Znak sprawy: RRG.271.6.2025

Załącznik nr 10 do SWZ. Szczegółowy opis przedmiotu zamówienia

Dotyczy zamówienia publicznego pn. Dostawa rozwiązań z zakresu cyberbezpieczeństwa, w tym sprzętu komputerowego i oprogramowania oraz przeprowadzenie audytu KRI z wdrożeniem systemu zarządzania bezpieczeństwem informacji i szkoleniami.

Kody CPV

- 48820000-2 Serwery
- 30233000-1 Urządzenie do przechowywania i odczytu danych
- 32420000-3 Urządzenie sieciowe
- 35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa
- 31682530-4 Awaryjne urządzenia energetyczne
- 48000000-8 Pakiety oprogramowania i systemy informatyczne
- 48422000-2 Zestawy pakietów oprogramowania
- 48600000-4 Pakiety oprogramowania dla baz danych i operacyjne
- 48900000-7 Różne pakiety oprogramowania i systemy komputerowe
- 79212000-3: Usługi audytu
- 79417000-0: Usługi doradcze w zakresie bezpieczeństwa
- 80550000-4: Usługi szkolenia w dziedzinie bezpieczeństwa
- 80510000-2 Usługi szkolenia specjalistycznego
- 80531200-7 Usługi szkolenia technicznego

1. Część 1. Dostawa sprzętu serwerowego, urządzeń sieciowych i zasilaczy awaryjnych wraz ze szkoleniem administratorów

Ogólne warunki realizacji zamówienia

1. Przedmiot zamówienia obejmuje dostawy do siedziby Zamawiającego, tj. Urzędu Gminy w Trawniki (dalej: UG) i do jednostek podległych Zamawiającego: Gminnego Ośrodka Pomocy Społecznej (dalej: GOPS) oraz Gminnego Zespołu Ekonomiczno-Administracyjnego Szkół (dalej: GZEAS) w zakresie i ilościach wskazanych w zestawieniu rzeczowo – ilościowym poniżej.
2. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
3. Dostarczany sprzęt i oprogramowanie muszą pochodzić z oficjalnego kanału dystrybucyjnego w UE.

4. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
5. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
6. Urządzenia przeznaczone do montażu w szafie rack Wykonawca zainstaluje w szafach wskazanych przez Zamawiającego. Wykonawca musi dostarczyć wszelkie akcesoria montażowe umożliwiające instalację urządzeń w szafach i ich uruchomienie oraz wykonać podłączenia elektryczne i logiczne według wskazówek Zamawiającego.
7. Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekaże adresy WWW, pod którymi można je pobrać.
8. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.

Zestawienie rzeczowo - ilościowe

Lp.	Przedmiot dostawy/usługi	Ilość	Miejsce dostawy
1.	Zakup serwera z systemem operacyjnym	1	OPS
2.	Zakup serwera z systemem operacyjnym (typ 2)	1	GZEAS
3.	Zakup biblioteki taśmowej	1	UG
4.	Zakup NAS (typ 1)	2	UG, OPS
5.	Zakup NAS (typ 2)	1	GZEAS
6.	Zakup UTM (typ 1)	1	UG
7.	Zakup UTM (typ 2)	2	GZEAS, OPS
8.	Zakup UPS dla stacji roboczych	37	UG, OPS, GZEAS
9.	Zakup UPS serwerowego (typ 1) (do UTM)	2	UG, GZEAS
10.	Zakup UPS serwerowego (typ 2)	1	OPS
11.	Zakup UPS serwerowego (typ 3) (do NAS)	2	UG, GZEAS
12.	Zakup usług szkolenia administratorów IT w zakresie wdrażanych rozwiązań (pakiet szkoleń)	1	UG lub on-line

1.1. Zakup serwera z systemem operacyjnym

Obszar wymagań	Wymagania minimalne
Obudowa	Typu rack o wysokości maksymalnie 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli
Płyta główna	Płyta główna z możliwością instalacji dwóch fizycznych procesorów Możliwości rozbudowy: co najmniej jeden wolny slot PCIe generacji co najmniej 4
Procesor	Zainstalowane dwa procesory ośmiordzeniowe klasy x86 dedykowane do pracy z oferowanym serwerem, umożliwiające osiągnięcie przez serwer wyniku co najmniej 165 punktów w teście SPECrate2017_int_base dla konfiguracji dwuprocesorowej według wyników publikowanych na stronie www.spec.org. Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim.
Pamięć RAM	Zainstalowane co najmniej 128 GB DDR5. Płyta główna musi obsługiwać do 1TB pamięci RAM DDR5 lub więcej.
Grafika	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości co najmniej 1920x1200
Sieć	Wbudowane co najmniej 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT. Ww. liczba portów nie może być osiągnięta poprzez kartę zajmującą złącze PCIe.
Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane: 3 dyski Hot-Plug SSD z interfejsem SATA o pojemności co najmniej 1,92GB każdy. Możliwość zainstalowania co najmniej dwóch dysków M.2 SATA z możliwością konfiguracji RAID 1.
Kontrolery dyskowe	Sprzętowy kontroler dyskowy posiadający co najmniej 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60 Wsparcie dla dysków samoszyfrujących

Porty	Co najmniej 3 zewnętrzne porty USB, w tym co najmniej 1 port USB 3.x, co najmniej 1 port USB musi być dostępny z przodu obudowy Co najmniej 2 porty VGA Ilość dostępnych portów nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCIe serwera.
Wentylacja	Redundantne wentylatory hotplug.
Zasilanie	Redundantne zasilacze hotplug o mocy nie większej niż 1100W każdy.
Zarządzanie	Dedykowany moduł zdalnego zarządzania, diagnostyki i monitorowania pracy serwera, niezależny od systemu operacyjnego, umożliwiający co najmniej: • zarządzanie poprzez graficzny interfejs, • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera), • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika, • możliwość podmontowania zdalnych wirtualnych napędów, • wirtualną konsolę z dostępem do myszy, klawiatury, • integrację z Active Directory, • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej, • możliwość podłączenia lokalnego i bezpośredniego zarządzania poprzez złącze RS-232 lub USB lub microUSB.
Bezpieczeństwo, diagnostyka	• Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera. • Blokada zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • Możliwość ustawienia w BIOS bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0.

	• Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.
System operacyjny	Zainstalowany na serwerze system operacyjny, kompatybilny z oferowanym serwerem, spełniający nw. wymagania minimalne: 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 migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 4) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 6) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 7) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 8) 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). 9) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 10) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET

	11) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 12) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 13) Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 14) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 15) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 16) 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), 17) 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. 18) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 19) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 20) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 21) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).

	22) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 23) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) 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: i) Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii) Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii) Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. iv) Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1 i wyższych. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej. e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i) dystrybucję certyfikatów poprzez http, ii) konsolidację CA dla wielu lasów domeny, iii) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv) automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów.

	g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). 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) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 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: i) Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii) Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii) Obsługi 4-KB sektorów dysków iv) Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v) Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi) Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 24) 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.

	25) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 26) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 27) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 28) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 29) Zorganizowany system szkoleń i dostępne materiały edukacyjne w języku polskim. Zaoferowana wraz z serwerem licencja na system operacyjny: 1. musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta i pozwalała na legalne używanie na oferowanym serwerze, 2. musi obejmować najnowszą wersję systemu dostępną na dzień składania oferty, 3. musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego, 4. musi obejmować licencje dostępowe dla 12 użytkowników, jeśli takie licencje są wymagane przez producenta do dostępu do oprogramowania serwerowego. Do oferty należy załączyć potwierdzenie kompatybilności serwera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim).
Wymagania środowiskowe	Oferowany serwer musi być zgodny z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Do oferty należy załączyć deklarację zgodności z dyrektywą RoHS.

Warunki gwarancyjne, wsparcie techniczne	Co najmniej pięcioletnia gwarancja producenta, obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji. Usługi serwisu gwarancyjnego muszą być realizowane w miejscu instalacji urządzenia. Czas reakcji serwisu - do końca następnego dnia roboczego. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. Możliwość zgłaszania awarii 7 dni w tygodniu w języku polskim poprzez ogólnopolską linię telefoniczną producenta oraz dedykowany polskojęzyczny portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji. Usługa realizowana przez polskojęzyczny portal producenta.

1.2. Zakup serwera z systemem operacyjnym (typ 2)

Obszar wymagań	**Wymagania minimalne**
Obudowa	Typu rack o wysokości maksymalnie 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli
Płyta główna	Płyta główna z możliwością instalacji dwóch fizycznych procesorów Możliwości rozbudowy: co najmniej jeden wolny slot PCIe generacji co najmniej 4
Procesor	Zainstalowane dwa procesory ośmiordzeniowe klasy x86 dedykowane do pracy z oferowanym serwerem, umożliwiające osiągnięcie przez serwer wyniku co najmniej 165 punktów w teście SPECrate2017_int_base dla konfiguracji dwuprocesorowej według wyników publikowanych na stronie www.spec.org. Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim.
Pamięć RAM	Zainstalowane co najmniej 128 GB DDR5. Płyta główna musi obsługiwać do 1TB pamięci RAM DDR5 lub więcej.

Grafika	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości co najmniej 1920x1200
Sieć	Wbudowane co najmniej 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT. Ww. liczba portów nie może być osiągnięta poprzez kartę zajmującą złącze PCIe.
Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane: 3 dyski Hot-Plug SSD z interfejsem SATA o pojemności co najmniej 1,92GB każdy. Możliwość zainstalowania co najmniej dwóch dysków M.2 SATA z możliwością konfiguracji RAID 1.
Kontrolery dyskowe	Sprzętowy kontroler dyskowy posiadający co najmniej 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60 Wsparcie dla dysków samoszyfrujących
Porty	Co najmniej 3 zewnętrzne porty USB, w tym co najmniej 1 port USB 3.x, co najmniej 1 port USB musi być dostępny z przodu obudowy Co najmniej 2 porty VGA Ilość dostępnych portów nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCIe serwera.
Wentylacja	Redundantne wentylatory hotplug.
Zasilanie	Redundantne zasilacze hotplug o mocy nie większej niż 1100W każdy.
Zarządzanie	Dedykowany moduł zdalnego zarządzania, diagnostyki i monitorowania pracy serwera, niezależny od systemu operacyjnego, umożliwiający co najmniej: • zarządzanie poprzez graficzny interfejs, • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera), • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika, • możliwość podmontowania zdalnych wirtualnych napędów, • wirtualną konsolę z dostępem do myszy, klawiatury,

	• integrację z Active Directory, • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej, • możliwość podłączenia lokalnego i bezpośredniego zarządzania poprzez złącze RS-232 lub USB lub microUSB.
Bezpieczeństwo, diagnostyka	• Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera. • Blokada zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • Możliwość ustawienia w BIOS bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0. • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.
System operacyjny	Zainstalowany na serwerze system operacyjny, kompatybilny z oferowanym serwerem, spełniający nw. wymagania minimalne: 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 migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 4) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.

	6) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 7) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 8) 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). 9) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 10) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 11) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 12) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 13) Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 14) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 15) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 16) 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), 17) 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. 18) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 19) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 20) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 21) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 22) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 23) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) 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: i) Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii) Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

	iii) Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. iv) Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1 i wyższych. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej. e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i) dystrybucję certyfikatów poprzez http, ii) konsolidację CA dla wielu lasów domeny, iii) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv) automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). 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) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 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: i) Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

	ii) Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii) Obsługi 4-KB sektorów dysków iv) Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v) Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi) Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 24) 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. 25) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 26) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 27) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 28) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 29) Zorganizowany system szkoleń i dostępne materiały edukacyjne w języku polskim. Zaoferowana wraz z serwerem licencja na system operacyjny: 1. musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta i pozwalała na legalne używanie na oferowanym serwerze, 2. musi obejmować najnowszą wersję systemu dostępną na dzień składania oferty, 3. musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego,

	4. musi obejmować licencje dostępowe dla 4 użytkowników, jeśli takie licencje są wymagane przez producenta do dostępu do oprogramowania serwerowego. Do oferty należy załączyć potwierdzenie kompatybilności serwera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim).
Wymagania środowiskowe	Oferowany serwer musi być zgodny z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Do oferty należy załączyć deklarację zgodności z dyrektywą RoHS.
Warunki gwarancyjne, wsparcie techniczne	Co najmniej pięcioletnia gwarancja producenta, obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji. Usługi serwisu gwarancyjnego muszą być realizowane w miejscu instalacji urządzenia. Czas reakcji serwisu - do końca następnego dnia roboczego. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. Możliwość zgłaszania awarii 7 dni w tygodniu w języku polskim poprzez ogólnopolską linię telefoniczną producenta oraz dedykowany polskojęzyczny portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji. Usługa realizowana przez polskojęzyczny portal producenta.

1.3. Zakup biblioteki taśmowej

Obszar wymagań	**Wymagania minimalne**
Obudowa	Typu rack o wysokości maksymalnie 1U, co najmniej 9 slotów przeznaczonych na zestaw taśm, z kompletem szyn umożliwiających montaż w szafie rack.
Połączenie	Co najmniej 1 port SAS o przepustowości co najmniej 6Gb/s w standardzie umożliwiającym podłączenie serwera Dell PowerEdge R660xs posiadanego przez Zamawiającego.

Napęd	Wyposażony w co najmniej 1 sztukę napędu SAS LTO 8.
Wymagane wyposażenie	Kabel SAS umożliwiający podłączenie biblioteki do serwera, o długości co najmniej 2 metry, 7 szt. taśm LTO8 o pojemności co najmniej 12/30TB, taśma czyszcząca. Dodatkowa, dwuportowa karta 12Gb SAS HBA do rozbudowy serwera Dell PowerEdge R660xs posiadanego przez Zamawiającego.
Warunki gwarancyjne	Co najmniej pięcioletnia gwarancja producenta. Warunki świadczenia serwisu gwarancyjnego: usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, czas reakcji serwisu - do końca następnego dnia roboczego. Możliwość zgłaszania awarii 7 dni w tygodniu w języku polskim poprzez ogólnopolską linię telefoniczną producenta oraz dedykowany polskojęzyczny portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - czasu obowiązywania i typ udzielonej gwarancji. Usługa realizowana przez polskojęzyczny portal producenta.

1.4. Zakup NAS (typ 1)

Obszar wymagań	**Wymagania minimalne**
Budowa	Obudowa do montażu w szafie rack, wymagane wyposażenie w szyny do szafy rack Redundantne wentylatory
Procesor	Wielordzeniowy procesor 64-bitowy, uzyskujący wynik co najmniej 5 000 punktów w teście PassMark - CPU Mark według wyników dostępnych na stronie http://www.cpubenchmark.net 30 dni przed terminem składania ofert lub później. Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim.
Pamięć RAM	Zainstalowane co najmniej 8 GB pamięci RAM z możliwością rozbudowy do 64 GB lub więcej.
Obsługa dysków	Ilość kieszeni dysków: co najmniej 4 (możliwość rozbudowy do 8 dysków z wykorzystaniem jednostki rozszerzającej lub równoważnie obudowa na 16 dysków). Obsługiwane typy dysków: 3,5” SATA HDD, 2.5" SATA HDD, 2,5” SATA SSD, M.2 2280 NVMe i SATA SSD.

Zamontowane dyski	Zamontowane co najmniej 4 dyski o pojemności co najmniej 8 TB każdy, o prędkości interfejsu co najmniej 6Gbps i deklarowanym średnim czasem bezawaryjnej pracy co najmniej 1 mln godzin. Oferowane dyski muszą znajdować się na liście kompatybilności producenta urządzenia dyskowego NAS.
RAID	Obsługa RAID co najmniej: Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6 i RAID 10. Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Funkcje i usługi	Wsparcie dla wirtualizacji Scentralizowana pamięć masowa na dane Kopia zapasowa Udostępnianie i przywracanie systemu po awarii Mechanizm szyfrowania sprzętowego Uprawnienia listy kontroli dostępu systemu Windows (ACL) Wymagana kompatybilność z usługą katalogową serwera Windows (możliwość logowania użytkowników domeny za pośrednictwem protokołów SMB/FTP/WebDAV/File Station).
Porty	Co najmniej 4 porty 1GbE RJ-45 Co najmniej 2 porty USB 3.x Co najmniej 1 port rozszerzenia
Zasilanie	Wbudowany zasilacz
Bezpieczeństwo	Obsługa WORM (Write Once Read Many - jeden zapis, wiele odczytów) dla folderów współdzielonych i migawek, zapora sieciowa, szyfrowanie folderu współdzielonego, szyfrowanie całego woluminu, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów HTTP, HTTPS, SMB, SSH, Telnet, rsync, FTP, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania), dwuetapowa weryfikacja logowania (2FA), adaptacyjna metoda logowania dla konta administratora (AMFA), możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2, U2F, grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail.
Oprogramowanie	• Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany

	system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych • Wymaga się zapewnienia aplikacji do realizacji chmury prywatnej, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI, a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Ww. usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ww. usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników. Usługa musi być dostępna bez dodatkowych opłat, co najmniej w okresie gwarancji na urządzenie. • Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych serwerów, bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego. • Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych i serwera rsync • Obsługa minimum 1024 migawek na folder współdzielony i minimum 65000 migawek na cały system • Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 40 jednoczesnych połączeń
Oprogramowanie do kopii zapasowej	Zakup urządzenia musi uprawniać do instalacji i eksploatacji oprogramowania do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów. Minimalne wymagane funkcje oprogramowania do backupu: • oprogramowanie musi być w pełni zgodne z oferowanym urządzeniem, • kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal, • kopia zapasowa maszyn wirtualnych (VMware, Hyper-V) • kopia zapasowa serwerów fizycznych (Windows, Linux) • obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania, • obsługa wielu wersji i retencji,

	• możliwość wyzwalania kopii zapasowej według harmonogramu, • obsługa klastra przełączania awaryjnego Microsoft Hyper-V, • centralne zarządzanie, • konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji, harmonogramu i woluminów objętych backupem dla poszczególnych zadań, • portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), • delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla użytkowników bez uprawnień administratora, • kopia zapasowa usług chmur publicznych Microsoft 365 i Google Workspace.
Gwarancja	Gwarancja producenta co najmniej 60 miesięcy.

1.5. Zakup NAS (typ 2)

Obszar wymagań	**Wymagania minimalne**
Budowa	Obudowa typu desktop Redundantne wentylatory
Procesor	Wielordzeniowy procesor 64-bitowy, uzyskujący wynik co najmniej 4 500 punktów w teście PassMark - CPU Mark według wyników dostępnych na stronie http://www.cpubenchmark.net 30 dni przed terminem składania ofert lub później. Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim.
Pamięć RAM	Zainstalowane co najmniej 4 GB pamięci RAM. Możliwość rozbudowy do 32 GB pamięci RAM lub więcej.
Obsługa dysków	Ilość kieszeni dysków: co najmniej 6 z możliwością rozszerzenia do 16 kieszeni lub jako rozwiązanie równoważne urządzenie z obsługą 16 dysków. Obsługiwane typy dysków: 3,5” SATA HDD, 2,5” SATA HDD, 2,5” SATA SSD. Co najmniej dwa wolne sloty M.2
Zamontowane dyski	Zamontowane co najmniej 4 dyski o pojemności co najmniej 12 TB każdy, o prędkości interfejsu co najmniej 6Gbps i deklarowanym średnim czasem bezawaryjnej pracy co najmniej 2 mln godzin.

	Oferowane dyski muszą znajdować się na liście kompatybilności producenta urządzenia dyskowego NAS.
RAID	Obsługa RAID co najmniej: Basic, JBOD, RAID 0, 1, 5, 6, 10.
Obsługiwane systemy plików	EXT3, EXT4, NTFS, FAT, HFS+
Obsługiwane protokoły	HTTP(S), FTP, SMB, AFP
Funkcje i usługi	Wsparcie dla wirtualizacji Scentralizowana pamięć masowa na dane Kopia zapasowa Udostępnianie i przywracanie systemu po awarii Mechanizm szyfrowania sprzętowego Uprawnienia listy kontroli dostępu systemu Windows (ACL) Wymagana kompatybilność z usługą katalogową serwera Windows (możliwość logowania użytkowników domeny za pośrednictwem protokołów SMB/FTP/WebDAV/File Station).
Oprogramowanie	Zakup urządzenia musi uprawniać do instalacji i eksploatacji oprogramowania do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów. Minimalne wymagane funkcje oprogramowania do backupu: • oprogramowanie musi być w pełni zgodne z oferowanym urządzeniem, • kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal, • kopia zapasowa maszyn wirtualnych (VMware, Hyper-V) • kopia zapasowa serwerów fizycznych (Windows, Linux) • obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania, • obsługa wielu wersji i retencji, • możliwość wyzwalania kopii zapasowej według harmonogramu, • obsługa klastra przełączania awaryjnego Microsoft Hyper-V, • centralne zarządzanie, • konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji, harmonogramu i woluminów objętych backupem dla poszczególnych zadań, • portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora),

	• delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla użytkowników bez uprawnień administratora, • kopia zapasowa usług chmur publicznych Microsoft 365 i Google Workspace.
Porty	Co najmniej: 4 porty 1 GbE Base-T Co najmniej 3 porty USB 3.x Co najmniej 1 gniazdo rozszerzenia
Zasilanie	Wbudowany zasilacz
Gwarancja	Gwarancja producenta co najmniej 36 miesięcy.

1.6. Zakup UTM (typ 1)

Obszar wymagań	**Wymagania minimalne**
Obsługa sieci	Urządzenie musi posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
Zapora korporacyjna (Firewall)	1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS,

	określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). 11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
Intrusion prevention system (IPS)	12. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 13. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 14. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 15. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 16. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 17. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. 18. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych

	adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 19. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 20. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
Kształtowanie pasma (Traffic Shapping)	21. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 22. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 23. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 24. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
Ochrona antywirusowa	25. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 26. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 27. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 28. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
Ochrona antyspam	29. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 30. Ochrona antyspam ma działać w oparciu o: białe/czarne listy, DNS RBL i skaner heurystyczny. 31. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.

	32. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
Wirtualne sieci prywatne (VPN)	33. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 34. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: PPTP VPN, IPSec VPN i SSL VPN. 35. SSL VPN ma działać co najmniej w trybach tunelu i portalu. 36. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 37. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) 38. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 39. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 40. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
Filtr dostępu do stron www	41. Urządzenie ma posiadać wbudowany filtr URL. 42. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 43. Administrator ma mieć możliwość dodawania własnych kategorii URL. 44. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 45. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 46. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 47. Filtr URL musi uwzględniać komunikację po protokole HTTPS. 48. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.

	49. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. 50. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
Uwierzytelnianie	51. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 52. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. 53. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły SSL, Radius i Kerberos. 54. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 55. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 56. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. 57. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). 58. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 59. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
Administracja łączami do Internetu (ISP)	60. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 61. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:

	a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 62. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 63. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). 64. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. 65. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 66. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
Routing (trasowanie)	67. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 68. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 69. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 70. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
Administracja urządzeniem	71. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 72. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 73. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 74. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 75. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 76. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)

	77. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 78. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 79. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. 80. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 81. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. 82. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). 83. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). 84. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. 85. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 86. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. 87. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: a. manualnego eksportu do pliku w dowolnym momencie czasu, b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu 88. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.

	89. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. 90. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
Raportowanie	91. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 92. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 93. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 94. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. 95. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 96. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 97. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 98. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 99. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
Monitorowanie, gromadzenie i raportowanie logów	100. Wraz z urządzeniem należy dostarczyć rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa. 101. Wymagania ogólne: a. Rozwiązanie musi zostać dostarczone w postaci maszyny wirtualnej instalowanej w środowisku Vmware lub Windows Hyper-V. b. Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym,

	użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW. c. Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów. d. Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP. e. Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta. f. Rozwiązanie musi posiadać predefiniowane panele dla informacji z urządzeń pracujących w sieci OT. 102. Zarządzanie logami: a. Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP. b. Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS. c. Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder). d. Rozwiązanie musi być lokalne i w związku z tym wymaga się instalacji w środowisku Zamawiającego. 103. Rodzaje wyszukiwań: a. Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie. b. Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.). c. Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne. d. Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP). e. Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów). f. Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV. 104. Raportowanie:

	a. Rozwiązanie musi umożliwiać tworzenie statycznych raportów. b. Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób. c. Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów. d. Rozwiązanie musi umożliwiać tworzenie własnych raportów. e. Rozwiązanie musi umożliwiać tworzenie dynamicznych raportów (w czasie rzeczywistym) z funkcjonalnością „drill-down”. 105. Zarządzanie incydentami: a. 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 e-mail. b. 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. 106. Wymagania systemowe: a. Liczba zdarzeń na sekundę (EPS): co najmniej 10 000 b. Liczba obsługiwanych urządzeń co najmniej 500 c. Liczba zapisu zdarzeń na dobę: co najmniej 13000 MB d. Rozwiązanie musi wspierać hiperwizory: Vmware ESXi oraz Microsoft HyperV.
Pozostałe usługi i funkcje	107. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. 108. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.

	109. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 110. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 111. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). 112. Urządzenie ma posiadać usługę DNS Proxy. 113. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. 114. Urządzenie musi mieć zaimplementowane Open API 115. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
Gwarancja i serwis	116. Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu. 117. Wszystkie funkcje bezpieczeństwa realizowane przez urządzenie muszą być dostępne bezpłatnie dla Zamawiającego, bez konieczności zakupu dodatkowych usług czy licencji subskrypcyjnych/do dnia 30.06.2026. 118. W okresie obowiązywania gwarancji musi być zapewnione bezpłatne wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
Parametry sprzętowe	119. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 120. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. 121. Liczba portów Ethernet 2,5Gbps – co najmniej 8. 122. Liczba portów światłowodowych 1Gbps – co najmniej 1. 123. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 124. Przepustowość Firewall (1518 bajtów UDP) – minimum 8Gbps. 125. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps. 126. Przepustowość filtrowania Antywirusowego – minimum 1Gbps.

	127. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2Gbps. 128. Maksymalna liczba tuneli VPN IPSec – minimum 100. 129. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 100. 130. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 100. 131. Obsługa interfejsów 802.11q (VLAN) – minimum 128 132. Liczba równoczesnych sesji – minimum 400 000 i nie mniej niż 25 000 nowych sesji/sekundę. 133. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 134. Urządzenie nie ma limitu na liczbę użytkowników. 135. Liczba reguł filtrowania – minimum 8 192. 136. Liczba tras statycznego routingu – minimum 512. 137. Liczba tras dynamicznego routingu – minimum 10 000. 138. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia. 139. Urządzenie musi być wyposażone w moduł TPM.

1.7. Zakup UTM (typ 2)

Obszar wymagań	**Wymagania minimalne**
Obsługa sieci	Urządzenie musi posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
Zapora korporacyjna (Firewall)	1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów.

	Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). 11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
Intrusion prevention system (IPS)	12. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 13. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 14. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.

	15. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 16. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 17. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. 18. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 19. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 20. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
Kształtowanie pasma (Traffic Shapping)	21. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 22. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 23. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 24. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
Ochrona antywirusowa	25. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 26. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 27. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 28. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla

	infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
Ochrona antyspam	29. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 30. Ochrona antyspam ma działać w oparciu o: białe/czarne listy, DNS RBL i skaner heurystyczny. 31. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. 32. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
Wirtualne sieci prywatne (VPN)	33. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 34. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: PPTP VPN, IPSec VPN i SSL VPN. 35. SSL VPN ma działać co najmniej w trybach tunelu i portalu. 36. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 37. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) 38. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 39. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 40. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
Filtr dostępu do stron www	41. Urządzenie ma posiadać wbudowany filtr URL. 42. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 43. Administrator ma mieć możliwość dodawania własnych kategorii URL. 44. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL,

	c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 45. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 46. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 47. Filtr URL musi uwzględniać komunikację po protokole HTTPS. 48. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 49. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. 50. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
Uwierzytelnianie	51. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 52. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. 53. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły SSL, Radius i Kerberos. 54. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 55. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 56. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. 57. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). 58. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).

	59. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
Administracja łączami do Internetu (ISP)	60. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 61. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 62. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 63. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). 64. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. 65. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 66. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
Routing (trasowanie)	67. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 68. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 69. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 70. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
Administracja urządzeniem	71. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 72. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 73. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.

	74. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 75. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 76. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) 77. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 78. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 79. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. 80. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 81. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. 82. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). 83. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). 84. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. 85. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 86. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. 87. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:

	a. manualnego eksportu do pliku w dowolnym momencie czasu, b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu 88. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. 89. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. 90. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
Raportowanie	91. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 92. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 93. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 94. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. 95. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 96. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 97. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 98. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 99. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
Pozostałe usługi i funkcje	100. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i

	statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 101. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 102. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 103. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). 104. Urządzenie ma posiadać usługę DNS Proxy. 105. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. 106. Urządzenie musi mieć zaimplementowane Open API 107. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
Gwarancja i serwis	108. Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu. 109. Wszystkie funkcje bezpieczeństwa realizowane przez urządzenie muszą być dostępne bezpłatnie dla Zamawiającego, bez konieczności zakupu dodatkowych usług czy licencji subskrypcyjnych do dnia 30.06.2026. 110. W okresie obowiązywania gwarancji musi być zapewnione bezpłatne wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
Parametry sprzętowe	111. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 112. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. 113. Liczba portów Ethernet 10/100/1000Mbps – co najmniej 4. 114. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 115. Przepustowość Firewall (1518 bajtów UDP) – co najmniej 3Gbps. 116. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – co najmniej 1Gbps.

	117. Przepustowość filtrowania Antywirusowego – co najmniej 300Mbps. 118. Przepustowość tunelu VPN przy szyfrowaniu AES – co najmniej 1Gbps. 119. Maksymalna liczba tuneli VPN IPSec – co najmniej 50. 120. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – co najmniej 25. 121. Obsługa interfejsów 802.11q (VLAN) – co najmniej 128 122. Liczba równoczesnych sesji – co najmniej 150 000 i nie mniej niż 15 000 nowych sesji/sekundę. 123. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 124. Urządzenie nie ma limitu na liczbę użytkowników. 125. Liczba reguł filtrowania – co najmniej 1024. 126. Liczba tras statycznego routingu – co najmniej 512. 127. Liczba tras dynamicznego routingu – co najmniej 10 000. 128. Urządzenie musi posiadać pasywny system chłodzenia.

1.8. Zakup UPS dla stacji roboczych

Obszar wymagań	**Wymagania minimalne**
Typ urządzenia	Zasilacz awaryjny w obudowie typu desktop
Moc	Co najmniej 600W, moc pozorna co najmniej 1000 VA
Topologia	Line interactive lub on-line
Typ przebiegu	Sinusoida
Czas podtrzymania	6 min. dla obciążenia 50% lub dłużej 2 min. dla obciążenia 100% lub dłużej
Gniazda	Co najmniej 4 gniazda wyjściowe typu francuskiego
Komunikacja	Złącze USB lub Ethernet
Ochrona linii danych	Port RJ-11 lub port RJ-45
Sygnalizacja	Wyświetlacz LCD lub diody LED, alarm dźwiękowy
Gwarancja	Gwarancja producenta co najmniej 24 miesiące

1.9. Zakup UPS serwerowego (typ 1) (do UTM)

Obszar wymagań	**Wymagania minimalne**

Typ urządzenia	Jednofazowy zasilacz awaryjny w obudowie tower z możliwością montażu w szafie RACK, zajmujący maksymalnie 2U
Moc	Co najmniej 800 W, moc pozorna co najmniej 1000 VA
Topologia	On-line
Typ przebiegu	Sinusoida
Czas podtrzymania	Co najmniej 2 min. przy obciążeniu 100 % Co najmniej 8 min. przy obciążeniu 50 %
Gniazda	Co najmniej 4 gniazda wyjściowe IEC 320 C13, co najmniej 1 gniazdo wejściowe IEC 320 C20 lub C14 Złącze dla dodatkowych baterii
Komunikacja	Porty: 1 x USB lub 1x Ethernet
Zabezpieczenia	Przeciwprzepięciowe, przeciwzwarciowe, przeciwprzeciążeniowe
Sygnalizacja	Wyświetlacz LCD lub diody LED, alarm dźwiękowy
Gwarancja	Gwarancja producenta co najmniej 24 miesiące.

1.10. Zakup UPS serwerowego (typ 2)

Obszar wymagań	**Wymagania minimalne**
Typ urządzenia	Jednofazowy zasilacz awaryjny w obudowie tower z możliwością montażu w szafie RACK, zajmujący maksymalnie 2U
Moc	Co najmniej 2700 W, moc pozorna co najmniej 3000 VA
Topologia	On-line
Typ przebiegu	Sinusoida
Czas podtrzymania	Co najmniej 2 min. przy obciążeniu 100 % Co najmniej 8 min. przy obciążeniu 50 %
Gniazda	Co najmniej 6 gniazd wyjściowych IEC 320 C13, co najmniej 1 gniazdo wejściowe IEC 320 C20 Złącze dla dodatkowych baterii
Komunikacja	Porty: 1 x USB lub 1x Ethernet
Zabezpieczenia	Przeciwprzepięciowe, przeciwzwarciowe, przeciwprzeciążeniowe
Sygnalizacja	Wyświetlacz LCD lub diody LED, alarm dźwiękowy
Gwarancja	Gwarancja producenta co najmniej 24 miesiące.

1.11. Zakup UPS serwerowego (typ 3) (do NAS)

Obszar wymagań	**Wymagania minimalne**

Typ urządzenia	Jednofazowy zasilacz awaryjny w obudowie tower z możliwością montażu w szafie RACK, zajmujący maksymalnie 2U
Moc	Co najmniej 1800 W, moc pozorna co najmniej 2000 VA
Topologia	On-line
Typ przebiegu	Sinusoida
Czas podtrzymania	Co najmniej 2 min. przy obciążeniu 100 % Co najmniej 8 min. przy obciążeniu 50 %
Gniazda	Co najmniej 4 gniazda wyjściowe IEC 320 C13, co najmniej 1 gniazdo wejściowe IEC 320 C20 Złącze dla dodatkowych baterii
Komunikacja	Porty: 1 x USB lub 1x Ethernet
Zabezpieczenia	Przeciwprzepięciowe, przeciwzwarciowe, przeciwprzeciążeniowe
Sygnalizacja	Wyświetlacz LCD lub diody LED, alarm dźwiękowy
Gwarancja	Gwarancja producenta co najmniej 24 miesiące.

1.12. Zakup usług szkolenia administratora IT w zakresie wdrażanych rozwiązań (pakiet szkoleń)

1. Zamówienie obejmuje pakiet szkoleń dla administratora IT jednostek Zamawiającego w zakresie wdrażanych funkcjonalności zabezpieczeń, w tym:
   1) szkolenie wstępne z zakresu administrowania systemem informatycznym,
   2) szkolenie wstępne z zakresu cyberbezpieczeństwa sieci,
   3) szkolenie z zakresu administrowania urządzeniami UTM.
2. Zamawiający przewiduje łączną liczbę jednej osoby w każdym ze szkoleń.
3. Szkolenia muszą być realizowane w kolejności wskazanej w ust. 1.
4. Szkolenia z zakresu administrowania urządzeniami UTM muszą dotyczyć urządzeń UTM zaoferowanych przez Wykonawcę i muszą być autoryzowane przez producentów tych rozwiązań.
5. Szkolenia muszą być przeprowadzone w języku polskim.
6. Szkolenia mogą być przeprowadzone w siedzibie Zamawiającego (Urząd Gminy Trawniki) lub mogą być realizowane w trybie on-line.
7. W przypadku realizacji szkoleń w siedzibie Zamawiającego Zamawiający zapewni jedną salę, w której przeprowadzone zostaną szkolenia; sala wyposażona jest w sprzęt audiowizualny.
8. Po zakończeniu szkoleń Wykonawca przekaże każdemu uczestnikowi zaświadczenie ukończenia szkolenia. Zaświadczenie musi zawierać co najmniej: imię i nazwisko uczestnika, informację o ilości godzin, zrealizowanym zakresie tematycznym oraz oznaczenia dotyczące współfinansowania projektu.
9. Wykonawca w cenie oferty zapewni każdemu z uczestników możliwość przystąpienia do autoryzowanego egzaminu.

10. Po zakończeniu szkoleń Wykonawca przekaże Zamawiającemu projektu jeden komplet wszystkich materiałów przekazanych uczestnikom w wersji papierowej oraz udostępni elektronicznie kompletną treść prezentacji multimedialnej wykorzystywanej przez prowadzącego w trakcie szkolenia. Wykonawca wyda odpowiedni certyfikat potwierdzający zdanie egzaminu dla osób, które zdały egzamin.
11. Wykonawca zapewni uczestnikom szkolenia kontakt z trenerem prowadzącym szkolenie przez 14 dni po zakończeniu szkolenia, w celu udzielania odpowiedzi na dodatkowe pytania, konsultacje itp.
12. Wszelkie dokumenty wytworzone i przekazane przez Wykonawcę w ramach realizacji Zamówienia, w tym materiały szkoleniowe i certyfikaty muszą spełniać standardy dostępności oraz muszą być prawidłowo oznaczone zgodnie z Podręcznikiem wnioskodawcy i beneficjenta programów polityki spójności 2021-2027 w zakresie informacji i promocji.
13. Wykonawca uwzględni w programie szkoleń minimalny zakres zagadnień wskazany dalszych rozdziałach, tj. 1.12.1, 1.12.2 i 1.12.3.

1.12.1. Szkolenie wstępne z zakresu administrowania systemem informatycznym

Wymagana długość szkolenia – co najmniej 12 godzin w podziale na co najmniej 2 dni.

Minimalny zakres zagadnień:

- Wprowadzenie: typy ataków, polityki bezpieczeństwa.
- Bezpieczeństwo stacji roboczych:
  - zarządzanie uprawnieniami,
  - filtrowanie URL,
  - ochrona antywirusowa,
  - backup,
  - kontrola podłączanych nośników.
- Ochrona serwerów:
  - DMZ,
  - Firewall,
  - WWW,
  - OWASP Top10,
  - szukanie podatności,
  - IPS/IDS,
  - Poczta,
  - serwery pośredniczące,
  - skanowanie AV,

  - ochrona sieci,
  - jak szukać luk w zabezpieczeniach,
  - sniffing.
- Inne zagrożenia
  - IoT,
  - urządzenia mobilne,
  - monitoring,
  - drukarki,
  - błędy użytkowników,
  - zabezpieczenia fizyczne,
  - logowanie zdarzeń i monitoring środowisk.

1.12.2. Szkolenie wstępne z zakresu cyberbezpieczeństwa sieci

Wymagana długość szkolenia – co najmniej 24 godziny w podziale na co najmniej 3 dni.

Minimalny zakres zagadnień:

- Google Hacking.
- Budowa własnych pakietów do skanowania sieci.
- Zaawansowane skanowanie jednostek w warstwie 2, 3 i 4 z wykorzystaniem szerokiej gamy dostępnych narzędzi.
- Identyfikowanie usług sieciowych oraz banerów aplikacji.
- Identyfikacja systemów oraz zapór sieciowych.
- Skanowanie TCP / UDP / zombie.
- Podsłuchiwanie transmisji nieszyfrowanych - ruch http.
- Podsłuchiwanie transmisji szyfrowanych - ruch HTTPS.
- ARP Spoofing.
- DNS Spoof.
- Ataki socjotechniczne.

1.12.3. Szkolenie z zakresu administrowania urządzeniami UTM

Wymagana długość szkolenia – co najmniej 24 godziny w podziale na co najmniej 3 dni.

Minimalny zakres zagadnień:

- Rozpoczęcie pracy z urządzeniem
  - Rejestracja w strefie klienta i dostęp zasobów
  - Rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego
  - Ustawienia systemowe i uprawnienia administratorów

  - Instalacja licencji i aktualizacja systemu
  - Tworzenie kopii zapasowej i przywracanie konfiguracji
- Zbieranie logów i monitorowanie
  - Przedstawienie kategorii zbieranych logów
  - Wykresy historyczne i monitorowanie
- Obiekty
  - Typy obiektów oraz ich wykorzystanie
  - Obiekty sieciowe i obiekt typu „router”
- Konfiguracja sieci
  - Tryby pracy urządzenia
  - Typy interfejsów (Ethernet, modem, bridge, VLAN, GRETAP)
  - Typy routingu oraz ich priorytety
  - Translacja adresów sieciowych (NAT)
  - Translacja połączeń wychodzących (maskarada)
  - Translacja połączeń przychodzących (przekierowanie)
  - Translacja dwukierunkowa (jeden do jeden)
- Filtrowanie ruchu sieciowego (Firewall)
  - Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection)
  - Szczegółowy opis parametrów reguły Firewall
  - Kolejność przetwarzania reguł Firewall i NAT
- Ochrona aplikacji
  - Implementacja filtrowania URL dla ruchu http i https
  - Konfigurowanie skanowania antywirusowego i modułu Breach Fighter
  - Moduł IPS i stosowanie profili inspekcji
- Użytkownicy i uwierzytelnianie
- Konfiguracja usługi katalogowej
  - Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL, SPNEGO, SSO)
  - Rejestracja użytkowników
  - Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania
- Wirtualne sieci prywatne (VPN)
  - Koncepcje i ogólne informacje dotyczące protokołu IPSec VPN (IKEv1 i IKEv2)
  - Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK)
  - Tunele VTI
- SSL VPN
  - Zasada działania,
  - Konfiguracja.

2. Część 2. Dostawa oprogramowania

Ogólne warunki realizacji zamówienia

1. Przedmiot zamówienia obejmuje dostawę do siedziby Zamawiającego:
   - oprogramowania do monitorowania infrastruktury informatycznej,
   - licencji subskrypcyjnych oprogramowania antywirusowego.
2. Dostarczane oprogramowanie musi być fabrycznie nowe, nieużywane i nieobciążone prawami osób trzecich.
3. Dostarczane oprogramowanie musi pochodzić z oficjalnego kanału dystrybucyjnego w UE.
4. Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.
5. Wykonawca zobowiązany jest do udzielenia wsparcia we wdrożeniu oprogramowania do monitorowania infrastruktury informatycznej (poz. 2.1), w tym do:
   a. zdalnej instalacji oprogramowania serwerowego na wskazanym przez Zamawiającego serwerze oraz do uruchomienia i skonfigurowania modułów systemu odpowiedzialnych za automatyczną inwentaryzację sprzętu komputerowego, oprogramowania oraz urządzeń peryferyjnych w urzędzie,
   b. zdalnej instalacji agentów systemowych na co najmniej 5 wskazanych przez Zamawiającego urządzeniach końcowych; szkolenie administratorów, o którym mowa w punkcie g. musi uwzględniać procedury instalacyjne agentów na urządzeniach końcowych,
   c. uruchomienia i skonfigurowania modułów systemu odpowiedzialnych za automatyczną inwentaryzację sprzętu komputerowego, oprogramowania oraz urządzeń peryferyjnych w urzędzie.
6. Wykonawca zobowiązany jest do przeprowadzenie szkolenia dla administratorów IT urzędu z zakresu dostarczanego rozwiązania, co najmniej w zakresie:
   a. instalacji agentów systemowych na urządzeniach końcowych,
   b. konfiguracji mechanizmów automatycznego zarządzania poprawkami,
   c. wdrożenia polityk bezpieczeństwa zapobiegających nieautoryzowanemu kopiowaniu, przesyłaniu i usuwaniu wrażliwych danych,
   d. integracji z istniejącymi systemami uwierzytelniania, takimi jak Active Directory, umożliwiającej import struktur, użytkowników oraz grup RBAC do systemu, a także opcję aktywowania harmonogramu skanowania Active Directory z możliwością określenia częstotliwości jego wykonywania.

7. Wykonawca wyda Zamawiającemu dokumentację administratora oprogramowania lub – jeśli jest ona udostępniana przez producenta w formie elektronicznej – przekaże adresy WWW, pod którymi można ją pobrać.

2.1. Zakup oprogramowania do monitorowania infrastruktury informatycznej

Obszar wymagań	**Wymagania minimalne**
Licencja	Licencja bezterminowa na 40 stanowisk
Budowa systemu	System musi składać się z następujących elementów: 1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej. 2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). 3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach. 4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami. 5. Baza danych SQL. 6. Komponenty systemu (klient, konsola administracyjna, serwer, baza danych) muszą aktualizować się automatycznie poprzez bezpieczne połączenie. 7. System musi posiadać mechanizmy automatycznej konserwacji zgodnie z harmonogramem.
Zgodność z systemami i usługami	1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (co najmniej Internet Explorer 11, FireFox, Chrome, Opera). 2. Klient musi działać na systemach operacyjnych: Windows Server 2019 i 2022, Windows 10 i 11. 3. Klient musi wspierać poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera, Chrome, Firefox.

	4. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare. 5. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie. 6. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server.
Funkcjonalność oprogramowania	1. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku. 2. Konsola administracyjna: a. musi być dostępna w języku polskim i posiadać intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać zestaw dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie. b. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem. c. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.

	3. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora. 4. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania. 5. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office. 6. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń. 7. System musi posiadać zdolności do identyfikacji urządzeń sieciowych. Wymagane jest posiadanie skanerów sieci i SNMP, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać generowanie map sieci. 8. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.

	9. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia. 10. System musi zapewniać zdalne zarządzanie komputerami przy użyciu technologii WEBRTC, umożliwiając jednoczesne połączenia z wieloma urządzeniami. Powinien oferować funkcje takie jak przejęcie kontroli nad pulpitami, zarządzanie plikami, uruchamianie i zarządzanie aplikacjami oraz instalowanie oprogramowania i aktualizacji. System powinien umożliwiać konfigurację połączeń WebRTC, w tym instalację i konfigurację odpowiednich serwerów i portów. Dodatkowo, system powinien obsługiwać różne tryby przejęcia sesji, włączając opcje z lub bez zgody użytkownika, a także umożliwiać nagrywanie i zarządzanie sesjami połączeń, w tym wykonywanie zrzutów ekranu i nagrywanie sesji. System powinien również wspierać różnorodne konfiguracje wyświetlania i jakości sesji, a także umożliwiać uruchomienie do 12 sesji na jednym ekranie. 11. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia. 12. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu. 13. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.

	14. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT. 15. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów. 16. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją. 17. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych. 18. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z

	możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania. 19. System musi posiadać możliwość eksportu / importu treści. 20. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych. 21. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści. 22. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie. 23. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii. 24. System musi umożliwiać monitorowanie komunikatów Syslog. 25. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników. 26. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów. 27. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych. 28. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych

	do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostepnienia w panelu pracownika. 29. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu. 30. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki. 31. System musi umożliwiać generowanie powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co predefiniowane powiadomienia oraz możliwość ich personalizacji. 32. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. System musi wymagać silnych haseł, obsługiwać wieloskładnikowe uwierzytelnianie i posiadać mechanizmy szyfrowania danych.
Wsparcie i pomoc	Oprogramowanie musi być objęte wsparciem technicznym producenta lub dystrybutora przez okres co najmniej do 30.06.2026. W ramach usług wparcia:

	• musi być świadczona pomoc techniczna, która musi być dostępna co najmniej w dni robocze w godzinach od 8.00-15.00, • Zamawiający musi mieć dostęp do aktualizacji oprogramowania.

2.2. Zakup licencji subskrypcyjnych oprogramowania antywirusowego

Obszar wymagań	**Wymagania minimalne**
Licencje	Dostarczone licencje muszą zapewniać ochronę 51 urządzeń (urządzenia końcowe i serwery), w tym: • 35 stanowisk w sieci UG • 4 stanowiska w sieci GZEAS • 12 stanowisk w sieci OPS w okresie od odbioru do 30.06.2026. Licencja dla ww. jednostek może opierać się o jeden wspólny klucz licencyjny. Wymagane wsparcie producenta lub dystrybutora na okres równy okresowi licencjonowania, w tym: • nielimitowany dostęp do poprawek i aktualizacji, • dostęp do nowych funkcji i funkcjonalności w obrębie modułów licencyjnych, • wsparcie telefoniczne i mailowe producenta w trybie 24 x 7. Wsparcie techniczne do programu musi być świadczone w języku polskim przez producenta lub dystrybutora, autoryzowanego przez producenta rozwiązania.
Administracja zdalna w chmurze	1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6.

	7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
Ochrona stacji roboczych	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

	7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne - jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej lub obu metod jednocześnie. 13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z

	możliwością wykorzystania reguł utworzonych przez użytkownika, b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, d. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. a. Funkcja, generująca taki log, ma posiadać możliwość filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. b. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. c. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). d. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
Ochrona serwera	1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux, w tym co najmniej: RedHat Enterprise Linux (RHEL),

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

	14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych . 16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe wymagania dla ochrony serwerów Linux 18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

3. Część 3. Przeprowadzenie audytu KRI oraz aktualizacja i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji wraz ze szkoleniami z zakresu cyberbezpieczeństwa

Przedmiot zamówienia w części 3 obejmuje:

- usług opracowania i wdrożenia SZBI,
- usług przeprowadzenia audytu zgodności KRI,
- usług szkolenia z cyberbezpieczeństwa dla pracowników.

3.1. Wymagania wspólne dla usług opracowania i wdrożenia SZBI i usług przeprowadzenia audytu zgodności KRI

1. Zamówienie będzie realizowane na rzecz Urzędu Gminy Trawniki (dalej: UG) oraz jednostek podległych Zamawiającego: Ośrodka Pomocy Społecznej w Trawnikach (dalej: OPS) i Gminnego Zespołu Ekonomiczno-Administracyjnego Szkół (dalej: GZEAS).
2. Wykonawca będzie zobowiązany do przeprowadzenia w latach 2025 i 2026 audytu systemu zarządzania bezpieczeństwem informacji w związku z zapisami w § 19 ust. 2 pkt 14 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773), zwanego dalej „audytem KRI" w jednostkach wskazanych w ust. 1.
3. Wykonawca jest zobowiązany do przeprowadzenia aktualizacji i wdrożenia kompletnego Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwany: SZBI) w jednostkach wskazanych w ust. 1.
4. Zakres audytu systemu bezpieczeństwa informacji każdorazowo obejmie zgodność z kryteriami zawartymi w § 19 ust. 2 ww. rozporządzenia KRI oraz zgodność z wymaganiami normy PN-EN ISO/IEC 27001:2023 lub równoważnej.
5. Raport z audytu KRI zostanie każdorazowo podpisany przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczony do Zamawiającego w formie elektronicznej.
6. Audyt KRI oraz aktualizacja i wdrożenie SZBI dla Zamawiającego muszą zostać przeprowadzone przez:
   1) audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) lub
   2) audytora wewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001:2023 lub równoważnej.
7. Wykonawca w trakcie realizacji zamówienia jest zobowiązany do zapoznania się z częściowo wypełnioną ankietą dojrzałości cyberbezpieczeństwa w zakresie wskazanym przez Zamawiającego oraz uwzględnić w ramach aktualizacji i wdrożenia SZBI planowany w ramach realizacji projektu zakres usprawnień SZBI.

8. Wykonawca po wykonaniu ostatniego audytu KRI jest zobowiązany do uzupełnienia ankiety dojrzałości cyberbezpieczeństwa. Ankietę dojrzałości cyberbezpieczeństwa należy wypełnić w oparciu o aktualny na dzień wypełnienia ankiety wzór ankiety opublikowany na stronie: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad (załącznik nr 6 - Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego i Jednostkach Podległych).
9. Wypełnienie ankiety dojrzałości cyberbezpieczeństwa polegać będzie wypełnieniu przez Wykonawcę kolumn H, I z arkusza „Ankieta" dla Zamawiającego na podstawie zebranych przez Wykonawcę danych. Zamawiający nie dopuszcza pozostawienia pustych pól dla określonych powyżej kolumn, w przypadku jeżeli w polu opisowym nie przewiduje się zmian wówczas należy zamieścić odpowiednią informację. Ankieta dojrzałości cyberbezpieczeństwa zostanie podpisana przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczona do Zamawiającego w formie elektronicznej.
10. Jednostki samorządu terytorialnego oraz ich jednostki podległe, które biorą udział w projekcie „Cyberbezpieczny Samorząd" są zobowiązane do przesłania do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (dalej: NASK) raportu z audytu KRI oraz wypełnionej ankiety dojrzałości cyberbezpieczeństwa. Niezwłocznie po ich przekazaniu przez Wykonawcę dokumenty te zostaną przekazane przez Zamawiającego do NASK za pośrednictwem platformy ePUAP. Dane z tej dokumentacji przekazane przez JST do NASK posłużą do opracowania raportu na temat stanu bezpieczeństwa systemów jednostek samorządowych. Wykonawca jest zobowiązany mieć na uwadze także powyżej wskazany cel przeprowadzenia zamówienia i jego przeznaczenie.
11. Wykonawca przy świadczeniu usług jest zobowiązany uwzględnić i zastosować wymagania Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) oraz akty wykonawcze wydane do niej. W przypadku jeżeli w okresie realizacji zamówienia zostanie przyjęta ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw bądź inne przepisy implementujące Dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) w polski system prawny Wykonawca ma obowiązek uwzględnić wszystkie ich wymagania przy świadczeniu usług objętych niniejszym zamówieniem

12. Wykonawca zrealizuje zamówienie w oparciu o dokumentację, którą Zamawiający dysponuje niezależnie od realizacji przedmiotu umowy i o wyjaśnienia udzielane przez Zamawiającego. W szczególności realizacja przedmiotu umowy przez Wykonawcę nie może być uwarunkowana wytwarzaniem lub uzupełnianiem dokumentów i opracowań przez Zamawiającego w związku z realizacją przedmiotu umowy, tj. Zamawiający nie może być zobowiązany do wypełniania ankiet, kwestionariuszy, sporządzania notatek itp., a informacje niezbędne Wykonawcy do wykonania przedmiotu umowy mogą być pozyskiwane wyłącznie w postaci materiałów źródłowych i wywiadu bezpośredniego.
13. Zamawiający dopuszcza prowadzenie prac związanych z: analizą dokumentacji, opracowaniem dokumentacji i polityk, opracowania raportów poza siedzibą Zamawiającego. Zamawiający nie dopuszcza prowadzenia instruktaży, konsultacji, audytów, analiz stanu istniejącego i określenie stanu faktycznego zabezpieczeń technicznych w formule zdalnej, tj. w postaci on-line lub innej poza siedzibami UG, OPS i GZEAS.
14. Zamawiający wymaga aby każdy etap (lub jego część) realizacji usługi aktualizacji i wdrożenia SZBI wskazany w dalszej części dokumentu był realizowany w siedzibie UG i jego jednostkach podległych w czasie nie krótszym niż jeden dzień roboczy odrębnie dla UG, dla OPS i dla GZEAS.
15. W ramach wynagrodzenia umownego Wykonawca będzie wprowadzał niezbędne zmiany w opracowanej dokumentacji SZBI, o ile okażą się one konieczne w związku ze zmianami regulacji prawnych lub w związku ze zmianami organizacyjnymi lub technicznymi w UG i/lub OPS i/lub GZEAS, jeżeli takie zmiany wystąpią.
16. Kody CPV:
    1) 79212000-3: Usługi audytu;
    2) 79417000-0: Usługi doradcze w zakresie bezpieczeństwa.

3.2. Zakup usług aktualizacji i wdrożenia SZBI

Celem usługi jest aktualizacja i wdrożenie procedur systemów zarządzania bezpieczeństwem informacji funkcjonujących u Zamawiającego z uwzględnieniem uwarunkowań i specyfiki projektu oraz specyfiki jednostki Zamawiającego. Analiza zostanie przeprowadzona zgodnie z wymogami ISO/IEC 19011:2002. W efekcie zostanie zaktualizowana także polityka bezpieczeństwa w zakresie ochrony danych osobowych. Usługa obejmuje również aktualizację dokumentów opisujących zbiory danych i ich zgodność z wymogami prawnymi oraz aktualizację dokumentów opisujących miejsca i sposoby przetwarzania danych osobowych.
Na usługę aktualizacji, opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji składają się co najmniej:

1. Wykonanie oceny obecnej dostępnej dokumentacji.

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

Ponadto:

6. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje procedury bezpieczeństwa fizycznego obejmujące obowiązek wyznaczania osoby odpowiedzialnej za bezpieczeństwo fizyczne.
7. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje zasady odpowiedzialności za cyberbezpieczeństwo wraz ze wskazaniem obowiązku wyznaczania osoby odpowiedzialnej za cyberbezpieczeństwo.
8. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę szkoleń z zakresu cyberbezpieczeństwa wraz z wprowadzeniem obowiązku regularnego, corocznego prowadzenia szkoleń.
9. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje treść zarządzenia wdrażającego SZBI dla Zamawiającego.
10. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan postępowania z ryzykiem obejmujący systematyczne tworzenie raportów oceny ryzyka w Jednostce oraz konieczność cyklicznego przeglądu tego raportu przez Kierownika JST.
11. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje szczegółowy sposób realizacji celów oraz we współpracy z Zamawiającym przypisze odpowiedzialności za ich realizację.
12. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje procedurę wprowadzającą obowiązek regularnego, corocznego przeglądu PBI jednostki.
13. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę szkoleń obejmującą obowiązek informowania o zmianach w PBI w toku okresowych szkoleń stanowiskowych.
14. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kluczowe aktywa informacyjne Jednostki (zbiory danych/systemy/usługi).
15. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje rejestr ryzyk uwzględniający aktywa Jednostki.
16. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje zagrożenia związane z cyberbezpieczeństwem w ramach procesów zarządczych oraz zarządzania ryzykiem.
17. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan postępowania z ryzykiem związanym z zagrożeniami bezpieczeństwa informacji.
18. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą obowiązek używania do określenia w Jednostce zagrożeń, podatności, prawdopodobieństwa ich wystąpienia i skutków.
19. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą obowiązek identyfikacji i priorytetyzacji odpowiedzi na ryzyka.

20. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem uwzględniającą system oceny ryzyka.
21. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania ryzykiem cyberbezpieczeństwa uwzględniającą identyfikowane, ustanawiane i oceniane ryzyka.
22. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania danymi uwzględniającą polityki ich niszczenia, plan backup, plany reagowania i odtwarzania danych.
23. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan zarządzania podatnościami.
24. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę zarządzania zapisami zdarzeń / logów/ inspekcji.
25. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę użytkowania dostępu do odczytu lub zapisu danych z zewnętrznych nośników danych.
26. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje kompleksową politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów.
27. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje plan zarządzania podatnościami uwzględniający obowiązek dokumentowania ryzyka z nimi związanego.
28. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów i ich aktualizacji w obszarze doświadczeń i wniosków z wykrytych i obsłużonych incydentów.
29. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę reagowania na incydenty uwzględniającą procedury procesowania incydentów wraz z obowiązkiem ich aktualizacji.
30. W ramach realizacji zamówienia Wykonawca opracuje/zaktualizuje politykę planów odtwarzania uwzględniającą obowiązek ich aktualizacji w obszarze doświadczeń i wniosków z prowadzonych procesów odtwarzania.

3.2.1 .Etapy realizacji usługi

Etap I. Audyt zerowy.

1. Określenie stanu spełnienia wymagań prawnych nałożonych na organizację w zakresie ochrony informacji.
2. Sprawdzenie spełnienia wymagań i zaleceń w ramach standardów PN-EN ISO/IEC 27001:2023 i norm pokrewnych.
3. Inwentaryzacja aktywów informacyjnych i ocena ryzyka.
4. Ocena zabezpieczeń technicznych, organizacyjnych oraz fizycznych.

5. Analiza dokumentacji Polityki Bezpieczeństwa Informacji.
6. Analiza dokumentacji Polityki Bezpieczeństwa Danych Osobowych.
7. Zestaw działań mających na celu określenie stanu faktycznego zabezpieczeń technicznych w systemie informatycznym:
   1) Ocena schematu sieci.
   2) Określenie rodzaju połączeń.
   3) Określenie segmentów sieci.
   4) Przeprowadzenie oceny środowiska informatycznego.
   5) Ocena sposobu identyfikowania i logowania użytkowników.
   6) Analiza zarządzania kontami użytkowników.
   7) Analiza strony www i Biuletynu Informacji Publicznej (dalej: BIP) pod kątem ochrony danych osobowych.
   8) Analiza systemu backupów i archiwizacji danych.
   9) Określenie miejsc redundancji w sieci i systemach informatycznych.
   10) Analiza konfiguracji zabezpieczeń systemów operacyjnych na serwerach.
   11) Analiza konfiguracji zabezpieczeń baz danych.
   12) Określenie bezpieczeństwa aplikacji i serwerów WWW.
   13) Analiza konfiguracji urządzeń sieciowych: switche, routery, IDS, IPS, UTM, firewall.
   14) Ocena zabezpieczeń dostępu do sieci publicznej.
   15) Badanie podatności systemów operacyjnych za pomocą specjalistycznego oprogramowania.
   16) Analiza zabezpieczeń stacji roboczych.
   17) Analiza ochrony danych na komputerach przenośnych.
   18) Badanie zabezpieczeń nośników zewnętrznych.
   19) Sprawdzenie procedur zarządzania ciągłością działania.
8. Opracowanie raportu z audytu zerowego zawierającego analizę bezpieczeństwa i adekwatności zabezpieczeń stosowanych przez Zamawiającego w odniesieniu do sieci i systemów informatycznych oraz rodzaju danych w nich przetwarzanych, z uwzględnieniem obowiązujących przepisów prawa, zasad wiedzy technicznej, wymagań normy PN-EN ISO/IEC 27001:2023 i zaleceń norm pokrewnych.

Etap II. Zastosowanie zabezpieczeń na podstawie zaleceń poaudytowych.

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

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

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

Etap IV. Inwentaryzacja i szacowanie ryzyka SZBI.

1. Przeprowadzenie instruktaży dla pracowników oraz kadry zarządzającej z metody inwentaryzacji i klasyfikacji aktywów informacyjnych.
2. Wykonanie wraz z pracownikami inwentaryzacji i klasyfikacji aktywów informacyjnych.
3. Zdefiniowanie planu postępowania z ryzykiem:
   1) przeprowadzenie instruktaży dla kadry zarządzającej z wybranej metody oceny ryzyka;
   2) szacowanie i ocena ryzyka – zaktualizowanie wartości ryzyka wynikające z audytu zerowego;
   3) zdefiniowanie planu postępowania z ryzykiem;

4) określenie planu zarządzania zidentyfikowanymi i oszacowanymi ryzykami;
5) określenie zadań do realizacji, zdefiniowanie odpowiedzialności i ram czasowych.

4. Opracowanie raportu z oceny ryzyka.

Etap V. Opracowanie niezbędnej dokumentacji SZBI.

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

Etap VI. Weryfikacja i monitorowanie SZBI.

1. Przeprowadzenie wraz z pracownikami organizacji audytu wewnętrznego.
2. Opracowanie raportu z audytu wewnętrznego.
3. Przeprowadzenie wraz z pracownikami organizacji przeglądu systemu SZBI:
   1) przegląd zagrożeń;
   2) przegląd podatności;
   3) określenie i weryfikacja ryzyk;
   4) weryfikacja planu postępowania z ryzykiem;
   5) sprawdzenie zabezpieczeń i celów zabezpieczeń;
   6) określenie zgodności zakresu SZBI;

7) weryfikacja zgodności z politykami i celami zabezpieczeń;
8) przegląd i ocena skuteczności zabezpieczeń;
9) weryfikacja zgodności wykorzystywania procedur;
10) weryfikacja zgodności obowiązków i uprawnień w ramach SZBI;
11) analiza audytów bezpieczeństwa;
12) weryfikacja dokumentacji i sposobu postępowania z incydentami;
13) weryfikacja sugestii oraz informacji zwrotnych od zainteresowanych stron;
14) sprawdzenie aktualności procedur ciągłości działania.

4. Opracowanie raportu z przeglądu.

3.3. Zakup usług przeprowadzenia audytu zgodności KRI

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

1. Przedmiotem zamówienia jest przeprowadzenie audytu dotyczącego spełnienia wymagań normy PN-EN ISO/IEC 27001:2023 oraz Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2024 poz. 773), zwanym dalej „Rozporządzeniem KRI".
2. Audyt KRI musi być przeprowadzony przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
3. Określenie minimalnego zakresu audytowanych obszarów:
    a) świadczenie usług w formie elektronicznej w tym udostępnionej na platformie ePUAP, zgodnie z art. 16 ust. 1a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2024 poz. 307);
    b) zamieszczenie na głównej stronie internetowej podmiotu (i/lub na stronie BIP), odesłania do opisów usług, które zawierają wymagane informacje dotyczące m.in. aktualnej podstawy prawnej świadczonych usług, nazwy usług, miejsca świadczenia usług (złożenia dokumentów), terminu składania i

załatwiania spraw oraz nazwy komórek odpowiedzialnych za załatwienie spraw, zgodnie z § 5 ust. 2 pkt 1 i 4 Rozporządzenia KRI;

c) poziom wspierania modelu usługowego w procesie świadczenia usług elektronicznych przez systemy teleinformatyczne podmiotu, zgodnie z §15 ust. 2 Rozporządzenia KRI;
d) poziom współpracy systemów teleinformatycznych z innymi systemami podmiotu publicznego lub systemami informatycznymi innych podmiotów publicznych w tym rejestrami referencyjnymi, zgodnie z §5 ust. 3 pkt 3 Rozporządzenia KRI;
e) sposób komunikacji z innymi systemami w tym wyposażenie w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami telekomunikacyjnymi za pomocą protokołów komunikacyjnych i szyfrujących zapewniających BI, zgodnie z §16 ust. 1 Rozporządzenia KRI;
f) regulacje wewnętrzne opisujące sposób zarządzania dokumentacją, w tym zakres stosowania elektronicznego obiegu dokumentów, zgodnie z §19 ust. 2 pkt 9 Rozporządzenia KRI;
g) sposób kodowania znaków w dokumentach wysyłanych i odbieranych z systemów teleinformatycznych podmiotu, zgodnie z §17 ust. 1 Rozporządzenia KRI;
h) sposób udostępniania zasobów informatycznych z systemów teleinformatycznych, zgodnie z §18 ust. 1 Rozporządzenia KRI;
i) sposób przyjmowania dokumentów elektronicznych przez systemy teleinformatyczne, zgodnie z §18 ust. 2 Rozporządzenia KRI;
j) dokumentacja SZBI, w tym Polityka BI oraz inne dokumenty stanowiące SZBI, Dokumentacja przeglądów SZBI, szacowania ryzyka, audytów, incydentów naruszenia BI, zgodnie z §19 ust. 1 Rozporządzenia KRI;
k) działania związane z aktualizacją regulacji wewnętrznych w zakresie zmieniającego się otoczenia będące konsekwencją wyników szacowania ryzyka, wniosków z przeglądów SZBI, zaleceń poaudytowych, wniosków z analizy incydentów naruszenia BI, zgodnie z §19 ust. 2 pkt 1 Rozporządzenia KRI;
l) stopień zaangażowania kierownictwa podmiotu w proces ustanawiania i funkcjonowania SZBI oraz zarządzania BI (przeglądy SZBI, szacowanie i obsługa ryzyka BI, egzekwowanie działań związanych z BI), zgodnie z §19 ust. 2 Rozporządzenia KRI;
m) regulacje wewnętrzne opisujące sposób zarządzania ryzykiem BI w podmiocie;
n) dokumentacja z przeprowadzania okresowej analizy ryzyka utraty integralności, poufności lub dostępności informacji, w tym rejestr ryzyk,

zawierający informacje o zidentyfikowanych ryzykach, ich poziomie, plan postępowania z ryzykiem, zgodnie z §19 ust. 2 pkt 3 Rozporządzenia KRI;

o) działania minimalizujące ryzyko zgodnie z planem postępowania z ryzykiem stosownie do szacowania ryzyka;
p) regulacje wewnętrzne opisujące sposób zarządzania sprzętem informatycznym i oprogramowaniem (w tym licencjami na oprogramowanie) oraz funkcjonowania rejestru zasobów teleinformatycznych;
q) rejestr zasobów teleinformatycznych zawierający informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku, zgodnie z §19 ust. 2 pkt 2 Rozporządzenia KRI;
r) sposób aktualizacji rejestru zasobów teleinformatycznych;
s) regulacje wewnętrzne opisujące zarządzania uprawnieniami użytkowników do pracy w systemach teleinformatycznych, w tym do przetwarzania danych osobowych;
t) adekwatność poziomu uprawnień do pracy w systemach teleinformatycznych do zakresu czynności i posiadanych upoważnień dostępu do informacji, w tym upoważnień do przetwarzania danych osobowych (rejestr wydanych upoważnień), zgodnie z §19 ust. 2 pkt 4 Rozporządzenia KRI;
u) działania w zakresie monitoringu i kontroli dostępu do zasobów teleinformatycznych, w tym przeglądy w celu wykrywania nieuprawnionego dostępu, nadmiernych uprawnień, konfliktu interesów czy nadzorowania samego siebie itp.;
v) sposób i szybkość odbierania uprawnień byłym pracownikom w systemach informatycznych, zgodnie z §19 ust. 2 pkt 5 Rozporządzenia KRI;
w) regulacje wewnętrzne dotyczące przeprowadzania szkoleń użytkowników zaangażowanych w procesie przetwarzania informacji w systemach teleinformatycznych;
x) dokumentacja z przeprowadzonych szkoleń pod kątem zakresu tematycznego, w tym: aktualności informacji o zagrożeniach, skutkach i zabezpieczeniach, wskaźnik liczby osób przeszkolonych w stosunku do wszystkich osób uczestniczących w procesie przetwarzania informacji, a także cykliczności szkoleń, zgodnie z §19 ust. 2 pkt 6 Rozporządzenia KRI;
y) regulacje wewnętrzne określające zasady bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, zgodne z §19 ust. 2 pkt 8 Rozporządzenia KRI;
z) działania w zakresie stosowania zasad bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, w tym stosowania

zabezpieczeń i procedur bezpieczeństwa przez użytkowników urządzeń przenośnych i pracy na odległość;

aa) umowy serwisowe oraz umowy dotyczące rozwoju systemów teleinformatycznych w zakresie zapisów gwarantujących odpowiedni poziom BI, zgodne z §19 ust. 2 pkt 1 Rozporządzenia KRI;

bb) regulacje wewnętrzne, w których określono zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji;

cc) sposób zgłaszania i postępowania z incydentami (działania korygujące), rejestr incydentów naruszenia BI, wpływ analizy incydentów na SZBI, ewentualna współpraca z CERT.GOV.PL, zgodnie z §19 ust. 2 pkt 13 Rozporządzenia KRI;

dd) regulacje wewnętrzne, w których określono zasady przeprowadzania audytów wewnętrznych w zakresie BI;

ee) sprawozdania z audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z §19 ust. 2 pkt 14 Rozporządzenia KRI;

ff) działania podjęte w wyniku zaleceń poaudytowych;

gg) określenie zasad tworzenia, przechowywania oraz testowania kopii zapasowych danych i systemów podmiotu, zgodnie §19 ust. 2 pkt 12 lit. b rozporządzenia KRI;

hh) działania związane z wykonywaniem, przechowywaniem i testowaniem kopii zapasowych danych i systemów oraz dokumentacja z tych działań;

ii) regulacje wewnętrzne, w których ustalono zasady postępowania z informacjami zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, oraz urządzeń mobilnych, w tym plan postępowania z ryzykiem, zgodne z §19 ust. 2 pkt 11 Rozporządzenia KRI;

jj) regulacje wewnętrzne dotyczące zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami poprzez ustalenie zabezpieczeń informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje usunięcie lub zniszczenie, zgodnie z §19 ust. 2 pkt 7 i 9 Rozporządzenia KRI;

kk) działania związane z monitorowaniem dostępu do informacji np. w systemie informatycznym odnotowującym w bazie danych wszystkie działania użytkowników i administratorów dotyczące systemów teleinformatycznych podmiotu publicznego. Działania związane z monitorowaniem ruchu osobowego w podmiocie, zgodnie z § 19 ust. 2 pkt 7 lit. a) Rozporządzenia KRI;

ll) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez kontrolę logów systemów, kontrolę wejść i wyjść do pomieszczeń serwerowni, analizę rejestru zgłoszeń

serwisowych, analizę rejestru incydentów naruszenia BI, zgodnie z §19 ust. 2 pkt 7 lit. b) Rozporządzenia KRI;

mm) działania związane z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych usług sieciowych i aplikacji poprzez stosowanie systemu kontroli dostępu do pomieszczeń serwerowni, systemu autoryzacji dostępu do systemów operacyjnych, sieci i aplikacji, stosowanie zabezpieczeń kryptograficznych, stosowanie systemów antywirusowych i antyspamowych, stosowanie zapór sieciowych typu firewall zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem, zgodnie z § 19 ust. 2 pkt 7 lit. c) Rozporządzenia KRI;

nn) działania związane z ochroną fizyczną informacji zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych, zgodne z wynikami analizy ryzyka i planem postępowania z ryzykiem;

oo) działania związane z utylizacją sprzętu informatycznego i nośników danych a także związane z przekazywaniem sprzętu informatycznego do naprawy w sposób gwarantujący zachowanie BI;

pp) regulacje wewnętrzne, w których ustalono zasady w celu zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych poprzez opisy stosowania zabezpieczeń, w tym plan postępowania z ryzykiem, zgodnie z §19 ust. 2 pkt 12 oraz ust. 4 Rozporządzenia KRI;

qq) regulacje wewnętrzne zawierające zasady prowadzenia i wykorzystania dzienników systemowych (logów), w których odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych, zgodnie z §20 Rozporządzenia KRI;

rr) sposób prezentacji informacji na stronach internetowych systemów telekomunikacyjnych podmiotu oraz zgodność z wymogami WCAG2.1.

Na podstawie przeprowadzonej analizy dokumentacji oraz audytu bezpieczeństwa, Wykonawca jest zobowiązany przedstawić pisemny raport zawierający wszystkie wyniki, wnioski wraz z propozycją zmian w zakresie spełnienia wymagań Rozporządzenia KRI. W raporcie muszą zostać uwzględnione wszystkie wyniki cząstkowe z audytowanych obszarów. Spełnienie poszczególnych wymagań zostanie określone w trzyelementowej skali: 1) spełnione – oznacza, że wymaganie normy zostało całkowicie wdrożone, 2) częściowo spełnione – może zaistnieć, czy dany obszar został udokumentowany (opracowano stosowną procedurę lub przygotowano inne zabezpieczenie), ale wybrany mechanizm nie został skutecznie wdrożony (np. zdefiniowano strefy bezpieczeństwa, ale system kontroli dostępu nie funkcjonuje poprawnie); najczęstszym przypadkiem oznaczenia wymagania jako „częściowo spełnionego” jest nieskuteczne wdrożenie

procedury (nie przestrzeganie zapisów procedury przez pracowników), 3) niespełnione – wymaganie niespełnione oznacza, że nie zostało ono w ogóle zidentyfikowane przez podmiot (podmiot nie jest świadomy danego zagrożenia) lub nie podjęto żadnych działań, aby wdrożyć odpowiednie mechanizmy zabezpieczające.

3.4. Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa

1. Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników jednostki Zamawiającego – Urzędu Gminy Trawniki (dalej: UG) oraz jednostek podległych Zamawiającego: Ośrodka Pomocy Społecznej w Trawnikach (dalej: OPS) i Gminnego Zespołu Ekonomiczno-Administracyjnego Szkół (dalej: GZEAS).
2. Miejsce świadczenia usługi: Urząd Gminy Trawniki. Nie dopuszcza się prowadzenia szkoleń za pomocą środków zdalnej komunikacji.
3. Zamawiający zapewni jedną salę, w której przeprowadzone zostaną szkolenia; sala wyposażona jest w sprzęt audiowizualny.
4. Udział w szkoleniach nie może wiązać się z dodatkowymi kosztami dla Zamawiającego, w szczególności nie może on być zobowiązany do nabywania dodatkowych usług czy licencji na oprogramowanie. Wykonawca zapewni wszelkie narzędzia konieczne do realizacji szkoleń inne, niż zapewnione przez Zamawiającego i wskazane w pkt. powyżej.
5. Szkolenie będzie przeprowadzone w godzinach pracy zamawiającego, tj. od 08.00 do 16.00 w poniedziałki oraz od 07.30 do 15.30 od wtorku do piątku.
6. Zamawiający przewiduje łączną liczbę uczestników szkoleń w ilości 45 osób.
7. Wykonawca przeprowadzi szkolenia dla grup maksymalnie 10 – osobowych, przewiduje się 5 grup.
8. Dla każdej grupy z osobna szkolenie będzie trwało co najmniej 4 godziny.
9. W terminie 7 dni od zawarcia umowy Wykonawca opracuje w porozumieniu z Zamawiającym i przekaże do akceptacji Zamawiającego:
   a. szczegółowy program szkoleń,
   b. harmonogram szkoleń,
   c. projekt certyfikatu ukończenia szkolenia.
10. Zamawiający zaleca, aby szczegółowy program szkoleń uwzględniał następujące zagadnienia:
    a. Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.
    b. Polityka bezpieczeństwa w organizacji.
    c. Definicja incydentu bezpieczeństwa i zasady postępowania z incydentem.

d. Rodzaje ataków: ataki socjotechniczne, ataki komputerowe, ataki przez sieci bezprzewodowe, ataki przez pocztę e-mail (fałszywe e-maile), ataki przez strony WWW, ataki przez telefon, phishing, spoofing, spam.
e. Bezpieczeństwo fizyczne - urządzenia, dokumenty, „czyste biurko".
f. Zabezpieczenie informatycznych nośników danych – pendrivy i pamięci zewnętrzne.
g. Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.
h. Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych.
i. Prawidłowe korzystanie z oprogramowania antywirusowego.
j. Zasady aktualizacji programów i aplikacji.
k. Szyfrowanie dokumentów i poczty elektronicznej.
l. Polityka haseł, zarządzanie dostępem i tożsamością.

11. Harmonogram szkoleń musi uwzględniać wymagania określone w niniejszym zapytaniu.
12. Wykonawca przeprowadzi szkolenia w języku polskim.
13. Wykonawca zapewni dokumentację wszystkich szkoleń:
    a. listy obecności uczestników szkoleń,
    b. listy odbioru certyfikatów o ukończonych szkoleniach.
14. Po zakończeniu szkoleń Wykonawca przekaże każdemu uczestnikowi certyfikat ukończenia szkolenia. Certyfikat musi zawierać co najmniej: imię i nazwisko uczestnika, informację o ilości godzin, zrealizowanym zakresie tematycznym oraz oznaczenia dotyczące współfinansowania projektu.
15. Po zakończeniu szkoleń Wykonawca przekaże Zamawiającemu na potrzeby archiwalne projektu jeden komplet wszystkich materiałów przekazanych uczestnikom w wersji papierowej oraz udostępni elektronicznie kompletną treść prezentacji multimedialnej wykorzystywanej przez prowadzącego w trakcie szkolenia.
16. Wszelkie dokumenty wytworzone i przekazane przez Wykonawcę w ramach realizacji Zamówienia, w tym materiały szkoleniowe i certyfikaty muszą spełniać standardy dostępności oraz muszą być prawidłowo oznakowane zgodnie z Podręcznikiem wnioskodawcy i beneficjenta programów polityki spójności 2021-2027 w zakresie informacji i promocji, z uwzględnieniem logotypów obowiązujących dla projektu „Cyberbezpieczny Samorząd".