Załącznik nr 5 do SIWZ

SR.271.17.2022

OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup i dostawa sprzętu IT wraz z oprogramowaniem w ramach realizacji projektu grantowego „Cyfrowa Gmina”

w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego **„Cyfrowa Gmina”** o numerze POPC.05.01.00-00-0001/21-00

Opis przedmiotu zamówienia wg Wspólnego Słownika Zamówień (CPV):

48620000-0 Systemy operacyjne
48000000-8 Pakiety oprogramowania i systemy informatyczne
48710000-8 Pakiety oprogramowania do kopii zapasowych i odzyskiwania
48820000-2 Serwery
48821000-9 Serwery sieciowe
48823000-3 Serwery plików
51610000-1 Usługi instalowania urządzeń komputerowych i przetwarzania informacji
72265000-0 Usługi konfiguracji oprogramowania
32428000-9 Modernizacja sieci
32420000-3 Urządzenia sieciowe


Fundusze
Europejskie
Polska Cyfrowa
Rzeczpospolita
Polska
Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego

Zawartość:

I. OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA I WYMAGAŃ ZAMAWIAJĄCEGO

1. Zakres przedmiotu zamówienia

Zakup i dostawa sprzętu IT wraz z oprogramowaniem w ramach realizacji projektu grantowego „Cyfrowa Gmina” .

Szczegółowy zakres projektu składa się z następujących zadań:

1. Dostawa, instalacja oraz konfiguracja platformy serwerowej wraz z oprogramowaniem systemowym

- Serwer wirtualizacji Rack 19" – 1 kpl
- Oprogramowanie systemowe serwera – 1 lic
- Licencje dla użytkowników serwera (np. Microsoft Windows Server User CAL, lub równoważny) – 25 lic.
- Usługi instalacji, konfiguracji oraz wdrożenia – zgodnie z wcześniej opracowaną koncepcją techniczną

2. Rozbudowa oraz konfiguracja systemu archiwizacji danych oraz wykonywania kopii zapasowych

- Dysk NAS 10TB SATA – 4 szt.
- Oprogramowanie do archiwizacji i backupu danych – 1 lic
- Usługi instalacji, konfiguracji oraz wdrożenia – zgodnie z wcześniej opracowaną koncepcją techniczną

3. Zakup usług chmurowych

- Usługi backupu i archiwizacji danych w zapasowym Data-Center – 1 kpl

4. Dostawa, instalacja oraz konfiguracja systemu zapewnienia bezpieczeństwa teleinformatycznego (cyberbezpieczeństwo)

- Oprogramowanie UTM security (zakup licencji oraz wykonanie migracji systemu UTM) – 1 kpl
- Dostawa, instalacja oraz konfiguracja urządzenia UTM min. 8x GE RJ45 – 1 kpl
- Usługi instalacji, konfiguracji oraz wdrożenia – zgodnie z wcześniej opracowaną koncepcją techniczną

2. Ogólne wymagania Zamawiającego

Niniejszy dokument ma celu umożliwienie dokonania wyboru najkorzystniejszej oferty na dostawy i usługi teleinformatyczne, których podstawowym celem jest podniesienie poziomu cyfryzacji Urzędu oraz bezpieczeństwa teleinformatycznego (cyberbezpieczeństwa) w ramach projektu „Cyfrowa Gmina”. Dokument zawiera opis wymagań pod kątem kryteriów funkcjonalnych, technicznych i jakościowych, oraz

wskazuje technologie, które powinny być wykorzystane tak aby osiągnąć założone cele i zapewnić optymalną relację ceny do jakości rozwiązania.
Opisane w dokumencie wymagania należy traktować jako podstawowe i minimalne.

W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”

W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.

W przypadku zastosowania materiałów, urządzeń, wyrobów lub rozwiązań równoważnych, Wykonawca zobowiązany jest do ich wskazania w ofercie oraz do złożenia wraz z ofertą kart technicznych lub innych dokumentów potwierdzających, że oferowane rozwiązania równoważne spełniają wymagania Zamawiającego opisane w przedmiocie zamówienia.

Wymagania ogólne dotyczące sprzętu:

1) Wszystkie dostarczone urządzenia muszą być fabrycznie nowe, bez wad i uszkodzeń, nieregenerowane, nieużywane i nie będące przedmiotem wystaw i prezentacji oraz o ile nie wyspecyfikowano inaczej w wymaganiach szczegółowych dla urządzeń, wyprodukowane nie wcześniej niż 2021 roku.
2) Wszystkie urządzenia będą pochodziły z oficjalnego, europejskiego kanału dystrybucji.
3) Urządzenia zostaną dostarczone przez Wykonawcę własnym transportem i na własny koszt w miejsce wskazane przez Zamawiającego. Wszystkie urządzenia muszą być dostarczone w oryginalnych opakowaniach producenta,
4) Wszystkie urządzenia powinny być zgodne z normami UE i przeznaczone na rynek UE, oraz powinny posiadać certyfikat CE.
5) Dostarczany sprzęt powinien być kompletny i gotowy do uruchomienia, tak aby nie był konieczny zakup dodatkowych elementów czy akcesoriów,
6) Wykonawca dostarczy stosowne potwierdzenie gwarancji sprzętu i oprogramowania zapewniające, że sprzęt objęty jest gwarancją producenta
7) Serwis sprzętu będzie świadczony przez producenta lub jego autoryzowanego partnera serwisowego posiadającego wdrożoną normę min. PN-EN ISO 9001 lub równoważną.
8) Sprzęt dostarczany w ramach niniejszego zamówienia, powinien być objęty 36 miesięczną gwarancją i wsparciem producenta chyba, że okres i warunki gwarancji zostały dodatkowo określony w opisie szczegółowym specyfikowanego wyposażenia/sprzętu. W okresie gwarancji Wykonawca jest zobowiązany zapewnić Zamawiającemu:

a. usuwanie wszelkich wad i nieprawidłowości powstałych na wskutek standardowej i zgodnej z przeznaczeniem eksploatacji przedmiotu zamówienia
b. przyjmowanie zgłoszeń serwisowych w godzinach 8.00-20.00 (faks lub e-mail) z możliwością zgłaszania awarii bezpośrednio u producenta (na wypadek braku reakcji serwisowej ze strony Wykonawcy)
c. dostęp do bezpośredniego wsparcia technicznego producenta wraz z prawem do aktualizacji oprogramowania systemowego

9) W ramach gwarancji wymagane jest wsparcie producenta sprzętu, a czas reakcji na zgłoszenia będzie realizowany w trybie następny dzień roboczy w miejscu instalacji i zastrzeżeniem, że uszkodzone nośniki danych pozostają u Zamawiającego. Ponadto wymagane jest, aby dostarczony poziom wsparcia producenta dawał możliwość kategoryzacji zgłoszeń i w przypadku awarii krytycznych gwarantował natychmiastową pomoc telefoniczną, szybką interwencję specjalisty ds. eskalacji zgłoszeń oraz wizytę serwisanta i/lub wysyłkę uszkodzonych części

10) Udzielona gwarancja producenta nie wyłącza uprawnień Zamawiającego z tytułu rękojmi w stosunku do Wykonawcy.

Wymagania ogólne dotyczące oprogramowania:

Wykonawca zobowiązany jest dostarczyć Zamawiającemu:

1) certyfikaty licencyjne wystawione przez producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na dedykowanym portalu klienckim;
2) nośniki instalacyjne Oprogramowania, o ile nie są dostępne w formie elektronicznej na dedykowanym portalu klienckim;
3) adresy poczty elektronicznej, numery telefonów oraz inne dane dostępowe umożliwiające Zamawiającemu korzystanie ze Wsparcia technicznego świadczonego przez producenta Oprogramowania w pełnym zakresie, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
4) zestawienie dostarczonych Zamawiającemu pozycji w zakresie Oprogramowania, zawierające m.in.: numer partii (SKU), pełna nazwa produktu, wersja i edycja oprogramowania, metryka licencyjna, rodzaj licencji (terminowa/bezterminowa), okres obowiązywania licencji, okres obowiązywania wsparcia technicznego, poziom wsparcia technicznego,
5) standardowe warunki licencyjne producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
6) standardowe warunki Wsparcia technicznego producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
7) oświadczenie producenta Oprogramowania potwierdzające dostawę licencji i objęcie ich wsparciem technicznym na poziomie zgodnym z wymaganiami Zamawiającego, o ile nie potwierdzają jej certyfikaty licencyjne i standardowe warunki Wsparcia technicznego;

Realizacja powyższego zakresu zamówienia musi być wykonana w oparciu o obowiązujące przepisy, przez Wykonawcę posiadającego stosowne doświadczenie, uprawnienia i potencjał wykonawczy oraz osoby o odpowiednich kwalifikacjach i doświadczeniu zawodowym.

II. SZCZEGÓŁOWE WŁAŚCIWOŚCI I WYMAGANIA FUNKCJONALNO - UŻYTKOWE

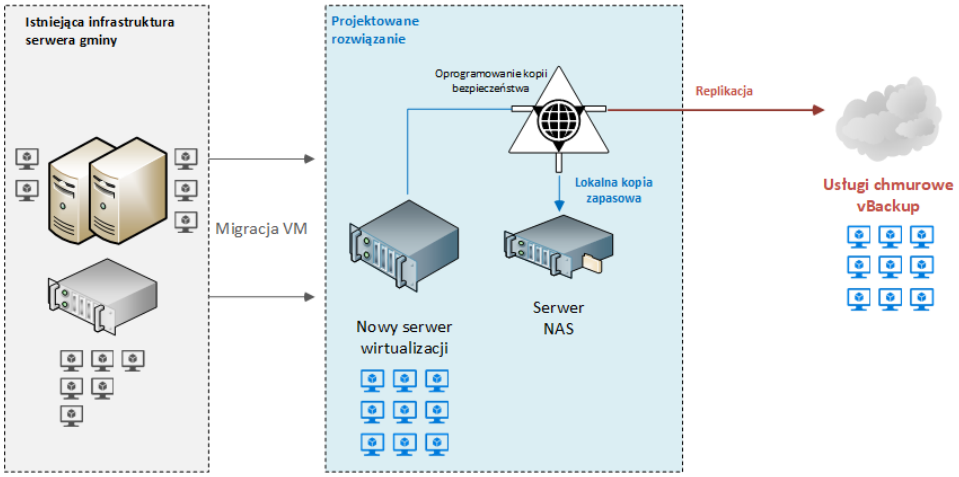
1. Dostawa, instalacja oraz konfiguracja platformy serwerowej wraz z oprogramowaniem systemowym

1.1. Koncepcja wdrożenia

Przeznaczenie:

1. Podstawowy kontroler domeny, usługi katalogowe LDAP
2. Dodatkowe usługi domenowe w zależności od potrzeb (DHCP, WSUS, PrintServer, Serwer Plików, Serwer Terminali, Centrum certyfikatów)
3. Wirtualna przystawka do zarządzania infrastrukturą backup'ową
4. Wirtualne serwery przeniesione ze starych hostów.

Poniżej przedstawiono ogólny schemat docelowego rozwiązania, obejmujący zasoby własne (istniejący serwer wraz z zasobami dyskowymi) oraz projektowany system serwerowy wraz z istniejącą, rozbudowaną macierzą dyskową:



Projektowane rozwiązanie obejmuje następujące elementy infrastruktury serwerowej:

- serwer wirtualizacji
- serwer plików NAS (backup i centralne repozytorium plików)
- oprogramowanie systemowe oraz oprogramowanie do wykonywania kopii bezpieczeństwa z uwzględnieniem dodatkowej lokalizacji (replika danych do chmury)

Dostawa oraz wdrożenie wszystkich wskazanych wyżej elementów infrastruktury odpowiada na zdiagnozowane potrzeby w ramach przeprowadzonej inwentaryzacji i wypełnia sugestie i zalecenia określone podczas przeprowadzonego audytu.

Projektowane rozwiązanie powinno również spełnić wymagania określone w rozdziale IV rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, obowiązujących norm oraz standardów rynkowych. Zgodnie bowiem z zapisami §20 ust. 2 (KRI) system powinien spełniać wymagania w zakresie :
- minimalizacji ryzyka utraty informacji w wyniku awarii
- zapewnienia bezpieczeństwa przechowywanych plików systemowych oraz innych ,
- zapewnienia możliwości regularnej aktualizacji oprogramowania (nowy system będzie posiadał wsparcie techniczne producenta w okresie eksploatacji).

Szczegółowe wymagania w zakresie parametrów technicznych i funkcjonalnych poszczególnych elementów infrastruktury zostały określone w dalszej części dokumentu.

1.2. Serwer wirtualizacji Rack 19" – 1 kpl

Parametr lub warunek	Minimalne wymagania
Typ	Serwer wirtualizacyjny typu Rack 19”. W ofercie wymagane jest podanie modelu i producenta serwera.
Obudowa	• Typu RACK, wysokość nie więcej niż 2U; • Szyny umożliwiające wysunięcie serwera z szafy stelażowej; • Możliwość zainstalowania 10 dysków twardych hot plug 3,5”; • Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych; • Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray

Płyta główna	• Dwuprocesorowa;
	• Wyprodukowana i zaprojektowana przez producenta serwera
	• Możliwość instalacji procesorów 38-rdzeniowych;
	• Zainstalowany moduł TPM 2.0;
	• 6 złącz PCI Express generacji 4 w tym:
	  • 4 fizyczne złącza o prędkości x16;
	  • Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
	  • Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e;
	• 32 gniazda pamięci RAM;
	• Obsługa minimum 4TB pamięci RAM DDR4;
	• Obsługa minimum 12TB pamięci RAM DDR4 + pamięć nieulotna
	• Wsparcie dla technologii:
	  • Memory Scrubbing
	  • SDDC
	  • ECC
	  • Memory Mirroring
	  • ADDDC;
	• Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci)
	Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug;

Procesory	• Jeden procesor 16-rdzeniowy, taktowanie min. 2,4GHz, architektura x86_64 osiągające w oferowanym serwerze w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base minimum 235 pkt (wynik

	musi być opublikowany na stronie https://www.spec.org/cpu2017/results/cpu2017.html
Pamięć RAM	• 128 GB pamięci RAM • DDR4 Registered 3200Mhz
Dyski	• Zainstalowane 4 szt. dysków SSD SATA 900GB DWPD>3,5 Hot-Plug; • Zainstalowane 4 szt. dysków SATA 2TB Hot-Plug;
Kontrolery LAN	Karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 4x 1Gbit Base-T, możliwość wymiany zainstalowanych interfejsów na 2x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;
Kontrolery I/O	Zainstalowany kontroler SAS RAID obsługujący poziomy 0,1,10,5,50,6,60 posiadający 2GB pamięci cache zabezpieczonej za pomocą baterii lub kondensatora.
Porty	• Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; • 2 port USB 3.0 wewnętrzne; • 2 porty USB 3.0 dostępne z tyłu serwera; • Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem; • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; • 2 porty USB 3.0 na panelu przednim
Zasilanie, chłodzenie	• Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy minimalnej 900W; • Redundantne wentylatory hotplug;

Zarządzanie	• Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii
	  • informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
	  o karty rozszerzeń zainstalowane w dowolnym slocie PCI Express
	  o procesory CPU
	  o pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM
	  o wbudowany na płycie głównej nośnik pamięci M.2 SSD
	  o status karty zrządzającej serwera
	  o wentylatory
	  o bateria podtrzymująca ustawienia BIOS płyty główne
	  o zasilacze
	Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
	• Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający zarządzanie, zdalny restart serwera;
	  • Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
	  • Dostęp poprzez przeglądarkę Web, SSH;
	  • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
	  • Zarządzanie alarmami (zdarzenia poprzez

	SNMP) • Możliwość przejęcia konsoli tekstowej • Możliwość zarządzania przez 6 administratorów jednocześnie • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Obsługa serwerów proxy (autentykacja) • Obsługa VLAN • Możliwość konfiguracji parametru Max. Transmission Unit (MTU) • Wsparcie dla protokołu SSDP • Obsługa protokołów TLS 1.2, SSL v3 • Obsługa protokołu LDAP • Integracja z HP SIM • Synchronizacja czasu poprzez protokół NTP • Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); • Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB; • Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; • Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. BIOS UEFI w specyfikacji 2.7;
Wspierane OS	• Microsoft Windows Server 2022, 2019, 2016 • VMWare vSphere 6.7, 7.0 • Suse Linux Enterprise Server 15 • Red Hat Enterprise Linux 7.9, 8.3 • Hyper-V Server 2016, 2019
Gwarancja	• 60 miesięcy gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. • Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; • Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej; • Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; • Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki

Dokumentacja, inne	• Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie producenta; • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie producenta; • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; • W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; • Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %; Zgodność z normami: CB, RoHS, WEEE, GS oraz CE;
Licencja wirtualizator	W ramach licencji wieczystej oprogramowanie musi spełniać następujące wymagania poprzez wbudowane mechanizmy: 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET

13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. 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),
19. 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..
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. 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:
    - Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
    - 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.
    - Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    - Zdalna dystrybucja oprogramowania na stacje robocze.
    - Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    - Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

	- Dystrybucję certyfikatów poprzez http - Konsolidację CA dla wielu lasów domeny, - Automatyczne rejestrowania 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). - Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. - Serwis udostępniania stron WWW. - Wsparcie dla protokołu IP w wersji 6 (IPv6), - Wsparcie dla algorytmów Suite B (RFC 4869), - Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, - Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, - Obsługi ramek typu jumbo frames dla maszyn wirtualnych. - Obsługi 4-KB sektorów dysków - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 26. 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. 27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Licencja serwerowy system operacyjny	Licencja musi uprawniać do zainstalowania serwerowego systemu operacyjnego w najnowszej dostępnej na rynku wersji w środowisku fizycznym, lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Wymaga się aby oferowane licencje umożliwiały korzystanie:

- **25 użytkownikom z zasobów serwera**

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    - Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    - Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
    - Login i hasło,
    - Karty z certyfikatami (smartcard),
    - Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. 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..

20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. 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:
    - Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
    - 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.
    - Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    - Zdalna dystrybucja oprogramowania na stacje robocze.
    - Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    - Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
    - Dystrybucję certyfikatów poprzez http
    - Konsolidację CA dla wielu lasów domeny,
    - Automatyczne rejestrowania 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).
    - Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
    - Serwis udostępniania stron WWW.
    - Wsparcie dla protokołu IP w wersji 6 (IPv6),
    - Wsparcie dla algorytmów Suite B (RFC 4869),
    - Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
    - Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych

	systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, - Obsługi ramek typu jumbo frames dla maszyn wirtualnych. - Obsługi 4-KB sektorów dysków - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 26. 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. 27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim

2. Rozbudowa oraz konfiguracja systemu archiwizacji danych oraz wykonywania kopii zapasowych

2.1. Koncepcja wdrożenia

Macierz dyskowa stanowi jeden z ważniejszych elementów infrastruktury IT ponieważ odpowiada za bezpieczeństwo przechowywania, przetwarzania oraz transmisji danych, w związku z tym rozwiązanie powinno spełniać wymagania określone w rozdziale IV rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, obowiązujących norm oraz standardów rynkowych.

Użytkowa przestrzeń dyskowa macierzy będzie wykorzystana na potrzeby:
1. Zapisu danych z systemów dziedzinowych i ich archiwizacja,
2. Przechowywania plików dziennika systemowego,
3. Udostępnienia przestrzeni na udziały współdzielone.

Należy dostarczyć dyski dużej pojemności i wysokiej dostępności klasy Enterprise dla istniejącej macierzy NAS.

2.2. Dysk NAS 10TB SATA – 4 szt.

Parametr lub warunek	Minimalne wymagania
Typ i przeznaczenie	Dysk twardy – wewnętrzny, kompatybilny z serwerem NAS
Pojemność	10 TB
Rodzaj obudowy	3,5"
Interfejs	SATA 6Gb/s
Wielkość bufora	256 MB
Cechy	Obsługa “podłączania na gorąco”, zaawansowany format 512e, dostępność 24x7, czujnik wibracji obrotowych
Wymiary	Szerokość 101.85 mm, Głębokość 146.99 mm, Wysokość 26.11 mm, Waga 722 g
Szybkość transmisji urządzenia	600 MBps (zewnętrzna)
Szybkość wewnętrzna danych	214 MBps
Średnie opóźnienie	4.16 ms
Prędkość obrotowa	7200 obr/min
MTBF	1 200 000 godziny
Praca 24x7	Tak
Błędy nienaprawialne	1 na 10^15
Interfejsy	1 x SATA 6 Gb/s
Zużycie energii	5.0 wat (bezczynność), 7.8 wat (aktywny), 0.8 wat (tryb czuwania), 0.8 wat (stan uśpienia)
Minimalna temperatura pracy	5 °C
Maksymalna temperatura pracy	60 °C
Odporność na wstrząsy (podczas pracy)	70 g @ 2 ms
Odporność na wstrząsy (w stanie spoczynku)	250 g @ 2 ms
Odporność na drgania (w stanie spoczynku)	2.27 g @ 10-500 Hz
Gwarancja i wsparcie techniczne	5-letnia gwarancja producenta

2.3. Oprogramowanie do archiwizacji i backupu danych – 1 lic

W ramach licencji wieczystej lub subskrypcji oprogramowania na okres nie krótszy niż 12 miesięcy oprogramowanie musi spełniać następujące wymagania poprzez wbudowane mechanizmy:

Parametr lub warunek	Minimalne wymagania
Wspierane systemy operacyjne	Dla hosta: • VMware ESX/ESX(i) 5.0, 5.1, 5.5, 6.0, 6.5, 6,7. • Hyper-V Dla maszyn wirtualnych: • Windows XP (SP3) i nowsze. • Windows Server 2003 i nowsze. • Windows SBS 2011/2008, 2003/2003R2. • Windows Storage Server 2012/2012R2, 2008R2/2008/2003. • Windows MultiPoint Server 2012/2011/2010. • Linux OS • macOS
Zarządzanie systemem kopii zapasowych	• Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www. • Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego). • Zarządzanie procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT. • Definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem). • Zdalna instalacja agentów kopi zapasowych na maszynach z systemem operacyjnym Windows. • Zdalne uaktualniania agentów kopi zapasowych. • Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych.
Wykonywanie kopii zapasowych	• Kopie zapasowe całych dysków i partycji. • Kopie zapasowe wybranych plików i folderów. • Technologia bezagentowego wykonywania kopii zapasowej dla maszyn wirtualnych (dotyczy Hyper-V i VMWare ESXi). • Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory). • Kopie zapasowe hostów Hyper-V i VMWare ESXi. • Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych. • Zapis kopi zapasowych na udziały sieciowe. • Zapis kopi zapasowych na serwer SFTP. • Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana. • Wyszukiwanie plików w kopiach zapasowych. • Szyfrowanie plików kopi zapasowych. • Wsparcie dla technologii VSS. • Kompresja plików kopi zapasowych. • Replikacja kopi zapasowych na kolejny nośnik (dysk, magazyn chmurowy).
Odtwarzanie kopii zapasowych	• Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore. • Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie. sprzętowej niż ta, z której wykonano kopię zapasową. • Odtworzenie całej maszyny wirtualnej. • Odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej platformie sprzętowej. • Odtworzenie poszczególnych plików i folderów. • Granularne odtwarzanie baz danych Microsoft Exchange. • Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange.

	• Wyszukiwanie i podgląd odtwarzanych wiadomości email. • Granularne odtwarzanie baz danych Microsoft SQL. • Granularne odtwarzanie witryn i plików Microsoft SharePoint. • Odtwarzanie kontrolerów domeny Microsoft Active Directory. • Dla hostów VMware ESXi i Hyper-V – uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej bez konieczności odtwarzania całej maszyny na hoście. Możliwość docelowego odtworzenia uruchomionej maszyny z pliku kopii zapasowej na wybranym hoście bez przerywania jej pracy.
Dodatkowe wymagania	• Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń

3. Zakup usług chmurowych

3.1. Usługi backupu i archiwizacji danych w zapasowym Data-Center – 1 kpl

Zamówienie obejmuje usługi alokacji przestrzeni dyskowej w wyniesionej lokalizacji (zewnętrznym Data Center) jako uzupełnienie bezpieczeństwa przechowywania danych i kopii zapasowych. Wymagane jest zapewnienie minimum 3TB użytecznej przestrzeni dyskowej przez okres 18 miesięcy od dnia zawarcia Umowy.
Do zadań Wykonawcy będzie należało:

A. Opracowanie planu (koncepcji) archiwizacji danych oraz wykonywania kopi zapasowych a także odtwarzania w przypadku awarii
B. Zapewnienie usług chmurowych – min 3 TB efektywnej przestrzeni dyskowej
C. Wdrożenie mechanizmów tworzenia kopii zapasowych i przechowywania danych w oparciu o zasoby lokalne oraz chmurowe
D. Zapewnianie bezpiecznej (szyfrowanej) komunikacji z Data-Center

Wymagania techniczno-organizacyjne dla zapasowego Data-Center:

- obiekt zlokalizowany na terenie Polski (Zamawiający nie dopuszcza wynoszenia danych poza granice kraju)
- budynek powinien spełniać standardy bezpieczeństwa fizycznego i technicznego dla tego typu obiektów (konstrukcja żelbetowa, bezpieczne położenie, podłogi techniczne itp.)
- obiekt powinien być położony powyżej poziomu gruntu (nie piwnica i nie na piętrze)
- obiekt położony na terenie niezurbanizowanym (mieszkańcy, bloki, itp.)
- minimalnie 2, a pożądane 3 różne źródła zasilania
- redundantny system podtrzymywania zasilania UPS
- redundantny system klimatyzacji precyzyjnej i filtrowania zanieczyszczeń
- system monitorowania parametrów środowiskowych z czujnikami temperatury, wilgotności oraz zalania
- bieżący nadzór Inżynierów DC na miejscu w ośrodku, możliwość wejścia do obiektu i korzystania z remote hands
- 24/7/365 ochrona całego terenu, na którym posadowione jest DC zapewniana przez dedykowaną, licencjonowaną agencję ochrony.

Technologia:

- zasoby dyskowe SATA, SAS podłączone w technologii NAS
- dostęp TCP IP (połączenie szyfrowane VPN)
- dostęp do zasobów z wykorzystaniem protokołów NFS, CIFS, FTP
- audyt log dostępu do zasobów
- redundancja RAID, redundancja kontrolerów macierzy, redundancja połączeń, redundancja zasilania.
- zasilacze, dyski, kontrolery powinny być w technologii hot swap
- dostępność do danych przynajmniej 99,95% w skali roku

Usługi dodatkowe:

- zapewnienie szyfrowanej transmisji danych o przepustowości min. 50 Mb/s
- wsparcie inżynierskie

4. Dostawa, instalacja oraz konfiguracja systemu zapewnienia bezpieczeństwa teleinformatycznego (cyberbezpieczeństwo)

4.1. UTM typ I min. 8x GE RJ45 – 1 kpl

Parametr lub warunek	Minimalne wymagania

Wymagania Ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. Uwaga! W przypadku dostawy tzw. produktów podwójnego zastosowania, Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania..
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall musi dysponować minimum: • 10 portami Gigabit Ethernet RJ-45. • 2 gniazdami SFP 1 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps
Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure • Google Cloud Platform (GCP). • OpenStack. • VMware NSX.
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
Funkcje SD-WAN	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs,

	Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.
Gwarancja, wsparcie oraz licencje	1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7 2. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall 3. Wymagane licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

*Zamawiający dopuszcza wykonanie migracji istniejącego systemu UTM do najnowszej wersji w ramach programu “Trade-UP”.

4.2. UTM typ II min. 8x GE RJ45 – 1 kpl

Architektura urządzenia, obudowa, interfejsy

1. Urządzenie będące dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia
2. Urządzenie pełniące rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall)
3. Urządzenie wyposażone w 8 portów 10/100/1000 Gigabit Ethernet RJ-45
4. Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – minimum 1 000 sieci VLAN
5. Urządzenie wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band
6. Urządzenie wyposażone w port USB 2.0
7. Wysokość urządzenia 1RU

Parametry wydajnościowe

8. Przepustowość teoretyczna urządzenia dla uruchomionych modułów firewall'a oraz kontroli aplikacji (AVC) na poziomie 650Mb\s, dla modułów AVC oraz systemu IPS na poziomie 650Mb\s
9. Maksymalna liczba sesji (z kontrolą aplikacji) na poziomie 100 000 z możliwością zestawiania co najmniej 6 000 nowych połączeń na sekundę

Funkcjonalność urządzenia

10. Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
11. Możliwość uruchomienia urządzenia w trybie firewall'a L3, jak i w trybie transparentym
12. Urządzenie obsługuje routing statyczny i dynamiczny (RIP, OSPF, BGP)
13. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory
14. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT)
15. Urządzenie zapewnia mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby
16. Urządzenie zapewnia funkcjonalność tzw. Firewall'a Next-Generation w zakresie:
    a. systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control)
    b. systemu IPS
    c. systemu ochrony przed malware
    d. systemu filtracji ruchu w oparciu o URL
17. System posiada możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System ma tworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów:
    a. Wiedza o użytkownikach – uwierzytelenienie
    b. Wiedza o urządzeniach – pasywne skanowanie ruchu
    c. Wiedza o urządzeniach mobilnych
    d. Wiedza o aplikacjach wykorzystywanych po stronie klienta
    e. Wiedza o podatnościach
    f. Wiedza o bieżących zagrożeniach
    g. Baza danych URL
18. System posiada otwarte API dla współpracy z systemami zewnętrznymi w tym co najmniej z systemami SIEM
19. System wykrywania aplikacji AVC zapewniający:
    a. możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji
    b. możliwość tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług
    c. wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji
    d. współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach
20. System IPS zapewniający:
    a. możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system)
    b. możliwość pracy w trybie pasywnym (IDS)
    c. możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym:
        i. złośliwe oprogramowanie
        ii. skanowanie sieci

   iii. ataki na usługę VoIP
   iv. próby przepełnienia bufora
   v. ataki na aplikacje P2P
   vi. zagrożenia dnia zerowego, itp.
d. możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna)
e. wiele sposobów wykrywania zagrożeń w tym:
   i. sygnatury ataków opartych na exploitach
   ii. reguły oparte na zagrożeniach
   iii. mechanizm wykrywania anomalii w protokołach
   iv. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego
f. możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu
g. mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives)
h. możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń
i. wiele możliwości reakcji na zdarzenia w tym takie, jak:
   i. tylko monitorowanie
   ii. blokowanie ruchu zawierającego zagrożenia
   iii. zastąpienie zawartości pakietów
   iv. zapisywanie pakietów
j. możliwość detekcji ataków i zagrożeń opartych na protokole IPv6
k. możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o:
   i. systemach operacyjnych
   ii. serwisach
   iii. otwartych portach, aplikacjach
   iv. zagrożeniach
l. możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych
m. możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.
n. możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji
o. możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego
p. mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne
q. możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie
r. obsługę reguł Snort
s. możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS
t. mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise)

u. mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa

21. System filtracji URL zapewniający:
    a. kategoryzację stron – w co najmniej 70 kategoriach
    b. bazę URL o wielkości nie mniejszej niż 250 mln URL
22. Urządzenie zapewnia możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym:
    a. pliki systemowe
    b. pliki graficzne
    c. pliki PDF
    d. pliki wykonywalne
    e. pliki multimedialne
    f. pliki pakietu Office
    g. pliki skompresowane
23. Urządzenie posiada możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download
24. Wbudowany podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez
    a. sprawdzenie reputacji plików w systemie globalnym
    b. sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze)
    c. statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu
25. Urządzenie zapewnia możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach:
    a. pliki wolne od złośliwego kodu
    b. pliki zawierające złośliwy kod
    c. pliki podejrzane
    d. pliki o własnej, zdefiniowanej przez użytkownika kategorii
26. Podsystem wykrywania oprogramowania złośliwego zawiera narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna)
27. Możliwość rozbudowy podsystemu antimalware o agenta instalowanego na stacjach roboczych i serwerach. Konsola zarządzająca posiadająca możliwość wyświetlenia szczegółowej trajektorii transferu danego pliku po monitorowanej sieci oraz korelacji zdarzeń przychodzących z rozwiązania antymalware rezydującego na serwerach i stacjach roboczych
28. Urządzenie objęte 3-letnim serwisem świadczonym bezpośrednio przez producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia.

4.3. Zakres prac konfiguracyjnych i wdrożeniowych

Zakres prac wdrożeniowych będzie obejmował zarówno dostarczone elementy systemu jak i te które są w posiadaniu Zamawiającego. Przed rozpoczęciem prac wdrożeniowych należy dokonać szczegółowej weryfikacji aktualnej konfiguracji oraz opracować koncepcję techniczną korekty konfiguracji wraz z założeniami polityki bezpieczeństwa.

Zakres prac wdrożeniowych (dla obu urządzeń UTM) powinien obejmować co najmniej:

- Przygotowanie polityki bezpieczeństwa komunikacji z Internetem,
- Aktualizacja oprogramowania urządzeń do najnowszej wersji stabilnej, zalecanej przez producenta,
- Instalacja urządzeń w szafach dystrybucyjnych, podłączenie okablowania i uruchomienie komunikacji w sieci LAN oraz na styku z Internetem,
- Konfiguracja środowiska zarządzania w szczególności: ustawienie wszystkich parametrów związanych z adresacją i routingiem IP, ograniczenie zdalnego dostępu do urządzeń, konfiguracja autentykacji użytkowników, zapewnienie możliwości zarządzania poprzez protokoły SSH i HTTPS,
- Konfiguracja autentykacji użytkowników w zakresie dostępu do poszczególnych usług (aplikacji) w oparciu o usługi katalogowe AD
- Konfiguracja analizy ruchu SSL na poziomie protokołów HTTPS oraz SSH,
- Konfiguracja inspekcji ruchu pod katem programów złośliwych, wirusów itp.,
- Konfiguracja mechanizmów zabezpieczających przed znanymi atakami w sieci typu DoS, Spoofing, Sniffing itp.,
- Konfiguracja systemu raportowania oraz rejestru zdarzeń,
- Testy poprawności konfiguracji,
- Przygotowanie instrukcji wykonywania kopii konfiguracji urządzenia i odtwarzania w przypadku awarii,

Ponadto zakres prac wdrożeniowych może obejmować inne usługi i mechanizmy, takie jak:

Kształtowania ruchu

- Kształtowanie ruchu na podstawie polityk
- Kształtowanie ruchu na podstawie IP lub aplikacji
- Wsparcie dla DiffServ
- Transfer gwarantowany/max/prirytetyzowany

Intruion Prevention System (IPS)

- ICSA Labs Certified (NIPS)
- Ochrona przed ponad 3000 zagrożeniami
- Wsparcie dla wykrywania anomalii protokołów
- Wsparcie dla Custom Signature Support
- Automatyczna aktualizacja bazy danych
- Wsparcie IPv6

Optymalizacji WAN

- Dwu-kierunkowa: brama do klienta klient do bramy
- Zintegrowane buforowanie oraz optymalizacja protokołów
- Akceleracja CIFS/FTP/MAPI/HTTP/HTTPS/Generic TCP

Data loss prevention (DLP)

- Identyfikacja i kontrola wrażliwych danych
- Wbudowana baza wzorców
- Indywidualne wzorce z silnikiem bazującym na RegEx
- Konfigurowalne akcje (blokowanie/logowanie)

- Wspiera IM, HTTP/HTTPS, i więcej
- Wsparcie dla międzynarodowych alfabetów

Antyspam
- Wsparcie dla SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS
- Czarne listy odświeżane w czasie rzeczywisty/Open Relay Database Server
- Sprawdzanie nagłówków MIME
- Filtrowanie słów kluczowych/frazy
- Czarne/białe listy adresów IP

Logowanie zdarzeń
- dostępu do internetu
- wystąpień naruszeń bezpieczeństwa
- logowania użytkowników
- wykrycia niepożądanego ruchu

III. WARUNKI URUCHOMIENIA I ODBIORU WDROŻONYCH ROZWIĄZAŃ ORAZ PRZEKAZANIA DO EKSPLOATACJI

1. **Pozostałe wymagania od Wykonawców**

Poza dostawami i usługami podstawowymi, wykonawca jest zobowiązany do skalkulowania wszelkich usług pomocniczych, jakie uzna za niezbędne do prawidłowego wykonania przedmiotu zamówienia dla przyjętej technologii, uwzględniając warunki ich wykonania.
Wykonawca musi ponadto uwzględnić w cenie w ramach kosztów dodatkowych –
- koszty dostawy sprzętu na miejsce instalacji
- koszty zabezpieczenia istniejących elementów obiektu oraz wyposażenia (urządzeń) Użytkownika przed ich zniszczeniem w trakcie wykonywania prac,
- koszty związane z zorganizowaniem pracy w sposób minimalizujący zakłócenie prowadzenia bieżącej działalności Zamawiającego
- koszty zapewnienia bezpieczeństwa bhp i ppoż. w trakcie realizacji prac
- koszty testów, prób, badań, odbiorów technicznych – jeśli będą wymagane
- koszty opracowania dokumentacji powykonawczej

Uwaga!
Podmioty realizujące zadania publiczne zobowiązane są do stosowania rozwiązań z zakresu interoperacyjności mi. na poziomie technologicznym. Interoperacyjność osiąga się poprzez stosowania minimalnych wymagań dla systemów teleinformatycznych. Zgodnie z §20 ust. 2 pkt. 12 Rozporządzenia Rady Ministrów w

sprawie Krajowych Ram Interoperacyjności (KRI) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega mi. na:
- zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa
- redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych
- zapewnienia bezpieczeństwa plików
- dbałość o aktualizację oprogramowania

Dodatkowym ważnym elementem systemu jest możliwość rejestrowania i przechowywania zapisów w dziennikach systemowych (logowanie zdarzeń).
Konieczność zapewnienia tej funkcjonalności wynika z:

a) §21 ust. 1 KRI (zapewnienie rozliczalności w systemach teleinformatycznych w postaci elektronicznej)
b) Art. 22 i 23 Ustawy z dnia 5 lipca 2018 o Krajowym Systemie Cyberbezpieczeństwa

Wdrożone rozwiązania powinny spełniając wymagania przywołanych aktów prawnych oraz standardów rynkowych.

2. Przeszkolenie dla przedstawicieli

W ramach przedmiotu zamówienia wymagane jest przeprowadzenie szkolenia dla wyznaczonych pracowników Zamawiającego w zakresie:

- Zarządzania systemami serwerowymi i wirtualizacją
- Archiwizacji danych oraz wykonywania kopi zapasowych
- Polityki autentykacji i autoryzacji użytkowników sieci, usług katalogowych
- Podstawowej konfiguracji systemu bezpieczeństwa UTM
- Wykonywania kopii bezpieczeństwa, plików konfiguracyjnych itp.

3. Dokumenty odbioru końcowego

- Protokoły odbiorów częściowych
- Protokoły z pomiarów i testów – jeśli dotyczy
- Odpowiednie atesty i certyfikaty - jeśli są wymagane
- Instrukcje obsługi, dokumentacje i inne dokumenty dostarczane wraz ze sprzętem, przez producenta

IV Przeprowadzenie diagnozy cyberbezpieczeństwa

1. W ramach przedmiotu zamówienia należy przeprowadzić audyt oraz wykonać diagnozę cyberbezpieczeństwa dla Gminy Besko zgodnie z wymaganiami programu „Cyfrowa Gmina" oraz obowiązującymi przepisami prawa w tym zakresie.

Szczegółowy zakres przedmiotu zamówienia zawiera formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa stanowiący załącznik nr 8 Regulaminu Konkursu Grantowego Cyfrowa Gmina załączony do opisu przedmiotu zamówienia – załącznik nr 1.

Regulamin Konkursu Grantowego Cyfrowa Gmina wraz z formularzem - załącznikiem nr 8 został zamieszczony na stronie Centrum Projektów Polska Cyfrowa [https://www.gov.pl/web/cppc/cyfrowa-gmina].

2. Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (zwane Rozporządzeniem KRI).

3. Audyt musi zostać przeprowadzony przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa – załącznik nr 2 do niniejszego opisu przedmiotu zamówienia.

Wykaz certyfikatów wskazanych w w/w rozporządzeniu:

Certified Internal Auditor (CIA)

Certified Information System Auditor (CISA)

Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018r. poz. 650 i 1138), w zakresie certyfikacji osób;

Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;

Certified Information Security Manager (CISM);

Certified in Risk and Information Systems Control (CRISC);

Certified in the Governance of Enterprise IT (CGEIT);

Certified Information Systems Security Professional (CISSP);

Systems Security Certified Practitioner(SSCP);

Certified Reliability Professional;

Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

4. Dokument końcowy musi być podpisany przez osobę posiadającą uprawnienia (wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu) raport oraz wypełniony formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa (załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina) należy dostarczyć w wersji elektronicznej oraz w wersji papierowej.

Załączniki do opisu diagnozy cyberbezpieczeństwa:

1. Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa (Załącznik nr 8 Regulaminu Konkursu Grantowego Cyfrowa Gmina konkursu grantowego).
2. Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018r. - wykaz certyfikatów uprawniających do przeprowadzenia audytu