Projekt dofinansowany z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Warmia-Mazury 2014-2020

Załącznik A. do ZMINAY TREŚCI SIWZ NR 1
ZAŁĄCZNIK NR 12 do SIWZ
Część 2 zamówienia

OPIS PRZEDMIOTU ZAMÓWIENIA
CZĘŚĆ II

Dostawa sprzętu teleinformatycznego w ramach projektu pn. „Projekt zintegrowanej informacji geodezyjno-kartograficznej powiatu elbląskiego"

System służący do utworzenia bezpiecznego połączenia:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT, i transparentnym.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy systemu w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów systemu.
System musi wspierać IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Passive. Dopuszcza się również możliwość łączenia w klaster Active-Passive ale nie jest wymagana. Powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 16 portami Gigabit Ethernet RJ-45.
   - 16 gniazdami SFP 1 Gbps.
   - 2 gniazdami SFP+ 10 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 256 GB.
5. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 9 mln jednoczesnych połączeń oraz 180.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 25 Gbps w trybie dla ruchu IMIX oraz nie mniejsza niż 28 Gbps dla ruchu pakietów, których rozmiar ustalają laboratoria certyfikujące.

Projekt dofinansowany z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Warmia-Mazury 2014-2020

3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 8 Gbps.
4. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 10 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.

Funkcje Systemu Bezpieczeństwa:

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

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

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

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

Projekt dofinansowany z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Warmia-Mazury 2014-2020

Routing i obsługa łączy WAN

1. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

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

Kontrola Antywirusowa

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
4. System musi dysponować sygnaturami do ochrony urządzeń mobilnych.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Baza sygnatur ataków powinna zawierać minimum ~~5000~~ 1500 wpisów.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 1000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

Projekt dofinansowany z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Warmia-Mazury 2014-2020

2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

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

Logowanie

1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

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

Projekt dofinansowany z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Warmia-Mazury 2014-2020

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla oferowanego urządzenia.
- Certyfikat ICSA lub rekomendacja respektowana przez NATO i Unię Europejską, NATO Restricted i UE Restricted.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: kontrolę Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres 24 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 24 lub okres wskazany w ofercie, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

Rozszerzone wsparcie serwisowe AHB/SOS

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres min. 24 miesięcy lub okres wskazany w ofercie.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. Oferent winien przedłożyć przed podpisaniem umowy dokumenty:
   - Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
   - Certyfikat ISO 9001 podmiotu serwisującego.

Opis do wymagań ogólnych

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

Projekt dofinansowany z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Warmia-Mazury 2014-2020

Opis sprzętu :

Wyposażenie serwerowni:

a) **2 zestawy serwer + macierz dyskowa,**
b) **System służący do utworzenia bezpiecznego połączenia**

Serwery – 2 szt.

Nazwa elementu, parametru lub cechy	Opis wymagań Serwerów
Ilość sztuk	2 szt.
Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.
Procesor	Architektura x86, maksymalny TDP dla procesora – 140W. Minimalna ilość rdzeni dla procesora – 14. Wynik wydajności procesora instalowanego w oferowanym serwerze powinien przekraczać 59 punktów baseline w SPEC w teście CINT2006 Rates, opublikowanych przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. Obsługa minimum dwóch procesorów.
Liczba procesorów	**Min**. 2
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon)
Pamięć operacyjna	Zainstalowane 128GB pamięci RAM Minimum 24 sloty na pamięć, wsparcie pamięci typu RDIMM oraz LRDIMM. Pamięć o częstotliwości 2666MHz.
Zabezpieczenie pamięci	ECC, and Chipkill.
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. Port VGA.
Dyski	Zainstalowane dyski: 6x 600GB w konfiguracji RAID 1
Rozbudowa dysków	Serwer musi posiadać min. 8 dostępnych zatok na dyski Hot-Swap 2,5", umożliwiających instalację dysków SATA/SAS – bez wymiany/dokładania jakichkolwiek elementów serwera. Możliwość instalacji dysków SED. Możliwość zastosowania w serwerze backplane'u umożliwiającego instalację zarówno dysków SATA/SAS jak i NVMe w tych samych zatokach z tym samym backplane zamiennie.
Kontroler dyskowy	Zintegrowany na płycie kontroler SATA Zainstalowany kontroler 12 Gb SAS/SATA z obsługą RAID 0, 1, 10, 5, 50.
Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 1100W z certyfikatem minimum Platinum.
Interfejsy sieciowe	Zintegrowane na płycie 4 porty 10Gb SFP+. Interfejsy te nie mogą wpływać na ilość dostępnych slotów PCIe wymienionych w punkcie Dodatkowe porty I/O Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty

Projekt dofinansowany z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Warmia-Mazury 2014-2020

	zarządzającej.
Karty sieciowe	Dodatkowo zainstalowane: Min. 2 karty FC 16Gbps Dual port
Dodatkowe sloty I/O	Dostępny, niezajęty i gotowy do użytku min. 1 port PCIe x8
Dodatkowe porty	• z przodu obudowy: 1x USB 3.0, 1x USB 2.0, 1x DB-15 video. • z tyłu obudowy: 2x USB 3.0, , 1x DB-15
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
Zarządzanie	• Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania • Monitoring statusu i zdrowia systemu • Logowanie zdarzeń • Umożliwiający Update systemowego firmware • Umożliwiający zdalną konfigurację serwera • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Przekierowanie kosnoli szeregowej przez IPMI • Zrzut ekranu w momencie zawieszenia system • Możliwość przejęcia zdalnego ekranu 1920x1200, 60 Hz,16 bpp • Zdalny dostęp do serwera • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych I historycznych dla użycia energii I temperatury serwera • Możliwość mapowania obrazów ISO z lokalnego dysku operatora • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API Możliwość przełączenia frontowego portu USB w taki sposób, aby ten port służył serwisantowi (był podłączony do karty zarządzającej) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.
Funkcje zabezpieczeń	Hasło włączania, hasło administratora, moduł TPM. Opcjonalny zamykany panel przedni serwera.
Urządzenia hot swap	Dyski twarde, zasilacze oraz wentylatory
Obsługa	Możliwość instalacji serwera oraz wymiany procesora, radiatora oraz tzw. Backplane'y dysków twardych do celów serwisowych bez użycia

	dodatkowych narzędzi mechanicznych.
Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera.
Systemy operacyjne	Microsoft Windows Server, 25 x windows serwer CAL USER lub równoważny. Parametry równoważności: Pełna integracja z domeną Active Directory MS Windows (posiadaną przez Zamawiającego) opartą na serwerach Windows Server 2012 pozwalająca na wdrożenie jednolitej polityki bezpieczeństwa dla wszystkich komputerów w sieci • Zarządzanie komputerami poprzez Zasady Grup (GPO) Active Directory MS Windows (posiadaną przez Zamawiającego), WMI.
Waga	maximum: 18,8 kg
Gwarancja	min. 24 miesięcy gwarancji producenta lub okres gwarancji wskazany w ofercie. Gwarantowany czas naprawy 24h. Wszelkie uszkodzone nośniki danych pozostają u zamawiającego. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Karty zdalnego zarządzania (tj. procesor, pamięć, VRM, dyski, zasilacze, wentylatory) wymagane jest rozszerzenie poziomu gwarancji do 36 miesięcy 7/24 fix 4h oraz zainstalowania dodatkowego dla każdej lokalizacji systemu monitoringu (na dedykowanym serwerze o parametrach rekomendowanych przez producenta oprogramowania monitorującego)

Macierz pamięci masowej

Komplet 2 szt. współpracujących ze sobą macierzy dyskowych typu Fibre Channel w obudowach maksymalnie 2U każda. Każda z macierzy musi posiadać:

Zasilacze, wentylatory, kontrolery RAID – redundantne.

Zamontowane dwa kontrolery posiadające minimum 8 portów FC8 do podłączenia serwerów. Przepustowość 8 Gb/s, obsługa w trybie bezpośrednim minimum 7 serwerów lub obsługa minimum 60 hostów z przełącznikami FC oraz dowolnej liczby hostów wirtualnych, minimum 2 GB pamięci cache zapisu mirrorowania między kontrolerami, obsługa RAID 0,1,5,6,10. 4 porty FC 8 Gb/s na kontroler, kontrolery będą pracowały nawet w przypadku zaniku jednej z faz zasilania, dodatkowy port umożliwiający podłączenie półek dyskowych, złącze zdalnego zarządzania macierzą przez Ethernet, możliwość podłączenia maksymalnie 190 napędów w dodatkowych półkach dyskowych. Zamontowanych 6 dysków 3,5 cala o pojemności minimum 600 GB każdy o prędkości transferu minimum 6 Gbps w tym 2 dyski hot-spare automatycznie. Typ dysków i obudowy wspierające operacje Hot-Plug. Na dyskach oraz obudowach dysków musi znajdować się oznaczenie o pojemności i typie dysku. Możliwość stosowania różnych dysków twardych w obrębie macierzy (pojemność, typ).

Pełne zarządzanie macierzą poprzez przeglądarkę Internetową lub przez dedykowane oprogramowanie producenta.

Macierz musi być wyposażona w oprogramowanie z wszelkimi niezbędnymi licencjami – bez konieczności zakupu dodatkowych umożliwiające:

1. Zarządzanie macierzą w tym powiadamianie –emailem o awarii,
2. Maskowanie i mapowanie dysków,
3. Replikacja danych (synchroniczna) pomiędzy macierzami on-line (synchronizacja).
4. Wykonywanie kopii migawkowych.
5. Wykonywanie kopii migawkowych minimum 16 na LUN,

Projekt dofinansowany z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Warmia-Mazury 2014-2020

6. Możliwość utworzenia minimum 128 LUN'ów
7. Podłączenie minimum 32 hostów.

Wsparcie dla systemów operacyjnych min.: MS Windows 2003/2008, RHEL, SUSE, Vmware.
W komplecie dwa kable FC o długości minimum 2m dla każdej macierzy.
Macierz musi być wyprodukowany zgodnie z normą ISO-9001 i ISO-14001.

Sprzęt komputerowy stanowiskowy - 2 szt

Komputer stacjonarny z systemem operacyjnym w wersji Professional, pełna integracja z posiadanym systemem Windows na obecnie funkcjonujących stanowiskach.

Typ: Komputer stacjonarny, obudowa typu Tower, kolor czarny.
Zastosowanie: Komputer będzie wykorzystywany w firmie, dla potrzeb:
- środowisk **VX CAD/CAM (zintegrowane oprogramowanie dla inżynierów z grup: (ang. Computer Aided Manufacturing) komputerowe wspomaganie wytwarzania i (ang. Computer Aided Design) komputerowe wspomaganie projektowania,**

Komputer musi zapewnić szybką i wydajną pracę w wymienionych wyżej zastosowaniach.
2 x Procesor: Osiągający w teście PassMark CPU Mark wynik min. 11300 punktów według wyników ze strony https://www.cpubenchmark.net/cpu_list.php lub ze strony https://www.cpubenchmark.net/cpu_lookup.php, z dnia 22-03-2018r.
Pamięć operacyjna RAM: Zainstalowane min. 24 GB, maksymalna obsługiwana pojemność min. 256 GB.
Płyta główna: Wyposażona w sloty:
- PCI-e x1 - min. 1 szt.,
- PCI-e x16 - min. 2 szt.

Porty i złącza: Wbudowane porty i złącza:
- USB 2.0 – min. 2 szt.,
- USB 3.0 – min. 4 szt.,
- RJ 45,1gbit
- wejście/wyjście audio mini Jack.

Obudowa:
Minimum 3 wyjścia USB muszą znajdować się z przodu obudowy w połowie jej wysokości lub na górze. Wymagana ilość portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.,3 wentylatory, pełny obieg powietrza.
Karta dźwiękowa: Zintegrowana z płytą główną.
Karta sieciowa: Zintegrowana z płytą główną.
Parametry pamięci masowej 1: Szybki i wydajny dysk twardy o pojemności min. 2TB, typu SATA w wersji min. III, 3,5".
Parametry pamięci masowej 2: Szybki i wydajny dysk twardy o pojemności min. 250GB, typu SSD w 2,5".
Karta graficzna: Oferująca odpowiednią moc do obsługi wspomaganego komputerowo projektowania, wytwarzania oraz prac inżynieryjnych, osiągająca w teście PassMark Per-formance Test wynik min. 13400 ~~13500~~ punktów (G3D Rating) według wyników ze strony:
http://www.videocardbenchmark.net/gpu_list.php z dnia 22-03-2018r.
Napędy wbudowane: Nagrywarka typu SATA DVD +/-RW.
Certyfikaty: Komputery w oferowanej konfiguracji muszą spełniać normy Energy Star 5.0 i EPEAT.
Oferowane modele komputerów muszą posiadać certyfikat ISV (ang. Independent Software Vendors), potwierdzający certyfikowanie w zakresie zgodności z najpopularniejszymi aplikacjami CAD/CAM, w tym:
- Dassault Systèmes, w tym CATIA i SolidWorks,
- Autodesk Product Design Suite, w tym Inventor® oraz AutoCAD, 3D CAD i Revit®,

Projekt dofinansowany z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Warmia-Mazury 2014-2020

- Siemens, w tym Solid Edge, Tecnomatix i NX.

Wymagania dodatkowe: Zainstalowany system operacyjny w wersji Professional w polskiej wersji językowej, nie wymagający aktywacji za pomocą telefonu lub Internetu + nośnik.
System operacyjny musi umożliwiać pracę na posiadanym przez Zamawiającego oprogramowaniu:
- Laboratorium Informatyki Elbox 2.0 (lub Windows XP za pośrednictwem Oracle VM Virtual Box),
- AutoCAD 12LT,
- Bloodsheed Dev-C++ 5.11,
- Visual Studio .NET Pro 2003 Win32 English,

oraz najpopularniejszych aplikacji CAD/CAM, w tym:
- Dassault Systèmes, w tym CATIA i SolidWorks,
- Autodesk Product Design Suite, w tym Inventor® oraz AutoCAD, 3D CAD i Revit®,
- Siemens, w tym Solid Edge, Tecnomatix i NX.

Komputery muszą posiadać oprogramowanie automatycznie dostrajające stację roboczą w celu uruchamiania niektórych najpopularniejszych aplikacji niezależnych dostawców oprogramowania (ISV).
Akcesoria: Patchcord UTP kat 6 0,5m, przewód zasilający.
Wsparcie techniczne producenta komputera:
- Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie internetowej producenta sprzętu w godzinach pracy urzędu
- Dostęp do najnowszych sterowników i uaktualnień na stronie producenta komputera realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera.

Gwarancja: minimum 2-letnia gwarancja producenta świadczona na miejscu u klienta. W przypadku awarii dysku nośnik, który uległ awarii, pozostaje u Zamawiającego.

Stacje robocze - Zestawy komputerowe - 5 szt

Komputer stacjonarny z systemem operacyjnym w wersji Professional, pełna integracja z posiadanym systemem Windows na obecnie funkcjonujących stanowiskach.

Typ: Komputer stacjonarny, obudowa typu Tower, kolor czarny.
Zastosowanie: Komputer będzie wykorzystywany w firmie, dla potrzeb:
- środowisk **VX CAD/CAM (zintegrowane oprogramowanie dla inżynierów z grup: (ang. Computer Aided Manufacturing) komputerowe wspomaganie wytwarzania i (ang. Computer Aided Design) komputerowe wspomaganie projektowania,**

Komputer musi zapewnić szybką i wydajną pracę w wymienionych wyżej zastosowaniach.
Procesor: Osiągający w teście PassMark CPU Mark wynik min. 11300 punktów według wyników ze strony https://www.cpubenchmark.net/cpu_list.php z dnia 22-03-2018r.
Pamięć operacyjna RAM: Zainstalowane min. 12 GB, maksymalna obsługiwana pojemność min. 256 GB.
Płyta główna: Wyposażona w sloty:
- PCI-e x1 - min. 1 szt.,
- PCI-e x16 - min. 2 szt.

Porty i złącza: Wbudowane porty i złącza:
- USB 2.0 – min. 2 szt.,
- USB 3.0 – min. 4 szt.,
- RJ 45,1gbit
- wejście/wyjście audio mini Jack.

Obudowa:
Minimum 3 wyjścia USB muszą znajdować się z przodu obudowy w połowie jej wysokości lub na górze. Wymagana ilość portów USB nie może być osiągnięta w wyniku stosowania konwerterów,

Projekt dofinansowany z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Warmia-Mazury 2014-2020

przejściówek itp.,3 wentylatory, pełny obieg powietrza.
Karta dźwiękowa: Zintegrowana z płytą główną.
Karta sieciowa: Zintegrowana z płytą główną.
Parametry pamięci masowej 1: Szybki i wydajny dysk twardy o pojemności min. 1TB, typu SATA w wersji min. III, 3,5".
Karta graficzna: Oferująca odpowiednią moc do obsługi wspomaganego komputerowo projektowania, wytwarzania oraz prac inżynieryjnych,osiągająca w teście PassMark Per-formance Test wynik min. 6700 punktów (G3D Rating) według wyników ze strony http://www.videocardbenchmark.net/gpu_list.php z dnia 22-03-2018r.
Napędy wbudowane: Nagrywarka typu SATA DVD +/-RW.
Certyfikaty: Komputery w oferowanej konfiguracji muszą spełniać normy Energy Star 5.0 i EPEAT.
Oferowane modele komputerów muszą posiadać certyfikat ISV (ang. Independent Software Vendors), potwierdzający certyfikowanie w zakresie zgodności z najpopularniejszymi aplikacjami CAD/CAM, w tym:
- Dassault Systèmes, w tym CATIA i SolidWorks,
- Autodesk Product Design Suite, w tym Inventor® oraz AutoCAD, 3D CAD i Revit®,
- Siemens, w tym Solid Edge, Tecnomatix i NX.

Wymagania dodatkowe: Zainstalowany system operacyjny w wersji Professional w polskiej wersji językowej, nie wymagający aktywacji za pomocą telefonu lub Internetu + nośnik.
System operacyjny musi umożliwiać pracę na posiadanym przez Zamawiającego oprogramowaniu:
- Laboratorium Informatyki Elbox 2.0 (lub Windows XP za pośrednictwem Oracle VM Virtual Box),
- AutoCAD 12LT,
- Bloodsheed Dev-C++ 5.11,
- Visual Studio .NET Pro 2003 Win32 English,

oraz najpopularniejszych aplikacji CAD/CAM, w tym:
- Dassault Systèmes, w tym CATIA i SolidWorks,
- Autodesk Product Design Suite, w tym Inventor® oraz AutoCAD, 3D CAD i Revit®,
- Siemens, w tym Solid Edge, Tecnomatix i NX.

Komputery muszą posiadać oprogramowanie automatycznie dostrajające stację roboczą w celu uruchamiania niektórych najpopularniejszych aplikacji niezależnych dostawców oprogramowania (ISV).
Akcesoria: Patchcord UTP kat 6 0,5m, przewód zasilający.
Wsparcie techniczne producenta komputera:
- Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie internetowej producenta sprzętu w godzinach pracy urzędu
- Dostęp do najnowszych sterowników i uaktualnień na stronie producenta komputera realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera.

Oprogramowanie biurowe	Microsoft Office PL lub równoważny, spełniający wymagania: • zawartość pakietu: arkusz kalkulacyjny, edytor tekstu, narzędzie do przygotowywania i prowadzenia prezentacji, narzędzie do zarządzania informacją prywatną (poczta elektroniczna, kalendarz, kontakty i zadania), narzędzie do tworzenia drukowanych materiałów informacyjnych • Pełna polska wersja językowa interfejsu użytkownika • Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (ActiveDirectory) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się. • W skład oprogramowania muszą wchodzić narzędzia

Projekt dofinansowany z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Warmia-Mazury 2014-2020

	programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy) • Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem. • Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa. • Oprogramowanie posiada funkcję zabezpieczenia dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

Laptopy – 3 szt

Laptop z systemem operacyjnym w wersji Professional, pełna integracja z posiadanym systemem Windows na obecnie funkcjonujących stanowiskach.
Ekran o przekątnej minimum 17,0" maksymalnie 17,3" o rozdzielczości minimum FHD 1920x1080 pikseli
Matryca z podświetlaniem LED,IPS
Procesor wielordzeniowy, osiągający w teście PassMark CPU Mark wynik min. 9450 ~~9500~~-punktów według wyników ze strony https://www.cpubenchmark.net/cpu_list.php z dnia 15-04-2018r.
Pamięć RAM Min. 16GB
Pamięć masowa: Minimum 512GB SSD
Karta graficzna osiągająca w teście Benchmark (według wyników ze strony https://www.videocardbenchmark.net/gpu_list.php) nie mniej niż 3900 pkt. na dzień 22-03-2018r.
Klawiatura qwerty
Wielokanałowa (24-bitowa) karta dźwiękowa zintegrowana z płytą główną, wbudowane głośniki stereo.
Mikrofon wbudowany.
Kamera internetowa trwale zainstalowana w obudowie matrycy.
Bateria i zasilanie
Bateria umożliwiająca pracę przez minimum 4 godzin przy normalnej pracy.
Waga i wymiary
Certyfikaty
- Deklaracja zgodności CE
Wbudowane porty i złącza minimum:
- 1x RJ-45 (10/100/1000)
- 4x USB 3.0
- 1 x Mini DisplayPort
- 1x Thunderbolt 3
- złącze słuchawkowe stereo i złącze mikrofonowe
- moduł bluetooth
Zainstalowany system operacyjny w wersji PRO.

Projekt dofinansowany z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Warmia-Mazury 2014-2020

UPS

Wymagania minimalne

UPS	Typ obudowy: rack 19"; Wysokość 3U; Architektura: line-interactive; Maks. czas przełączenia na baterię: 4 ms; Ilość gniazd wyj. z podtrzymaniem zasilania: 6 x IEC320 C13 (10A); Ilość gniazd wyj. z ochroną antyprzepięciową: 4 x IEC320 C19 (16A); Czas podtrzymania dla obciążenia 100%: 4 min; Czas podtrzymania przy obciążeniu 50%: 12 min; Zakres napięcia wejściowego w trybie podstawowym: 160-286 V; Zmienny zakres napięcia wejściowego zawierający zakres: 151-302 V; Układ automatycznej regulacji napięcia (AVR); Sinus podczas pracy na baterii; Porty komunikacji: RJ45, SmartSlot, USB; Diody sygnalizacyjne: praca z sieci zasilającej, praca z baterii, konieczna wymiana baterii, przeciążenia UPSa, stan obciążenia UPSa; Alarmy dźwiękowe: praca z baterii, znaczne wyczerpanie baterii; klamry do montażu w szafach przemysłowych rack 19"; Dołączone oprogramowanie do zarządzania; Kolor: czarny UPS z kartą zarządzającą powinien stanowić integralny system i zapewniać zarządzanie i monitorowanie pracy i stanu ups'a poprzez sieć Ethernetowi.

WICESTAROSTA
mgr Zbigniew Lichuszewski

CZŁONEK ZARZĄDU
Joanna Naszyńska

ZARZĄD POWIATU
W ELBLĄGU