

Znak sprawy: RSO.OM.042.2.2025

ZAŁĄCZNIK NR 1 DO SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

na dostawę i wdrożenie infrastruktury sprzętowej
oraz oprogramowania dla Gminy Ciasna

Ciasna 2025

Spis treści

ROZDZIAŁ I. ZAŁOŻENIA POCZĄTKOWE ORAZ WYMAGANIA OGÓLNE
3

I.1 WPROWADZENIE I CEL PROJEKTU	3
I.2 AKTY PRAWNE.....	3
I.3 OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA.....	3
I.4 TERMIN REALIZACJI PRZEDMIOTU ZAMÓWIENIA.....	6
I.5 ORGANIZACJA WDROŻENIA	6
I.6 PRZYGOTOWANIE DOKUMENTACJI.....	7
I.7 HARMONOGRAM WDROŻENIA.....	8
I.8 ANALIZA PRZEDWDROŻENIOWA.....	8
I.9 DOKUMENTACJA POWYKONAWCZA	9
I.10 ODBIÓR DOKUMENTACJI/KOŃCOWY	10
I.11 TESTY	10
I.12 DODATKOWE ZOBOWIĄZANIA WYKONAWCY	10

ROZDZIAŁ II. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA
11

II.1 DOSTAWA I WDROŻENIE INFRASTRUKTURY SPRZĘTOWEJ I OPROGRAMOWANIA	11
II.3 DOSTAWA I WDROŻENIE SERWERA BACKUP	12
II.4 DOSTAWA I WDROŻENIE SERWERA NAS	16
II.5 OPRACOWANIE PROJEKTU WYKONAWCZEGO BACKUPU ORAZ POLITYKI I HARMONOGRAMU TWORZENIA KOPII ZAPASOWYCH, OBEJMUJĄCEGO WYKONYWANIE KOPII ZAPASOWYCH NA DYSKACH SERWERA KOPII ZAPASOWEJ ORAZ SERWERA NAS	21
II.6 DOSTAWA ZESTAWU TAŚM DO BIBLIOTEKI TAŚMOWEJ RDX 4TB.....	23
II.7 DOSTAWA I INSTALACJA ZASILACZA AWARYJNEGO UPS DO SZAFY RACK – 2 SZT.	24
II.8 DOSTAWA ZASILACZY AWARYJNYCH UPS DO STANOWISK PRACY – 30 SZT.....	26
II.9 DOSTAWA I WDROŻENIE OPROGRAMOWANIA BACKUP	28
II.10 ZAKUP OPROGRAMOWANIA SERWEROWEGO SYSTEMU OPERACYJNEGO.....	33
II.11 DOSTAWA I WDROŻENIE ZARZĄDZALNYCH URZĄDZEŃ SIECIOWYCH DLA RDZENIA SIECI – 2 SZT.....	37
II.12 DOSTAWA I WDROŻENIE ZARZĄDZALNYCH URZĄDZEŃ SIECIOWYCH DLA PUNKTÓW DOSTĘPOWYCH – 3 SZT.....	40
II.13 DOSTAWA I WDROŻENIE SYSTEMU DLP	44
II.14 USŁUGA KOMPLEKSOWEGO PRZEGLĄDU I REORGANIZACJI POSIADANEGO ŚRODOWISKA SERWEROWEGO, DOMENY, WRAZ Z MECHANIZMEM REPLIKACJI	49
II.15 ZAKUP, DOSTAWA I WDROŻENIE OPROGRAMOWANIA SIEM WRAZ Z DEDYKOWANYM SERWEREM FIZYCZNYM... ..	54
II.16 ZAKUP USŁUGI SOC ZAPEWNIAJĄCYCH PREWENCJĘ, DETEKCJĘ I REAKCJĘ NA ZAGROŻENIA CYBERBEZPIECZEŃSTWA.....	70
II.17 SZKOLENIE ADMINISTRATORÓW ZARZĄDZANIA USŁUGĄ ACTIVE DIRECTORY W ŚRODOWISKU MICROSOFT WINDOWS SERVER 2019/2022.....	89
II.18 DOSTAWA I WDROŻENIE OPROGRAMOWANIA BACKUP SZKOLENIE ADMINISTRATORÓW Z UŻYWANYCH URZĄDZEŃ UTM NA POZIOMIE ODPOWIADAJĄCYM CERTIFIED STORMSHIELD NETWORK ADMINISTRATOR CSNA	90

ROZDZIAŁ III. GWARANCJA
93

III.1 WADY.....	95
-----------------	----

Rozdział I. Założenia początkowe oraz wymagania ogólne

I.1 Wprowadzenie i cel projektu

Gmina bierze udział w projekcie „Cyberbezpieczny Samorząd”, którego celem jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego (JST) poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych.

Realizacja projektu poprzez wsparcie grantowe jednostek samorządowych, przyczyni się do:

- wdrożenia lub aktualizacji w JST polityk bezpieczeństwa informacji (SZBI),
- wdrożenia w JST środków zarządzania ryzykiem w cyberbezpieczeństwie,
- wdrożenia w JST mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni,
- podniesienia poziomu wiedzy i kompetencji personelu JST kluczowego z punktu widzenia SZBI wdrożonego w urzędzie,
- przeprowadzenia w JST audytów SZBI potwierdzających uzyskanie wyższego poziomu odporności na cyberzagrożenia.

I.2 Akty prawne

Dostarczone rozwiązania teleinformatyczne, ze szczególnym uwzględnieniem dostarczanego i wdrażanego Oprogramowania, muszą być zgodne z powszechnie obowiązującymi przepisami prawa polskiego i europejskiego. Rozwiązania muszą pozwalać na gromadzenie, przetwarzanie i analizowanie danych i informacji w obszarach objętych wdrożeniem.

I.3 Ogólny opis przedmiotu zamówienia

Dostawa i wdrożenie infrastruktury sprzętowej oraz oprogramowania dla Gminy Ciasna.

Przedmiot zamówienia niniejszego postępowania przetargowego obejmuje:

Poz. OPZ	Opis	Ilość sztuk/kpl
Rozdział	Rodzaj zamawianego asortymentu	
II.2	Zakup oprogramowania bezpieczeństwa dla używanego Urządzenia UTM	1 szt.
II.3	Dostawa i wdrożenie serwera backup	1 szt.
II.4	Dostawa i wdrożenie serwera NAS	1 szt.
II.5	Opracowanie projektu wykonawczego backupu oraz polityki i harmonogramu tworzenia kopii zapasowych, obejmującego wykonywanie kopii zapasowych na dyskach serwera kopii zapasowej oraz serwera NAS	1 szt.
II.6	Zakup zestawu taśm do biblioteki taśmowej RDX 4TB	4 szt.
II.7	Zakup i instalacja zasilacza awaryjnego UPS do szafy RACK	2 szt.
II.8	Dostawa zasilaczy awaryjnych UPS do stanowisk pracy	30 szt.
II.9	Dostawa i wdrożenie oprogramowania backup	1 szt.
II.10	Zakup oprogramowania Serwerowego Systemu Operacyjnego Windows Server 2022	2 szt.
II.11	Dostawa i wdrożenie zarządzalnych urządzeń sieciowych dla rdzenia sieci	2 szt.
II.12	Dostawa i wdrożenie zarządzalnych urządzeń sieciowych dla punktów dostępowych	3 szt.

II.13	Dostawa i wdrożenie systemu DLP	30 szt.
II.14	Usługa kompleksowego przeglądu i reorganizacji posiadanego środowiska serwerowego, domeny, wraz z mechanizmem replikacji	1 szt.
II.15	Zakup, dostawa i wdrożenie oprogramowania SIEM wraz z dedykowanym serwerem fizycznym	1 szt.
II.16	Zakup usługi SOC zapewniających prewencję, detekcję i reakcję na zagrożenia cyberbezpieczeństwa	1 szt.
II.17	Szkolenie administratorów zarządzania usługą Active Directory w środowisku Microsoft Windows Server 2019/2022	2 szt.
II.18	Szkolenie administratorów z używanych urządzeń UTM na poziomie odpowiadającym Certified Stormshield Network Administrator CSNA	2 szt.

1. Przedmiot zamówienia musi być dostarczany, wdrożony i zainstalowany w całości do siedziby Zamawiającego.
2. Wszystkie dostarczane:
 - Produkty (rozumiane jako elementarny efekt działań/prac/dostaw objętych całym zakresem Przedmiotu Zamówienia wykonywanych przez Wykonawcę podczas realizacji Umowy w poszczególnych Etapach).
 - Komponenty (rozumiane jako integralna część dostawy i wdrożenia Przedmiotu Zamówienia, składający się przynajmniej z jednego Produktu lub wielu Produktów powiązanych ze sobą merytorycznie) podlegają usługom projektowania, dostaw, instalacji, konfiguracji i wdrożenia.
3. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca przeprowadzi zgodnie z zapisami niniejszego SOPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów teleinformatycznych oraz najlepszymi praktykami w ich realizacji.
4. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, zapisami SOPZ oraz Umowy.

5. Tam, gdzie w opisie przedmiotu zamówienia został wskazany znak towarowy (marka), producent, dostawca, patent, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty dostarczone przez konkretnego Wykonawcę lub nastąpiło wskazanie norm, europejskich ocen technicznych, wspólnych specyfikacji technicznych lub innych odniesień, o których mowa w art. 101 ust. 1 pkt 2 lub ust. 3 ustawy, Zamawiający zgodnie z art. 99 ust. 5 ustawy dopuszcza złożenie oferty równoważnej lub zgodnie z art. 101 ust. 4 ustawy zaoferowanie rozwiązań „równoważnych” w stosunku do wskazanych w opisie przedmiotu zamówienia pod warunkiem, że zapewnią uzyskanie parametrów technicznych nie gorszych od założonych w SWZ.
6. Wykonawca musi dostarczyć wszelkie urządzenia i elementy, które są niezbędne do prawidłowego funkcjonowania całości. W przypadku, gdy w trakcie realizacji Przedmiotu Zamówienia okaże się, że brakuje jakiegokolwiek urządzenia, elementu i/lub licencji, którego brak spowoduje nieprawidłowe funkcjonowanie całości Przedmiotu Zamówienia, Wykonawca dostarczy je na własny koszt.
7. Wszelkie dostarczane urządzenia:
 - Muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych. Wszelkie dostarczane urządzenia muszą być wyprodukowane po dniu 1 stycznia 2025r.
 - Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.
 - Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.
 - Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
 - Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.
 - Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.

I.4 Termin realizacji Przedmiotu Zamówienia

Termin realizacji całości Przedmiotu zamówienia wynosi nie więcej niż **90 dni** kalendarzowych od dnia zawarcia Umowy.

I.5 Organizacja wdrożenia

Założenia podstawowe:

1. Przedmiot Zamówienia będzie realizowany w oparciu o zdefiniowany uprzednio przez Wykonawcę i zaakceptowany Harmonogram wdrożenia, który powinien być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia.
2. Wykonawca w Harmonogramie wdrożenia musi uwzględnić w szczególności podział na zadania takie jak projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.
3. Wykonawca umożliwi Zamawiającemu udział we wszystkich pracach realizowanych przez Wykonawcę w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie projektowania, dostawach, instalacji/budowie, konfiguracji i wdrożeniu i testowaniu).
4. Wykonawca zobowiązany jest do udziału w cyklicznych naradach przeglądu prac przez Zamawiającego. Zamawiający przewiduje częstotliwość narad maksymalnie 1 raz w miesiącu, chyba że, nadzwyczajna sytuacja w realizacji przedmiotu umowy wymagała będzie częstszych spotkań.
5. Wykonawca zobowiązany jest przeprowadzić dostawy Przedmiotu Zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
6. W przypadku dostarczania Infrastruktury Serwerowej musi być ona oznakowana w taki sposób, aby możliwa była identyfikacja systemowa zarówno produktu jak i producenta, pochodzić z oficjalnych kanałów dystrybucji producentów i dostarczona w oryginalnych opakowaniach fabrycznych.
7. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie Przedmiotu Zamówienia.
8. Wdrożenie będzie realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.
9. W ramach wdrożenia Wykonawca przygotowuje informacje na temat struktury organizacyjnej Zespołu Wykonawcy zajmującą się realizacją Przedmiotu Zamówienia, w ramach której muszą zostać powołane minimum następujące role:
 - a. Kierownik Projektu ze strony Wykonawcy,
 - b. Zespół Wdrożeniowy ze strony Wykonawcy
10. Wykonawca zorganizuje prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania prac u Zamawiającego.
11. Wykonawca musi uwzględnić, że wszystkie prace wykonywane będą w użytkowanych obiektach przy dużym ruchu pracowników i interesantów urzędu.

1.6 Przygotowanie Dokumentacji

1. W ramach procesu prac Wykonawca opracuje dla Zamawiającego Dokumentację Przedmiotu Zamówienia (zwaną dalej Dokumentacją), która składa się z nw. zakresów:
 - a) Harmonogram Wdrożenia.

- b) Dokumentacja Analizy Przedwdrożeńiowej (DAP).
 - c) Dokumentacja Powykonawcza.
2. Dokumentacja powyższa będzie zawierać bazowe zapisy opisujące budowane rozwiązania, procesy oraz sposób organizacji prac i wdrożenia. Na podstawie zapisów w Dokumentacji będą prowadzone i odbierane poszczególne etapy realizowane w ramach Przedmiotu zamówienia. Dokumenty te wraz ze Specyfikacją Warunków Zamówienia wraz z załącznikami (dalej zwanych SWZ) będą stanowiły podstawę do weryfikacji wdrożenia w trakcie odbiorów.
 3. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia i DAP warunkuje rozpoczęcie prac Wykonawcy.
 4. Dokumentacja Analizy Przedwdrożeńiowej DAP wraz z Harmonogramem wdrożenia zostaną opracowane w oparciu o wymagania określone w niniejszym SOPZ.

I.7 Harmonogram wdrożenia

Wykonawca zobowiązany jest opracować na podstawie SWZ oraz SOPZ szczegółowy harmonogram wdrożenia. Harmonogram należy przedstawić Zamawiającemu w terminie do 14 dni od podpisania Umowy.

I.8 Analiza Przedwdrożeńiowa

1. Analiza przedwdrożeńiowa, którą należy rozumieć jako zakres czynności do wykonania przez Wykonawcę mający na celu analizę środowiska biznesowego i informatycznego Zamawiającego. W wyniku przeprowadzenia Analizy Przedwdrożeńiowej Wykonawca przedstawi Zamawiającemu Dokumentację analizy przedwdrożeńiowej (zwana dalej DAP), na podstawie, której będzie realizowany organizacyjnie i technicznie Przedmiot Zamówienia. Dokumentacja Analizy Przedwdrożeńiowej będzie podlegała uzgodnieniu i akceptacji Zamawiającego.
2. Dokumentacja Analizy Przedwdrożeńiowej DAP powinna zawierać w szczególności:

SKŁAD DAP
ZARZĄDCZE
– plan i sposób komunikacji Stron
INFRASTRUKTURA SERWEROWA I SIECIOWA

- podział Przedmiotu Zamówienia na Produkty, a następnie ich pogrupowanie w Komponenty
- analizę wymagań Przedmiotu Zamówienia zawierającą opis sposobu realizacji wymagań, sposób testowania i odbioru
- karty katalogowe urządzeń potwierdzające spełnienie wymagań
- plan dostaw
- opis instalacji i wdrożenia oprogramowania wdrażanego wraz z Infrastrukturą
- Procedura testowania – scenariusze testowe dla wdrażanych systemów
- harmonogram instruktażu personelu oraz administratorów

1.9 Dokumentacja Powykonawcza

1. Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową, techniczną i eksploatacyjną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej w formacie edytowalnym oraz w co najmniej jednym egzemplarzu papierowym.
2. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.
3. Wykonawca wraz z dokumentacją powykonawczą dostarczy propozycję scenariuszy testowych, które będą podlegały akceptacji Zamawiającego.
4. W szczególności dokumentacja ta powinna zawierać następujące elementy:
 - a. Schemat infrastruktury i architekturę rozwiązania wraz z opisem.
 - b. Zasady licencjonowania dostarczonych elementów.
 - c. Konfigurację sprzętową i logiczną elementów infrastruktury dla wdrożonych systemów.
 - d. Procedury uruchamiania, zatrzymywania wdrożonych systemów oraz elementów infrastruktury.
 - e. Procedury konfiguracji kont w dostarczonych systemach.
 - f. Procedury awaryjne umożliwiające dostęp do infrastruktury w przypadku awarii.
 - g. Procedury opisujące standardowe działania administracyjne.
 - h. Procedury odzyskania wdrożonych systemów po awarii.
 - i. Wytyczne (dobre praktyki) dla administratorów.
 - j. Spis dokumentacji zewnętrznej do której odwołuje się Dokumentacja Powykonawcza.

I.10 Odbiór Dokumentacji/Końcowy

1. Odbiór końcowy Przedmiotu Zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy oraz dostarczenia wymaganej zamówieniem Dokumentacji.
2. Odbiory będą odbywać się zgodnie z zapisami w Umowie stanowiącej Załącznik nr 8 do SWZ.

I.11 Testy

1. W ramach postępowania zostaną przeprowadzone wszystkie testy opisane w Dokumentacji. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji Przedmiotu Zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale Zamawiającego jak i wskazanych przez Zamawiającego osób lub podmiotów zewnętrznych.
2. Pozytywne zakończenie testów wraz z usunięciem wskazanych Wad jest niezbędne, aby dla poszczególnych Komponentów oraz całego Przedmiotu Zamówienia dokonać odbiorów w ramach poszczególnych Etapów i Odbioru końcowego.
3. Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. Koszt zewnętrznego audytora będzie kosztem Zamawiającego. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.
4. Zamawiający w końcowej fazie wdrożenia oczekuje realizacji przez Wykonawcę testów bezpieczeństwa.
5. W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed odbiorem Końcowym Przedmiotu Zamówienia.
6. Zamawiający wymaga, aby Wykonawca przeprowadził testy odbiorcze co najmniej z zakresu:
 - a) Uruchamianie i zatrzymywanie wdrożonych systemów
 - b) Weryfikacja wdrożonych systemów zgodnie ze scenariuszami opisanymi w dokumentacji.
 - c) Weryfikacja poprawności działania procedur.
 - d) Symulację awarii wdrożonych systemów.

I.12 Dodatkowe zobowiązania Wykonawcy

1. Wykonanie Przedmiotu Zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.

2. Wykonanie w całości Przedmiotu Zamówienia w zakresie określonym w Umowie będącej Załącznikiem nr 8 do SWZ.
3. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającym na każdym etapie realizacji.
4. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.
5. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
6. Współdziałanie z osobami wskazanymi przez Zamawiającego.

Szczegółowy opis przedmiotu zamówienia

II.1 Dostawa i wdrożenie infrastruktury sprzętowej i oprogramowania

1. Jeżeli zajdzie potrzeba, wraz z dostarczaną Infrastrukturą, Wykonawca zobowiązany jest dostarczyć niezbędne elementy np. urządzenia i wyposażenie – kable połączeniowe, elementy mocujące, uznane przez Wykonawcę za niezbędne i umożliwiające prawidłowe działanie dostarczanej infrastruktury. Dostarczona Infrastruktura musi zapewniać bezproblemową pracę po podłączeniu do sieci informatycznej Zamawiającego.
2. Wykonawca jest zobowiązany dokonać montażu dostarczonej Infrastruktury oraz oprogramowania w miejscach wskazanych przez Zamawiającego.
3. Wszystkie elementy Infrastruktury serwerowej powinny zostać zamontowane w szafie serwerowej rack, w sposób umożliwiający ich prawidłową wentylację.
4. Szczegóły dotyczące instalacji i uruchomienia Infrastruktury zostaną ustalone w trakcie prac nad harmonogramem wdrożenia.

Po zakończonym montażu Wykonawca przekaze Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników” oraz dokumentację do wszystkich oferowanych urządzeń, oprogramowania narzędziowego (systemowego, bazodanowego, wirtualizacyjnego, backupowego itd.) wraz z dokumentami potwierdzającymi nabycia dla Zamawiającego licencji oraz nośnikami danych zawierającymi zainstalowane oprogramowanie (o ile dostarcza je producent). Wykonawca wykona

również instruktaże użytkowe dla wskazanych przez Zamawiającego administratorów, z zakresu konfiguracji, obsługi i prawidłowej eksploatacji zainstalowanego Sprzętu.

II.2 Zakup oprogramowania bezpieczeństwa dla używanego urządzenia UTM

Zamawiający użytkuje urządzenie klasy UTM Stormshield SN210 o numerze seryjnym: SN210A29D8255A7. Należy przedłużyć komplet posiadanych serwisów: UTM Security Pack (FW+IPS, VPN, filtr URL, AV, AS, Obsługa kart SD) na kolejne 12 miesięcy.

II.3 Dostawa i wdrożenie serwera backup

Wymagane jest dostarczenie 1 szt. serwera spełniającego poniżej opisane minimalne parametry funkcjonalne:

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami umożliwiającymi wysunięcie i wszystkimi elementami niezbędnymi do zamontowania serwera w szafie).
Procesor	Procesor max. 16 rdzeniowy, osiągający w teście SPECrate®2017_int_base wynik co najmniej 174 punkty. Płyta główna obsługująca procesory od 16 do 128 rdzeni, wymagających mocy 400W i obsługujących do 3TB pamięci RAM.
Liczba procesorów	Min. 1
Pamięć operacyjna	Zainstalowanych min. cztery moduły 32 GB DDR5 4800MT/s każdy. Płyta główna z minimum 12 slotami na pamięć, umożliwiającą instalację do minimum 3TB pamięci RAM, obsługująca moduły 6400 MT/s Obsługa zabezpieczeń: min. Advanced ECC.
Sloty rozszerzeń	Możliwość instalacji do min. 6 kart PCI-Express generacji 5 pełnej wysokości, x16(szybkość slotu – bus width).
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę min. 8 napędów dyskowych oraz obsługujący poziomy: RAID 0,1,10,5,50,6,60, nie zajmujący gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.
Dysk twardy	Możliwość instalacji do 20 dysków 3,5”. Zatoki dyskowe gotowe do zainstalowania dysków Hot Swap SAS/SATA/SSD. Zainstalowane min. 2 dyski

	min. 480 GB SSD na system operacyjny oraz 6 dysków o pojemności min. 16TB SATA 7200rpm każdy.
Interfejsy sieciowe	Zainstalowana karta sieciowa z dwoma portami 10/25Gb SFP+/SFP28, wraz z modułami SFP+. Zainstalowana karta 1Gb 4- portowa BASE-T. Karty sieciowe nie mogą zajmować slotów PCI-ex.
Karta graficzna	Zintegrowana karta graficzna z pamięcią min. 16 MB , umożliwiającą wyświetlenie obrazu min. 1920 x 1200@60Hz
Porty	Min. 4 porty USB 3.2 wbudowane (w tym min. 1 port wewnętrzny i 1 z przodu obudowy) 1 port VGA Możliwość rozbudowy/rekonfiguracji o port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express 1x port RJ-45 dedykowany dla interfejsu zdalnego zarządzania
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy maximum 1000W, efektywność zasilacza min. 94%
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) z dedykowanym portem RJ45 pozwalającą na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe i nie zajmująca wymaganych slotów PCI. Jeśli jest wymagana to załączona odpowiednia licencja.
Karta/moduł zarządzający i system zarządzania	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slotcie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: <ul style="list-style-type: none"> • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez

- dedykowany port RJ45 z tyłu serwera lub
- przez współdzielony port zintegrowanej karty sieciowej serwera

dostęp do karty możliwy

- z poziomu przeglądarki internetowej (GUI)
 - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)
 - z poziomu skryptu (XML/Perl)
 - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)
- wbudowane narzędzia diagnostyczne
 - zdalna konfiguracja serwera (BIOS) i instalacji systemu operacyjnego
 - obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przysyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie
 - wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
 - przysyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)
 - obsługa zdalnego serwera logowania (remote syslog)
 - wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów
 - mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie
 - funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności
 - monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji
 - konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)
 - zdalna aktualizacja oprogramowania (firmware)
 - zarządzanie grupami serwerów, w tym:
 - tworzenie i konfiguracja grup serwerów

	<ul style="list-style-type: none"> - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power capping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz IPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	<p>Min. Microsoft Windows Server 2019, 2022, 2025</p> <p>Min. Red Hat Enterprise Linux (RHEL): 8.6, 9.0</p> <p>Min. SUSE Linux Enterprise Server (SLES) 15</p> <p>Min. VMware ESXi 7.0 U3, 8.0</p>
Gwarancja	<p>Minimum 3-letnia gwarancja na części, robociznę i naprawę w miejscu instalacji typu On-Site z 2 godzinnym czasem reakcji na zgłoszenie. Rozpoczęcie naprawy w miejscu instalacji w następnym dniu roboczym. Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń.</p> <p>Możliwość rozszerzenia usługi gwarancyjnej do 5 lat realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy 6 godzin i pozostawieniem uszkodzonych dysków u zamawiającego.</p>
Inne	<p>Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.</p> <p>Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.</p>

Wykonawca dostarczy serwer, zainstaluje w szafie rack, skonfiguruje do pracy w sieci Zamawiającego. Zainstaluje system operacyjny na dyskach SSD, utworzy RAID 6 na dyskach 16TB. W celu skrócenia czasu tworzenia kopii zapasowych z obecnie eksploatowanych serwerów Zamawiającego konieczne będzie podłączenie serwerów do nowego rdzenia sieci LAN poprzez szybkie połączenia 10Gbit. Wszystkie prace muszą się odbywać poza godzinami pracy Zamawiającego, w wyznaczonym oknie serwisowym.

II.4 Dostawa i wdrożenie serwera NAS

Wykonawca dostarczy, zainstaluje w szafie rack, skonfiguruje do pracy sieci Zamawiającego, zintegruje urządzenie z użytkowaną przez Zamawiającego domeną Active Directory. Urządzenie będzie przeznaczone do przechowywania kopii zapasowych systemów Zamawiającego oraz kopii danych/plików użytkowników. Urządzenie musi umożliwiać wykonanie kopii zapasowej przy pomocy oprogramowania opisanego w punkcie II.9 SOPZ. Urządzenie musi spełniać poniższe wymagania minimalne:

Typ urządzenia	Serwer plików NAS
Procesor	Architektura min. 64 bit
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 4GB DDR4
Pamięć RAM liczba slotów	Minimum 1 slot
Pamięć Flash	Nie mniej niż 512MB
Liczba zatok na dyski twarde	Minimum 8
Obsługiwane dyski twarde	Min. 3.5" oraz 2.5" SATA
Pojemność możliwych do stosowania dysków twardych	do min. 20TB
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej dwóch
Porty LAN	Minimum 2 x 2,5 Gb/s
Porty LAN 10 Gb/s	Minimum 2 złącza SFP+

Diody LED	Minimum Status, LAN, HDD,
Porty USB 3.2	Minimum 4
Port PCIe umożliwiające rozbudowę urządzenia o dodatkowe karty rozszerzeń	Tak, minimum 1
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 2U
Dopuszczalna temperatura pracy	od 0 do 40°C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Zasilacz redundantny max. 2x260 W, 100-240 V
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie wolumenów	min. AES 256
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, 50, 60, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku)

	Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek woluminów i LUN blokowych Obsługa replikacji migawek
Dyski twarde	Zainstalowanych 8 dysków o pojemności min. 20TB każdy, dyski klasy enterprise, znajdujące się na liście kompatybilności producenta NAS, o parametrach: prędkość obrotowa 7200, MTBF min. 2,48 mln godzin, cache min. 500MB,
Wbudowana obsługa iSCSI	Multi-LUN na Target Obsługa LUN Mapping & Masking Obsługa MPIO Migawka LUN Kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,

Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring i zarządzanie urządzeniem Synchronizacja plików Obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediiów UPnP Serwer pobierania (HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Zarządzanie zdarzeniami systemowymi, rejestr, bieżące

	<p>połączenie użytkowników on-line</p> <p>Aktualizacja oprogramowania</p> <p>Ustawienia: Back up, przywracania, resetowania systemu</p>
Konteneryzacja	<p>Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker</p>
Zabezpieczenia	<p>Filtracja IP</p> <p>Ochrona dostępu do sieci z automatycznym blokowaniem oraz blokowanie na podstawie Geolokalizacji</p> <p>Połączenie HTTPS</p> <p>FTP z SSL/TLS (Explicit)</p> <p>Obsługa SFTP (tylko admin)</p> <p>Szyfrowanie AES 256-bit</p> <p>Szyfrowana zdalna replikacja (Rsync poprzez SSH)</p> <p>Import certyfikatu SSL</p> <p>Powiadomienia o zdarzeniach za pośrednictwem Email i SMS</p>
Liczba połączeń współbieżnych (CIFS) dla oferowanej konfiguracji	Min. 700
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek

Gwarancja	<p>Urządzenie NAS: 3 lata gwarancji oraz serwisu realizowanego przez producenta serwera min. door-to-door</p> <p>Dyski twarde: 5 lat gwarancji producenta min. door-to-door</p>
-----------	---

II.5 Opracowanie projektu wykonawczego backupu oraz polityki i harmonogramu tworzenia kopii zapasowych, obejmującego wykonywanie kopii zapasowych na dyskach serwera kopii zapasowej oraz serwera NAS

System backup zostanie wdrożony w taki sposób, aby był zgodny z zasadą 3-2-1. Jest to strategia tworzenia kopii zapasowych danych zaprojektowana w celu zapewnienia możliwości szybkiego odzyskania i przywrócenia danych w przypadku incydentu utraty danych. W szczególności ta strategia tworzenia kopii zapasowych musi zapewniać posiadanie trzech niezależnych kopii danych:

- Pierwsza kopia będzie przechowywana lokalnie na wewnętrznych dyskach twardej serwera backupowego,
- Druga kopia będzie przechowywana na serwerze NAS,
- Trzecia kopia danych będzie przechowywana na nośnikach wymiennych (napędu RDX),

Celem wdrożenia strategii tworzenia kopii zapasowych 3-2-1 jest zmniejszenie potencjalnego wpływu „pojedynczego punktu podatności na awarię”. Oznacza to, że jeśli jedno z urządzeń ulegnie awarii i znajdująca się na nim kopia danych zostanie utracona, do dyspozycji są jeszcze pozostałe dwie kopie danych. Wyniesienie nośników wymiennych RDX poza budynek Gminy umożliwia natomiast odzyskanie kluczowych danych Zamawiającego w przypadku awarii dużych rozmiarów bądź fizycznego zniszczenia siedziby Zamawiającego (pożar, wybuch, działania terrorystyczne, klęski żywiołowe).

Kluczowym elementem wdrożenia jest opracowanie polityki backupowej, w której opisane zostaną wszystkie zasady, według których będą tworzone kopie zapasowe z wyszczególnieniem kto je wykonuje, kiedy, gdzie przenoszone będą nośniki danych oraz kto będzie odpowiedzialny za poszczególne etapy wykonywania czynności, kto będzie odpowiedzialny za monitoring i weryfikację tworzonych kopii zapasowych.

Polityka backup oraz uruchomione środowisko backup musi być również zgodne z rekomendacją dotyczącą wykonywania kopii zapasowych opublikowaną pod adresem:

<https://www.gov.pl/web/baza-wiedzy/tworzenie-zapasowych-kopii-danych>

Wymagany zakres prac do wykonania w ramach zadania Backup 3-2-1:

1. System do tworzenia kopii na nośnikach wymiennych, niezbędnych licencji oprogramowania do

- tworzenia kopii zapasowych z wsparciem technicznym oraz dostępem do aktualizacji
2. Instalacja, konfiguracja systemów do pracy w infrastrukturze Zamawiającego, uruchomienie; aktualizacja firmware; instalacja hypervizora na serwerze backupowym na potrzeby dostarczonego oprogramowania; konfiguracja maszyny wirtualnej dla systemu backupu; instalacja serwera/konsoli zarządzającej kopiami zapasowymi;
 3. Opracowanie polityki backupu 3-2-1 w oparciu o:
 - dostarczony sprzęt, oprogramowanie,
 - sprzęt Zamawiającego
 - przeprowadzoną analizę środowiska Zamawiającego (liczba maszyn wirtualnych, krytyczność systemu, wielkość maszyny wirtualnych czy ilość danych na serwerach fizycznych)

Na podstawie zebranych danych oraz wymagań Zamawiającego, Wykonawca opracuje Harmonogram tworzenia kopii zapasowych z podziałem na maszyny fizyczne/wirtualne; określeniem: częstotliwości tworzenia kopii pełnych, częstotliwości tworzenia kopii przyrostowych, częstotliwości tworzenia kopii na nośnikach wymiennych, częstotliwości weryfikacji poprawności tworzonych kopii zapasowych, częstotliwości i zakresu przeprowadzania testów odtworzeniowych. Na podstawie Harmonogramu Wykonawca skonfiguruje zadania backupowe na dostarczonym oprogramowaniu. Uruchomi tworzenie kopii zapasowych na serwerze backupowym, serwerze NAS oraz taśmach RDX (nośnikach wymiennych RDX). Na żądanie Zamawiającego Wykonawca skonfiguruje dodatkowo tworzenie kopii zapasowych na wskazanych przez Zamawiającego zasobach dyskowych lub chmurowych.

4. Począwszy od dnia uruchomienia tworzenia kopii zapasowych, Wykonawca będzie zobowiązany do monitorowania pracy systemu backupowego przez min. 7 dni. Nadzór będzie miał na celu potwierdzenie prawidłowości wykonywanych kopii na serwerze oraz nośnikach wymiennych; potwierdzenie tworzenia kopii zgodnie z Harmonogramem.
5. Po zakończeniu pełnego cyklu tygodniowego tworzenia kopii zapasowych zgodnie z Harmonogramem, Wykonawca odtworzy wszystkie serwery fizyczne/maszyny wirtualne z kopii zapasowych na serwerze backupowym. Testy odtworzeniowe będą przeprowadzone przy udziale administratora Zamawiającego
6. Po okresie monitorowania, na podstawie potwierdzenia przez Zamawiającego zgodności wykonywanych kopii zgodnie z Harmonogramem oraz na podstawie zakończonych sukcesem testów odtworzeniowych, Wykonawca przeprowadzi instruktaż z zakresu:
 - bieżącej obsługi systemu, podstaw administracji,
 - modyfikacji Harmonogramu i zadań backupowych,
 - czynności sprawdzania prawidłowości wykonywanych kopii zapasowych na serwerze oraz

- nośnikach wymiennych,
- procedury i czynności przeprowadzania testów odtworzeniowych,
7. Ostatnim etapem wdrażania systemu backupu 3-2-1 jest opracowanie dokumentacji powykonawczej, która będzie zawierać opis wszystkich wykonanych prac, niezbędne dane konfiguracyjne, opis polityki backupowej wraz z harmonogramem oraz instrukcjami umożliwiającymi samodzielne użytkowanie, administrowanie wdrożonym środowiskiem przez Zamawiającego.

II.6 Dostawa zestawu taśm do biblioteki taśmowej RDX 4TB

Wykonawca dostarczy system do zapisywania kopii zapasowych na nośnikach wymiennych spełniający poniższe wymagania minimalne:

1. napęd w obudowie umożliwiającej przenoszenie z interfejsem min. USB 3.0
2. system musi być zasilany przez oferowany interfejs USB
3. musi obsługiwać tryby operacyjne jako dysk wymienny i dysk stały
4. średnia prędkość transferu danych min. 250 MB/s, w zależności od używanego nośnika
5. obsługa nośników wymiennych HDD o pojemności min. 4 TB oraz dysków SSD o pojemności min. 8 TB
6. Zgodność wstecznie i przyszłościowo z wszystkimi systemami przechowywania kopii bezpieczeństwa na nośnikach wymiennych, umożliwiając odczyt i zapis danych na różnych nośnikach
7. Dedykowane do oferowanego napędu nośniki muszą być odporne na upadek z wysokości min. 1 m na płytki betonowe
8. Napęd musi wytrzymać min. 10,000 cykli włożenia i wyjęcia taśmy
9. Pojedyncza taśma musi wytrzymać min. 5,000 cykli włożenia i wyjęcia
10. średni czas między awariami (MTBF) oferowanej taśmy co najmniej 550,000 godzin
11. odporność na wibracje min. 0,5G w stanie operacyjnym i min. 1,0G w stanie nieoperacyjnym
12. temperaturowy zakres pracy od min. od +10°C do +40°C w stanie operacyjnym
13. system musi wspierać szyfrowanie sprzętowe min. FIPS 140-2 na SATA III oraz szyfrowanie programowe
14. system musi umożliwiać archiwizowanie danych z funkcją WORM np. z użyciem odpowiedniego oprogramowania, które może być opcjonalnie certyfikowane przez niezależną jednostkę audytorską
15. system musi obsługiwać tryb dysku stałego dla narzędzia kopii zapasowych Windows we wszystkich wersjach USB 3.0
16. system do przechowywania kopii bezpieczeństwa na nośnikach wymiennych musi mieć możliwość konfiguracji jako nośniki startowe do szybkiego odzyskiwania systemu po awarii

17. system do przechowywania kopii bezpieczeństwa na nośnikach wymiennych musi obsługiwać min. systemy operacyjne: Windows, Mac OS i Linux oraz min. rozwiązania do tworzenia kopii zapasowych: Veeam, Veritas, Commvault, Arcserve
18. napęd należy dostarczyć wraz z kompletem 4 taśm o pojemności min. 4TB każda
19. gwarancja producenta na oferowane rozwiązanie min. 36 miesięcy

II.7 Dostawa i instalacja zasilacza awaryjnego UPS do szafy RACK – 2 szt.

Oferowane urządzenie do bezprzerwowego zasilania musi być fabrycznie nowe i pochodzić z seryjnej produkcji. Producent oferowanego urządzenia powinien posiadać własny certyfikat ISO 9001 oraz 14001 jako potwierdzenie wymagań międzynarodowego standardu jakości. Oferowane urządzenie musi posiadać oznakowanie CE. Na żądanie Zamawiającego Wykonawca przedstawi wymagane dokumenty. Oferent ma obowiązek przedstawienia karty katalogowej producenta urządzenia, karta dystrybutora własnej marki nie jest wystarczającym potwierdzeniem parametrów urządzenia. Zasilacz musi spełniać poniższe wymagania minimalne:

1. Moc wyjściowa UPS 3 kVA / 2,7 kW
2. Możliwość instalacji UPS Rack / Tower
3. Wysokość pojedynczego zasilacza UPS powinna wynosić 2U
4. Zakres napięcia wejściowego: 120 – 280V AC
5. THDi < 5%
6. Zakres dopuszczalnej częstotliwości wejściowej: 40 – 70Hz
7. Współczynnik mocy wejściowy: >0,99
8. Wyjściowy współczynnik mocy równy: 0,9
9. THDu < 2%
10. Regulacja napięcia wyjściowego: $\pm 1\%$
11. Dopuszczalne przeciążenie: < 105% praca ciągła; 106 – 125%: 1 min; 126 – 150%: 15 sek;
12. Minimalny czas podtrzymania dla obciążeń:
 - 100% min. 46 minut
 - 50% min. 103 minuty
 - 25% min. 205 minut

13. Gniazda wyjściowe IEC C13 – 6szt., IEC C19 – 1 szt.
 14. Funkcja REPO
 15. Urządzenie musi zapewnić ciągłe bezprzerwowe zasilanie w trybie TRUE ON-LINE z podwójną konwersją przy zupełnych lub chwilowych zanikach napięcia i wahaniach częstotliwości w sieci elektrycznej przez cały czas pracy urządzenia.
 16. Urządzenie powinno być wyposażone w komunikacyjny wyświetlacz LCD z odczytem parametrów elektrycznych wejścia/wyjścia i komunikatów o stanie pracy UPS
- Tryb Online
 - Tryb ECO
 - Tryb Bateriajny
 - Tryb konwersji częstotliwości
 - Napięcie wejściowe
 - Napięcie wyjściowe
 - Pojemność baterii
 - Czas podtrzymania
 - Wartość online XkVA
17. Preferowany kolor obudowy: czarny.
 18. Poziom hałasu urządzenia w trybie podwójnego przetwarzania przy obciążeniu znamionowym nie może przekraczać 46 dB.
 19. Sprawność w trybie TRUE ONLINE
 20. do 94% w trybie normalnym
 21. do 97% osiągnięte w ekonomicznym trybie pracy
 22. UPS musi posiadać panel komunikacyjny, w którym powinny być zainstalowane:
 - REPO
 - Gniazda umożliwiającej instalację karty SNMP z obsługą protokołu SNMP v1/v3 /Relay/Modbus
 - U1SB
 - Gniazdo komunikacji RS-232
 23. UPS musi posiadać regulację prędkości obrotowej wentylatorów uzależnioną od obciążenia oraz automatyczne wykrywanie awarii wentylatorów
 24. UPS musi posiadać programowalne gniazda wyjściowe umożliwiające odłączenie wybranych odbiorów
 25. UPS musi posiadać w zestawie szyny umożliwiającymi montaż w szafie RACK

26. UPS musi posiadać możliwość podłączenia dodatkowych zewnętrznych modułów bateryjnych każdy w celu wydłużenia czasu autonomii do 70 min dla 100% obciążenia - każdy o maksymalnej wysokości 2U.
27. UPS musi mieć możliwość podłączenia dodatkowego zewnętrznego bypassu o wysokości 2U z dystrybucją gniazd 6x IEC C13 + 1x IEC C19
28. UPS musi być dostarczony wraz z kartą SNMP z obsługą protokołu SNMP v1/v3
29. Oprogramowanie zarządzające z możliwością zamykania systemów operacyjnych poprzez sieć logiczną:
 - Windows 8, 10,11
 - Windows Serwer
 - Linux Opens USE, Ubuntu, Fedora
 - CentOS
 - Citrix XenServer
 - Linux KVM
 - VMWare ESXi
30. Gwarancja min. 24 miesięcy zarówno dla zasilacza UPS oraz dodatkowych modułów bateryjnych. Oferent dostarczy pisemną gwarancję producenta urządzenia, gwarancja dystrybutora nie jest wystarczająca. Producent zapewnia dostępność części zamiennych przez co najmniej 10 lat. Na żądanie Zamawiającego Wykonawca przedstawi wymagane dokumenty.

Wykonawca dostarczy, zainstaluje zasilacz w wskazanej szafie rack, podłączy wszystkie kluczowe urządzenia Zamawiającego, skonfiguruje kartę SNMP do współpracy z urządzeniami Zamawiającego. Zamawiający wymaga, aby osoba wykonująca usługę posiadała stosowne uprawnienia w zakresie wykonywania prac elektrycznych.

II.8 Dostawa zasilaczy awaryjnych UPS do stanowisk pracy – 30 szt.

W celu zapewnienia ciągłości działania stanowisk komputerowych wymagane jest dostarczenie zasilaczy awaryjnych, które umożliwią bezpieczne zakończenie pracy na stanowisku, na wypadek zaniku zasilania sieciowego. Wraz z zasilaczem należy dostarczyć oprogramowanie umożliwiające automatyczne zamknięcie systemu operacyjnego przez całkowitym rozładowaniem baterii zasilacza awaryjnego.

Minimalne wymagania dla zasilacza awaryjnego:

zasilacz awaryjny do stanowisk pracy	
Moc pozorna	mi. 650 VA
Moc czynna	Min, 400 W
Architektura UPS-a	off-line (standby)
Czas ładowania	Max. 4 h
Czas podtrzymania 100W	Min. 19,5 minuty
Czas podtrzymania 150W	Min. 14 minut
Czas podtrzymania 200W	Min. 9 minut
Typ obudowy	Rack / Tower
Zabezpieczenia / filtry	<ul style="list-style-type: none"> – Nadmierne rozładowanie – Przeciwprzepięciowe – Linii danych
Funkcje specjalne	<ul style="list-style-type: none"> – Ochrona linii transmisji danych – Automatyczny wyłącznik – Kontrolki LED + alarm dźwiękowy – Automatyczny test akumulatora – Ochrona przed głębokim rozładowaniem – Zimny start
Zarządzanie akumulatorem	<ul style="list-style-type: none"> – automatyczny test baterii – ochrona przed głębokim rozładowaniem – możliwość zimnego startu
Porty zasilania wyjściowe	3 gniazda wyjściowe z podtrzymaniem i ochroną + 1 z ochroną

Dolączone oprogramowanie	umożliwia min. bezpieczne zamknięcie systemu, pomiar zużycia energii oraz konfigurację ustawień zasilacza
Wymiary max.	Wysokość: 27 cm Głębokość: 24 cm Szerokość: 9 cm
Waga max.	Max. 3,8 kg
Akumulatory	Wymienialne szczelne baterie ołowiowo-kwasowe
Certyfikaty	Min. IEC/EN 62040-1; IEC/EN 62040-2; CE; EAC
Gwarancja producenta	Min. 36 miesięcy door-to-door

II.9 Dostawa i wdrożenie oprogramowania backup

W ramach realizacji zadania Wykonawca dostarczy licencje oprogramowania do tworzenia kopii zapasowej wszystkich maszyn wirtualnych działających na hostach Zamawiającego. Zainstaluje oprogramowanie, skonfiguruje do pracy w środowisku Zamawiającego, przeprowadzi testy odtworzeniowe, instruktaż z obsługi wdrożonego systemu tworzenia kopii.

Wymagane jest dostarczenie licencji bezterminowych z wsparciem technicznym przez okres min. 24 miesięcy dla 2 procesorów serwerów fizycznych Zamawiającego, spełniających poniższe wymagania minimalne:

1. Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji
 - a. Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012
 - b. Vmware vSphere min. w wersjach v5.5-7.0.3
 - c. Nutanix AHV 5.15, 5.20 (LTS)
 - d. Maszyny fizyczne: Windows Server 2022, 2019, 2016, 2012R2, 2012

- e. Microsoft 365 (Exchange online, One Drive for Business, Sharepoint, Teams)
2. Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V
3. Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:
 - a. na serwerze Windows lub Linux
 - b. jako maszyna wirtualna VMware
 - c. jako maszyna wirtualna Amazon
 - d. na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital
4. Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS
5. Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania
6. Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
7. Oprogramowanie ma umożliwiać wdrożenie schematu backupu według zasady 3-2-1
8. Oprogramowanie ma umożliwiać zapewnienie niezmienności kopii chroniąc przed oprogramowaniem ransomware z zastosowaniem niezmiennych kopii zapasowych (worm lub chmura) oraz ze szczeliną powietrzną (rozłączane taśmy, napędy usb lub nas)
9. Wszystkie funkcje i komponenty oprogramowania dla środowisk VMware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariantcie wieczystym, w którym licencja nie ma terminu ważności
10. W ramach dostawy wymagane jest dostarczenie licencji na ochronę min. 2 gniazd procesorów w hostach VMware lub Hyper-V
11. Dostarczona wersja oprogramowania i licencji, powinna mieć możliwość rozbudowy ilości chronionych zasobów w przyszłości
12. W ramach dostarczonej licencji wymagane jest zapewnienie wsparcia technicznego producenta, które umożliwi min. dostęp do aktualizacji i poprawek oprogramowania oraz umożliwia kontakt z działem technicznym producenta w zakresie obsługi oferowanego oprogramowania.
13. Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska
14. Oprogramowanie musi posiadać funkcje backupu i replikacji:
 - a. Backup maszyn wirtualnych VMware

- b. Replikacja maszyn wirtualnych VMware (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
- c. Backup maszyn wirtualnych Hyper-V
- d. Replikacja maszyn wirtualnych Hyper-V (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
- e. Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
- f. Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
- g. Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
- h. Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
- i. Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych
- j. Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem
- k. Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
- l. Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
- 15. Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
 - a. Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
 - b. Kompresja backupu, w tym konfigurowalny stopień kompresji
 - c. Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne
- 16. Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
 - a. Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
 - b. Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
 - c. Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji: Microsoft Exchange 2013, 2016, 2019
 - d. Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022

- e. Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
- 17. Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
- 18. Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
- 19. Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji
- 20. Oferowany system tworzenia kopii zapasowych musi umożliwiać wysyłanie zaszyfrowanych kopii zapasowych do zasobów chmurowych.
- 21. Oprogramowanie musi posiadać poniższe funkcje:
 - a. Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
 - b. Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)
 - c. Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
 - d. Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
 - e. Microsoft Exchange, MS Active Directory, MS SQL
 - f. Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.
- 22. Oprogramowanie do backupu musi pozwalać na:
 - a. Tworzenie backupu i replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
 - b. Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
 - c. Backup z pominięciem sieci LAN dzięki opcjom dostępu bezpośredniego w sieciach SAN
 - d. Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
 - e. Wsparcie dla urządzeń oferujących dodatkową deduplikację danych
- 23. Oprogramowanie musi pozwalać na następujące formy zarządzania:
 - a. Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
 - b. Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność

- odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
- c. Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania
 - d. wielu harmonogramów dla pojedynczego zadania
 - e. Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków, do których będzie robiony eksport.
 - f. Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
 - g. Oprogramowanie musi umożliwiać integrację z używaną przez Zamawiającego usługą katalogową Microsoft Active Directory

✓ **Instalacja, konfiguracja systemu do tworzenia kopii zapasowej**

Wykonawca przeprowadzi pełne wdrożenie oferowanego systemu kopii bezpieczeństwa, które będzie obejmować minimum:

1. instalację i konfigurację dostarczonego systemu kopii bezpieczeństwa na serwerze backupowym Zamawiającego
2. skonfigurowanie przestrzeni dla kopii bezpieczeństwa na serwerze backupowym Zamawiającego
3. konfigurację miejsc przechowywania, w tym urządzenia NAS, napędu taśmowego RDX
4. konfigurację polityki składowania oraz harmonogramów
5. konfigurację zabezpieczeń wewnętrznych, w tym kopii ratunkowej (ang. disaster recovery) systemu kopii bezpieczeństwa
6. instalację i konfigurację dodatkowych maszyn wirtualnych klientów, jeśli są wymagane, w środowisku Zamawiającego
7. konfigurację kopii zapasowych maszyn wirtualnych Zamawiającego dla dwóch repozytoriów: serwera backupowego, serwera NAS oraz napędu RDX
8. instalację niezbędnych agentów dla środowiska bazodanowego Zamawiającego i konfigurację kopii zapasowych baz danych
9. konfigurację automatycznej weryfikacji kopii bezpieczeństwa maszyn wirtualnych Zamawiającego.
10. konfigurację powiadomień i codziennych raportów

Wykonawca opracuje i przedstawi Zamawiającemu dokumentację powykonawczą zawierającą:

1. podstawowe procedury obsługowe

2. opis skonfigurowanych polityk i harmonogramów
3. opis odtworzenia maszyn wirtualnych
4. opis odtworzenia pojedynczego pliku
5. opis odtworzenia bazy danych Zamawiającego
6. opis sposobu aktualizacji systemu

Wykonawca przeprowadzi jednodniowy instruktaż w czasie do 21 dni kalendarzowych od daty zakończenia wdrożenia dla administratorów Zamawiającego, który obejmie co najmniej:

1. podstawową wiedzę dotyczącą systemu
2. dodawania i usuwanie z systemu maszyn wirtualnych
3. dodawanie i usuwanie z systemu fizycznych urządzeń
4. zagadnienia dotyczące zmian platform wirtualizacji
5. możliwości dodawania, zmiany i usuwania kolejnych miejsc przechowywania kopii zapasowych
6. procedurę aktualizacji systemu
7. procedurę odtworzenia konfiguracji po awarii dysków głównego serwera backupu, np. po ponownej instalacji hypervizora, systemu operacyjnego serwera

II.10 Zakup oprogramowania Serwerowego Systemu Operacyjnego

Minimalne wymagania dla licencji Serwerowego Systemu Operacyjnego (SS):

Należy dostarczyć 2 licencje bezterminowe na Serwerowy System Operacyjny – SSO. Dostarczone licencje muszą uprawniać do uruchamiania, na dwóch eksploatowanych przez Zamawiającego serwerach (max. 16 rdzeni na serwer), min. 2 maszyn wirtualnych. Dostarczone licencje muszą obejmować wszystkie rdzenie procesora zainstalowanego w serwerze. Serwerowy System Operacyjny musi posiadać następujące, wbudowane cechy minimalne:

1. Współpraca z procesorami o architekturze x86-64 bit
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Pojedyncza licencja musi obsługiwać serwer fizyczny wyposażony w 2 procesory po 8 rdzeni każdy.
4. Praca w roli klienta domeny Microsoft Active Directory.
5. System musi być wspierany przez producenta oprogramowania do 2030 r. (wsparcie techniczne, aktualizacje bezpieczeństwa)

6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2022.
7. Możliwość uruchomienia roli klienta i serwera czasu (NTP).
8. Możliwość uruchomienia roli serwera pliku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
9. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
10. Możliwość uruchomienia roli serwera stron WWW.
11. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiające wirtualizowanie zasobów sprzętowych serwera.
12. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
13. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania.
14. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
15. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
16. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
 - a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
17. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość
18. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
19. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilkoma serwerami.
20. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
21. Zlokalizowane w języku polskim lub angielskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
22. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
23. Mechanizmy logowania w oparciu o:
 - a. login i hasło,
 - b. karty z certyfikatami (smartcard),

- c. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
24. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
- określonych grup użytkowników.
 - zastosowanej klasyfikacji danych,
 - centralnych polityk dostępu w sieci,
 - centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
25. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
26. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
27. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
28. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
29. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
- podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
 - usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
 - zdalna dystrybucja oprogramowania na stacje robocze,
 - Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - Dystrybucję certyfikatów poprzez http,
 - Konsolidację CA dla wielu lasów domeny
 - Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen,
 - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
 - szyfrowanie plików i folderów,
 - szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
 - szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,

- h. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail - over) oraz rozłożenia obciążenia serwerów,
- i. serwis udostępniania stron WWW,
- j. wsparcie dla protokołu IP w wersji 6 (IPv6),
- k. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- l. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),
- m. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (Hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- n. mechanizmy wirtualizacji mające wsparcie dla:
 - a. dynamicznego podłączania zasobów dyskowych typu hot plug do maszyn wirtualnych,
 - b. obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - c. możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
 - d. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
 - e. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
 - f. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
 - g. mechanizm konfiguracji połączenia VPN do platformy Azure.
 - h. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
 - i. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
 - j. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard)

II.11 Dostawa i wdrożenie zarządzalnych urządzeń sieciowych dla rdzenia sieci – 2 szt.

Obecnie używane przez Zamawiającego przełączniki tworzące sieć LAN są przestarzałe, nie ma wydzielonych przełączników do rdzenia sieci, brak możliwości instalacji nowego oprogramowania wewnętrznego. Przedmiotem zadania jest dostawa 2 nowych przełączników umożliwiających utworzenie rdzeń sieci LAN. Wraz z przełącznikami należy dostarczyć wszystkie niezbędne moduły SFP+, przewody połączeniowe umożliwiające uruchomienie nowej sieci LAN oraz podłączenie urządzeń do nowych przełączników. Przełączniki muszą spełniać opisane niżej parametry minimalne:

Element konfiguracji	Wymagania minimalne
Fizyczne	Wysokość w szafie 19” – 1U, głębokość nie większa niż 250mm, możliwość montażu w szafie rack
Techniczne	Minimum 24 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). Minimum 2 porty SFP28, pozwalające na instalację wkładek 25Gbit. Minimum 1 port konsoli: RJ45
Wydajność	Pojemność matrycy przełączania: minimum 216 Gbps Wydajność: minimum 108 Gbps Tablica adresów MAC o wielkości minimum 32k pozycji
Procesor	Min. 1 procesor 650Mhz
Pamięć RAM	Min. 64 MB
Pamięć wbudowana	Min. 16 MB

Stackowanie / MLAG	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) lub możliwość wykonania MLAG (Multichassis Link Aggregation)
Funkcje minimalne	<p>Obsługa ramek Jumbo minimum 9k</p> <p>Routing IPv4 – minimum: statyczny, RIP, OSPF, BFD, VRF, VRRP</p> <p>Routing IPv6 – minimum: statyczny, RIPng, OSPF</p> <p>Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping</p> <p>Obsługa vxlan</p> <p>Obsługa Port isolation</p> <p>Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol</p> <p>Obsługa funkcji Loop Protect</p> <p>Obsługa funkcji Traffic Shaping</p> <p>Obsługa 4094 tagów IEEE 802.1Q oraz minimum 1000 jednoczesnych sieci VLAN z BPDU protection</p> <p>Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie lub MLAG</p> <p>Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping ze wsparciem opcji 82</p> <p>Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI</p> <p>Obsługa standardu 802.1p</p>

	<p>Funkcja mirroringu portów</p> <p>Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) lub CDP Cisco Discovery Protocol</p> <p>Funkcja autoryzacji użytkowników zgodna z 802.1x</p> <p>Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo RADIUS Accounting</p>
Zarządzanie	<p>Zarządzanie poprzez port konsoli (pełne),</p> <p>Musi wspierać możliwość zarządzania przez następujące protokoły:</p> <ul style="list-style-type: none"> • SNMP v.1, 2c i 3, • Telnet, SSH v.2, • http • https • Syslog • NTP <p>Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej</p>
Zasilanie	<p>Urządzenie musi być wyposażone w dwa redundantne, dedykowane zasilacze</p> <p>Możliwość zasilania PoE</p>
Wyposażenie	<p>Wraz z przełącznikiem należy dostarczyć niezbędne wkładki SFP+, przewody do redundantnego podłączenia wszystkich wskazanych przez Zamawiającego urządzeń do tworzonego rdzenia sieci LAN.</p> <p>Zestaw do montażu w szafie rack</p>

Gwarancja	Min. 24 miesiące gwarancji w miejscu instalacji
-----------	---

Zakres wdrożenia przełączników tworzących rdzeń sieci LAN:

Wykonawca dostarczy nowe urządzenia, przedstawi projekt wdrożenia przełączników do rdzenia sieci LAN Zamawiającego. Na podstawie zaakceptowanego projektu zainstaluje przełączniki w wskazanej szafie rack, skonfiguruje do pracy w sieci LAN Zamawiającego. Wszystkie prace muszą się odbywać poza godzinami pracy Urzędu, w oknie serwisowym wyznaczonym przez Zamawiającego. Projekt musi obejmować minimum:

- aktualizację oprogramowania układowego przełączników do najnowszej stabilnej wersji
- konfigurację sieci wirtualnych przełącznika na podstawie obecnej infrastruktury
- konfigurację agregacji połączeń do serwerów pomiędzy przełącznikami
- konfigurację agregacji połączeń dla przełączników dostępowych
- konfigurację syslog dla przełączników
- konfigurację protokołu SNMP zgodnie z obecnym systemem monitoringu
- konfigurację użytkowników administracyjnych przełącznika zgodnie z wytycznymi bezpieczeństwa

II.12 Dostawa i wdrożenie zarządzalnych urządzeń sieciowych dla punktów dostępowych – 3 szt.

Obecnie używane przez Zamawiającego przełączniki tworzące sieć LAN są przestarzałe, nie ma wydzielonych przełączników do rdzenia sieci, brak możliwości instalacji nowego oprogramowania wewnętrznego. Przedmiotem zadania jest dostawa 3 nowych przełączników dostępowych. Wraz z przełącznikami należy dostarczyć wszystkie niezbędne moduły SFP+ oraz przewody połączeniowe umożliwiające podłączenie przełączników dostępowych do rdzenia sieci LAN. Przełączniki muszą spełniać opisane niżej parametry minimalne:

Cecha	Wymagania minimalne
Fizyczne	Wysokość w szafie 19” – 1U, głębokość nie większa niż 150mm, możliwość montażu w szafie rack

Techniczne	<p>Minimum 24porty gigabitowe w standardzie 100/1000BaseT</p> <p>Minimum 2 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP).</p> <p>Dedykowany port konsoli zarządzającej RJ-45</p>
Wydajność	<p>Prędkość matrycy przełączania: minimum 78Gbps</p> <p>Wydajność: minimum 60Mpps</p> <p>Tablica adresów MAC o wielkości minimum 16k pozycji</p>
Procesor	Min. 750Mhz
Pamięć RAM	Min. 500MB
Pamięć wbudowana flash	Min. 15MB
Stackowanie / MLAG	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) lub możliwość wykonania MLAG (Multichassis Link Aggregation)
Funkcje minimalne	<p>Obsługa ramek Jumbo minimum 9k</p> <p>Routing IPv4 – minimum: statyczny, RIP, OSPF, BFD, VRF, VRRP</p> <p>Routing IPv6 – minimum: statyczny, RIPng, OSPF</p> <p>Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping</p> <p>Obsługa vxlan</p> <p>Obsługa Port isolation</p>

	<p>Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol</p> <p>Obsługa funkcji Loop Protect</p> <p>Obsługa funkcji Traffic Shaping</p> <p>Obsługa 4094 tagów IEEE 802.1Q oraz minimum 1000 jednoczesnych sieci VLAN z BPDU protection</p> <p>Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie lub MLAG</p> <p>Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping ze wsparciem opcji 82</p> <p>Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI</p> <p>Obsługa standardu 802.1p</p> <p>Funkcja mirroringu portów</p> <p>Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) lub CDP Cisco Discovery Protocol</p> <p>Funkcja autoryzacji użytkowników zgodna z 802.1x</p> <p>Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo RADIUS Accounting</p>
Zarządzanie	<p>Zarządzanie poprzez port konsoli (pełne),</p> <p>Musi wspierać możliwość zarządzania przez następujące protokoły:</p> <ul style="list-style-type: none"> • SNMP v.1, 2c i 3,

	<ul style="list-style-type: none"> • Telnet, SSH v.2, • http • https • Syslog • NTP <p>Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej</p>
Zasilanie	<p>Urządzenie musi być wyposażone w dedykowany zasilacz</p> <p>Możliwość zasilania PoE przez dedykowany port RJ-45</p>
Wyposażenie	<p>Zainstalowane 2 wkładki 10Gb SFP+ SR LC MM</p> <p>Dwa przewody światłowodowe LC-LC min. OM3 o długości min. 5m</p> <p>Zestaw do montażu w szafie rack</p>
Gwarancja	<p>Min. 24 miesiące gwarancji w miejscu instalacji</p>

Projekt i wdrożenie będzie obejmować minimum:

- aktualizacja firmware przełączników do najnowszej stabilnej wersji
- konfiguracja portów do zarządzania (management port)
- wymiana przełączników w szafie rack i podłączenie klientów z demontowanych przełączników
- podłączenie przełączników do rdzenia sieci LAN portami 10Gbit SFP+
- wykonanie testów poprawności działania po przełączeniu produkcyjnym

II.13 Dostawa i wdrożenie systemu DLP

Należy dostarczyć, zainstalować, skonfigurować system klasy DLP czyli system monitorowania i ochrony poufnych informacji, zapobiegania utracie danych, wyciekom danych. Wymagane jest dostarczenie licencji bezterminowej dla 30 urządzeń ze wsparciem technicznym na min. 24 miesiące. Minimalne wymagania dla systemu DLP:

1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10/Windows 11.
2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012 i nowszych.
3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim.
4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL oraz AzureSQL.
6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.
7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
8. Serwer administracyjny musi umożliwiać wykonanie instalacji/deinstalacji zdalnej klienta na stacjach roboczych.
9. Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem, a serwerem zarządzającym.
10. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.
11. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.
12. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania: kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.
13. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.
14. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania oraz edycji wyżej wymienionych kategorii.

15. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania.
16. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:
 - a. Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module,
 - b. Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.
17. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory.
18. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:
 - a. logowanie oraz wylogowanie użytkownika,
 - b. włączenie oraz wyłączenie stacji roboczej,
 - c. blokada oraz odblokowanie stacji roboczej,
 - d. przejście w stan bezczynności stacji roboczej.
19. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym.
20. Serwer administracyjny musi mieć możliwość ustawienia powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji.
21. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.
22. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików.
23. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF oraz XLS.
24. Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
25. Serwer musi posiadać możliwość wysyłania alertów, co najmniej za pośrednictwem wiadomości email.
26. Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.

27. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
28. Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail.
29. Serwer administracyjny musi posiadać domyślnie skonfigurowany serwer SMTP udostępniony przez producenta oprogramowania.
30. Serwer administracyjny musi umożliwiać kategoryzację (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku.
31. Serwer administracyjny musi umożliwiać wykonanie zadania kategoryzacji (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie już skategoryzowanych (otagowanych) plików.
32. Serwer administracyjny musi mieć możliwość kategoryzacji (tagowania) plików wrażliwych w oparciu o:
 - a. aplikacje, z której zostały utworzone,
 - b. lokalizację,
 - c. adres URL,
 - d. format pliku,
 - e. zawartość pliku.
33. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych jak i sieciowych.
34. Dla plików skategoryzowanych (otagowanych), musi być możliwe utworzenie następujących reguł:
 - a. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych,
 - b. blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń,
 - c. blokowanie oraz zezwalanie na drukowanie na określonych drukarkach,
 - d. blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej,
 - e. blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen,
 - f. blokowanie oraz zezwalanie na wysyłanie do poczty webowej,
 - g. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:
 - Dropbox,
 - Google Drive,

- SharePoint,
 - OneDrive Business,
 - OneDrive Personal.
- h. blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów,
- i. blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego,
- j. blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości oraz wirtualnego drukowania,
- k. uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikację,
35. Serwer administracyjny musi umożliwiać możliwość zabezpieczenia korzystania z niezaufanych repozytoriów GIT.
36. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.
37. Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.
38. Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę klasyfikacji na niższą.
39. Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających urządzenia pamięci masowej, drukarki fizycznych i sieciowych, lokalizacji sieciowych, adresów e-mail oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu.
40. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury.
41. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.
42. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
43. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika.
44. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych.
45. Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o:

- a. numery kart kredytowych,
 - b. numer PESEL,
 - c. numer polskiego dowodu osobistego,
 - d. polski numer paszportu,
 - e. wyrażenia regularne,
 - f. określone ciągi znaków,
 - g. numer IBAN.
46. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
47. Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition) z wsparciem języka polskiego.
48. System musi posiadać możliwość importu własnych słowników do wyszukiwania danych.
49. W przypadku incydentu bezpieczeństwa, system musi wykonać duplikat pliku lub wiadomości e-mail, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy”).
50. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie klasyfikacji (tagowania).
51. Serwer administracyjny musi posiadać możliwość integracji klasyfikacji danych, z modułem DLP dostępnym na rozwiązaniu FortiGate.
52. Serwer administracyjny musi umożliwiać eksport logów do rozwiązania klasy SIEM.
53. Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych plików do systemu umożliwiającego ochrony poczty, które będzie w stanie kontrolować przesyłanie tak oznaczonych plików.
54. Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na:
- a. audyt i logowanie wiadomości e-mail,
 - b. audyt operacji na plikach Sharepoint Online.
55. System musi umożliwiać integrację z narzędziami analitycznymi tj. Power BI, Tableau).
56. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi.
57. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na:
- a. Bezpieczeństwo danych:
 - Przegląd informacji o incydentach bezpieczeństwa.
 - Przegląd danych przychodzących.
 - Przegląd danych wychodzących.
 - Podłączane/odłączane urządzenia przenośne.

b. Produktowość:

- Przegląd informacji na temat produktywności użytkowników.
- Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.
- Trendy.

c. Eksploatacja sprzętu:

- Przegląd informacji na temat eksploatacji sprzętu komputerowego.
- Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.
- Eksploatacja drukarek.
- Eksploatacji sieci.

58. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.

59. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.

60. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje nt.:

- plików przenoszonych na nośniki USB i inne urządzenia przenośne,
- plików przesłanych za pomocą wiadomości e-mail,
- plików przesłanych za pomocą poczty webowej,
- plików przesłanych do Internetu,
- plików wysłanych za pomocą komunikatorów,
- plików przesłanych na dyski chmurowe,
- analiza sposobu korzystania z aplikacji,
- analiza korzystania z Internetu,
- analiza wykorzystania portali do poszukiwania pracy.

61. Konsola aplikacyjna musi umożliwiać możliwość konfiguracji podwójnej autoryzacji

62. Konsola aplikacyjna musi umożliwiać konfigurację dwóch języków dla mechanizmu OCR

II.14 Usługa kompleksowego przeglądu i reorganizacji posiadanego środowiska serwerowego, domeny, wraz z mechanizmem replikacji

Wymagane jest wykonanie kompleksowego przeglądu stanu domeny Active Directory lub wykonanie ponownej konfiguracji domeny w zgodzie z zaleceniami producenta oraz najlepszymi praktykami. Wymagane jest uruchomienie usługi na min. 2 serwerach: główny kontroler oraz zapasowy kontroler domeny w taki

sposób, aby w przypadku awarii pojedynczego serwera, był zapewniony ciągły dostęp do usługi katalogowej, a w szczególności do mechanizmów uwierzytelniania, rozwiązywania nazw oraz serwera plików. Zamawiający dopuszcza wykorzystanie serwerów wirtualnych uruchomionych na hostach Zamawiającego przy wykorzystaniu nowych licencji SSO.

Wymagane jest uruchomienie funkcji szyfrowania partycji systemowej za pomocą wbudowanych w system operacyjny mechanizmów. Należy zainstalować niezbędne aktualizacje oraz poprawki związane z bezpieczeństwem udostępnione przez producenta systemu operacyjnego.

Uruchomienie usługi katalogowej, komponentów odpowiedzialnych za rozwiązywanie nazw. Usługa katalogowa musi być uruchomiona na wszystkich serwerach przewidzianych do rozbudowy. Na wszystkich serwerach muszą być uruchomione także komponenty odpowiedzialne za rozwiązywanie nazw. Należy skonfigurować mechanizm replikacji wszystkich maszyn wirtualnych Zamawiającego pomiędzy eksploatowanymi hostami (serwerami fizycznymi). Usługę katalogową należy skonfigurować w taki sposób, aby możliwe było wykorzystanie możliwie wszystkich funkcjonalności oferowanych przez zastosowane systemy operacyjne, a w szczególności możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń, możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem.

Utworzenie struktury jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego. Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi:

- Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości;
- Śledzenie zmian dotyczących tworzenia, usuwania obiektów.

Zamawiający wymaga konfiguracji polityk grup w zakresie min:

1. Konfiguracja polityki haseł dla użytkowników domeny.
2. Instalacja oprogramowania w formie paczek .msi
3. Konfiguracja i personalizacja systemu operacyjnego według zaleceń Zamawiającego
4. Konfiguracja drukarek udostępnionych z serwera wydruku
5. Mapowanie dysków sieciowych z serwera plików

Szczegółowe dane zostaną przekazane na etapie konfiguracji.

Po oddaniu wdrożonego systemu do eksploatacji konieczne będzie tworzenie nowych kont użytkowników, grup zabezpieczeń oraz jednostek organizacyjnych.

Zamawiający wymaga wykorzystania obecnych lub wygenerowania identycznych kont użytkowników, katalogów domowych użytkowników, jednostek organizacyjnych, grup zabezpieczeń do już istniejących.

Zamawiający wymaga zintegrowania z urządzeniem UTM oraz weryfikację nawiązywania połączenia poprzez nazwę użytkownika z domeny. Zamawiający wymaga wdrożenia autoryzacji transparentnej stosowanej w posiadanym urządzeniu klasy UTM, która umożliwi tworzenie polityk bezpieczeństwa w oparciu o użytkowników i grupy usługi katalogowej

✓ Uruchomienie i skonfigurowanie serwera plików oraz wydruków

Serwery plików muszą być skonfigurowane z wykorzystaniem dostępnych w zaoferowanych systemach operacyjnych serwerów mechanizmów zwiększających dostępność danych poprzez zastosowanie technologii replikacji systemu plików. Konieczność taka podyktowana jest zapewnieniem ciągłości dostępu do krytycznych danych Wnioskodawcy w przypadku awarii jednego z serwera plików. Zastosowane mechanizmy replikacji systemu plików muszą zapewniać:

- Replikację multi-master z rozwiązywaniem konfliktów;
- Wykorzystanie algorytmów kompresji danych wykrywających zmiany na poziomie bloków danych w obrębie plików – replikacji podlegają tylko zmienione bloki danych, a nie całe pliki.

Serwery plików muszą być skonfigurowane w taki sposób, aby ograniczać ekspozycję danych dla użytkowników oraz grup, które nie mają do nich dostępu.

Na serwerach plików muszą być skonfigurowane przydziały dyskowe dla użytkowników i grup. Zamawiający wymaga także skonfigurowania przydziałów dyskowych dla wskazanych folderów. Zamawiający wymaga włączenia i skonfigurowania mechanizmów uniemożliwiających przechowywanie niedozwolonych typów plików.

Zamawiający wymaga skonfigurowania mechanizmów przekierowania lokalnych folderów „Moje Dokumenty” oraz „Pulpit” ze stacji roboczych na serwer plików. Funkcjonalność musi zostać poprawnie skonfigurowana na stacjach roboczych Zamawiającego.

Zamawiający wymaga opracowania koszyka dozwolonych aplikacji wraz z implementacją polityk globalnych ograniczających dostęp do aplikacji z wykorzystaniem np.: dedykowanych ustawień związanych z polityką kontroli uruchomienia aplikacji. Zamawiający wymaga skonfigurowania parametrów audytu dla serwerów plików umożliwiających między innymi:

- Określenie daty, czasu, nazwy użytkownika, który usunął / próbował usunąć plik/folder;
- Określenie daty, czasu, nazwy użytkownika, który zapisał / próbował zapisać plik/folder;
- Określenia daty, czasu, nazwy użytkownika, który próbował uzyskać nieuprawniony dostęp do zasobów, do których nie ma uprawnień.

Zamawiający wymaga uruchomienia serwera wydruków oraz podłączenia i skonfigurowania 3 wybranych drukarek sieciowych. Zamawiający wymaga opracowania i skonfigurowania odpowiednich polityk globalnych mapujących odpowiednie drukarki użytkownikom. Niedopuszczalne jest przyłączenie wszystkim użytkownikom wszystkich dostępnych drukarek. Użytkownicy powinni mieć przyłączone drukarki znajdujące się najbliżej jego komputera.

✓ **Dołączenie stacji roboczych do domeny**

Jeżeli w procesie reorganizacji lub ponownej konfiguracji Domeny zajdzie konieczność, wtedy Wykonawca przeprowadzi dołączenie stacji roboczych do domeny, wykona migracji profili użytkowników z zachowaniem specyficznych ustawień lokalnych kont użytkowników (między innymi zachowanie ustawień aplikacji oraz poczty elektronicznej). Po zalogowaniu się na konto domenowe, użytkownik powinien mieć zachowaną tapetę oraz ustawienia pulpitu, dotychczas działające aplikacje powinny działać jak wcześniej bez potrzeby ponownej konfiguracji.

Zamawiający wymaga uruchomienia i skonfigurowania usług dostępnych w dostarczonych systemach operacyjnych serwerów umożliwiających zarządzanie aktualizacjami stacji roboczych i serwerów według założeń:

- Aktualizacje i poprawki mają być pobierane na serwer instalacyjny za pośrednictwem sieci Internet;
- Administrator zatwierdza aktualizacje do instalacji;
- Stacje robocze i serwery pobierają i automatycznie instalują zatwierdzone przez Administratora aktualizacje według określonego harmonogramu.

Zamawiający wymaga skonfigurowania co najmniej następujących parametrów:

- Systemów operacyjnych, aplikacji oraz wersji językowych, dla których będą pobierane aktualizacje;
- Kategorii aktualizacji;
- Grup komputerów;
- Polityk globalnych przypisujących komputery znajdujące się w określonych jednostkach organizacyjnych do odpowiednich grup komputerów;
- Zasad automatycznego zatwierdzania nowych aktualizacji;
- Mechanizmów raportowania (e-mail).

Zamawiający wymaga przeszkolenia administratorów Zamawiającego z zakresu samodzielnego podłączania stacji oraz migracji profili użytkowników w przyszłości.

✓ **Wdrożenie infrastruktury PKI w oparciu o dodatkowy moduł usługi katalogowej**

Zamawiający wymaga przygotowania i uruchomienia wewnętrznej infrastruktury PKI. Zamawiający posiada stacje robocze pracujące w oparciu o następujące systemy operacyjne: Windows 10 i nowsze.

Wymagana przez Zamawiającego konfiguracja musi uwzględniać:

- Zaplanowanie i uruchomienie wewnętrznej struktury CA;
- Konfigurację szablonów certyfikatów;
- Wydanie certyfikatów dla wskazanych przez Zamawiającego serwerów i użytkowników;
- Zastosowanie mechanizmów bezpieczeństwa poprzez możliwość backupu archiwizacji kluczy prywatnych wydawanych certyfikatów;
- Wskazanie wszystkich możliwych dróg publikacji list CRL;

✓ **Wdrożenie systemu zarządzania aktualizacjami o poprawkami dla systemów operacyjnych Windows**

Zamawiający wymaga przygotowania oraz uruchomienia serwera umożliwiającego zarządzanie dystrybucją aktualizacji oraz poprawek dla posiadanych przez Zamawiającego komputerów osobistych z systemami

operacyjnymi Microsoft Windows 10/11. Serwer powinien pobierać aktualizacje z oficjalnych serwerów producenta oprogramowania a później umożliwiać rozpropagowanie aktualizacji poprzez sieć do komputerów w strukturze usługi katalogowej. Komputery pracujące w strukturze usługi katalogowej należy odpowiednio przygotować z wykorzystaniem polityk grupowych tak aby aktualizacje były pobierane nie bezpośrednio z serwerów aktualizacyjnych producenta a z przygotowanego serwera aktualizacji. Serwer aktualizacji musi umożliwiać Zamawiającemu pełną kontrolę nad wdrażanymi poprawkami bezpieczeństwa i aktualizacjami, wymagana jest kontrola wersji wdrażanego oprogramowania, możliwość dystrybucji do określonych komputerów oraz możliwość blokowania określonych aktualizacji.

II.15 Zakup, dostawa i wdrożenie oprogramowania SIEM wraz z dedykowanym serwerem fizycznym

Zamawiający wymaga dostarczenia i wdrożenia systemu SIEM z gwarancją oraz wsparciem technicznym na okres min. 12 miesięcy (parametr punktowany dodatkowo) oraz świadczenie usługi SOC (Security Operations Center) przez okres min. 6 miesięcy (parametr punktowany dodatkowo).

1.1 Wymagania dla Systemu Zbierania i Analizy Logów oraz Systemu SIEM.

✓ Wymagania dla Systemu Analizy Logów

- a) W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa.
- b) Rozwiązanie musi zostać dostarczone w postaci maszyn wirtualnej instalowanych w środowisku Vmware lub Windows Hyper-V
- c) Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach i zagrożeniach.
- d) Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukiwujących automatycznie zdarzenia z logów.
- e) Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP.
- f) Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta.
- g) Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.
- h) Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS.
- i) Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder).

- j) Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta.
- k) Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie.
- l) Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.).
- m) Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne.
- n) Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP).
- o) Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów)
- p) Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV.
- q) Rozwiązanie musi umożliwiać tworzenie statycznych raportów.
- r) Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF.
- s) Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów.
- t) Rozwiązanie musi umożliwiać tworzenie własnych raportów.
- u) Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email.
- v) Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie.

✓ Wymagania systemowe

- a) Liczba obsługiwanych zdarzeń na sekundę (EPS): min. 9 000
- b) Przechowywanie, zarządzanie logami: min. 2 lata
- c) Liczba obsługiwanych urządzeń min. 90
- d) Liczba zapisu zdarzeń na dobę: min 9 000 MB
- e) System logów musi wspierać hiperwizory: Vmware ESXi oraz Microsoft HyperV

1.2 Wymagania dla Systemu SIEM.

- a) W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące incydenty na urządzeniach sieciowych Zamawiającego
- b) Rozwiązanie musi w pełni realizować swoją funkcjonalność lokalnie (instalacja on-prem)

- c) Architektura rozwiązania musi umożliwiać wykorzystanie fizycznych lub wirtualnych sond monitorujących, których rolą jest odbieranie kopii ruchu sieciowego, generowanie alarmów oraz/lub metadanych o zdarzeniach, przygotowanie przechwyconych plików do dalszej analizy oraz przekazywanie przetworzonych danych do urządzenia administracyjnego.
- d) Architektura rozwiązania musi być oparta także o fizyczne urządzenie administrujące, którego rolą jest zarządzanie sondami, włącznie z regułami detekcji, sygnaturami i nadzorem stanu, dogłębna analiza odebranych plików, prezentacja wyników detekcji, a także przekazywanie danych do rozwiązań stron trzecich
- e) Platformy muszą obsługiwać szyfrowanie dysków w standardzie LUKS.
- f) Rozwiązanie musi wspierać implementację na środowisku wirtualnym takim jak m.in. VMWare, Hyper-V, Proxmox, KVM, OVM, OVF.
- g) Należy dostarczyć dedykowany serwer sprzętowy dla oferowanego systemu SIEM, który musi spełniać wymagania minimalne:

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami umożliwiającymi wysunięcie i wszystkim elementami niezbędnymi do zamontowania serwera w szafie).
Procesor	Procesor max. 16 rdzeniowy, osiągający w teście SPECrate@2017_int_base wynik co najmniej 174 punkty. Płyta główna obsługująca procesory od 16 do 128 rdzeni, wymagających mocy 400W i obsługujących do 3TB pamięci RAM.
Liczba procesorów	Min. 1
Pamięć operacyjna	Zainstalowanych min. cztery moduły 64 GB DDR5 4800MT/s każdy. Płyta główna z minimum 12 slotami na pamięć, umożliwiającą instalację do minimum 3TB pamięci RAM, obsługująca moduły 6400 MT/s Obsługa zabezpieczeń: min. Advanced ECC.
Sloty rozszerzeń	Możliwość instalacji do min. 6 kart PCI-Express generacji 5 pełnej wysokości, x16(szybkość slotu – bus width).
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę min. 8 napędów dyskowych oraz obsługujący poziomy: RAID 0,1,10,5,50,6,60, nie zajmujący gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.
Dysk twardy	Możliwość instalacji do 20 dysków 3,5”. Zatoki dyskowe gotowe do zainstalowania dysków Hot Swap SAS/SATA/SSD. Zainstalowane min. 4 dyski o pojemności min. 1.9TB SSD każdy oraz min. 4 dyski o pojemności min. 16TB SATA 7200rpm każdy.

Interfejsy sieciowe	Zainstalowane 2 karty sieciowe z dwoma portami 10/25Gb SFP+/SFP28, wraz z modułami SFP+. Karty sieciowe nie mogą zajmować slotów PCI-ex. Zainstalowana karta 4 portowa 1Gb BASE-T.
Karta graficzna	Zintegrowana karta graficzna z pamięcią min. 16 MB , umożliwiającą wyświetlenie obrazu min. 1920 x 1200@60Hz
Porty	Min. 4 porty USB 3.2 wbudowane (w tym min. 1 port wewnętrzny i 1 z przodu obudowy), 1 port VGA Możliwość rozbudowy/rekonfiguracji o port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express 1x port RJ-45 dedykowany dla interfejsu zdalnego zarządzania
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy maximum 1000W, efektywność zasilaczy min. 94%
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) z dedykowanym portem RJ45 pozwalającą na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe i nie zajmująca wymaganych slotów PCI. Jeśli jest wymagana to załączona odpowiednia licencja.
Karta/moduł zarządzający i system zarządzania	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slotcie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: <ul style="list-style-type: none"> • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez <ul style="list-style-type: none"> - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy <ul style="list-style-type: none"> - z poziomu przeglądarki webowej (GUI)

- z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)
- z poziomu skryptu (XML/Perl)
- poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)
- wbudowane narzędzia diagnostyczne
- zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego
- obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przysyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie
- wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
- przysyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)
- obsługa zdalnego serwera logowania (remote syslog)
- wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów
- mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie
- funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności
- monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji
- konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)
- zdalna aktualizacja oprogramowania (firmware)
- zarządzanie grupami serwerów, w tym:
 - tworzenie i konfiguracja grup serwerów
 - sterowanie zasilaniem (wł/wył)
 - ograniczenie poboru mocy dla grupy (power capping)
 - aktualizacja oprogramowania (firmware)
 - wspólne wirtualne media dla grupy
- możliwość równoczesnej obsługi przez 6 administratorów

	<ul style="list-style-type: none"> • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz IPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	<p>Min. Microsoft Windows Server 2019, 2022, 2025</p> <p>Min. Red Hat Enterprise Linux (RHEL): 8.6, 9.0</p> <p>Min. SUSE Linux Enterprise Server (SLES) 15</p> <p>Min. VMware ESXi 7.0 U3, 8.0</p>
Gwarancja	<p>Minimum 3-letnia gwarancja na części, robociznę i naprawę w miejscu instalacji typu On-Site z 2 godzinnym czasem reakcji na zgłoszenie. Rozpoczęcie naprawy w miejscu instalacji w następnym dniu roboczym. Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń.</p> <p>Możliwość rozszerzenia usługi gwarancyjnej do 5 lat realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy 6 godzin i pozostawieniem uszkodzonych dysków u zamawiającego.</p>
Inne	<p>Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.</p> <p>Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.</p>

- h) Serwer dedykowany musi obsługiwać do 2 900 zdarzeń na sekundę, musi przechowywać do 5 milionów zdarzeń, musi mieć możliwość detekcji malware, a także musi analizować przy pomocy silnika detekcji shellcode/powershell.
- i) Licencja z gwarancją i wsparciem technicznym musi bazować na ilości aktywnie występujących w ruchu sieciowym adresów IP. Ilość adresów, objętych monitorowaniem min. 90.
- j) Musi posiadać moduły zabezpieczone połączeniem (HTTPS) w przeglądarce
- k) Konsola rozwiązania musi zawierać informacje o kluczowych z punktu widzenia bezpieczeństwa detekcjach, uwzględniając adresy IP, adresy MAC, porty sieciowe, protokoły sieciowe, wyniki skanów plików, payload, sygnatury czasowe.
- l) Konsola rozwiązania musi szacować poziom ryzyka dla każdego wykrytego zagrożenia oraz musi dawać możliwość tagowania zdarzeń i załączania opisu (notatek).

- m) Konsola musi umożliwiać grupowanie takich samych zdarzeń w ramach jednego wpisu oraz podawać liczbę wystąpień identycznego zdarzenia
- n) Konsola musi umożliwiać utworzenie zgłoszenia z dowolnego zdarzenia
- o) Konsola musi posiadać dedykowany widok dla utworzonych zgłoszeń
- p) Z poziomu konsoli musi być dostępna opcja zmiany statusu zgłoszenia
- q) Rozwiązanie musi obsługiwać silniki detekcji takie jak Analiza Shellcode i Powershell, tj. detekcja technik wykorzystywanych przez cyberprzestępców w postaci specyficznego kodu służącego do wywoływania podatności oprogramowania zainstalowanego na stacjach roboczych czy serwerach.
- r) Rozwiązanie musi umożliwiać analizowanie całego ruchu sieciowego w oparciu o dostarczone reguły opisujące charakter niebezpiecznych połączeń.

1.3 Administracja Systemem Analizy Logów:

W ramach realizacji zadań administracji Systemem Analizy Logów Wykonawca będzie odpowiedzialny za:

- a) Informowanie Zamawiającego o awariach Systemu Analizy Logów, mogących uniemożliwić poprawne działanie systemów informacyjnych Zamawiającego i/lub świadczenie usług ujętych w niniejszym dokumencie,
- b) Rekomendowanie zmiany zasobów takich jak: vCPU, vRAM, pamięć masowa.
- c) Optymalizowanie konfiguracji Systemu Analizy Logów w celu nieprzekraczania wartości licencji Systemu posiadanego przez Zamawiającego oraz niezwłocznego zgłaszania sytuacji przekroczenia poziomu utylizacji licencji.
- d) Konfigurację Systemu Analizy Logów w celu gromadzenia i normalizowania logów ze wskazanych systemów Zamawiającego zgodnie z tabelą z punktu: Systemy Zamawiającego wymagające monitorowania
- e) Weryfikację czy System Analizy Logów prawidłowo analizuje logi
- f) Tworzenie wymagań dla systemów Zamawiającego wysyłających logi w zakresie poziomu logowania zdarzeń.

1.4 Testowanie Systemu Analizy Logów:

W ramach realizacji zadań testowania Systemu Analizy Logów Wykonawca będzie odpowiedzialny za:

- a) Przygotowanie i uzyskanie aprobaty Zamawiającego dla scenariuszy testów Systemu Analizy Logów,
- b) Weryfikację wdrożonych scenariuszy użycia oraz implementacji nowych przypadków zgłoszonych przez Zamawiającego,
- c) Weryfikację możliwości wdrożenia przypadków użycia w środowisku Zamawiającego,

1.5 Analiza złośliwego oprogramowania:

- a) W ramach realizacji umowy, Zamawiający będzie mógł zlecić Wykonawcy wykonanie analizy złośliwego oprogramowania, nie więcej niż 6 w ciągu roku. Sposób zgłaszania analizy złośliwego oprogramowania zostanie uzgodniony po podpisaniu umowy.
- b) Zakres analizy złośliwego oprogramowania będzie nie mniejszy niż:
- c) Analiza statyczna wskazanej próbki złośliwego oprogramowania,
- d) Analiza dynamiczna w kontrolowanym środowisku pozwalającym na wyłączenie funkcji ukrywania lub wykrywania analizy,
- e) W przypadku wykorzystywania rodziny malware określenia wersji
- f) Każdorazowo po wykonanej analizie złośliwego oprogramowania Wykonawca prześle drogą mailową raport z wykonanej analizy. Zakres raportu zostanie ustalony po podpisaniu umowy.

1.6 Opcjonalny moduł EDR (Endpoint Detection and Response – (moduł punktowany dodatkowo).

Wykonawca wraz z system SIEM może dostarczyć system klasy Endpoint Detection and Response wraz z centralną konsolą zarządzającą w postaci licencji bezterminowej dla min. 90 urządzeń wraz z wsparciem technicznym na okres min. 24 miesięcy. Minimalne wymagania dla modułu EDR:

1. Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS umożliwiające bezproblemową współpracę z systemem antywirusowym do ochrony stacji roboczych, użytkowanym przez Zamawiającego.
2. Rozwiązanie musi zawierać centralną konsolę administracyjną umożliwiającą monitorowanie oraz wizualizację zebranych danych z zarządzanych urządzeń.
3. Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej.
4. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia.
6. Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, nazwę komputera, grupę, użytkownika.
7. Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, rozmiar pliku.
8. Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne lub niebezpieczne.
9. Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli.

10. Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania komend zdalnych.
11. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
12. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
13. Rozwiązanie musi umożliwiać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
14. Rozwiązanie musi zapewniać integrację z przynajmniej takimi systemami jak: konsola programu antywirusowego, moduł EDR.
15. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: numer seryjny, informacje o systemie, procesor, pamięć RAM, karty sieciowe).
16. Serwer administracyjny musi posiadać możliwość tworzenia grup komputerów.
17. Rozwiązanie musi zapewniać korzystanie z min. 100 szablonów raportów, przygotowanych przez producenta lub własnych raportów tworzonych przez administratora.
18. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email oraz do dziennika syslog.
19. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami.
20. Rozwiązanie musi informować administratora o niezainstalowanych aktualizacjach systemowych.

1.7 Opcjonalny moduł NDR (Network Detection and Response – (moduł punktowany dodatkowo).

Wykonawca wraz z system SIEM może dostarczyć moduł Network Detection and Response wraz z centralną konsolą zarządzającą w postaci licencji bezterminowej dla min. 90 adresów IP wraz z wsparciem technicznym na okres min. 24 miesięcy. Minimalne wymagania dla modułu NDR:

1. Wielowątkowy silnik detekcji umożliwiający obsługę ruchu liczonego w dziesiątkach Gigabitów
 - Możliwość obsługi wielu podsieci VLAN
 - Możliwość obsługi wielu fizycznych połączeń sieciowych do różnych segmentów sieci LAN
 - Obsługa biblioteki wyrażeń regularnych HyperScan
 - Możliwość aktualizacji reguł bez wyłączania/ponownego uruchamiania silnika detekcji
2. Obsługa wielowątkowości procesora
3. Możliwość analizy kopii ruchu w sieci LAN w czasie rzeczywistym bez ingerencji w ruch sieciowy
4. Rejestracja żądań HTTP
5. Rejestracja i przechowywanie certyfikatów TLS

6. Możliwość wyodrębnienia plików z analizowanego ruchu sieciowego i zapisania ich na dysku do późniejszej analizy
7. Możliwość przechwytywania pakietów danych przesyłanych w sieci LAN i zapisywanie ich dla późniejszej analizy offline
8. Tworzenie raportów w przypadku wykrycia ruchu opisanego regułami jako ruch niebezpieczny
9. Rejestrowanie i dogłębna analiza ruchu szyfrowanego TLS/SSL
10. Rejestrowanie wszystkich kluczy wymiany do analizy oraz w celu zapobiegania podmianie
11. Rejestrowanie, zapisywanie ruchu HTTP z dowolnego portu do pliku w celu późniejszej analizy
12. Możliwość identyfikacji, wyodrębniania i rejestrowania plików w ruchu HTTP
13. Rejestracja wszystkich zapytań i odpowiedzi DNS
14. Funkcja wykrywania włamań sieciowych
15. Funkcja zapobiegania włamaniom sieciowym
16. funkcja monitorowania bezpieczeństwa sieci LAN
17. Pełne wsparcie dla protokołu IPv6
18. Możliwość dekodowania tuneli: IP-IP, IP6-IP4, IP4-IP6, GRE, VXLAN, Geneve, Teredo
19. Silnik analizy strumienia danych TCP
20. Defragmentacja pakietów w celu poddania ich analizie IPS
21. Możliwość obsługi wielu podsieci VLAN
22. Możliwość obsługi wielu fizycznych połączeń sieciowych do różnych segmentów sieci LAN
23. Możliwość modyfikacji reguł
24. Możliwość zdefiniowania niebezpiecznych plików przez parametry: wielkość, nazwa, rozszerzenie
25. Możliwość wykrywania złośliwego oprogramowania w oparciu o odcisk palca JA3, JA3S
26. Możliwość wykrywania złośliwego oprogramowania w oparciu o metodę HASSH
27. Obsługa dekodowania pakietów: IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE, Ethernet, PPP, PPPoE, Raw, SLL, VLAN, QINQ, MPLS, ERSPAN, VXLAN
28. Dekodowanie warstwy aplikacji: HTTP, HTTP/2, SSL, TLS, SMB, DCERPC, SMTP, FTP, SSH, DNS, ENIP/CIP, DNP3, NFS, NTP, DHCP, TFTP, KRB5, IKEv2, SIP, SNMP, RDP, RFB
29. Możliwość tworzenia raportów zgodnych z standardem JSON, SYSLOG,
30. Możliwość filtrowania alertów z podziałem na wagę/priorytet
31. Możliwość filtrowania alertów dla wybranej reguły z podziałem na wagę/priorytet
32. Wspierane systemy operacyjne: Windows, Linux, FreeBSD, OpenBSD, MacOS, Mac OS X
33. Obsługa przekazywania alertów „dalej” do systemów takich jak: syslog, eve.log, JSON, Unified 2
34. Filtrowanie alertów na poziomie: reguł, hostów, sieci

1.8 Opcjonalny moduł SOAR (moduł punktowany dodatkowo).

Wykonawca wraz z system SIEM może dostarczyć moduł SOAR wraz z centralną konsolą zarządzającą w postaci licencji bezterminowej dla min. 90 adresów IP wraz z wsparciem technicznym na okres min. 24 miesięcy. Minimalne wymagania dla modułu SOAR:

1. Możliwość wysyłania powiadomień Push UP o wykrytym incydencie powyżej zdefiniowanego priorytetu wysyłane na urządzenie mobilne z system Android lub iOS.
2. Możliwość wysyłania powiadomień SMS o wykrytym incydencie powyżej określonego priorytetu wysyłane na zdefiniowane numery telefonów.
3. Możliwość integracji zewnętrznego systemu z oferowanym systemem SIEM poprzez dedykowane API
4. Możliwość zablokowania podejrzanego, potencjalnie niebezpiecznego ruchu sieciowego (LAN, WAN) do danych adresów IP na zarządzanych hostach (serwery, stacje robocze)
5. Możliwość obserwacji w czasie rzeczywistym lub wyznaczonych interwałach czasowych określonych plików (np. systemowych) generując alerty, gdy te pliki zostaną zaatakowane lub zmodyfikowane.
6. Min. jedna zintegrowana z modułem zarządzania incydentami baza przetworzonych incydentów, znanych zagrożeń, regularnie aktualizowana o nowe incydenty, zagrożenia.
7. Możliwość porównania nowo utworzonego incydentu z posiadaną bazą opracowanych incydentów, znanych zagrożeń w wyniku czego administrator otrzymuje listę podobnych incydentów oraz listę incydentów zawierających zmienne obserwacyjne zawarte w nowym incydencie.
8. Możliwość przeszukiwania bazy incydentów pod kątem konkretnej zmiennej obserwacyjnej.
9. Możliwość klasyfikacji wykrytych zdarzeń na podstawie min. 16 stopniowej skali oraz możliwość modyfikacji poziomów skali wg potrzeb administratora.
10. Możliwość klasyfikacji utworzonych incydentów na podstawie kryteriów:
 - waga, min. 4 poziomy
 - poufność, możliwość nadania incydentowi parametru poufny czyli incydent zawierający dane wrażliwe wymagające szczególnej ochrony
 - tagi, możliwość przypisania tagu dla incydentu
 - zadanie, możliwość tworzenia zadań w ramach incydentów oraz przypisywania operatora dla zadania
11. Możliwość integracji SOAR z usługą katalogową Windows Active Directory.
12. Możliwość automatycznego uruchamiania zdefiniowanych działań w odpowiedzi na wykryty incydent, na przykład izolacja hosta, zablokowanie ruchu sieciowego lub zatrzymanie procesu.

13. Możliwość integracji z różnymi narzędziami bezpieczeństwa, takimi jak systemy antywirusowe, firewalle, czy też narzędzia do monitorowania ruchu sieciowego.
14. Możliwość wykorzystania algorytmów heurystycznych do automatycznego analizowania podejrzanych zachowań lub wzorców w systemie.
15. Możliwość dostosowania filtrów, które pomagają w identyfikacji istotnych zdarzeń oraz redukcji fałszywych alarmów, zwiększając ciągłość przepływu pracy.
16. Możliwość tworzenia dynamicznych skryptów i reguł reakcji na incydenty, umożliwiających dostosowanie się do zmieniających się warunków i nowych rodzajów zagrożeń.
17. Możliwość integracji z platformami chmurowymi oraz możliwość monitorowania i zarządzania SOAR w środowisku chmurowym.
18. Możliwość dynamicznego zarządzania dostępem do zasobów w przypadku wykrycia podejrzanego ruchu sieciowego, obejmujące blokowanie dostępu do określonych adresów IP na zarządzanych hostach.
19. Możliwość współpracy z systemem IDS i IPS poprzez dedykowane API, umożliwiając wspólne korzystanie z informacji o wykrytych incydentach i zoptymalizowanie działań obronnych.
20. Możliwość generowania automatycznych zadań w ramach incydentów.

1.9 Opcjonalne oprogramowanie do monitorowania infrastruktury informatycznej (moduł punktowany dodatkowo).

W ramach realizacji zadania Wykonawca dostarczy, zainstaluje oprogramowanie z gwarancją i wsparciem technicznym na okres min. 24 miesięcy. Wykonawca przeprowadzi instalację, konfigurację oraz podłączenie wszystkich wymaganych systemów będących celem monitorowania. System musi spełniać poniższe wymagania minimalne:

Użytkownicy	
1	<ul style="list-style-type: none"> ▪ Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat. ▪ Zapewnienia równoległego dostępu do systemu dla wielu użytkowników. ▪ Ograniczania użytkownikom dostępu do wybranych grup hostów.
Monitorowanie	
2	<ul style="list-style-type: none"> ▪ Monitorowania serwerów fizycznych. ▪ Monitorowania urządzeń sieciowych. ▪ Monitorowania stanu połączeń.

- Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów
- Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux.
- Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych.
- Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń.
- Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu.
- Grupowanie hostów.
- Definiowanie planowanych przerw serwisowych dla hostów i usług.
- Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK).
- Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania, powiadomień; konfiguracje przerw serwisowych).
- Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www).
- Monitorowanie serwerów za pomocą agentów
- Monitorowanie serwerów aplikacji: Tomcat, Oracle WebLogic Server, Oracle Application Server.
- Monitorowanie Active Directory.
- Monitorowanie serwerów plików, udziałów sieciowych.
- Monitorowanie statusu serwerów Apache.
- Monitorowanie baz danych:
 - ORACLE,
 - MySQL,
 - Postgress.
 - MSSQL Server
 - DB2
- Monitorowanie urządzeń przez następujące protokoły:
 - SNMP,
 - WMI,
 - IPMI.
- Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW.
- Monitorowanie poprawności działania DNS.
- Monitorowanie środowiska VMware.
- Monitorowanie środowiska Hyper-V.

	<ul style="list-style-type: none"> ▪ Monitorowanie środowisk Proxmox ▪ Monitorowanie działania serwera czasu NTP. ▪ Monitorowanie offsetu czasu na serwerach. ▪ Monitorowanie ping - czasy odpowiedzi, straty pakietów. ▪ Monitorowanie zajętości miejsca na poszczególnych partycjach. ▪ Monitorowanie obciążenia dysków. ▪ Monitorowanie wykorzystania pamięci RAM. ▪ Monitorowanie obciążenia CPU. ▪ Monitorowanie logów systemowych Windows. ▪ Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia. ▪ Dodawanie własnych wtyczek / agentów dla urządzeń i usług, które standardowo nie są obsługiwane. ▪ Zgodność z wtyczkami programu Nagios służącego do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach Linux i Unix. ▪ Agregację usług niskiego poziomu do procesów biznesowych (tzw. Business Intelligence) ▪ Symulację awarii elementów infrastruktury i badanie jej wpływu na procesy biznesowe ▪ Monitorowanie rozproszone (podgląd w pojedynczym panelu stanu wielu instancji monitorujących, np. z kilku lokalizacji/oddziałów). ▪ Wykrywanie niestabilnie działających usług. ▪ Monitorowanie dostępności stron internetowych. ▪ Konfigurację hierarchiczną (dziedziczenie konfiguracji dla grup urządzeń).
Prezentacja	
3	<ul style="list-style-type: none"> ▪ Prezentację stanu urządzeń na mapie. ▪ Prezentację danych na dashboardach. ▪ Elastyczną konfigurację dashboardów, wybór elementów. ▪ Wizualizację stanu działania całej infrastruktury na jednym dashboardzie. ▪ Tworzenie indywidualnych dashboardów przez użytkowników
Powiadomienia	
4	<ul style="list-style-type: none"> ▪ Globalne wyłączanie powiadomień. ▪ Powiadamianie użytkownika o problemach przez e-mail. ▪ Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie. ▪ Definiowanie przedziałów czasowych w których wysyłane są powiadomienia do

	<p>poszczególnych użytkowników.</p> <ul style="list-style-type: none"> Definiowanie różnych wartości progowych alertów na poziomie globalnym, grupy urządzeń, pojedynczych urządzeń, pojedynczych usług
Konfiguracja	
5	<ul style="list-style-type: none"> Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW Automatyczna konfiguracja i działanie z REST-API Centralne zarządzanie agentami Integracja danych z różnych źródeł danych (JSON, XML, SNMP)
Monitoring bazy danych systemu HIS	
6	<p>Możliwość monitorowania bazy danych systemu HIS w zakresie co najmniej:</p> <ul style="list-style-type: none"> Instance state Version Jobs Locks Processes Number of active sessions Recovery area Log switch activity General tablespace information Tablespaces performance Long active sessions Undo retention Checkpoint and online backup state Custom SQLs RMAN backup status RMAN backups ASM disk groups Apply and transport lag of Oracle Data-Guard Możliwość dodania własnych zapytań SQL i monitorowanie zwracanych wartości
Kolektor logów	

7	<ul style="list-style-type: none"> System posiada własny kolektor logów syslog Może odbierać wiadomości bezpośrednio z syslog lub SNMP traps Za pomocą agentów potrafi oceniać logi tekstowe oraz logi Windows Event Klasyfikuje wiadomości bazując zdefiniowanych przez użytkownika regułach, potrafi korelować, podsumowywać, liczyć, opisywać i przepisywać wiadomości, a także uwzględniać ich relacje czasowe.
Cyberbezpieczeństwo	
8	<ul style="list-style-type: none"> System monitoruje urządzenia klasy UTM minimum w zakresie: <ul style="list-style-type: none"> wykrywanie włamań i szybkość blokowania WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika monitoruje stan synchronizacji klastra High-Availability. Status „zsynchronizowany” jest uważany za OK, a status „niezsynchronizowany” CRIT. monitoruje ogólny stan alarmów czujników urządzenia Firewall. Status kontroli jest OK, jeśli wszystkie czujniki mają status alarmu „fałsz” (0) i CRIT, jeśli co najmniej jeden czujnik ma stan alarmu „prawda” (1). monitoruje aktualną liczbę sesji na urządzeniu monitoruje liczbę dostępnych tuneli IPSec VPN monitoruje wykrywanie wirusów i szybkość blokowania systemów FortiGate AntiVirus. Przechodzi WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika. monitoruje poziom wykorzystania procesora Górne domyślne poziomy to 80,0, 90,0 procent. Poziomy są konfigurowalne. System ma możliwość odbierania i prezentacji danych z UTM z wykorzystaniem kolektora logów syslog System ma możliwość odbierania danych z systemu EDR z wykorzystaniem kolektora logów syslog.
Monitoring	
9	<p>W ramach usługi Wykonawca monitoruje krytyczne elementy infrastruktury IT:</p> <ul style="list-style-type: none"> Serwer fizyczny – do 5 sztuk maszyna wirtualna Windows / Linux / hosty – do 15 sztuk serwer AD - 2 sztuki Macierze / NASy – do 2 sztuk Przełącznik rdzeniowy – 2 sztuki

	<ul style="list-style-type: none"> – Przełącznik dostępowy (LAN) – do 5 sztuk – Zasilacz awaryjny (UPS) - 2 sztuki – Serwer bazodanowy - 1 sztuka – Serwer Backupu - 1 sztuka ▪ W ramach usługi wykonawca monitoruje krytyczne systemy Zamawiającego: ▪ Baza danych systemu dziedzinnowego ▪ System dziedzinnowy użytkowany przez Zamawiającego
--	--

II.16 Zakup usługi SOC zapewniających prewencję, detekcję i reakcję na zagrożenia cyberbezpieczeństwa

1.1 Słownik pojęć:

Skrót lub Pojęcie	Opis
Best Effort	Stan realizacji usługi, w którym zostały przekroczone ograniczenia SLA ze względu na wystąpienie zwiększonego zapotrzebowania na usługę. W przypadku przekroczenia ograniczeń SLA Wykonawca niezwłocznie poinformuje Zamawiającego o zaistniałej sytuacji.
Cyberbezpieczeństwo	Adekwatny do potrzeb stan ochrony zapewniający możliwość wykrycia oraz reagowania na zdarzenia niepożądane oraz wskazane w dokumentacji systemu zarządzania bezpieczeństwem informacji Zamawiającego.
Cyberprzestrzeń	Przestrzeń, w której następuje wymiana, gromadzenie i udostępnianie informacji za pośrednictwem komputerów oraz komunikacja między człowiekiem i komputerem.

Czas	Wszystkie wskazania w dokumencie w zakresie czasu dotyczą czasu w aktualnej strefie czasowej przyjętej jako czas urzędowy obowiązujący w Polsce.
Departament Bezpieczeństwa	Komórka organizacyjna w strukturach Zamawiającego, odpowiedzialna za bezpieczeństwo informacji.
Dzień roboczy	Od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych u Zamawiającego.
Incydent Bezpieczeństwa Informacji (Incydent)	Pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
Koordinator Wykonawcy	Osoba z ramienia Wykonawcy odpowiedzialna za podejmowanie decyzji w zakresie realizacji spełniania warunków SLA usługi oraz za kontakt z Zamawiającym. Koordynator może mieć jednego lub wielu zastępców.
Okres przejściowy	Czas, w którym Wykonawca zobowiązany będzie do podjęcia działań, których celem będzie przejęcie wiedzy od Zamawiającego o jego systemie monitoringu, uzgodnienia z Zamawiającym wzoru Miesięcznego Raportu Rozliczenia Usług, ustalenia z Zamawiającym harmonogramu wdrożenia dla pierwszych scenariuszy użycia oraz dopasowanie i uzgodnienie zasad współpracy z systemami Wykonawcy. Zakończenie okresu przejściowego potwierdzone zostanie Protokołem Odbioru.

Koordinator Zamawiającego	Osoba z ramienia Zamawiającego odpowiedzialna za podejmowanie decyzji w zakresie realizacji usługi. Koordynator może mieć jednego lub wielu zastępców.
Miejsce świadczenia usługi monitorowania cyberbezpieczeństwa	Miejsce świadczenia usługi Monitorowania Cyberbezpieczeństwa przez zespół Wykonawcy spełniające wymagania ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).
Pierwsza Linia Wsparcia	Pierwsza Linia Wsparcia SOC – usługa realizująca w szczególności zadania: <ul style="list-style-type: none"> • Identyfikacji zdarzeń; • Analizy i eliminacji najprostszych znanych zdarzeń
Druga Linia Wsparcia	Druga Linia Wsparcia SOC – usługa realizująca w szczególności zadania: <ul style="list-style-type: none"> • Współpracy w reakcji na zdarzenia skomplikowane i nieznane; • Tworzenie Scenariuszy Reakcji na powtarzalne zdarzenia; • Nadzór nad poprawnością działania konfiguracji scenariuszy użycia;
On-call	Dyżur pod telefonem, czekanie w gotowości na zgłoszenie Drugiej Linii Wsparcia, wyłącznie dla Incydentów o priorytecie Poważnym.
CTI/OSINT	Ang. Cyber Threat Intelligence/OpenSource Intelligence - narzędzia dostarczające szczegółowe informacje o technikach hackerskich, zagrożeniach, podatnościach, artefaktach lub umiejętności ich interpretowania i dekodowania oraz czynności pozwalające na pozyskanie informacji z powszechnie dostępnych źródeł umożliwiających powiększenie zakresu wiedzy na temat potencjalnych zagrożeń.

Praca ciągła	Praca systemu w trybie 24/7/365 dni.
PUODO	Prezes Urzędu Ochrony Danych Osobowych – organ właściwy do spraw ochrony danych osobowych na terytorium Polski, utworzony ustawą z 10 maja 2018 roku o ochronie danych osobowych. Jest również organem nadzorczym w rozumieniu ogólnego rozporządzenia o ochronie danych.
RODO	Ustawa o ochronie danych osobowych z dnia 28 maja 2018 roku uszczegółowiające wymagania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) jest odpowiedzią na wyzwania związane ze zmieniającą się gospodarką danych osobowych.
SOC	Security Operations Center – centrum operacji bezpieczeństwa, którego zadaniem jest monitorowanie, zapobieganie, wykrywanie, badanie i reagowanie na cyber zagrożenia.
Scenariusz Reakcji	<p>Dokument opisujący wymagane czynności w przypadku wykrycia zdarzenia nieporządnego, składający się z:</p> <ul style="list-style-type: none"> • Zestawu możliwości technicznych wykrycia zdarzenia; • Zdefiniowanych warunków wywołania zdarzenia niepożądanego; • Opisu identyfikacji zdarzeń zależnych; • Instrukcji reakcji na zdarzenie; • Instrukcji uruchomienia działań korekcyjnych; • Instrukcji wykonywania działań informacyjnych; • Ogólnych i szczegółowych ścieżek eskalacyjnych.

Scenariusz użycia systemu bezpieczeństwa	<p>Dokument opisujący zestaw zadań wymaganych do wykonania w ramach Drugiej Linii Wsparcia, w skład którego wchodzi między innymi:</p> <ul style="list-style-type: none"> • Skonfigurowanie jednego lub kilku źródeł zdarzeń; • Przygotowanie Scenariuszy Reakcji w zakresie czynności wykonywanych przez Pierwszą Linie Wsparcia.
SLA	Zestaw wartości granicznych dla kluczowych wskaźników wydajności, dla których określona realizacja usługi jest wymagany w zakresie jakościowym.
System analizy logów	System umożliwiający zbieranie i analizę logów z urządzeń, sieci i systemów informatycznych
Transfer Wiedzy	Usługa przekazywania kompetencji w zakresie realizacji usług Pierwszej i Drugiej Linii Wsparcia.
Usługa monitorowania Cyberbezpieczeństwa	Zestaw czynności wykonywanych przez Wykonawcę w ramach umowy w celu identyfikacji Incydentów Bezpieczeństwa Informacji.
Zdarzenia niepożądane	Zdarzenie mogące wskazywać na wystąpienie incydentu bezpieczeństwa w środowisku chronionym.
Zdarzenie False-Negative	Wykrycie przez Drugą Linie Wsparcia, zdarzenia nie poprawnie rozpoznanego przy zastosowaniu ustalonych i zaakceptowanych procedur bezpieczeństwa. Realizacja i rozpoznawanie zdarzeń „False-Negative”.

Zdarzenie False-Positive	Wykrycie przez automatyczne systemy zdarzenia, które po analizie zostało uznane jako zdarzenie poprawne. W przypadku notorycznego występowania, statystycznie rozumianego jako więcej niż 100 zdarzeń „False - Positive” na 1 incydent bezpieczeństwa w miesiącu, należy uznać regułę automatyczną tworzącą takie zdarzenia jako błędną konfigurację systemu bezpieczeństwa.
Przypadek testowy	Celowe wykonanie pełnego przebiegu zdarzenia od momentu wystąpienia sytuacji niepożądanego do momentu zakończenia przetwarzania fazy analizy incydentu. Gdy jest to możliwe, obejmuje wykonanie odwracalnych kroków reakcji na incydent, sprawdzenie scenariusza end-to-end łącznie z zablokowaniem wskaźników kompromitacji w narzędziach prewencyjnych.

1.2 Termin realizacji usługi SOC

1. Świadczenie Usługi SOC rozpoczęte zostanie w terminie określonym na etapie tworzenia planu wdrożenia.
2. Termin, o którym mowa w punkcie 1.2 podpunkt 1 licząc od dnia podpisania umowy do rozpoczęcia świadczenia usługi, traktuje się jako okres przejściowy, w którym Wykonawca zobowiązany będzie do podjęcia działań, których celem będzie dopasowanie i uzgodnienie zasad współpracy. Zakończenie okresu przejściowego potwierdzone zostanie Protokołem Odbioru.
3. Wykonawca do świadczenia usługi będzie wykorzystywał narzędzia dostarczone w niniejszym postępowaniu oraz udostępnione przez Zamawiającego. Dostęp do narzędzi i systemów Zamawiającego musi być zrealizowany za pomocą bezpiecznego połączenia szyfrowanego.

1.3 Wymagania dla Usługi SOC (Security Operations Center)

W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie Analizy Logów zgodnie z opisanymi poniżej wymaganiami.

1.4 Pierwsza i Druga Linia Wsparcia

W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie Analizy Logów zgodnie z opisanymi poniżej wymaganiami.

✓ Pierwsza Linia Wsparcia

W ramach realizacji zadań Pierwszej Linii Wsparcia Wykonawca będzie odpowiedzialny za:

- a) Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa zgodnie warunkami określonymi w punkcie: Ogólne warunki SLA.
- b) Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji.
- c) Analizę i eliminację najprostszych znanych zdarzeń określonych w ramach Scenariusza Reakcji.
- d) Łączenie (korelowanie) zdarzeń i incydentów cyberbezpieczeństwa.
- e) Dokumentowanie wykonanych czynności zgodnie z przygotowanymi i zaakceptowanymi Scenariuszy Reakcji.
- f) Eskalowanie zdarzenia zgodnie w ramach ustalonego Scenariusza Reakcji.
- g) Zamykanie zdarzeń błędnie rozpoznanych przez system bezpieczeństwa jako zagrożenie (tzw. False-Positive).
- h) Priorytetyzowanie i kategoryzowanie zdarzeń bezpieczeństwa.
- i) Przygotowywanie raportów wykrytych zdarzeń bezpieczeństwa.

✓ Druga Linia Wsparcia

W ramach realizacji zadań Drugiej Linii Wsparcia Wykonawca będzie odpowiedzialny za:

- a) Dostępność usługi dla Zamawiającego zgodnie z określonymi warunkami SLA (Ogólne warunki SLA).
- b) Analizę zgłoszonych przez Pierwszą Linie Wsparcia Incydentów cyberbezpieczeństwa oraz przygotowanie raportów i zaleceń poincydentalnych.
- c) Przygotowywanie i realizację Scenariuszy użycia systemu bezpieczeństwa zgodnie z wymaganiami przedstawionymi przez Zamawiającego.
- d) Przygotowanie Scenariuszy Reakcji.
- e) Przygotowanie Miesięcznych raportów z realizacji prac.

1.5 Scenariusze

✓ Scenariusz użycia systemu bezpieczeństwa

Zamawiający wymaga przygotowania i wdrożenia możliwych scenariuszy użycia dla zidentyfikowanych przez Zamawiającego ryzyk. Harmonogram wdrożenia zostanie ustalony w okresie przejściowym dla pierwszych scenariuszy użycia, pozostałe scenariusze zostaną przygotowane w uzgodnionym terminie. Każdorazowo Scenariusz użycia musi zostać zaakceptowany

przez Zamawiającego. Zamawiający posiada listę przykładowych scenariuszy użycia, które należy przygotować i wdrożyć. Przykładowe scenariusz użycia:

- Wykrywanie logowania z pominięciem kanału szyfrowanego
- Wykrywanie utworzenia użytkownika (lokalnego i domenowego)
- Wykrycie złośliwego oprogramowania na chronionym obiekcie

Minimalny zakres zadań, z których ma być zbudowany Scenariusz użycia systemu bezpieczeństwa zawiera:

- Skonfigurowanie jednego lub kilku źródeł zdarzeń,
- Stworzenie Scenariusza Reakcji w zakresie czynności wykonywanych przez Pierwszą Linię Wsparcia,
- Opisanie szczegółowej ścieżki eskalacji,

Opracowanie scenariusza manualnego lub automatycznego sprawdzania poprawności działania. W przypadku pojawienia się nowych skuteczniejszych technik identyfikacji zagrożeń, Wykonawca ma obowiązek zaktualizować w porozumieniu z Zamawiającym istniejące Scenariusze użycia systemu bezpieczeństwa.

✓ Scenariusz Reakcji

Przygotowany przez Wykonawcę oraz zatwierdzony przez Zamawiającego Scenariusz Reakcji określa minimalny zestaw czynności konieczny do udokumentowania oraz wyciągnięcia powtarzalnych wniosków, na podstawie których zostaną podjęte określone czynności. Scenariusz Reakcji składa się z podzadań realizujących funkcje:

- Wzbogacenia wiedzy o artefaktach tj. adresy IP, domeny, hash'e plików, nazwy plików, rozpoznawalność wskaźników kompromitacji w celu wyciągania adekwatnych wniosków i podejmowania trafnych decyzji,
- Analizy zidentyfikowanego zdarzenia, w tym w szczególności potwierdzenia, że zagrożenie w przypadku uruchomienia w środowisku Zamawiającego może stać się incydem lub jest

incydentem, jak również rozpoczęcia pobierania lub zabezpieczenia dodatkowych danych z zaatakowanego źródła ataku zasobu na potrzeby realizacji Pierwszej Linii Wsparcia,

- Reakcji rozumianej jako ograniczenie możliwości wystąpienia zdarzenia niepożądanego, uruchomienia procesu eskalacyjnego lub innych czynności stosownych do zagrożenia w zakresie uzgodnionym z Zamawiającym,
- Informowania i raportowania obejmującego dokumentowanie wykonanych czynności oraz rezultatów przeprowadzonej analizy lub zasadności czynności reakcji.

1.6 Raport Poincydentalny

Zamawiający wymaga przygotowania Raportu Poincydentalnego dla incydentów o priorytecie Poważnym i Wysokim nie później niż do 2 dni roboczych od zakończenia realizacji zawierającego informacje:

- Unikalny identyfikator zdarzenia
- Kiedy incydent wystąpił?
- Kiedy incydent został zauważony / wykryty?
- Kto lub jaki proces był sprawcą incydu?
- Co się wydarzyło?
- Gdzie wydarzenie miało miejsce?
- Dlaczego zdarzenie mogło wystąpić?
- Jakie czynności zostały przeprowadzone w celu powstrzymania incydu?
- Zalecenia Poincydentalne zawierające informację jakie zabezpieczenia zostały ustanowione lub powinny zostać ustanowione w celu zapobieżenia ponownemu wystąpieniu incydu.

W przypadku przygotowania zaleceń, dla których konieczne jest wprowadzenie istotnych zmian do systemów bezpieczeństwa lub jakiegokolwiek rekonfiguracji systemów Zamawiającego Koordynator Wykonawcy przedstawi do akceptacji Koordynatorowi Zamawiającego zakres i szczegółową listę zmian. Zwolnione z takiej czynności są Zalecenia Poincydentalne konieczne do powstrzymania zidentyfikowanego Incydu zagrażającego cyberbezpieczeństwu infrastruktury lub danych Zamawiającego.

1.7 Systemy Zamawiającego wymagające monitorowania

Usługa monitorowania, będąca przedmiotem zamówienia, będzie oparta o logi/dane z poniższych systemów Zamawiającego (źródła logów) udostępnionych przez Zamawiającego:

Rodzaj usługi lub urządzenia	Liczba urządzeń / nodów będących źródłami logów
Active Directory (liczba serwerów)	2
Windows Server (liczba serwerów)	Do 10
Linux Server (liczba serwerów)	Do 5
Stacje robocze (Windows/Linux)	Do 60
DNS, DHCP	Do 4
Systemy bezpieczeństwa np.: serwer systemu antywirusowego, Web Application Firewall, NAC, DLP	Antywirus, DLP
Serwer poczty, system antyspamowy	---
Centralny Firewall / UTM	1
Pomocniczy Firewall / UTM	---
IPS / IDS	2

VPN	Tak
Przełączniki sieci LAN, punkty dostępowe WiFi	Do 6

Zamawiający na bieżąco będzie aktualizował listę źródeł logów wysyłających nowe dane do Wykonawcy.



1.8 Ogólne warunki SLA

Wykonawca zapewni świadczenie Usługi monitorowania zgodnie z określonym poziomem SLA.



Nazwa usługi	Poziom świadczonej usługi																	
<p>Pierwsza Linia Wsparcia</p> <p>Czasy dla pierwszych zdarzeń każdego dnia w wymiarze 30 zdarzeń, pozostałe zadania realizowane będą w trybie „<i>Best Effort</i>”</p>	<p>Dostępność usługi w dni robocze pomiędzy godzinami 8:00 a 17:00.</p> <table><tr><th rowspan="2">Priorytet zdarzenia</th><th colspan="2">Czas od wykrycia przez L1 do</th></tr><tr><th>Podjęcia</th><th>Realizacji</th></tr><tr><td>Poważny</td><td>30 min</td><td>4 h</td></tr><tr><td>Wysoki</td><td>60 min</td><td>8 h</td></tr><tr><td>Średni</td><td>2 h</td><td>12 h</td></tr><tr><td>Niski</td><td>4 h</td><td>24 h</td></tr></table>	Priorytet zdarzenia	Czas od wykrycia przez L1 do		Podjęcia	Realizacji	Poważny	30 min	4 h	Wysoki	60 min	8 h	Średni	2 h	12 h	Niski	4 h	24 h
Priorytet zdarzenia	Czas od wykrycia przez L1 do																	
	Podjęcia	Realizacji																
Poważny	30 min	4 h																
Wysoki	60 min	8 h																
Średni	2 h	12 h																
Niski	4 h	24 h																

Druga Linia Wsparcia

Czasy dla pierwszych Incydentów
każdego dnia w wymiarze 5 incydentów,
pozostałe zadania realizowane w trybie
„Best Effort”

Dostępność usługi w dni robocze pomiędzy
godzinami
8:00 a 17:00.

Priorytet incydentu	Czas od eskalacji pierwszej linii wsparcia do	
	Podjęcia	Realizacji
Poważny	30 min	24 h
Wysoki	60 min	2 dni
Średni	2 h	4 dni

Analiza złośliwego oprogramowania

Rozpoczęcie analizy w terminie do 2 dni roboczych od
przekazania podejrzanej próbki oprogramowania przez
Koordynatora Zamawiającego do Koordynatora
Wykonawcy oraz potwierdzenia otrzymania próbki przez
Koordynatora Wykonawcy.

Scenariusz użycia systemu bezpieczeństwa	Przygotowanie i wdrożenie scenariusza użycia systemu wraz ze scenariuszami reakcji w terminie do 5 dni roboczych od przekazania informacji od Koordynatora Zamawiającego do Koordynatora Wykonawcy z wyjątkiem scenariuszy ujętych w harmonogramie przygotowanym w okresie przejściowym.
---	--

1. W uzasadnionych przypadkach Wykonawca ma prawo zwrócenia się do Zamawiającego o zgodę na zawieszenie SLA na usługę Pierwszej i Drugiej Linii Wsparcia na uzgodniony z Zamawiającym okres jednak nie dłuższy niż 14 dni. Wniosek o zawieszenie SLA musi zawierać uzasadnienie. Zamawiający w takim przypadku zobowiązany jest do rozpatrzenia prośby w ciągu 1 dnia roboczego od chwili uzyskania informacji o tym fakcie. W przypadku odmowy Zamawiający jest zobowiązany w ciągu 3 Dni Roboczych do przedstawienia pisemnego uzasadnienia odmowy, wskazując obiektywne czynniki świadczące o bezzasadności wniosku Wykonawcy.
2. Czas podjęcia Incydentu będzie liczony jako delta czasu pomiędzy odnotowaniem wystąpienia zdarzenia przez pierwszą linię wsparcia a czasem nadania priorytetu.
3. Czas realizacji Incydentu będzie liczony jako delta czasu pomiędzy podjęciem incydentu a zakończeniem obsługi podsumowanym wydanymi wstępnymi rekomendacjami i/lub raportem, w zależności od przypisanego scenariusza reakcji.
4. Zamawiający wyróżnia cztery poziomy incydentów: Poważny, Wysoki, Średni, Niski. Domyślnie każdy incydent zarejestrowany, jeżeli nie zostanie to uszczegółowione inaczej ma priorytet Średni.
5. Minimalny miesięczny czas świadczenia usług analizy zdarzeń to 12 godzin miesięcznie.

Priorytet	Opis
Poważny	<ol style="list-style-type: none"> 1. Priorytet jest stosowany wyłącznie w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać powyżej 50 rekordów danych objętych definicją rozporządzenia RODO; 2. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika;

	<ol style="list-style-type: none"> 3. Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) trwającej co najmniej od 30 minut w tym aktywnie wykorzystywanego (więcej niż 1kb/min); 4. Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych; 5. Informacja od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszonego w ramach inicjatywy Trusted Introducers; 6. Potwierdzona informacja od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową; 7. Informacja od Dyrektora lub Kierownika Departamentu Bezpieczeństwa; 8. Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; 9. Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności; 10. Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, przesłanie na dyski webowe lub danych z wykorzystaniem nieautoryzowanych nośników przenośnych; 11. Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego wspierającego działanie usługi kluczowej; 12. Zgłoszenie incydentu Poważnego skutkuje bezzwłocznym uruchomieniem u 13. Zamawiającego procesu eskalacyjnego KSC lub RODO;
Wysoki	<ol style="list-style-type: none"> 1. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym; 2. Ujawnienie zestawionej sesji zwrotnej z C&C, trwającej co najmniej od 30 minut, aktywnie wykorzystywanej przez atakującego (więcej niż 1kb/min); 3. Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych w strefie chronionej;

	<ol style="list-style-type: none"> Informacja od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszony w ramach inicjatywy Trusted Introducers; Potwierdzona Informacja od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową; Informacja od Dyrektora lub Kierownika Departamentu Bezpieczeństwa; Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na utworzenie tylnej furty, podsłuchu transmisji lub wykorzystania podatności; Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, upload na dyski webowe lub przenoszenie przez nieautoryzowane pendrive; Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamania zabezpieczeń (tzw. grayware); Ujawnienie nieznanego przez VirusTotal lub inne bazy reputacyjne oprogramowania mającego złośliwe funkcje pozwalające operatorowi na uruchomienie nieautoryzowanych skryptów lub kodu; Celowany atak na personel Zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;
Średni	<ol style="list-style-type: none"> Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym; Nieautoryzowane dysponowanie uprawnieniami administracyjnymi; Częściowo personalizowany atak na personel zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym; Wszystkie przypadki wystąpienia na chronionych systemach komputerowych złośliwego oprogramowania, które jest rozpoznawane przez system antywirusowy, ale nie zostało zatrzymane przez inny system bezpieczeństwa;

	5. Wszystkie potwierdzone przypadki z naruszenia poufności, dostępności lub integralności wykryte przez systemy bezpieczeństwa dla których użytkownik wyklucza świadome lub nieświadome działanie;
Niski	1. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu zdefiniowanego zdarzenia bezpieczeństwa opisanego scenariuszem reakcji, ale udało się potwierdzić, że wywołanie zdarzenia było efektem realizacji autoryzowanych czynności służbowych z pominięciem ustalonych procedur bezpieczeństwa.

1.9 Transfer wiedzy.

1. Zamawiający wymaga, aby w każdym półroczu trwania umowy, Wykonawca przeprowadził dla grupy nie większej niż 6 osób wskazanych przez Koordynatora Zamawiającego warsztaty. Łączny wymiar godzin w półroczu wynosi nie więcej niż 4. Spotkanie ma formę Warsztatów prowadzonych w formie zdalnej. Niewykorzystane godziny nie kumulują się i nie przechodzą na kolejne okresy.
2. Warsztaty swoim zakresem będą obejmować:
 - Wyjaśnianie zagrożeń płynących z wykrytych i opisanych incydentów
 - Wyjaśnianie sposobów implementacji zaleceń opisanych w Raportach Miesięcznych
 - Szczegółowy harmonogram warsztatów oraz lista uczestników zostaną uzgodnione przez Koordynatorów stron.
3. Raportowanie i rozliczanie pracy
4. Miesięczny Raport Rozliczenia Usług
 - a) Każdy miesiąc świadczenia Usług podsumowany zostanie Raportem Miesięcznym wg według wzoru przedstawionego przez Wykonawcę. Wykonawca zobowiązany jest przedstawić Raport wraz z listą zaleceń do wykonania przez personel Zamawiającego w terminie 5 Dni Roboczych od dnia zakończenia miesiąca kalendarzowego, w którym była świadczona Usługa.
 - b) Zamawiający zastrzega sobie prawo zgłoszenia zastrzeżeń do Raportu, w terminie do 5 Dni roboczych od dnia jego otrzymania i zażądać uzupełnienia lub poprawy Raportu w terminie do 3 dni roboczych. Po uwzględnieniu przez Wykonawcę uwag do Raportu, Zamawiający w terminie kolejnych 3 Dni roboczych zweryfikuje ostateczną treść Raportu.
 - c) Dostarczony Raport Miesięczny bez uwag jest potwierdzeniem prawidłowego wykonania Usługi w miesiącu, którego dotyczy.
 - d) Raport składa się z sekcji:

Monitorowanie cyberbezpieczeństwa

- Data świadczenia usług
- Zestawienie obsługiwanych incydentów
 - Identyfikator incyduentu
 - Nazwa
 - Klasyfikacja priorytetu Incyduentu
 - Dokładna data i godzina ujawnienia incyduentu
 - Statusy końcowe
- Ogólne rekomendacje i zalecenia Zamawiającego w zakresie cyberbezpieczeństwa w nawiązaniu do obsługiwanych Incyduentów w celu eliminacji możliwości pojawienia się incyduentów w przyszłości.

Analiza złośliwego oprogramowania

- Data świadczenia usług
- Lista zgłoszonych analiz złośliwego oprogramowania
- Liczba analiz przeprowadzonych zgodnie z SLA

1.10 Zespół SOC

Dla zapewnienia prawidłowej realizacji usługi SOC Zamawiający stawia minimalny wymóg dla składu zespołu SOC:

1. Operatorzy I linii SOC – 3 osoby
2. Operatorzy II linii SOC – 2 osoby
3. SOC manager – 1 osoba
4. Zarządzania podatnościami – 1 osoba
5. Eksperti od bezpieczeństwa urządzeń – 1 osoba
6. Eksperti od ochrony danych osobowych – 1 osoba
7. Eksperti od zgodności z NIS2 i KSC – 1 osoba

1.11 Wymagania dodatkowe

1. Cała dokumentacja powinna być dostarczana w edytowalnej postaci elektronicznej, w formacie przetwarzanym przez MS Word, Excel (od wersji 2007) lub PDF.
2. Zamawiający wymaga zatrudnienia przez Wykonawcę na podstawie umowy o pracę przez cały okres realizacji zamówienia 2 (dwóch) osób, wykonujących usługi w zakresie czynności Pierwszej oraz Drugiej Linii Wsparcia związanych z obsługą realizacji przedmiotu zamówienia, jeżeli wykonywane przez nich czynności polegają na wykonywaniu pracy w rozumieniu przepisu art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t. j. Dz. U. z 2018 r., poz. 917, z późn. zm.). Zamawiający uzna za spełniony obowiązek zatrudnienia osób wykonujących usługi w zakresie czynności pierwszej linii wsparcia przy realizacji przedmiotu zamówienia na podstawie umowy o pracę w przypadku, gdy Wykonawca skieruje do realizacji zamówienia własnych pracowników (dwóch) lub pracowników zatrudnionych na umowę o pracę. Zamawiający nie będzie ingerować w sposób prowadzenia działalności oraz organizację pracy administracyjno-biurowej Wykonawcy.
3. Wykonawca zobowiązany zostanie do przestrzegania polityki bezpieczeństwa opisanej w Polityce Bezpieczeństwa Informacji dla dostawców, która stanowi załącznik do umowy. O zmianach polityki mogących mieć wpływ na realizację umowy Wykonawca zostanie bezzwłocznie poinformowany.

II.17 Szkolenie administratorów zarządzania usługą Active Directory w środowisku Microsoft Windows Server 2019/2022

Zamawiający wymaga dostarczenia vouchera na szkolenie z zakresu administracji systemem Windows Server w wersji 2019 i nowszej. Voucher musi być ważny przez okres min. 6 miesięcy. Szkolenie musi być prowadzone przez profesjonalnego instruktora w formie zdalnej, w dni robocze. Czas trwania min. 2 dni. Celem szkolenia jest zdobycie wiedzy z zakresu: zarządzania tożsamościami użytkowników m.in. za pomocą usług i kontrolerów domeny usług Active Directory Domain Services (ADDS), wykorzystanie Group Policy Object (GPO) oraz automatyzacji zarządzania użytkownikami np. za pomocą zasad grupy. Minimalny, przykładowy zakres szkolenia przedstawiono poniżej:

Moduł 1: Instalacja i konfiguracja kontrolerów domeny

- Omówienie usług AD DS
- Omówienie kontrolerów domeny usług AD DS
- Wdrożenie kontrolera domeny
- Encrypted DNS – szyfrowana usługa rozpoznawania nazw w Windows Server 2022

Moduł 2: Zarządzanie obiektami w AD DS

- Zarządzanie kontami użytkowników
- Zarządzanie grupami w usługach AD DS
- Zarządzanie obiektami typu komputer w AD DS
- Wdrażanie i zarządzanie OU

Moduł 3: Zarządzanie zaawansowaną infrastrukturą AD DS

- Wprowadzenie do zaawansowanych wdrożeń AD DS
- Wdrożenie rozproszonego środowiska AD DS
- Konfiguracja relacji zaufania AD DS

Moduł 4: Wdrażanie i zarządzanie lokacjami i repliką AD DS

- Omówienie replikacji usług AD DS
- Konfigurowanie lokacji usług AD DS
- Konfigurowanie i monitorowanie replikacji usług AD DS

Moduł 5: Wdrażanie zasad grupy

- Wprowadzenie do zasad grupy
- Wdrażanie i zarządzanie obiektami GPO (Group Policy Object)
- Konfiguracja zakresu i przetwarzania obiektów GPO
- Rozwiązywanie problemów z GPO

Moduł 6: Zarządzanie ustawieniami użytkowników za pomocą zasad grupy

- Wdrażanie szablonów administracyjnych
- Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów
- Konfiguracja preferencji zasad grupowych

II.18 Dostawa i wdrożenie oprogramowania backup Szkolenie administratorów z używanych urządzeń UTM na poziomie odpowiadającym Certified Stormshield Network Administrator CSNA

Szkolenie techniczne dla administratora z zakresu obsługi używanych urządzeń UTM – 2 vouchery

Zamawiający wymaga dostarczenia vouchera na szkolenie z zakresu administracji systemem UTM używanym przez Zamawiającego. Voucher musi być ważny przez okres min. 6 miesięcy. Szkolenie musi być prowadzone przez profesjonalnego instruktora w formie zdalnej, w dni robocze. Szkolenie musi być zakończone

egzaminem oraz certyfikatem, czas trwania min. 3 dni roboczych. Szkolenie musi łączyć teorię oraz zajęcia praktyczne (warsztaty) przy użyciu nowoczesnego sprzętu i oprogramowania. Po zakończeniu szkolenia Zamawiający będzie miał możliwość kontaktu z trenerem w terminie do 14 dni od zakończenia szkolenia. Minimalny zakres szkolenia:

1. Zbieranie logów i monitorowanie
 - a. Przedstawienie kategorii zbieranych logów
 - b. Wykresy historyczne i monitorowanie
2. Obiekty
 - a. Typy obiektów oraz ich wykorzystanie
 - b. Obiekty sieciowe i obiekt typu „router”
3. Konfiguracja sieci
 - a. Tryby pracy urządzenia
 - b. Typy interfejsów (Ethernet, modem, bridge, VLAN, GRE/TAP)
 - c. Typy routingu oraz ich priorytety
4. Translacja adresów sieciowych (NAT)
5. Translacja połączeń wychodzących (maskarada)
6. Translacja połączeń przychodzących (przekierowanie)
7. Translacja dwukierunkowa (jeden do jeden)
8. Filtrowanie ruchu sieciowego (Firewall)
9. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection)
 - a. Szczegółowy opis parametrów reguły Firewall
 - b. Kolejność przetwarzania reguł Firewall i NAT
10. Ochrona aplikacji
 - a. Implementacja filtrowania URL dla ruchu http i https
 - b. Konfigurowanie skanowania antywirusowego i modułu Breach Fighter
 - c. Moduł IPS i stosowanie profili inspekcji
11. Użytkownicy i uwierzytelnianie
12. Konfiguracja usługi katalogowej
 - a. Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL, SPNEGO, SSO)
 - b. Rejestracja użytkowników
 - c. Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania
13. Wirtualne sieci prywatne (VPN)
 - a. Koncepcje i ogólne informacje dotyczące protokołu IPsec VPN (IKEv1 i IKEv2)
 - b. Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK)

c. Tunele VTI

14. SSL VPN

- a. Zasada działania
- b. Konfiguracja



Rozdział II. Gwarancja

1. Wykonawca w ramach realizacji Przedmiotu Zamówienia udzieli Zamawiającemu gwarancji jakości (dalej zwanej „gwarancją”) na niniejszy przedmiot zamówienia:

1) Dostawa i wdrożenie Infrastruktury sprzętowej wraz z oprogramowaniem:

Poz. OPZ	Opis	Gwarancja
Rozdział	Rodzaj zamawianego asortymentu	
II.2	Zakup oprogramowania bezpieczeństwa dla używanego Urządzenia UTM*	12 miesięcy
II.3	Dostawa i wdrożenie serwera backup*,**	36 miesięcy
II.4	Dostawa i wdrożenie serwera NAS*,**	36 miesięcy na urządzenie 60 miesięcy na dyski
II.5	Opracowanie projektu wykonawczego backupu oraz polityki i harmonogramu tworzenia kopii zapasowych, obejmującego wykonywanie kopii zapasowych na dyskach serwera kopii zapasowej oraz serwera NAS	12 miesięcy
II.6	Zakup zestawu taśm do biblioteki taśmowej RDX 4TB	36 miesięcy
II.7	Zakup i instalacja zasilacza awaryjnego UPS do szafy RACK*	24 miesiące
II.8	Dostawa zasilaczy awaryjnych UPS do stanowisk pracy*	36 miesięcy
II.9	Dostawa i wdrożenie oprogramowania backup*	24 miesiące

II.10	Zakup oprogramowania Serwerowego Systemu Operacyjnego Windows Server 2022	bezterminowe
II.11	Dostawa i wdrożenie zarządzalnych urządzeń sieciowych dla rdzenia sieci*	24 miesiące
II.12	Dostawa i wdrożenie zarządzalnych urządzeń sieciowych dla punktów dostępowych*	24 miesiące
II.13	Dostawa i wdrożenie systemu DLP	24 miesiące
II.14	Usługa kompleksowego przeglądu i reorganizacji posiadanego środowiska serwerowego, domeny, wraz z mechanizmem replikacji	12 miesięcy
II.15	Zakup, dostawa i wdrożenie oprogramowania SIEM wraz z dedykowanym serwerem fizycznym*,**	12 miesięcy
II.16	Zakup usługi SOC zapewniających prewencję, detekcję i reakcję na zagrożenia cyberbezpieczeństwa	6 miesięcy
II.17	Szkolenie administratorów zarządzania usługą Active Directory w środowisku Microsoft Windows Server 2019/2022	6 miesięcy
II.18	Szkolenie administratorów z używanych urządzeń UTM na poziomie odpowiadającym Certified Stormshield Network Administrator CSNA	6 miesięcy

* W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).

** W przypadku awarii dysków pozostają one własnością Zamawiającego.

2. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem podpisania Protokołu Odbioru Końcowego bez uwag przez Zamawiającego.

III.1 Wady

1. W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu Zamówienia rozumianych jako Awaria lub Błąd lub Usterka zgodnie z definicjami jak poniżej:
 - 1) **Awaria** - Kategoria Wady w Oprogramowaniu lub Infrastrukturze Sprzętowej powodująca brak działania lub niepoprawne działanie Przedmiotu Zamówienia u Zamawiającego, uniemożliwiający jego użytkowanie. Sytuacja, w której dane rozwiązanie w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Komponentów/Produktów Przedmiotu Zamówienia
 - 2) **Usterka** - Należy przez to rozumieć kategorię Wady w Oprogramowaniu lub Infrastrukturze Sprzętowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz OPZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.
2. Przyjęcie zgłoszenia Wady przez Wykonawcę, odbywać się będzie poprzez dostępny on-line System Zgłaszania i przyjmowania uwag oraz Wad (dalej zwany SZ) przy czym:
 - 1) System Zgłoszeń dostarczy Wykonawca (będzie on utrzymywany i administrowany przez Wykonawcę), wpis zgłoszenia do SZ będzie dokonywał Zamawiający,
 - 2) za skuteczne przyjęcie zgłoszenia Wady uważa się będzie wprowadzenie przez Zamawiającego wpisu do SZ zawierającego opis zgłaszanej Wady i termin jej zgłoszenia; w razie trudności z dostępem on-line do SZ, zgłoszenia Wady mogą odbywać się także telefonicznie pod ustalonym numerem telefonu lub pisemnie na formularzu przesyłanym na ustalony adres e-mail, opcjonalnie faksem, których numery i adresy zostaną podane przez Wykonawcę w terminie 15 dni roboczych od dnia podpisania Umowy wraz ze wzorem formularza zgłoszenia Wady.
3. Gwarancja musi zapewniać wymianę uszkodzonego sprzętu, kabli i elementów oraz zapewniać dostęp do aktualizacji oprogramowania, bez wiedzy i wsparcia technicznego producenta.
4. W ramach gwarancji Wykonawca będzie świadczył następujące usługi:
 - 1) Usuwanie Wad w dostarczonym Przedmiocie Zamówienia w przypadku stwierdzenia przez Zamawiającego Wady w jego działaniu, w terminach określonych poniżej:

Tabela 1. Usługi gwarancji dla Infrastruktury sprzętowej i oprogramowania:

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE*	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	24/7/365	niezwłocznie, nie później niż 48 godzin od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 14 dni od czasu przyjęcia zgłoszenia
USTERKA		nie dotyczy	niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 30 dni od dnia przyjęcia zgłoszenia

* nie dotyczy sprzętu zastępczego

- 2) dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego. Do czasu potwierdzenia zmiany kwalifikacji, uznaje się za obowiązującą kwalifikację pierwotną,
- 3) czasy naprawy mogą być inne niż wskazane w powyższej tabeli, jeżeli Zamawiający zaakceptuje zmianę kwalifikacji zgłoszenia, o której mowa w punkcie 2),
- 4) w przypadku braku możliwości usunięcia Wady lub przedstawienia rozwiązania zastępczego zdalnie, Wykonawca zobowiązany jest do świadczenia gwarancji bezpośrednio w lokalizacji Zamawiającego,
- 5) Wykonawca w okresie trwania gwarancji, do 5 dnia każdego miesiąca, przedstawi Zamawiającemu raport zawierający co najmniej: numer zgłoszenia, kwalifikację zgłoszenia, godzinę i datę zgłoszenia, temat zgłoszenia, status zgłoszenia, godzinę i datę usunięcia Wady, czas naprawy,

Uwaga:

W przypadku zapisu terminu jako:

- Dzień Roboczy należy rozumieć każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
- Godziny Robocze należy rozumieć godziny od 8.00 do 16.00 w każdym Dniu Roboczym.

W innych przypadkach należy rozumieć jako dzień kalendarzowy.

