami normy **PN-EN ISO/IEC 27001:2023** dla Zamawiającego i dotyczyć będzie istniejącej na czas przeprowadzenia audytu dokumentacji systemu zarządzania bezpieczeństwem oraz warunków technicznych bezpieczeństwa informacji (BI) zgodnie z minimalnymi wymaganiami wykonania usługi określonymi poniżej.

Wymagania minimalne wykonania usługi:

1. Przedmiotem zamówienia jest przeprowadzenie audytu dotyczącego spełnienia wymagań normy **PN-EN ISO/IEC 27001:2023** oraz Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2024 poz. 773), zwanym dalej „Rozporządzeniem KRI”.
2. Audyt KRI musi być przeprowadzony przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
3. Określenie minimalnego zakresu audytowanych obszarów:
   1. świadczenie usług w formie elektronicznej w tym udostępnionej na platformie ePUAP, zgodnie z art. 16 ust. 1a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2024 poz. 307);
   2. zamieszczenie na głównej stronie internetowej podmiotu (i/lub na stronie BIP), odesłania do opisów usług, które zawierają wymagane informacje dotyczące m.in. aktualnej podstawy prawnej świadczonych usług, nazwy usług, miejsca świadczenia usług (złożenia dokumentów), terminu składania i załatwiania spraw oraz nazwy komórek odpowiedzialnych za załatwienie spraw, zgodnie z § 5 ust. 2 pkt 1 i 4 Rozporządzenia KRI;
   3. poziom wspierania modelu usługowego w procesie świadczenia usług elektronicznych przez systemy teleinformatyczne podmiotu, zgodnie z §15 ust. 2 Rozporządzenia KRI;
   4. poziom współpracy systemów teleinformatycznych z innymi systemami podmiotu publicznego lub systemami informatycznymi innych podmiotów publicznych w tym rejestrami referencyjnymi, zgodnie z §5 ust. 3 pkt 3 Rozporządzenia KRI;
   5. sposób komunikacji z innymi systemami w tym wyposażenie w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami telekomunikacyjnymi za pomocą protokołów komunikacyjnych i szyfrujących zapewniających BI, zgodnie z §16 ust. 1 Rozporządzenia KRI;
   6. regulacje wewnętrzne opisujące sposób zarządzania dokumentacją, w tym zakres stosowania elektronicznego obiegu dokumentów, zgodnie z §19 ust. 2 pkt 9 Rozporządzenia KRI;
   7. sposób kodowania znaków w dokumentach wysyłanych i odbieranych z systemów teleinformatycznych podmiotu, zgodnie z §17 ust. 1 Rozporządzenia KRI;
   8. sposób udostępniania zasobów informatycznych z systemów teleinformatycznych, zgodnie z §18 ust. 1 Rozporządzenia KRI;
   9. sposób przyjmowania dokumentów elektronicznych przez systemy teleinformatyczne, zgodnie z §18 ust. 2 Rozporządzenia KRI;
   10. dokumentacja SZBI, w tym Polityka BI oraz inne dokumenty stanowiące SZBI, Dokumentacja przeglądów SZBI, szacowania ryzyka, audytów, incydentów naruszenia BI, zgodnie z §19 ust. 1 Rozporządzenia KRI;
   11. działania związane z aktualizacją regulacji wewnętrznych w zakresie zmieniającego się otoczenia będące konsekwencją wyników szacowania ryzyka, wniosków z przeglądów SZBI, zaleceń poaudytowych, wniosków z analizy incydentów naruszenia BI, zgodnie z §19 ust. 2 pkt 1 Rozporządzenia KRI;
   12. stopień zaangażowania kierownictwa podmiotu w proces ustanawiania i funkcjonowania SZBI oraz zarządzania BI (przeglądy SZBI, szacowanie i obsługa ryzyka BI, egzekwowanie działań związanych z BI), zgodnie z §19 ust. 2 Rozporządzenia KRI;
   13. regulacje wewnętrzne opisujące sposób zarządzania ryzykiem BI w podmiocie;
   14. dokumentacja z przeprowadzania okresowej analizy ryzyka utraty integralności, poufności lub dostępności informacji, w tym rejestr ryzyk, zawierający informacje o zidentyfikowanych ryzykach, ich poziomie, plan postępowania z ryzykiem, zgodnie z §19 ust. 2 pkt 3 Rozporządzenia KRI;
   15. działania minimalizujące ryzyko zgodnie z planem postępowania z ryzykiem stosownie do szacowania ryzyka;
   16. regulacje wewnętrzne opisujące sposób zarządzania sprzętem informatycznym i oprogramowaniem (w tym licencjami na oprogramowanie) oraz funkcjonowania rejestru zasobów teleinformatycznych;
   17. rejestr zasobów teleinformatycznych zawierający informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku, zgodnie z §19 ust. 2 pkt 2 Rozporządzenia KRI;
   18. sposób aktualizacji rejestru zasobów teleinformatycznych;
   19. regulacje wewnętrzne opisujące zarządzania uprawnieniami użytkowników do pracy w systemach teleinformatycznych, w tym do przetwarzania danych osobowych;
   20. adekwatność poziomu uprawnień do pracy w systemach teleinformatycznych do zakresu czynności i posiadanych upoważnień dostępu do informacji, w tym upoważnień do przetwarzania danych osobowych (rejestr wydanych upoważnień), zgodnie z §19 ust. 2 pkt 4 Rozporządzenia KRI;
   21. działania w zakresie monitoringu i kontroli dostępu do zasobów teleinformatycznych, w tym przeglądy w celu wykrywania nieuprawnionego dostępu, nadmiernych uprawnień, konfliktu interesów czy nadzorowania samego siebie itp.;
   22. sposób i szybkość odbierania uprawnień byłym pracownikom w systemach informatycznych, zgodnie z §19 ust. 2 pkt 5 Rozporządzenia KRI;
   23. regulacje wewnętrzne dotyczące przeprowadzania szkoleń użytkowników zaangażowanych w procesie przetwarzania informacji w systemach teleinformatycznych;
   24. dokumentacja z przeprowadzonych szkoleń pod kątem zakresu tematycznego, w tym: aktualności informacji o zagrożeniach, skutkach i zabezpieczeniach, wskaźnik liczby osób przeszkolonych w stosunku do wszystkich osób uczestniczących w procesie przetwarzania informacji, a także cykliczności szkoleń, zgodnie z §19 ust. 2 pkt 6 Rozporządzenia KRI;
   25. regulacje wewnętrzne określające zasady bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, zgodne z §19 ust. 2 pkt 8 Rozporządzenia KRI;
   26. działania w zakresie stosowania zasad bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, w tym stosowania zabezpieczeń i procedur bezpieczeństwa przez użytkowników urządzeń przenośnych i pracy na odległość;
   27. umowy serwisowe oraz umowy dotyczące rozwoju systemów teleinformatycznych w zakresie zapisów gwarantujących odpowiedni poziom BI, zgodne z §19 ust. 2 pkt 1 Rozporządzenia KRI;
   28. regulacje wewnętrzne, w których określono zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji;
   29. sposób zgłaszania i postępowania z incydentami (działania korygujące), rejestr incydentów naruszenia BI, wpływ analizy incydentów na SZBI, ewentualna współpraca z CERT.GOV.PL, zgodnie z §19 ust. 2 pkt 13 Rozporządzenia KRI;
   30. regulacje wewnętrzne, w których określono zasady przeprowadzania audytów wewnętrznych w zakresie BI;
   31. sprawozdania z audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z §19 ust. 2 pkt 14 Rozporządzenia KRI;
   32. działania podjęte w wyniku zaleceń poaudytowych;
   33. określenie zasad tworzenia, przechowywania oraz testowania kopii zapasowych danych i systemów podmiotu, zgodnie §19 ust. 2 pkt 12 lit. b rozporządzenia KRI;
   34. działania związane z wykonywaniem, przechowywaniem i testowaniem kopii zapasowych danych i systemów oraz dokumentacja z tych działań;
   35. regulacje wewnętrzne, w których ustalono zasady postępowania z informacjami zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, oraz urządzeń mobilnych, w tym plan postępowania z ryzykiem, zgodne z §19 ust. 2 pkt 11 Rozporządzenia KRI;
   36. regulacje wewnętrzne dotyczące zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami poprzez ustalenie zabezpieczeń informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje usunięcie lub zniszczenie, zgodnie z §19 ust. 2 pkt 7 i 9 Rozporządzenia KRI;
   37. działania związane z monitorowaniem dostępu do informacji np. w systemie informatycznym odnotowującym w bazie danych wszystkie działania użytkowników i administratorów dotyczące systemów teleinformatycznych podmiotu publicznego. Działania związane z monitorowaniem ruchu osobowego w podmiocie, zgodnie z § 19 ust. 2 pkt 7 lit. a) Rozporządzenia KRI;
   38. czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez kontrolę logów systemów, kontrolę wejść i wyjść do pomieszczeń serwerowni, analizę rejestru zgłoszeń serwisowych, analizę rejestru incydentów naruszenia BI, zgodnie z §19 ust. 2 pkt 7 lit. b) Rozporządzenia KRI;
   39. działania związane z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych usług sieciowych i aplikacji poprzez stosowanie systemu kontroli dostępu do pomieszczeń serwerowni, systemu autoryzacji dostępu do systemów operacyjnych, sieci i aplikacji, stosowanie zabezpieczeń kryptograficznych, stosowanie systemów antywirusowych i antyspamowych, stosowanie zapór sieciowych typu firewall zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem, zgodnie z § 19 ust. 2 pkt 7 lit. c) Rozporządzenia KRI;
   40. działania związane z ochroną fizyczną informacji zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych, zgodne z wynikami analizy ryzyka i planem postępowania z ryzykiem;
   41. działania związane z utylizacją sprzętu informatycznego i nośników danych a także związane z przekazywaniem sprzętu informatycznego do naprawy w sposób gwarantujący zachowanie BI;
   42. regulacje wewnętrzne, w których ustalono zasady w celu zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych poprzez opisy stosowania zabezpieczeń, w tym plan postępowania z ryzykiem, zgodnie z §19 ust. 2 pkt 12 oraz ust. 4 Rozporządzenia KRI;
   43. regulacje wewnętrzne zawierające zasady prowadzenia i wykorzystania dzienników systemowych (logów), w których odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych, zgodnie z §20 Rozporządzenia KRI;
   44. sposób prezentacji informacji na stronach internetowych systemów telekomunikacyjnych podmiotu oraz zgodność z wymogami WCAG2.1.
4. Na podstawie przeprowadzonej analizy dokumentacji oraz audytu bezpieczeństwa, Wykonawca jest zobowiązany przedstawić pisemny raport zawierający wszystkie wyniki, wnioski wraz z propozycją zmian w zakresie spełnienia wymagań Rozporządzenia KRI. W raporcie muszą zostać uwzględnione wszystkie wyniki cząstkowe z audytowanych obszarów. Spełnienie poszczególnych wymagań zostanie określone w trzyelementowej skali: 1) spełnione – oznacza, że wymaganie normy zostało całkowicie wdrożone, 2) częściowo spełnione – może zaistnieć, czy dany obszar został udokumentowany (opracowano stosowną procedurę lub przygotowano inne zabezpieczenie), ale wybrany mechanizm nie został skutecznie wdrożony (np. zdefiniowano strefy bezpieczeństwa, ale system kontroli dostępu nie funkcjonuje poprawnie); najczęstszym przypadkiem oznaczenia wymagania jako „częściowo spełnionego” jest nieskuteczne wdrożenie procedury (nie przestrzeganie zapisów procedury przez pracowników), 3) niespełnione – wymaganie niespełnione oznacza, że nie zostało ono w ogóle zidentyfikowane przez podmiot (podmiot nie jest świadomy danego zagrożenia) lub nie podjęto żadnych działań, aby wdrożyć odpowiednie mechanizmy zabezpieczające.

# Równoważność rozwiązań.

1. Zamawiający informuje, że tam, gdzie Zamawiający opisał przedmiot zamówienia przez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, dopuszcza się rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany udowodnić, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.
2. Zamawiający informuje, że tam, gdzie w Zapytaniu oraz załącznikach opisał przedmiot zamówienia przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty dostarczane przez konkretnego Wykonawcę, co mogłoby doprowadzić do uprzywilejowania lub wyeliminowania niektórych Wykonawców lub produktów, Zamawiający dopuszcza rozwiązanie równoważne opisywanym pod warunkiem, że będą one o nie gorszych właściwościach i jakości. Zamawiający informuje, iż w takiej sytuacji przedmiotowe zapisy są jedynie przykładowe i stanowią wskazanie dla Wykonawcy jakie cechy powinny posiadać materiały użyte do realizacji przedmiotu zamówienia. Ewentualne użycie nazwy producenta ma wyłącznie charakter przykładowy i ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania.
3. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez usługi spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, uwiarygodniających te rozwiązania.
4. Wykonawca, który posługuje się równoważnymi certyfikatami lub normami musi je załączyć do oferty. Przez certyfikat lub normę równoważną Zamawiający rozumie certyfikat lub normę analogiczną co do zakresu z certyfikatami lub normami wskazanymi z nazwy, który potwierdza spełnianie certyfikacji lub normy charakteryzującej się cechami właściwymi dla certyfikacji lub normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do certyfikacji.
5. Za równoważne do normy PN-EN ISO/IEC 27001:2023 Zamawiający uzna inne normy dotyczące międzynarodowego standardu w zakresie bezpieczeństwa informacji obejmujące wymagania normy PN-EN ISO/IEC 27001:2023 określone w rozdziałach 4-10 tej normy.