**Załącznik nr 1 do SWZ**

# OPIS PRZEDMIOTU ZAMÓWIENIA

**„Podniesienie stopnia bezpieczeństwa IT w Gminie Gniewkowo w ramach projektu Cyberbezpieczny Samorząd”**

1. **DOSTAWA INFRASTRUKTURY SPRZĘTOWEJ ORAZ OPROGRAMOWANIA**

Przedmiotem zamówienia jest dostawa sprzętu i oprogramowania podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych w Gniewkowie

Poniżej wyspecyfikowano minimalne parametry sprzętu oraz oprogramowania, które należy dostarczyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

Wymagania ogólne:

* Całość dostarczanego sprzętu i oprogramowania standardowego musi pochodzić z autoryzowanego kanału sprzedaży producenta.
* Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, musi być nowe, wcześniej nieużywane, rok produkcji nie starszy niż 2024.
* Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, w którym nie wskazano szczegółowych warunków gwarancji, musi być objęte minimum 24 miesięczną gwarancją jeśli w opisie parametrów nie wskazano inaczej
* Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji danego elementu.
* Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
* Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
* Wszystkie urządzenia muszą posiadać oznakowanie CE.
* Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL)
* Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
* Wymagane jest, aby infrastruktura sprzętowa była gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.
* Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).

Zamawiający wymaga aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:

* posiadane środowisko domenowe,
* posiadaną konfigurację sieci wraz z segmentacją VLAN, oraz strefą DMZ,
* posiadaną konfiguracją baz danych i backupów,
* konfigurację stacji roboczych.

**Wykonawca w ramach postępowania zobowiązany jest do wykonania co najmniej następujących usług związanych z montażem i konfiguracją dostarczanej infrastruktury sprzętowej:**

1. Wykonanie Projektu Technicznego dostarczanej infrastruktury sprzętowej, który będzie składał się co najmniej z następujących elementów:
	* Dokładna specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów,
	* Nazwy oraz szczegółowa adresacja poszczególnych elementów,
	* Planowana konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsca, zaprojektowanie kompleksowego systemu ochrony danych opartego na funkcjach macierzy oraz oprogramowania standardowego z uwzględnieniem specyfiki całego projektu,
	* Wymagane działania ze strony Zamawiającego w celu poprawnego montażu i konfiguracji,
	* Harmonogram prac.

Projekt techniczny musi zostać wykonany po wcześniejszej analizie środowiska wykonanej przez Wykonawcę oraz musi zostać zaakceptowany przez Zamawiającego.

1. Konfiguracja serwerów.
2. Instalacja oraz konfiguracji oprogramowania.
3. Testy rozwiązania.
4. Instruktaż dla administratorów demonstrujący sposób zarządzania środowiskiem.
5. Dostarczenie dokumentacji powykonawczej infrastruktury sprzętowej i oprogramowania standardowego, która będzie składała się co najmniej z następujących elementów:
	* Specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów oraz numerami seryjnymi poszczególnych elementów,
	* Końcowe nazwy oraz szczegółowa adresacja poszczególnych elementów,
	* Konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsc
	* Komplety poświadczeń do całej infrastruktury – wymagana zmiana haseł domyślnych – dostarczone jako osobny załącznik w postaci zaszyfrowanego pliku kdbx,
	* Dokumentacja techniczna w formie elektronicznej do każdego elementu w języku polskim lub angielskim
	* Szczegóły dotyczące instalacji i uruchomienia infrastruktury sprzętowej, w zakresie modernizacji infrastruktury szpitala, zostaną ustalone pomiędzy Stronami w trakcie Analizy Przedwdrożeniowej.
	* Zamawiający zapewni odpowiedni zapas mocy oraz odpowiednie warunki środowiskowe w komorach serwerowni.
	* Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników”.

**Opis parametrów minimalnych:**

1. **Część 1Wdrożenie/aktualizacja dokumentacji SZBI** **oraz PBI wraz z audytem**

**Opracowywanie pełnej dokumentacji i procedur Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z normą PN-ISO/IEC 27001, oraz wdrożenie ustanowionego SZBI.**

**1.1. Zakres zamówienia**

Zamówienie obejmuje trzy główne obszary, za które odpowiedzialny będzie wykonawca:

1. **Opracowanie dokumentacji i procedur SZBI.** Wykonawca musi stworzyć kompleksową dokumentację, w tym Polityki Bezpieczeństwa Informacji, procedury operacyjne oraz procedury reagowania na incydenty.
2. **Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji.** Wykonawca musi zaplanować system w strukturach zamawiającego, włączając odpowiednie konfiguracje techniczne i organizacyjne.
3. **Monitorowanie i doskonalenie systemu.** Wykonawca musi zaplanować procesy monitorowania efektywności wdrożonego systemu oraz jego ciągłe doskonalenie.

Opracowanie SZBI ma zapewnić spełnienie wymogów 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. Na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307).

**Opracowanie dokumentacji i procedur SZBI**

**Struktura i format dokumentacji**

Wykonawca musi opracować kompletną dokumentację Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), która będzie zgodna z wymaganiami normy PN-ISO/IEC 27001:2022. Struktura dokumentacji powinna być jasna i zrozumiała dla wszystkich użytkowników systemu w Urzędzie. Dokumentacja ma być zorganizowana w sposób umożliwiający łatwy dostęp do poszczególnych sekcji i procedur, co ułatwi zarządzanie systemem i jego przegląd. Format dokumentacji powinien obejmować wersje elektroniczne, zapewniające pełną dostępność i możliwość archiwizacji, a także dostępność dla osób o różnych potrzebach, w tym osoby z niepełnosprawnościami oraz promując praktyki zapewniające równość i niedyskryminację. Wersja w postaci papierowej **nie jest wymagana**.

**Opracowanie procedur operacyjnych i kontrolnych**

Wykonawca musi opracować szczegółowe procedury operacyjne i kontrolne, które umożliwią skuteczne zarządzanie SZBI i odpowiednie reagowanie na incydenty bezpieczeństwa. Procedury te muszą zawierać instrukcje dotyczące zarządzania aktywami, zarządzania dostępem, oceny ryzyka, zarządzania incydentami bezpieczeństwa oraz procedur odzyskiwania danych. Procedury muszą uwzględniać mechanizmy monitorowania i przeglądu efektywności działań bezpieczeństwa, zapewniające ciągłą ochronę informacji zgodnie z najnowszymi standardami i najlepszymi praktykami.

Poniżej znajduje się tabela z wykazem minimalnej ilości opisanych dokumentów (lub ich wzorów) i procedur, które wykonawca musi dostarczyć w ramach zamówienia. Dodatkowo, jeżeli wykonawca uzna, że konieczne jest dołączenie dodatkowych dokumentów lub procedur, może je włączyć do projektu w ramach wdrożenia, aby jeszcze bardziej dostosować system do specyficznych potrzeb Urzędu Miasta w Gniewkowie. Wykonawca może również zaproponować własne nazwy dla dokumentów lub procedur, pod warunkiem że będą one adekwatnie odzwierciedlać obszary bezpieczeństwa określone w kolumnie “opis” w poniższej tabeli. Zamawiający dopuszcza także dokonywanie zmian w poniższej mapie dokumentów i procedur, o ile wprowadzone modyfikacje będą obejmowały obszar bezpieczeństwa ujęty w kolumnie “opis” w poniższej tabeli oraz będą zgodne z normą ISO 27001:2022.

**1.2. Etapy i harmonogram wdrożenia**

**Etap 1: przygotowanie i zatwierdzenie planu projektowego** - wykonawca opracuje i zatwierdzi w porozumieniu z zamawiającym szczegółowy plan wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

**Etap 2: zdobycie wsparcia kierownictwa organizacji:**

* Wykonawca musi zidentyfikować i omówić specyficzne cele, które kierownictwo zamawiającego chce osiągnąć poprzez wdrożenie systemu, w tym związane z tym korzyści biznesowe i operacyjne. Zadaniem wykonawcy jest zapewnienie, że cele te są jasno zrozumiałe i że SZBI będzie odpowiednio dostosowany do potrzeb organizacyjnych zamawiającego.
* Wykonawca odpowiedzialny jest za organizację sesji informacyjnych i dyskusji z kluczowymi członkami kierownictwa zamawiającego, aby uzyskać ich opinie, doprecyzować oczekiwania i zbudować silne poparcie dla projektu. Spotkania te będą miały na celu zapewnienie, że wszystkie strony mają jednolite rozumienie zakresu i oczekiwań projektu.

**Etap 3: Definicja zakresu SZBI:**

* Wykonawca wspólnie z zamawiającym zdefiniuje, które części organizacji, funkcje, dane, lokalizacje i technologie zostaną objęte SZBI. Definicja ta powinna być spójna z celami biznesowymi i operacyjnymi zamawiającego oraz uwzględniać wszystkie zewnętrzne i wewnętrzne wymogi dotyczące bezpieczeństwa informacji.
* Wykonawca przygotuje formalny dokument zakresu SZBI, który zostanie przedłożony do zatwierdzenia przez zamawiającego. Dokument ten będzie zawierał szczegółowy opis zakresu, cele związane z bezpieczeństwem informacji, a także zobowiązania organizacji dotyczące przestrzegania wymogów prawnych i regulacyjnych.
* Wykonawca musi zapewnić, że zakres SZBI jest w pełni zintegrowany z obecnymi procesami biznesowymi oraz infrastrukturą technologiczną zamawiającego, co umożliwi sprawną implementację i późniejsze funkcjonowanie systemu.

**Etap 4: Inwentaryzacja zasobów informacyjnych:**

* W ramach tego etapu, wykonawca współpracując z zamawiającym, musi przeprowadzić szczegółową inwentaryzację wszystkich zasobów informacyjnych istotnych dla organizacji oraz musi ocenić potencjalne ryzyka związane z ich bezpieczeństwem. Wykonawca musi zidentyfikować i skatalogować wszystkie zasoby informacyjne należące do zamawiającego, które mogą obejmować dane cyfrowe, fizyczne nośniki informacji, oprogramowanie, sprzęt komputerowy oraz infrastrukturę sieciową.
* Po zidentyfikowaniu zasobów, wykonawca wraz z zamawiającym muszą przypisać każdemu z nich poziom ważności i poufności.

**Etap 5: Przygotowanie oświadczenia stosowania:**

* Wykonawca musi zredagować formalny dokument oświadczenia stosowania.
* Dokument oświadczenia stosowania będzie przedmiotem konsultacji z zamawiającym, aby upewnić się, że wszystkie zainteresowane strony zgadzają się co do zakresu i charakteru oświadczenia. Następnie dokument zostanie ostatecznie zatwierdzony i przyjęty przez zamawiającego.
* Wykonawca musi zadbać, aby oświadczenie stosowania było zintegrowane z innymi dokumentami i procesami w ramach SZBI, takimi jak polityka bezpieczeństwa, procedury operacyjne oraz plany reagowania na incydenty.

**Etap 6: Przygotowanie programu wdrożenia SZBI:**

Wykonawca przygotuje plan projektu wdrożenia, który określi kluczowe działania, ich kolejność, przypisane zasoby, odpowiedzialności i terminy. Plan powinien także uwzględniać wszelkie zależności między działaniami oraz sposoby ich zarządzania.

**Etap 7: Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI):**

* Wykonawca musi wdrożyć wszystkie komponenty SZBI, zapewniając ich integrację oraz funkcjonalność.
* Wykonawca musi opracować i zaimplementować politykę bezpieczeństwa informacji, która będzie integralnie powiązana z kluczowymi procesami biznesowymi zamawiającego. Polityka ta określi standardy, procedury oraz odpowiedzialności związane z zarządzaniem informacjami.
* Wykonawca musi zapewnić, że wszystkie wymagane dokumenty, takie jak polityki, procedury, instrukcje operacyjne i rejestry ryzyka, będą opracowane.
* Wykonawca opracuje szablony dokumentów i narzędzia wspomagające, które będą wykorzystywane w codziennej pracy związanej z SZBI, takie jak formularze do zgłaszania incydentów bezpieczeństwa, checklisty audytowe, narzędzia do monitorowania zgodności itp.
* Wykonawca stworzy i zaimplementuje procedury odpowiedzi na incydenty bezpieczeństwa informacji, które określą, jak identyfikować, reagować i zarządzać incydentami.

Zamawiający wymaga od Wykonawcy opracowania szczegółowego harmonogramu wdrożenia SZBI, który będzie obejmować wszystkie kluczowe etapy projektu, od przygotowania planu projektowego po pełne wdrożenie systemu. Harmonogram ten musi być zatwierdzony przez Zamawiającego przed rozpoczęciem implementacji.

Szczegółowe wymagania dotyczące harmonogramu są następujące:

* Wykonawca musi przygotować szczegółowy harmonogram projektu, który jasno określi sekwencję i czas trwania wdrożenia SZBI, wymienionych poniżej:

- **Etap 1:** Przygotowanie i zatwierdzenie planu projektowego.

- **Etap 2:** Zdobycie wsparcia kierownictwa organizacji.

- **Etap 3:** Definicja zakresu SZBI.

- **Etap 4:** Inwentaryzacja zasobów informacyjnych.

- **Etap 5:** Przygotowanie oświadczenia stosowania.

- **Etap 6:** Przygotowanie programu wdrożenia SZBI.

- **Etap 7:** Wdrożenie SZBI.

* Harmonogram wdrożenia musi zostać przedłożony zamawiającemu do akceptacji przed rozpoczęciem jakichkolwiek działań w ramach projektu. Zatwierdzenie to musi być udokumentowane i może wymagać modyfikacji na żądanie zamawiającego w celu lepszego dopasowania do warunków operacyjnych zamawiającego.
* Wykonawca jest zobowiązany do regularnego przeglądu i aktualizacji harmonogramu w odpowiedzi na zmieniające się okoliczności projektu lub na wniosek zamawiającego. Wszelkie zmiany w harmonogramie muszą być niezwłocznie komunikowane zamawiającemu i podlegają jego zatwierdzeniu.
* Wykonawca jest odpowiedzialny za monitorowanie postępów w realizacji harmonogramu i regularne raportowanie statusu zamawiającemu. Raporty powinny zawierać szczegółowe informacje o ukończonych, bieżących oraz planowanych działaniach, a także o wszelkich wyzwaniach czy odchyleniach od pierwotnego planu.

**Zakończenie i formalne przekazanie systemu zarządzania bezpieczeństwem informacji (SZBI)**

Wykonawca wraz z zamawiającym muszą przeprowadzić szczegółowy przegląd końcowy SZBI, w tym ocenę zgodności z pierwotnie ustalonymi celami i specyfikacjami. Przegląd ten ma na celu upewnienie się, że wszystkie elementy systemu działają prawidłowo i spełniają wymagania bezpieczeństwa.

Po pomyślnym przeglądzie, projekt wymaga formalnego zatwierdzenia przez zamawiającego. To zatwierdzenie będzie dokumentowane w formie formalnego dokumentu przekazania, który potwierdza pełne przyjęcie projektu.

Wykonawca musi przekazać zamawiającemu kompletną dokumentację systemu, która obejmuje instrukcje obsługi, procedury bezpieczeństwa, polityki oraz wszelkie inne dokumenty niezbędne do zarządzania i utrzymania SZBI.

Zamawiający wymaga, aby Wykonawca wykonujący zadanie odbył stosowną ilość wizyt w jednostce Zamawiającego, minimum 4 wizyty po min 4 godziny.

**Przeprowadzenie audytów KRI**

Wykonanie audytu zgodnie z wymaganiami art. 21 - 23 ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) i § 19 rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI) w szczególności:

1. Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)

a) wyznaczenie osoby do kontaktu – KSC

b) przekazanie danych osoby wyznaczonej – KSC

c) zapewnienie zarządzania incydentem – KSC

d) zgłaszanie incydentu – KSC

e) zapewnienie obsługi incydentu – KSC

f) zapewnienie dostępu do wiedzy – KSC

g) opracowanie, ustanowienie i wdrożenie SZBI – KRI

h) monitorowanie i przegląd SZBI – KRI

i) doskonalenie SZBI – KRI

j) aktualizowanie regulacji wewnętrznych – KRI

k) inwentaryzacja sprzętu i oprogramowania – KRI

l) przeprowadzanie okresowych analiz ryzyka – KRI

m) postępowanie z ryzykiem – KRI

n) zarządzanie uprawnieniami – KRI

o) szkolenia i uświadamianie – KRI

p) monitorowanie dostępu do informacji – KRI

q) monitorowanie nieautoryzowanych zmian – KRI

r) zabezpieczenie nieautoryzowanego dostępu – KRI

s) ustanowienie zasad bezpiecznej pracy mobilnej – KRI

t) zabezpieczenie informacji przed nieuprawnionym ujawnieniem – KRI

u) zabezpieczenie informacji przed nieuprawnioną modyfikacją – KRI

v) zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem – KRI

w) zawieranie w umowach serwisowych zapisów o bezpieczeństwie – KRI

x) ustalenie zasad postępowania z informacjami w celu minimalizacji kradzieży informacji i środków przetwarzania – KRI

y) aktualizowanie oprogramowania – KRI

z) minimalizowanie ryzyka utraty informacji w wyniku awarii systemu – KRI

aa) ochrona systemu przed błędami – KRI

bb) stosowanie mechanizmów kryptograficznych w systemach – KRI

cc) zapewnienie bezpieczeństwa plików systemowych – KRI

dd) zarządzanie podatnościami systemów – KRI

ee) kontrola zgodności systemów z regulacjami – KRI

ff) zapewnienie audytu bezpieczeństwa informacji nie rzadziej niż raz na rok – KRI

2. Opracowanie raportu z audytu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących. Audyt systemu bezpieczeństwa informacji wdrożonego w urzędzie JST obejmie zgodność z kryteriami zawartymi w § 19 ust. 2 ww. rozporządzenia KRI lub zgodność z wymaganiami normy PN-EN ISO/IEC 27001:2023. Dodatkowo audyt musi spełniać wymagania Regulaminu Konkursu Grantowego pn. “Cyberbezpieczny Samorząd” Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.

**Pierwszy audyt należy wykonać w terminie 90 dni od podpisania umowy. Drugi audyt na zakończenie projektu „Cyberbezpieczny Samorząd” zgodnie z wytycznymi regulaminu grantu jednak nie później niż do 09.04.2026 r.**

1. Szkolenia dla kadry kierowniczej oraz pozostałych pracowników

Celem szkolenia jest wyposażenie pracowników Urzędu Miasta w Gniewkowie w niezbędną wiedzę i umiejętności potrzebne do efektywnego wykorzystania i zarządzania Systemem Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnie z normą PN-ISO/IEC 27001. Zamawiający oczekuje, że w wyniku szkolenia pracownicy będą mogli nie tylko zrozumieć podstawowe koncepcje i wymogi SZBI, ale także nauczą się praktycznych aspektów związanych z codziennym stosowaniem systemu w pracy urzędniczej.

Wykonawca zobowiązany jest zapewnić, aby szkolenie pokrywało kluczowe obszary takie jak polityki bezpieczeństwa informacji, procedury operacyjne i reagowania na incydenty, zarządzanie ryzykiem, a także prawne i regulacyjne aspekty ochrony danych. Szkolenie powinno również skupić się na umiejętnościach praktycznych, takich jak właściwe postępowanie w przypadku wykrycia zagrożeń dla bezpieczeństwa informacji, oraz na rozwijaniu świadomości i kultury bezpieczeństwa wśród pracowników.

Zamawiający podkreśla znaczenie szkolenia jako integralnej części procesu wdrażania i utrzymywania SZBI, mającej na celu nie tylko zwiększenie kompetencji pracowników, ale także poprawę ogólnego poziomu bezpieczeństwa informacji w Urzędzie. Wykonawca musi więc zaprojektować program szkoleniowy, który jest angażujący, interaktywny i dostosowany do różnych poziomów wiedzy uczestników, aby maksymalizować jego efektywność i zapewnić, że wszystkie cele szkoleniowe są osiągane.

**Podział na grupy i zróżnicowanie treści**

W przypadku szkolenia stacjonarnego w siedzibie zamawiającego, będzie przeprowadzone w grupach po maksymalnie 20 osób, przy czym łączna liczba osób do przeszkolenia wynosi 65. W przypadku szkoleń zdalnych grupy mogą być liczniejsze, ale wymaga to dodatkowych ustaleń z zamawiającym.

Zamawiający wymaga, aby treści szkoleniowe były zróżnicowane w zależności od roli uczestników:

* **Dla zwykłych użytkowników** – program szkolenia skupi się na podstawowych aspektach SZBI, w tym na zrozumieniu polityk bezpieczeństwa, zasadach postępowania w przypadku zauważenia potencjalnego zagrożenia, oraz na codziennych procedurach operacyjnych i kontrolnych.
* **Dla kadry kierowniczej** – szkolenie będzie zawierało rozszerzone moduły dotyczące zarządzania ryzykiem, strategii odpowiedzi na incydenty bezpieczeństwa oraz zaawansowanych aspektów tworzenia i utrzymania polityk bezpieczeństwa. Kadra kierownicza zostanie również przeszkolona w zakresie przywództwa w zarządzaniu bezpieczeństwem informacji oraz w aspektach motywowania zespołów do przestrzegania procedur bezpieczeństwa.

Na zakończenie szkoleń należy przeprowadzić test oraz wystawić imienne certyfikaty potwierdzające odbycie szkolenia.

**CZĘŚĆ 2**

### **Zestawienie wymaganego sprzętu i oprogramowania**

|  |  |  |
| --- | --- | --- |
|  ***Lp.*** | **Typ sprzętu**  | **Ilość**  |
|  | Oprogramowanie EDR plus serwer | 1 klp. |
|  | Oprogramowanie do Inwentaryzacji aktywów i ich konfiguracji | 1 klp. |
|  | NAS Klasy Enterprise | 2 szt. |
|  | Przełącznik LAN | 3 szt. |
|  | Firewall NextGeneration | 2 szt. |
|  | System do backup, serwer, biblioteka taśmowa | 1 klp. |
|  | UPS Centralny | 1 szt. |
|  | Agregat prądotwórczy | 1 szt. |
|  | Szkolenie dla pracowników IT | 1 klp. |

# Zamawiający dopuszcza również rozwiązanie równoważne zgodne z poniższymi zapisami:

1. **Architektura / budowa**
	1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 75 klientów jednocześnie.
	2. **Architektura / budowa:**
		1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
		2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).
		3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.
		4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.
	3. **Konfiguracja Architektury:**
		1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.
		2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.

# Wymagania systemowe

* 1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 .
	2. Klient musi działać na systemach 32 i 64 bitowych: min. Windows Server 2019/2022, Windows 8.1/10/11.
		1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci min.: Opera, Chrome, FireFox
	3. Serwer musi działać na systemach 64 bitowych min.: m.in. Windows Server 2019/2022, Windows 8.1/10/11.

2.4. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

# Interfejsy

* 1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
	2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL
	3. System zapewnia integrację z modelem LLM.

# Funkcjonalności systemu zarządzania infrastrukturą IT

* 1. Funkcjonalność Klienta
		1. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku.
	2. Funkcjonalność konsoli administracyjnej.
		1. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.
		2. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.
	3. Funkcjonalność panelu pracownika
		1. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.
	4. Zarządzanie licencjami
		1. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.
	5. Wzorce aplikacji i pakietów
		1. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.
	6. Inwentaryzacja sprzętu komputerowego i urządzeń.
		1. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń.
	7. Inwentaryzacja urządzeń sieciowych.
		1. System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.
	8. Inwentaryzacja sprzętu.
		1. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.
	9. Ochrona danych (DLP)
		1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.
	10. Zdalna administracja komputerami
		1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.
	11. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.
	12. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.
	13. Zarządzanie Poprawkami i Aktualizacjami
		1. System musi zapewniać ciągłe monitorowanie i identyfikację brakujących aktualizacji systemowych i komponentów infrastruktury IT, oferując funkcje rozpoznawania niezainstalowanych poprawek, ich pobierania, oraz klasyfikacji. Musi umożliwiać aktualizacje bez zakłócania pracy użytkowników, zarówno zbiorowo jak i indywidualnie, z opcją szybkiego przywrócenia poprzedniego stanu systemu poprzez odinstalowanie niechcianych poprawek. System powinien również umożliwiać pomijanie niechcianych poprawek i dostarczać szczegółowe raporty dotyczące stanu aktualizacji oraz urządzeń, które mogą wymagać restartu.
	14. Zdalne Zarządzanie Zaporą (Firewall)
		1. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.
	15. Automatyzacja
		1. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.
	16. Zarządzanie magazynem IT
		1. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.
	17. Repozytorium
		1. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.
	18. Kody kreskowe
		1. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.
	19. Wysyłanie wiadomości
		1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.
	20. System musi posiadać możliwość eksportu / importu treści.Monitorowanie drukarek sieciowych i wydruków
		1. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.
	21. Monitorowanie stron www
		1. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.
	22. Monitorowanie serwerów WWW
		1. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.
	23. Monitorowanie dziennika zdarzeń
		1. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.
	24. System musi umożliwiać monitorowanie komunikatów Syslog.
	25. Monitorowanie pracy komputerów
		1. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.
	26. Monitorowanie uprawnień ACL
		1. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami.
	27. Monitorowanie sensorów
		1. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.
	28. Repozytorium CMDB
		1. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.
	29. Worktime manager
		1. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostepnienia w panelu pracownika.
	30. Raportowanie i eksport danych
		1. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.
	31. System musi zapewnić interfejs API.
		1. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.
	32. Powiadomienia
		1. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e- maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji.
	33. Bezpieczeństwo
		1. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.

# Wsparcie i pomoc

* + 1. Pomoc techniczna
			1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.
			2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.
			3. Czas trwania usługi SLA od dnia zakupu do 09.04.2026 r.

# Wymagania Ogólne

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 1 oddzielnego (fizycznego lub logicznego) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

Wraz z urządzeniem należy dostarczyć 2 wkładki sfp+ SR kompatybilne do dostarczanych urządzeń.

# Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: 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. W ramach postępowania system musi zostać dostarczony w postaci pojedynczego urządzenia.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

# Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
* 8 portów Gigabit Ethernet RJ-45.
* 2 gniazdami SFP+ 10 Gbps.
1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System mieć możliwość podłączenia 2 zasilaczy . Należy dostarczyć 2 zasilacze.

# Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz nie mniej niż 124 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.7 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 25 Gbps.
5. 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 4.5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.2 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.2 Gbps.

# Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe 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.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. 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

1. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
1. 4. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
3. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
* Amazon Web Services (AWS).
* Microsoft Azure
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.

# Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
* Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19 i 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.
1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
* 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.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

# Routing i obsługa łączy WAN

1. 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. Baza sygnatur ataków powinna zawierać minimum 1000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. 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.
7. 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. Baza Kontroli Aplikacji powinna zawierać minimum 1000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

# Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów 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.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

# 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. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. 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.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

# Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.

# Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

# Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

# Opisy do wymagań ogólnych

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

**Wymagania dla oprogramowania:**

1. W celu zapewnienia dużej elastyczności i skalowalności środowiska kopii zapasowych oprogramowanie systemu powinno posiadać trójwarstwową architekturę: Serwer Zarządzający, Serwer Mediów, Klient.

2. Oprogramowanie systemu powinno umożliwiać wykonywanie kopii zapasowych w środowisku heterogenicznym za pomocą, dedykowanego dla platformy systemowej, klienta systemu kopii zapasowych.

3. System powinien umożliwiać łatwą rozbudowę w miarę rozrastania się infrastruktury informatycznej Zamawiającego, poprzez dokładanie kolejnych centralnie zarządzanych Serwerów Mediów.

4. Proponowane rozwiązanie musi umożliwiać uruchomienie serwera zarządzającego kopiami zapasowymi na głównych platformach Windows i Linux.

5. Proponowane rozwiązanie musi wspierać wysoką dostępność (klastrowanie) serwera kontrolującego kopie zapasowe.

6. Oprogramowanie musi być niezależne pod względem sprzętowym i nie może preferować instalacji na platformie sprzętowej jednego producenta. Powinno udostępniać te same funkcjonalności niezależnie od tego na jakiej platformie systemowej będzie zainstalowane. Zamawiający musi posiadać możliwość zmiany platformy sprzętowej bez utraty funkcjonalności systemu kopii zapasowej.

7. Proponowane rozwiązanie musi wspierać wdrożenia na sprzęcie fizycznym, infrastrukturze wirtualnej, w chmurze oraz w kontenerach

8. Proponowane rozwiązanie musi umożliwiać administrację za pomocą GUI (aplikacja lub web),

9. System powinien posiadać centralną konsolę zarządzania środowiskiem kopii zapasowych. Konsola musi umożliwiać:

9.1 monitorowanie i zarządzanie wszystkimi zadaniami wykonywania i odtwarzania kopii zapasowych, tworzenia duplikatów wykonanych kopii zapasowych,

9.2 ustawianie harmonogramów wykonywania kopii zapasowych,

9.3 monitorowanie i kontrolowanie urządzeń składowania kopii zapasowych podłączonych do Serwerów Mediów,

9.4 centralne zarządzanie konfiguracją, właściwych dla oprogramowania systemu, ustawień Serwera Zarządzającego, Serwera Mediów, Klientów,

9.5 uruchomienie odtwarzania kopii zapasowych na klienta systemu

10. Oprogramowanie systemu musi posiadać obsługę z poziomu wiersza poleceń w systemach Linux, Unix i Windows. Obsługa z poziomu wiersza poleceń musi umożliwiać:

10.1 konfigurację i modyfikację polityk wykonywania kopii zapasowych,

10.2 konfigurację i modyfikację harmonogramów wykonywania kopii zapasowych,

10.3 konfigurację i modyfikację urządzeń składowania kopii zapasowych podłączonych do Serwerów Mediów,

10.4 konfigurację i modyfikację nośników taśmowych,

10.5 monitorowanie i kontrolowanie zadań kopii zapasowych,

10.6 konfigurację i modyfikację nośników taśmowych

10.7 konfigurację i modyfikację właściwych dla oprogramowania systemu, ustawień Serwera Zarządzającego, Serwera Mediów, Klientów,

10.8 konfigurację, modyfikację i przeglądanie dzienników Serwera Zarządzającego, Serwera Mediów, Klientów,

11. Rozwiązanie powinno być dostępne także jako zintegrowane programowo i sprzętowo urządzenie (appliance), a więc sprzęt i oprogramowanie backupowe razem. Zintegrowane urządzenia powinny umożliwiać zbudowanie w pełni funkcjonującej trzywarstwowej architektury backupowej z funkcjonalnością deduplikacji danych.

12. Baza katalogowa dla systemu backupowego musi być częścią systemu backupowego i wspierać platformy minimum Linux oraz Windows oraz nie powinna posiadać ograniczeń wynikających z ilości używanych w serwerze procesorów i rdzeni procesorów.

13. Baza katalogowa musi być w cenie systemu kopii zapasowych i nie ograniczona co do ilości środowisk backupowych, mocy czy ilości serwerów czy to backupowych czy produkcyjnych. Jakakolwiek rozbudowa środowiska backupowego czy dodanie następnego nie może powodować konieczności dokupienia licencji dla tej bazy.

14. Oprogramowanie systemu kopii zapasowych musi posiadać zintegrowane zarządzanie kluczami szyfrującymi oraz musi posiadać możliwość integracji z zewnętrznymi usługami zarządzania kluczami szyfrowania,

15. Oprogramowanie systemu kopii zapasowych musi integrować się z urządzeniami dyskowymi (deduplikatory) wspierającymi mechanizm WORM w celu ochrony danych przed zaszyfrowaniem, modyfikacją i usunięciem. Funkcjonalność musi zapewniać, że obraz kopii zapasowej jest tylko do odczytu i nie może być modyfikowany, uszkodzony lub zaszyfrowany po utworzeniu kopii zapasowej oraz chronić obraz kopii zapasowej przed usunięciem przed upływem terminu ważności.

16. Proponowane rozwiązanie musi wspierać ochronę klientów pracujących pod kontrolą:

16.1 Windows 7 - 11

16.2 Windows Server 2008 - 2022, w tym wydania półroczne

16.3 Oracle Linux 6.8 i nowsze

16.4 Oracle Solaris 10 Update 11 i nowsze na architekturach Sparc i x64

17. Proponowane rozwiązanie musi wspierać architekturę składowania kopii zapasowych D2D2T i D2D2C.

18. Proponowane rozwiązanie musi obsługiwać dowolny typ pamięci dyskowej (DAS, NAS, SAN) dla repozytorium backupu.

19. Proponowane rozwiązanie musi wspierać storage taśmowy (samodzielne napędy taśmowe oraz biblioteki taśmowe w tym m.in. biblioteki robotów sterowane ACS) głównych producentów.

20. Proponowane rozwiązanie musi deduplikować dane na źródle i celu.

21. Deduplikacja musi umożliwiać wybór pomiędzy zmiennym i stałym rozmiarem bloku. Rozmiar bloku musi umożliwiać jego wybór.

22. Proponowane rozwiązanie musi wspierać deduplikację zarówno inline jak i postprocesową

23. Proponowane rozwiązanie musi wspierać urządzenia deduplikacyjne głównych producentów takich jak Dell EMC, Exagrid, HPE, Quantum, NEC

24. Proponowane rozwiązanie musi obsługiwać wirtualne biblioteki taśmowe (VTL)

25. Proponowane rozwiązanie musi wspierać transfer danych zarówno przez sieć LAN jak i SAN

26. Proponowane rozwiązanie musi wspierać głównych dostawców chmur publicznych jako magazyn kopii zapasowych

27. Proponowane rozwiązanie musi obsługiwać deduplikację do chmury w celu minimalizacji transferu danych

28. Proponowane rozwiązanie musi umożliwiać wznowienie nieudanego zadania backupowego od ostatniego punktu kontrolnego

29. Proponowane rozwiązanie musi automatyzować tworzenie wielu kopii zapasowych na różnych urządzeniach magazynowych z różną długością przechowywania danych.

30. Proponowane rozwiązanie powinno posiadać możliwość wykonywania wysokowydajnych kopii zapasowych serwerów z bardzo obciążonymi systemami plików na dyskach z dużą liczbą plików (np. backup typu disk-image)

31. Proponowane rozwiązanie musi zapewniać możliwość wykonywania backupu syntetycznego

32. Proponowane rozwiązanie musi umożliwiać tworzenie ręcznych kopii zapasowych ad-hoc

33. Proponowane rozwiązanie musi wspierać topologie replikacji danych typu jeden-do-jednego, wiele-do-jednego, jeden-do-wielu oraz kaskadową z wykorzystaniem deduplikacji danych w celu zminimalizowania ilości przesyłanych danych

34. Proponowane rozwiązanie musi wspierać szyfrowanie danych

35. Proponowane rozwiązanie musi umożliwiać wznowienie nieudanego zadania przywracania z ostatniego punktu kontrolnego

36. Proponowane rozwiązanie musi zapewniać funkcje umożliwiające natywne odzyskiwanie "bare metal" (w pełni zautomatyzowane odzyskiwanie obejmujące system operacyjny, konfigurację, aplikacje i dane) klientów Windows, Linux, Solaris bez konieczności korzystania z zewnętrznych/rodzimych narzędzi do odzyskiwania/reimaging systemu operacyjnego.

37. Proponowane rozwiązanie musi umożliwiać przywracanie różnych konfiguracji systemu oraz różnych układów dysków.

38. Proponowane rozwiązanie musi zapewniać możliwość konwersji P2V i V2P

39. Proponowane rozwiązanie musi umożliwiać przywracanie nawet po wygaśnięciu wsparcia technicznego oprogramowania

40. Proponowane rozwiązanie musi umożliwiać przywracanie pojedynczych obiektów Active Directory z kopii zapasowej Windows System State

**Backup**

1. Proponowane rozwiązanie musi wspierać platformę wirtualizacyjną Hyper-V

2. Proponowane rozwiązanie musi wspierać serwery zarządzane przez jak i samodzielne serwery

5. Proponowane rozwiązanie musi wspierać wszystkie tryby transportu danych obsługiwane przez VDDK (takie jak SAN, NBD, NBDSSL, hot-add)

6. Proponowane rozwiązanie nie może wymagać instalacji agentów w maszynach wirtualnych w celu wykonywania kopii zapasowych

7. Proponowane rozwiązanie musi wspierać śledzenie zmian (CBT - change block tracking)

8. Proponowane rozwiązanie musi wspierać tworzenie syntetycznych kopii zapasowych (tworzonych na podstawie ostatniego pełnego backupu oraz backupu przyrostowego CBT) maszyn wirtualnych w celu umożliwienia wykonywania backupów przyrostowych (incremental-forever)

9. Proponowane rozwiązanie musi zawierać mechanizm automatycznego wykrywania i ochrony maszyn wirtualnych Hyper-V bez konieczności zmiany polityk backupu

10. Proponowane rozwiązanie musi umożliwiać wyłączenie z backupu maszyn wirtualnych usuniętych bloków oraz pliku swap

11. Proponowane rozwiązanie musi wspierać przywracanie pojedynczego pliku z kopii zapasowej maszyny wirtualnej Hyper-V bez konieczności uruchamiania agenta w maszynie wirtualnej oraz umieszczania wirtualnego dysku wirtualnego dysku w tymczasowej lokalizacji, jeżeli obraz kopii zapasowej jest przechowywany na taśmach

12. Proponowane rozwiązanie musi wspierać jednoprzebiegowy backup Microsoft Exchange, Microsoft SQL Server oraz Microsoft SharePoint z możliwością przywracania elementów granularnych zgodnie z opisem w dalszej części.

13. Proponowane rozwiązanie nie może wymagać wykonywania osobnego backupu na poziomie aplikacji backupu na poziomie aplikacji lub wysyłki logów w przypadku backupu Microsoft Exchange, Microsoft SQL Server i Microsoft SharePoint

14. Proponowane rozwiązanie musi wspierać limitowanie zasobów takich jak liczba jednoczesnych zadań backupu na serwer, klaster lub magazyn danych

15. Proponowane rozwiązanie musi umożliwiać uruchomienie maszyny wirtualnej bezpośrednio z dyskowego repozytorium kopii zapasowych

16. Proponowane rozwiązanie musi zapewniać natychmiastowy dostęp do chronionych maszyn wirtualnych i ich plików

**Backup oprogramowania do wirtualizacji fizycznych maszyn**

1. Proponowane rozwiązanie musi wspierać Microsoft Hyper-V 6.2 i nowsze użytkowane przez Zamawiającego

2. Proponowane rozwiązanie musi wspierać ochronę maszyn wirtualnych rezydujących na systemach plików NTFS, ReFS, Windows Storage Spaces, Storage Spaces Direct oraz SMB 3.0

3. Proponowane rozwiązanie musi wspierać Resilient Change Tracking (RCT)

4. Proponowane rozwiązanie musi wspierać tworzenie syntetycznych kopii zapasowych (tworzonych na podstawie ostatniego pełnego i przyrostowego backupu RCT) maszyn wirtualnych w celu umożliwienie tworzenia kopii zapasowych przyrostowych na zawsze

5. Proponowane rozwiązanie musi wspierać ograniczenie liczby aktywnych snapshotów lub backupów na serwer i klaster

6. Proponowane rozwiązanie musi zawierać mechanizm automatycznego wykrywania i ochrony maszyn wirtualnych bez konieczności zmiany polityk backupu.

7. Proponowane rozwiązanie musi umożliwiać wykluczenie usuniętych bloków i plików swap z kopii zapasowej maszyny wirtualnej

8. Proponowane rozwiązanie musi wspierać wyłączenie dysków startowych z backupu maszyn wirtualnych Hyper-V z kopii zapasowych maszyn wirtualnych

9. Proponowane rozwiązanie musi wspierać wyłączenie dysków danych z backupu maszyn wirtualnych kopii zapasowej maszyny wirtualnej

10. Proponowane rozwiązanie musi wspierać przywracanie pojedynczego pliku z kopii zapasowej maszyny wirtualnej Hyper-V bez konieczności przenoszenie dysku wirtualnego w lokalizacji tymczasowej, jeżeli obraz kopii zapasowej jest przechowywany na taśmach

11. Proponowane rozwiązanie musi zapewniać integrację z System Center Virtual Machine Manager (SCVMM) w celu umożliwienia odzyskiwania maszyn wirtualnych

**Backup MS SQL Server**

1. Proponowane rozwiązanie musi wspierać Microsoft SQL Server 2014 i nowsze

2. Proponowane rozwiązanie musi wspierać SQL Server Availability Groups

3. Proponowane rozwiązanie musi wspierać automatyczne wykrywanie instancji SQL

4. Proponowane rozwiązanie nie powinno wymagać skryptów wsadowych tworzonych przez użytkownika, które posiadały instrukcje tworzenia kopii zapasowych instancji baz danych SQL oraz logów transakcyjnych

5. Proponowane rozwiązanie musi zapewniać wykonywanie pełnych, różnicowych i dzienników transakcji kopii zapasowych baz danych SQL

6. Proponowane rozwiązanie nie może wykorzystywać metody log-shipping do ochrony logów transakcyjnych SQL

7. Proponowane rozwiązanie musi umożliwiać wykonywanie kopii zapasowych MS SQL Server poza hostem SQL Server, Instant Recovery oraz wykonywanie kopii zapasowych u dostawcy sprzętu.

8. Proponowane rozwiązanie musi wspierać pełne przywracanie i odzyskiwanie baz danych SQL

9. Proponowane rozwiązanie musi wspierać przywracanie grup plików SQL

10. Proponowane rozwiązanie musi wspierać przywracanie plików bazy danych SQL

11. Proponowane rozwiązanie musi wspierać przywracanie logów transakcyjnych SQL do określonego punktu w czasie

12. Proponowane rozwiązanie musi wspierać przywracanie logu transakcyjnego SQL do określonego punktu w czasie konkretnej transakcji

**Backup NDMP**

1. Proponowane rozwiązanie musi wspierać wykorzystanie protokołu Network Data NDMP (Network Data Management Protocol) do inicjowania i sterowania kopiami zapasowymi i przywracaniem systemów NAS (Network Attached Storage)

2. Proponowane rozwiązanie musi obsługiwać NDMP v2, v3 i v4

3. Proponowane rozwiązanie musi wykorzystywać techniki wykrywania zmian w filerze w celu identyfikacji modyfikacji, które nastąpiły od momentu wykonania ostatniego backupu

4. Proponowane rozwiązanie musi obsługiwać lokalne i trójstronne kopie zapasowe NDMP

5. Proponowane rozwiązanie musi obsługiwać funkcję NDMP DirectCopy

6. Proponowane rozwiązanie musi umożliwiać przywracanie pojedynczych plików z kopii zapasowych NDMP

7. Proponowane rozwiązanie musi obsługiwać funkcję NDMP Direct Access Recovery (DAR)

**Raportowanie**

1. Proponowane rozwiązanie musi posiadać możliwość centralnego zarządzania, monitorowanie i raportowanie w odniesieniu do środowisk oprogramowania i urządzeń, w tym wielu środowisk backupowych

2. Proponowane rozwiązanie musi umożliwiać wysyłanie powiadomień o zadaniach za pomocą poczty elektronicznej lub SNMP

**Odporność na Ransomware**

1. Proponowane rozwiązanie musi posiadać wbudowany mechanizm wykrywania i powiadamiania o podejrzanych zmianach podczas tworzenia kopii zapasowych

2. Proponowane rozwiązanie musi posiadać własny skaner złośliwego oprogramowania oraz mieć możliwość integracji z zewnętrznymi skanerami złośliwego oprogramowania w celu skanowania składowanych obrazów kopii zapasowych

3. Proponowane rozwiązanie musi posiadać możliwość automatycznego wstrzymywania zadań kopii zapasowych dla chronionego zasobu po wykryciu infekcji w jego kopii zapasowej, powinno obejmować tworzenie nowych kopii zapasowych, ich powielanie i wygaszanie

4. Proponowane rozwiązanie musi posiadać możliwość identyfikowania ostatniej znanej dobrej kopii zapasowej przed przywróceniem maszyny wirtualnej

Zamawiający wymaga przeprowadzenie szkoleń stacjonarnych w min. wymiarze 24 godzin dla pracowników IT z zakresu dostarczonych rozwiązań EDR, NextGeneretion Firewall, System do backup-u, systemu do inwentaryzacji.

**Program szkolenia dla NextGeneretion Firewall musi obejmować min. :**

* Wprowadzenie i wstępna konfiguracja
* Polityki zapory sieciowej
* Translacja adresów sieciowych (NAT)
* Uwierzytelnianie użytkowników
* Logowanie i monitoring
* Operacje oparte na certyfikatach
* Filtr stron www
* Kontrola aplikacji
* Antywirus
* System ochrony przed włamaniami i atakami DoS
* Koncepcja Security Fabric

**Program szkolenia dla Systemu do backup-u musi obejmować min. :**

* Tworzenie możliwości tworzenia kopii zapasowych
* Tworzenie możliwości replikacji
* Dodatkowe kopie zapasowe
* Zaawansowane możliwości repozytorium
* Ochrona danych w chmurze
* Przywracanie z kopii zapasowej
* Odzyskiwanie z repliki
* Testowanie kopii zapasowych i replikacji
* Kopia zapasowa konfiguracji

Zamawiający wymaga, aby szkolenia w zakresie NextGeneretion Firewall oraz Systemu do backup-u były przeprowadzone przez trenerów posiadających najwyższe certyfikaty producentów oferowanych rozwiązań.

Po przeprowadzanych szkoleniach Zamawiający wymaga wystawienia stosownych certyfikatów potwierdzających odbycie szkolenia.

**Wymagania w zakresie instalacji i konfiguracji dostarczanego sprzętu i oprogramowania :**

1. Montaż serwerów w posiadanej szafie rack 42U w pomieszczeniu udostępnionym przez Zamawiającego.
2. Podłączenie serwera i NAS-a do listw zasilających PDU.
3. Aktualizacja oprogramowania układowego wszystkich komponentów.
4. Instalacja przełączników , konfiguracja zabezpieczeń w tym MAC-to\_VLAN
5. Podłączenie do sieci LAN ( rekonfiguracja przełączników )
6. Konfiguracja RAID serwera.
7. Instalacja i konfiguracja systemu operacyjnego.
8. Konfiguracja systemu zdalnego zarządzania.
9. Instalacja , uruchomienie i konfiguracja systemu backupowego na NAS.
10. Opracowanie polityki backupu .
11. Wymagane jest wykonanie testowego backupu oraz odtworzenia z weryfikacją prawidłowości działania systemów odtworzonych .
12. Wykonawca po zainstalowaniu i skonfigurowaniu sprzętu i oprogramowania będzie miał obowiązek przeprowadzenia instruktażu dla administratorów Zamawiającego w zakresie konfiguracji i zarządzania dostarczonego sprzętu oraz oprogramowania.