SZCZEGÓŁOWA SPECYFIKACJA TECHNICZNA

Zadania: Modernizacja sieci LAN, dostawa sprzętu komputerowego, aktywnego i bezpieczeństwa realizowanego w ramach projektu: „Bezpieczna sieć szerokopasmowa Miasta Ełku”

W ramach niniejszego projektu należy wykonać, dostarczyć i wdrożyć:

I. Budowa sieci LAN
II. Modernizacja sieci LAN
III. PIAP
IV. Zapasowe Centrum Zarządzania Siecią
V. Link radiowy
VI. Sprzęt komputerowy
VII. Modernizacja centrum zarządzania siecią
VIII. Archiwum backupów
IX. Serwery, serw telekom wraz z oprogramowaniem
X. Macierz
XI. System bezpieczeństwa wiz , KD
XII. Modernizacja systemu zasilania
XIII. Modernizacja sprzętu aktywnego
XIV. Przyłącza teletechniczne
XV. Sprzęt aktywny

Dla zadania, w dalszej części dokumentu przedstawiono szczegółowe zakresy oraz określono min. wymagania techniczno-funkcjonalne dla każdego z systemów.

Wymagania ogólne dla dostarczanego sprzętu i oprogramowania (dotyczy wszystkich systemów opisanych w tym dokumencie):
- Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów z obszaru Unii Europejskiej,
- Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by nie były używane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem);
- Musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis) kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej;
- Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów. Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa);
- Wykonawca zobowiązuje się iż czas reakcji na zgłoszone awarie i usterki nie będzie dłuższy niż 12 godzin;

- Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich;
- Do każdego urządzenia musi być dostarczony komplet nośników umożliwiających odtworzenie oprogramowania zainstalowanego w urządzeniu;
- Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej, tj. dostępnym na etapie realizacji projektu, włącznie z momentem zakończenia wdrożenia urządzeń;
- Zamawiający dopuszcza realizację poszczególnych grup funkcjonalnych przez zespoły urządzeń pod następującymi warunkami:
  a) połączenie urządzeń będzie zrealizowane w sposób nie ograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu, jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność urządzenia),
  b) łączna wielkość zestawu nie będzie przekraczać wymaganej wielkości urządzenia,
  c) zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zespołu urządzeń,
  d) wszystkie elementy zestawu będą spełniały wymagania związane z zarządzaniem,
- Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ±10%, 50Hz;
- Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej.

Definicje i minimalne parametry urządzeń i oprogramowania obowiązujące w całym niniejszym dokumencie:

Komputer typ 1:

Komputer stacjonarny. Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.

Wydajność obliczeniowa:
- SYSmark® 2012 PerformanceTest ;
- SYSmark Rating – co najmniej wynik 195 punktów,
- Office Productivity – co najmniej wynik 160 punktów,
- Media Cration – co najmniej wynik 195 punktów,
- Web Development – co najmniej wynik 181 punktów,
- Data/Financial Analysis – co najmniej wynik 215 punktów,
- 3D Modeling – co najmniej wynik 240 punktów,
- System Management – co najmniej wynik 180 punktów,

Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).

Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 7240 punktów.
Pamięć operacyjna RAM 8GB (2x4096MB) DDR3 1600MHz możliwość rozbudowy do min 32GB, dwa sloty wolne.
Parametry pamięci masowej min. 500 GB SATA 7200 obr./min.

Dedykowana karta graficzna posiadająca własną pamięć RAM min.: 1GB o pełnej wysokości, posiadająca wbudowane wyjścia DVI oraz DP osiągająca w teście wydajności PassMark - G3D Mark wynik min.: 620pkt
Min 24-bitowa Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik 2W w obudowie komputera
Porty słuchawek i mikrofonu na przednim oraz na tylnym panelu obudowy.
Obudowa Typu MiniTower z obsługą kart PCI Express o pełnym profilu, wyposażona w min. 4 kieszenie: 2 szt. 5,25” zewnętrzne pełnych wymiarów i 2 szt. 3,5” wewnętrzne,
Obudowa powinna fabrycznie umożliwiać montaż min. 2 szt. dysku 3,5” lub dysków 2,5”.
Suma wymiarów obudowy nie może przekraczać 96cm i objętości 27 litrów, waga max. 11 kg,
Zasilacz o mocy max. 290W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 90% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 87% przy obciążeniu zasilacza na poziomie 100%.
Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego i 3,5” dysku twardego bez konieczności użycia narzędzi.
Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym producenta komputera.
Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) oraz kłódki (oczko w obudowie do założenia kłódki).
Obudowa musi być wyposażona w zamek szybkiego dostępu, który nie wystaje poza obrys obudowy i musi być usytuowany na bocznym panelu.
Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, a w szczególności musi sygnalizować:

- uszkodzenie lub brak pamięci RAM
- uszkodzenie złączy PCI i PCIe, płyty głównej
- uszkodzenie kontrolera Video
- uszkodzenie dysku twardego
- awarię BIOS’u
- awarię procesora

Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
Zgodność z systemami operacyjnymi i standardami.
Potwierdzenie kompatybilności komputera na daną platformę systemową
Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego.

Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System opatrzony min. o funkcjonalność :
- sprawdzenie Master Boot Record na gotowość do uruchomienia oferowanego systemu operacyjnego,
- test procesora
- test pamięci,
- test wentylatora dla procesora
- test wentylatora dodatkowego
- test napędu
- test portów USB
- test dysku twardego
- test podłączonych kabli.

Obudowa w jednostce centralnej musi posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym producenta komputera.
Zdalne zarządzanie: Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca min.:
- monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej;
- zdalną konfigurację ustawień BIOS,
- zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego;
- zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej.
- Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.
- Możliwość polegająca na kontrolowaniu urządzeń wykorzystujących magistralę komunikacyjną PCI, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych. Pod pojęciem kontroli Zamawiający rozumie funkcjonalność polegającą na blokowaniu/odblokowaniu slotów PCI.
- Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora.
- Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowy tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe.
- Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, portu równoległego, portu szeregowego z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
- Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.

- Możliwość wyłączania portów USB w tym:
- wszystkich portów USB 2.0 i 3.0,
- tylko portów USB 2.0 znajdujących się na przedzie obudowy, porty USB 3.0 na panelu przednim aktywne,
- wszystkich portów znajdującym się na panelu przednim, z zachowaniem min. 4 portów aktywnych na panelu tylnym,
- tylko tylnych portów USB 2.0, porty USB 3.0 na panelu tylnym aktywne,
- wszystkich portów znajdujących się na panelu tylnym z zachowaniem min. 2 aktywnych na panelu przednim.
- tylko dwa porty USB 2.0 aktywne na panelu tylnym, wszystkie pozostałe nieaktywne
- tylko cztery porty USB 2.0 aktywne na panelu tylnym, wszystkie pozostałe nieaktywne
- tylko porty USB 2.0 aktywne, porty USB 3.0 nieaktywne
- tylko porty USB 3.0 aktywne, porty USB 2.0 nieaktywne
Zainstalowany system operacyjny umożliwiający podłączenie i pełną integrację z posiadaną przez Zamawiającego domeną AD opartą o Windows Server 2012.
- Wbudowane porty:
min. 1 x RS232,
min. 1 x VGA,
min. 2 x PS/2,
min. 2 x DisplayPort v1.1a;
min. 10 portów USB wyprowadzonych na zewnątrz komputera w tym min 4 porty USB 3.0; min. 4 porty z przodu obudowy w tym 2 porty USB 3.0 i 6 portów na tylnim panelu w tym min 2 porty USB 3.0, wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy.
- Możliwość podłączenia dwóch pracujących równolegle dodatkowych zewnętrznych kart graficznych.
- Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE 2.1, umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem z poziomu konsoli zarządzania - niezależnie od stanu zasilania komputera - łącznie z obsługą stanu S3 (uśpienie) oraz S4-S5 (hibernacja i wyłączenie);
- Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w :
min 2 złącza PCI Express x16 Gen.3 w tym jedno elektrycznie jak PCIe x4, min. 1 złącze PCI Epress x 1,
min. 1 złącze PCI 32bit,
min. 4 złącza DIMM z obsługą do 32GB DDR3 pamięci RAM,
min. 4 złącza SATA w tym 2 szt SATA 3.0;
Zintegrowany z płytą główną kontroler RAID 0 i RAID 1
- Klawiatura USB w układzie polski programisty
- Mysz USB
Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt.
Dołączony nośnik ze sterownikami.

Monitor tego samego producenta co jednostka centralna o parametrach:
Ekran ciekłokrystaliczny z aktywną matrycą TFT 21”
Rozmiar plamki 0,248 mm

Jasność 250 cd/m2
Kontrast 1000:1, dynamiczny 2 000 000:1
Kąty widzenia (pion/poziom)178/178 stopni
Czas reakcji matrycy max. 8 ms
Rozdzielczość 1920 x 1080 przy 60Hz
Częstotliwość odświeżania poziomego 30 – 83 kHz
Częstotliwość odświeżania pionowego 56 – 76 Hz
Pochylenie monitora W zakresie 25 stopni
Wydłużenie w pionie, min. 130 mm
PIVOT
Powłoka powierzchni ekranu Antyodblaskowa
Podświetlenie System podświetlenia LED
Monitor musi być wyposażony w tzw. Kensington Slot
Złącze 1x 15-stykowe złącze D-Sub,
1x złącze DVI-D z HDCP,
1x złącze DisplayPort (v1.2)
4 x USB (HUB)
Monitor musi posiadać trwałe oznaczenie logo producenta jednostki centralnej
Odłączana stopa z VESA 100mm
Na cały powyższy zestaw komputer wraz z monitorem gwarancja 5 lat na miejscu u Zamawiającego, czas reakcji serwisu - do końca następnego dnia roboczego w przypadku monitora gwarancja zero martwych pikseli.

Komputer typ 2:

Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej o minimalnych parametrach: Wydajność obliczeniowa:
- SYSmark Rating – co najmniej wynik 148 punktów,
- Office Productivity – co najmniej wynik 140 punktów,
- Media Cration – co najmniej wynik 140 punktów,

Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 4950 punktów
Pamięć operacyjna RAM 8GB (2x4096MB) DDR3 1600MHz możliwość rozbudowy do min 32GB.
Parametry pamięci masowej min. 500 GB SATA 7200 obr./min.
Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową z wsparciem DirectX 11.1, OpenGL 4.0, OpenCL 1.2; pamięć współdzielona z pamięcią RAM, dynamicznie przydzielana do min. 1,5 GB
Min 24-bitowa Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik 2W w obudowie komputera.
Porty słuchawek i mikrofonu na przednim oraz na tylnym panelu obudowy.
Małogabarytowa typu small form factor, umożliwiająca pracę w pionie ja i w poziomie, z obsługą kart PCI Express wyłącznie o niskim profilu, fabrycznie przystosowana do pracy w układzie pionowym i poziomym wyposażona w min. 2 kieszenie: 1 szt 5,25” zewnętrzne typu „slim” i 1 szt 3,5” wewnętrzne,
Obudowa powinna fabrycznie umożliwiać montaż min 1 szt. dysku 3,5” lub 2 szt. dysków 2,5”.

Zasilacz o mocy max. 255W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 90% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 87% przy obciążeniu zasilacza na poziomie 100%,
Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego i 3,5" dysku twardego bez konieczności użycia narzędzi.
Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym producenta komputera.
Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) oraz kłódki (oczko w obudowie do założenia kłódki).
Obudowa musi być wyposażona w zamek szybkiego dostępu który nie wystaje poza obrys obudowy i musi być usytuowany na bocznym panelu.
Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, a w szczególności musi sygnalizować:
- uszkodzenie lub brak pamięci RAM
- uszkodzenie złączy PCI i PCIe, płyty głównej
- uszkodzenie kontrolera Video
- uszkodzenie dysku twardego
- awarię BIOS'u
- awarię procesora
Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji,
Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
Zgodność z systemami operacyjnymi i standardami.
Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego.
Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System opatrzony min. o funkcjonalność :
- sprawdzenie Master Boot Record na gotowość do uruchomienia oferowanego systemu operacyjnego,
- test procesora [min. cache]
- test pamięci,
- test wentylatora dla procesora
- test wentylatora dodatkowego
- test napędu
- test portów USB
- test dysku twardego
- test podłączonych kabli.
Obudowa w jednostce centralnej musi posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym producenta komputera

Wirtualizacja Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
BIOS BIOS zgodny ze specyfikacją UEFI, pełna obsługa BIOS za pomocą klawiatury i myszy.
Wbudowane porty:
min. 1 x RS232,
min. 1 x VGA,
min. 2 x PS/2,
min. 2 x DisplayPort v1.1a;
min. 10 portów USB wyprowadzonych na zewnątrz komputera w tym min 4 porty USB 3.0; min. 4 porty z przodu obudowy w tym 2 porty USB 3.0 i 6 z tyłu w tym 2 porty USB 3.0, wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy.
Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE 2.1,
Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w :
min. 1 złącze PCI Express x16 Gen 3
min. 1 złącze PCIe x4,
min. 4 złącza DIMM z obsługą do 32GB DDR3 pamięci RAM,
min. 3 złącza SATA w tym 2 szt SATA 3.0;
Zintegrowany z płytą główną kontroler RAID 0 i RAID 1;
Klawiatura USB w układzie polski programisty
Mysz USB
Nagrywarka DVD +/-RW wraz z oprogramowaniem do nagrywania i odtwarzania płyt.
Dołączony nośnik ze sterownikami.

Monitor tego samego producenta co jednostka centralna o parametrach:
Ekran ciekłokrystaliczny z aktywną matrycą TFT 21”
Rozmiar plamki 0,248 mm
Jasność 250 cd/m2
Kontrast 1000:1, dynamiczny 2 000 000:1
Kąty widzenia (pion/poziom)178/178 stopni
Czas reakcji matrycy max. 8 ms
Rozdzielczość 1920 x 1080 przy 60Hz
Częstotliwość odświeżania poziomego 30 – 83 kHz
Częstotliwość odświeżania pionowego 56 – 76 Hz
Pochylenie monitora W zakresie 25 stopni
Wydłużenie w pionie, min. 130 mm
PIVOT
Powłoka powierzchni ekranu Antyodblaskowa
Podświetlenie System podświetlenia LED
Monitor musi być wyposażony w tzw. Kensington Slot
Złącze 1x 15-stykowe złącze D-Sub,
1x złącze DVI-D z HDCP,
1x złącze DisplayPort (v1.2)

4 x USB (HUB)
Monitor musi posiadać trwałe oznaczenie logo producenta jednostki centralnej.
Odłączana stopa z VESA 100mm.
Na cały powyższy komputer wraz z monitorem gwarancja 5 lat na miejscu u Zamawiającego, czas reakcji serwisu - do końca następnego dnia roboczego w przypadku monitora gwarancja zero martwych pikseli.

Laptop Typ 1:

Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej.
Przekątna Ekrenu 15,6" o rozdzielczości: HD (1366 x 768) z podświetleniem LED.
Komputer przenośny musi osiągać w teście wydajności :
Sysmark 2014 Media Creation: min 680 pkt.
Data/Financial Analysis: min. 850 pkt.
Procesor powinien osiągać w teście wydajności PassMark Performance Test co najmniej wynik 2680 punktów Passmark CPU Mark. Wynik dostępny na stronie: http://www.passmark.com/products/pt.htm Płyta główna wyposażona przez producenta w dedykowany chipset dla oferowanego procesora. Zaprojektowana na zlecenie producenta i oznaczona trwale na etapie produkcji nazwą lub logiem producenta oferowanego komputera.
Pamięć RAM 4GB (1x4096MB) DDR3 1600MHz możliwość rozbudowy do min 8GB,
Pamięć masowa min. 500 GB SATA, 5400 RMP, z wbudowana 8GB pamiecia flash cache
Napęd optyczny Nagrywarka DVD-RW
Klawiatura z powłoką antybakteryjna z wydzieloną strefą klawiszy numerycznych, (układ US -QWERTY), min 102 klawiszy,
Multimedia dwukanałowa (24-bitowa) karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki stereo o średniej mocy 2x 2W, wbudowany wewnętrzny wzmacniacz głośników o mocy 2W,
Cyfrowy mikrofon z funkcja redukcji szumów i poprawy mowy wbudowany w obudowę matrycy.
Kamera internetowa o rozdzielczości min. 1280x720 pixels trwale zainstalowana w obudowie matrycy, dioda informująca użytkownika o aktywnej kamerze.
Czas pracy na baterii min. 320 minut.
Obudowa notebooka wzmocniona, szkielet i zawiasy notebooka wykonany z wzmacnianego metalu. Kąt otwarcia notebooka min 140 stopni.
Sprzętowe wsparcie technologii wirtualizacji procesorow, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowym tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe.
Możliwość wyłączenia/włączenia: zintegrowanej karty sieciowej, portów USB,
Możliwość włączenia/wyłączenia hasła dla dysku twardego
Porty i złącza Wbudowane porty i złącza :
- 1x 15-pin VGA
- 1x RJ-45 (10/100/1000) z LOM

- 2x USB 3.0
- 2x USB 2.0
- czytnik kart multimedialny wspierający min. karty SD 4.0
- współdzielone złącze słuchawkowe stereo i złącze mikrofonowe tzw. combo
- port zasilania
- moduł bluetooth 4.0
- touchpad z strefą przewijania w pionie, poziomie wraz z obsługą gestów
- Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN obsługująca łącznie standardy IEEE 802.11

Zainstalowany system operacyjny umożliwiający podłączenie i pełna integrację z posiadaną przez Zamawiającego domeną AD opartą o Windows Server 2012.
Warunki gwarancji: 5-letnia gwarancja producenta świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego.

Projektor:

rozdzielczość: 1280x800
technologia projekcji Laser & LED
kontraście 1400:1
jasność: 3500 ANSI lumenów
Głośność urządzenia max. 33 dB
żywotność lampy 150000 h
korekcji obrazu w pionie o +/- 30°
10-watowy głośnik
1 x HDMI type A (480p–1,080p)
Video: 1 x S-Video
2 x 3.5 mm stereo mini jack
Warunki gwarancji: 5-letnia gwarancja

Sieciowy System Operacyjny typ 1:

System musi wspierać (na umożliwiającym to sprzęcie) dodawanie pamięci RAM bez przerywania pracy.
System musi automatycznie weryfikować cyfrowe sygnatury sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu.
System musi mieć możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
System musi umożliwiać instalację i pracę na wolumenach, które:
Pozwalają na zmianę rozmiaru w czasie pracy systemu
Umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów
Umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów
Umożliwiają zdefiniowanie list kontroli dostępu (ACL)
System musi być wyposażony w mechanizmy klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

System musi umożliwiać szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
System musi umożliwiać uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
System musi umożliwiać dystrybucję ruchu sieciowego HTTP pomiędzy kilka serwerów.
System musi umożliwiać wirtualizację systemową (pozwalać na tworzenie maszyn wirtualnych z innym, zgodnym z platformą sprzętową systemem operacyjnym).
System musi umożliwiać instalację minimum 20 maszyn wirtualnych z danym systemem operacyjnym na serwerze w ramach jednej licencji.
System musi umożliwiać tworzenie rozwiązań, w których wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami.
System musi umożliwiać instalację sieciową, w której obraz systemu przesyłany jest przy pomocy transmisji Multicast.
System musi umożliwiać automatyczną aktualizację w oparciu o poprawki publikowane przez producenta.
System musi umożliwiać instalację poprawek poprzez wgranie ich do obrazu instalacyjnego.
System musi udostępniać mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
System musi umożliwiać zarządzanie przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
System musi obsługiwać protokoły:
TCP/IP
IPv6
PSec
System musi być wyposażony w:
usługi sieciowe DHCP oraz DNS wspierający DNSSEC,
usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych Windows XP i nowszych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach
usługi pozwalające na dystrybucję oprogramowania na stacje z systemami Windows XP i nowszymi, bez konieczności instalowania dodatkowego oprogramowania na stacjach
usługi pracy zdalnej pozwalające na udostępnienie całych pulpitów i/lub pojedynczych aplikacji
usługi centrum certyfikacji PKI
usługi VPN pozwalające na zestawienie minimum 500 równoczesnych połączeń i nie wymagające instalacji dodatkowego oprogramowania na komputerach przenośnych z systemem Windows XP lub nowszym
System musi umożliwiać zmianę języka interfejsu i posiadać, co najmniej polską i angielską wersję językową.
System musi być objęty polskojęzycznym, autoryzowanym przez producenta cyklem szkoleń i zestawem materiałów szkoleniowych.
System musi mieć polskojęzyczne wsparcie producenta sprzętu.
System musi być dostarczony przez producenta serwera wraz z nośnikiem instalacyjnym.
System musi posiadać licencję do instalowania i używania oprogramowania serwera.
System musi posiadać:
możliwość obsługi do 1024 maszyn wirtualnych na jednym hoście fizycznym
wsparcie dla 64 węzłów w klastrze

możliwość obsługi do 8.000 maszyn wirtualnych w klastrze
możliwości zmiany rozmiaru pliku z maszyną wirtualną na bez przerywania pracy maszyny wirtualnej
funkcjonalność kompresji pliku z maszyną wirtualną podczas migracji bez przerywania pracy maszyny wirtualnej na innego hosta

Sieciowy System operacyjny typ 2:

System musi wspierać (na umożliwiającym to sprzęcie) dodawanie pamięci RAM bez przerywania pracy.
System musi automatycznie weryfikować cyfrowe sygnatury sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu.
System musi mieć możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
System musi umożliwiać instalację i pracę na wolumenach, które:
Pozwalają na zmianę rozmiaru w czasie pracy systemu
Umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów
Umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów
Umożliwiają zdefiniowanie list kontroli dostępu (ACL)
System musi być wyposażony w mechanizmy klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
System musi umożliwiać szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
System musi umożliwiać uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
System musi umożliwiać dystrybucję ruchu sieciowego HTTP pomiędzy kilka serwerów.
System musi umożliwiać wirtualizację systemową (pozwalać na tworzenie maszyn wirtualnych z innym, zgodnym z platformą sprzętową systemem operacyjnym).
System musi umożliwiać instalację dwóch maszyn wirtualnych z danym systemem operacyjnym na serwerze w ramach jednej licencji.
System musi umożliwiać tworzenie rozwiązań, w których wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami.
System musi umożliwiać instalację sieciową, w której obraz systemu przesyłany jest przy pomocy transmisji Multicast.
System musi umożliwiać automatyczną aktualizację w oparciu o poprawki publikowane przez producenta.
System musi umożliwiać instalację poprawek poprzez wgranie ich do obrazu instalacyjnego.
System musi udostępniać mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
System musi umożliwiać zarządzanie przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
System musi obsługiwać protokoły:
TCP/IP
IPv6

PSec
System musi być wyposażony w:
usługi sieciowe DHCP oraz DNS wspierający DNSSEC,
usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych Windows XP i nowszych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach
usługi pozwalające na dystrybucję oprogramowania na stacje z systemami Windows XP i nowszymi, bez konieczności instalowania dodatkowego oprogramowania na stacjach
usługi pracy zdalnej pozwalające na udostępnienie całych pulpitów i/lub pojedynczych aplikacji
usługi centrum certyfikacji PKI
usługi VPN pozwalające na zestawienie minimum 500 równoczesnych połączeń i nie wymagające instalacji dodatkowego oprogramowania na komputerach przenośnych z systemem Windows XP lub nowszym
System musi umożliwiać zmianę języka interfejsu i posiadać, co najmniej polską i angielską wersję językową.
System musi być objęty polskojęzycznym, autoryzowanym przez producenta cyklem szkoleń i zestawem materiałów szkoleniowych.
System musi mieć polskojęzyczne wsparcie producenta sprzętu.
System musi być dostarczony przez producenta serwera wraz z nośnikiem instalacyjnym.
System musi posiadać licencję do instalowania i używania oprogramowania serwera
System musi posiadać:
możliwość obsługi do 1024 maszyn wirtualnych na jednym hoście fizycznym
wsparcie dla 64 węzłów w klastrze
możliwość obsługi do 8.000 maszyn wirtualnych w klastrze
możliwości zmiany rozmiaru pliku z maszyną wirtualną na bez przerywania pracy maszyny wirtualnej
funkcjonalność kompresji pliku z maszyną wirtualną podczas migracji bez przerywania pracy maszyny wirtualnej na innego hosta

Przełącznik sieciowy

Przełączniki sieci LAN musi charakteryzować się następującymi minimalnymi parametrami:
liczba portów 10/100/ 1000 Mbit 24 szt.
obsługiwane protokoły :
IEEE 802.3u
IEEE 802.3i
IEEE 802.3ad
IEEE 802.3ab
IEEE 802.3
IEEE 802.1w
IEEE 802.1s
IEEE 802.1Q
IEEE 802.1p
IEEE 802.1D
IEEE 802.3z
IEEE 802.3x flow control
rozmiar tablicy adresów MAC 8000
warstwa przełączania 2

możliwość instalacji w szafach 19”

Przełącznik sieciowy Typ 1

Musi być wyposażony w minimum 48 portów 10/100/1000 RJ45, 4 porty SFP oraz 1 port konsolowy.
Musi obsługiwać łączenie w jeden przełącznik wirtualny pod kątem zarządzania dowolnego typu kombinacji przełączników tej samej serii, umożliwiając podłączanie do sieci przełączników z 24 i 48 portami 10/100/1000, z portami 100Base-FX i Power-over-Ethernet, poprzez media miedziane, światłowody wielomodowe i jednomodowe.
Musi zapewniać przepustowość przełączania na poziomie minimum 100 Gbps
Musi obsługiwać pojedynczy adres IP do zarządzania wieżą.
Musi obsługiwać redundantne zarządzanie wieżą.
Musi obsługiwać opcjonalnie zapasowe źródło zasilania.
Musi obsługiwać technologię zamkniętej pętli w stosie.
Musi obsługiwać technologie IEEE 802.1D (MAC Bridges) i IEEE 802.1t (802.1D Maintenance)
Musi obsługiwać technologię IEEE 802.1s Multiple Spanning Tree.
Musi obsługiwać technologię IEEE 802.1w Rapid Reconfiguration of Spanning Tree.
Musi obsługiwać do 16,000 adresów MAC.
Musi zapewniać 8 przypisanych do użytkowników kolejek o określonych priorytetach na każdy port.
Musi obsługiwać technologię Link Aggregation (IEEE 802.3ad).
Musi obsługiwać technologie Many-to-One Port Mirroring oraz One-to-One Port Mirroring
Musi obsługiwać technologię IGMP Snooping v1, v2i v3.
Musi obsługiwać technologie Weighted Round Robin Queuing (WRR) i Strict Priority Queuing.
Musi obsługiwać jednocześnie do 4,094 ID sieci VLAN oraz do 255 dynamicznych VLAN w jednym przełączniku.
Musi mieć możliwość obsługi statycznego routingu
Musi obsługiwać sieci VLAN IEEE 802.1Q oparte na portach i tagach z pełnym wsparciem protokołów GARP i GVRP.
Musi obsługiwać uwierzytelnianie IEEE 802.1X na wszystkich portach.
Musi obsługiwać uwierzytelnianie wykorzystujące adres MAC
Musi być w pełni zarządzany przy pomocy standardowych interfejsów z wierszami poleceń (CLI), wbudowanych interfejsów webowych z SSL, technologii Telnet z SSH i dowolnej aplikacji zarządzającej SNMP oraz po http.
Musi obsługiwać następujące grupy RMON: Statistics, History, Alarms, Events.
Musi obsługiwać protokół SNMP v1/2 i v3
Musi działać w temperaturze otoczenia do 50°C
Musi posiadać gwarancję obejmującą aktualizację oprogramowania firmware i łaty naprawiające błędy oprogramowania (bug fixes), wsparcie telefoniczne oraz zaawansowaną wymianę sprzętu (wysyłka następnego dnia roboczego).
Musi być w pełni kompatybilny z posiadanym przez Zamawiającego systemem zarządznia infrastrukturą aktywną.

I. Budowa sieci LAN

Sieć LAN zostanie wykonana w trybie zaprojektuj i wybuduj w budynku Urzędu Miasta Ełku przy ulicy Marsz. J. Piłsudskiego 4

Wymagania dla okablowania i standardu wykonania sieci LAN

1. Struktura systemu okablowania.
Na system okablowania strukturalnego składają się następujące elementy:
- Główny punkt dystrybucyjny GPD
- Okablowanie poziome
Projekt infrastruktury logicznej zakłada stworzenie 60 punktów logicznych PEL na obszarze całego budynku.
Zakończenia punktów logicznych zarówno po stronie krosownicy centralnego punktu dystrybucyjnego GPD jak i punktu PEL powinny być wykonane w standardzie TIA568-B.
Główny Punkt Dystrybucyjny (GPD) umożliwia krosowanie przebiegów poziomych do portów sprzętu aktywnego. GPD zlokalizowany jest w piwnicy budynku w pomieszczeniu serwerowni.
Kable, na całej długości od gniazda logicznego do GPD, powinny być wolne od sztukowań, zagnieceń i nacięć lub złamań. Całość instalacji wykonać należy w kanałach kablowych z PCV.
Gniazda logiczne montować na wysokości i w miejscu uzgodnionym z Zamawiającym.
Każdy punkt PEL składa się z trzech gniazd 2xRJ45 oraz trzech podwójnych gniazd do zasilania sprzętu komputerowego 230V przy czym układ 2x230V musi przypadać na każdy układ 2xRJ45.
Zamawiający dopuszcza (po wcześniejszym uzyskaniu zgody Zamawiającego) możliwość podziału punktu PEL z układu 3x(2xRJ45) na układ 2x(2xRJ45) oraz 1x(2xRJ45) z koniecznością zachowania ogólnej ilości punktów.
Całość okablowania logicznego powinna zostać wykonana za pomocą nieekranowanego 4 parowego kabla UTP Cat.6 (klasa E) 4x2x23AWG LSOH
Całość okablowania elektrycznego powinna zostać wykonana przy wykorzystaniu okablowania spełniającego standardy i normy bezpieczeństwa PN-87/E-90056, PNHD 21.1.S4. Dla okablowania strukturalnego przeznaczonego na obwody zasilające stacje robocze przewidziano wykorzystanie kabla YDYżo o minimalnym przekroju 3x2,5mm w izolacji PCV przystosowanego do instalacji na jak i podtynkowych. Wykonawca dokona wszelkich niezbędnych wyliczeń i na ich podstawie dokona ostatecznego doboru parametrów podzespołów instalacji elektrycznych. Na każde stanowisko komputera przypadać będzie 1 Punkt PEL (Punkt Elektryczno-Logiczny), w skład którego wchodzą: trzy podwójne moduły RJ-45 oraz jedno podwójne gniazdo elektryczne 230V (2x2P+Z). Wykonawca zaprojektuje i wykona instalację elektryczna w taki sposób, aby można było ją zasilić z upsa oraz przyłacza agregatowego znajdującego się w GPD. Wskazane przez zamawiającego gniazda elektryczne które mają służyć do zasilania drukarek nie będą zasilane z UPS. Instalacja elektryczna musi być podzielona na minimum sekcje kondygnacyjne z możliwością swobodnego ich załączania.
Wykonawca na każdym piętrze wykona wyprowadzenia kablem UTP pod punkty bezpieczeństwa oraz bezprzewodowe w ilości po 8 szt. na piętro.
Okablowanie Wykonawca podda procesowi certyfikacyjnemu, który zakończy się udzieleniem przedłużonej gwarancji.
Wykonawca dostarczy cztery przełączniki sieciowe.

Wykonawca w ramach zadania przeniesie Kondygnacyjny Punktu Dystrybucyjnego (KPD) sieci zlokalizowanego na parterze budynku w pomieszczeniu działu informatyki do pomieszczenia GPD zlokalizowanego w serwerowni zlokalizowanej w piwnicy w odległości ok. 30 m. Wykonawca wykona przeniesienia KPD z zachowaniem wszystkich obowiązujących norm, wiedzy technicznej oraz dobrych praktyk stosowanych przy tego typu zadaniu.
Wykonawca dostarczy i zamontuje klimatyzator o wydajności 5 kW złożony z jednostki wewnętrznej i zewnętrznej oraz dokona przeniesienia obecnie zainstalowanego w pomieszczeniu KPD klimatyzatora.
Wykonawca dokona adaptacji pomieszczenia po KPD o wymiarach 201 cm x 350 cm polegającej na, wyrównaniu ścian, podłogi i położeniu wykładziny antystatycznej.
Wykonawca dostarczy szafę na nośniki danych o wymiarach: wysokość: 1900, szerokość: 1000, głębokość: 400, pojemność dm3: 800 i minimalnych wymaganiach:
- Korpus wykonany z blachy 1,0 mm, płaszcz zewnętrzny drzwi z blachy stalowej grubości 0,8 mm.
- Szafa wyposażona w rygle pionowe i poziome (po 2 sztuki),
- Korpus i drzwi wykonane z blachy stalowej o grubości 0,8 mm, nadającej odpowiednią sztywność oraz zabezpieczonej przed korozją.
- Wyposażone w zamek
- 4 półki

Stół techniczny serwisowy o minimalnych wymiarach 2000 mm x 750 mm wraz z nadbudową na całej jego długości złożoną z blachy otwornicowej na wysokości minimum 500 mm a następnie na całej długości z minimum 2 półek.

II. Modernizacja sieci LAN

Wykonawca w ramach niniejszego zadania zmodernizuje dwie sieci LAN w poniższym zakresie:

1. Modernizacja sieci LAN w budynku UM Ełku przy ulicy Piłsudskiego 2. Do zadań wykonawcy należy:
   wykonanie przeniesienia Głównego Punktu Dystrybucyjnego (GPD) sieci zlokalizowanego w piwnicy budynku do pomieszczenia serwerowni zlokalizowanej w tej samej piwnicy w odległości ok. 30 m. Wykonawca wykona przeniesienia GPD z zachowaniem wszystkich obowiązujących norm, wiedzy technicznej oraz dobrych praktyk stosowanych przy tego typu zadaniu.
   Wykonanie 10 punktów logicznych PEL wykonanych zgodnie z opisem technicznym w punkcie I SST.
   Wykonanie wyprowadzeń pod 4 punkty Wifi.

2. Modernizacja sieci LAN w budynku UM Ełku przy ulicy Piłsudskiego 6. Do zadań wykonawcy należy:
   Wykonanie 10 punktów logicznych PEL wykonanych zgodnie z opisem technicznym w punkcie I SST.
   Wykonanie wyprowadzeń pod 4 punkty Wifi

W ramach modernizacji sieci Wykonawca dostarczy i wdroży dwa przełączniki Typu I oraz 8 punktów bezprzewodowych, które muszą spełniać następujące wymagania minimalne:
Punkty dostępowe muszą obsługiwać równolegle dwa pasma częstotliwości: 802.11ac/a/n (5 GHz) i 802.11b/g/n (2.4 GHz).
Musi posiadać 1 port 10/100/1000 Base-T RJ-45 z technologią autosensing
Punkt dostępowy musi obsługiwać następujące funkcjonalności:
- Zgodność z DFS2 (Dynamic Frequency Selection) by dopuścić dodatkowe kanały w paśmie 5 GHz,
- Punkty dostępowe muszą obsługiwać IP QoS w środowisku przewodowym i bezprzewodowym. Rozróżnianie pakietów musi być realizowane dla przychodzących i wychodzących pakietów z sieci bezprzewodowej, w oparciu o DiffServ, IP ToS oraz IP Precedence,
- Obsługa protokołu 802.11e, w tym WMM oraz U-APSD,
- Szybki i bezpieczny roaming oraz handover (wstępne uwierzytelnienie, OKC),
- Obsługa minimum 12 SSID (6 na częstotliwość radiową),
- Obsługa minimum 254 użytkowników jednocześnie,
- RADIUS Authentication & Accounting,
- Płynny roaming pomiędzy podsieciami IP,
- Płynny roaming pomiędzy wieloma kontrolerami,
- Wsparcie dla protokołu IEEE 802.1p prioritization,
- Możliwość wykonania minimum 12 jednoczesnych połączeń VoIP w ramach protokołu IEEE 802.11 a/b/g/n,
- Wsparcie dla protokołu: IEEE 802.1X z wykorzystaniem metod: EAP-SIM, EAPFAST, EAP-TLS, EAP-TTLS, and PEAP,
- Wsparcie dla protokołu: MAC address authentication przy wykorzystaniu lokalnych access-list lub przesyłanych z serwera RADIUS,
- Mechanizmy: RADIUS AAA, przy wykorzystaniu EAP-MD5, PAP, CHAP oraz MS-CHAPv2,
- RADIUS Client,
- Mechanizm izolacji klientów na poziomie L2,
- Mechanizmy IEEE 802.11i, WPA2 oraz WPA, przy zastosowaniu algorytmów szyfracji: Advanced Encryption Standard (AES) oraz Temporal Key Integrity Protocol (TKIP),
- Obsługa technologii 802.11ac pracując w konfiguracji 2x2 MIMO
- Musi mieć możliwość zapewnienia równego czasu antenowego (Airtime) dla wszystkich klientów w środowiskach, w których wspólnie występują technologie 802.11a/b/g, 802.11n oraz 802.11ac.
Min. 4 anteny wewnętrzne.
Tryb działania radia WLAN: Client access, Local mesh, Packet capture, WDS,
Możliwość pracy punktu dostępowego bez kontrolera WLAN na wypadek awarii łącza,
Obsługa technologii 802.11ac i praca w technice transmisji wieloantenowej MIMO 2x2 przy zasilaniu przez jedno źródło zgodne ze standardem IEEE 802.3af, bez wpływu na działanie kluczowych funkcji i wydajność,
Wsparcie dla mechanizmu minimum „Three spatial stream MIMO” dla wszystkich nadajników,

WDS (Wireless Distribution System) z możliwością tworzenia łączy typu backhaul na dowolnym łączu radiowym lub wykorzystania jednego łącza radiowego zarówno na potrzeby backhaul, jak i świadczenia usług klientom,
Jednoczesna obsługa ruchu tunelowanego i mostowanego,
Wszystkie punkty dostępowe muszą mieć możliwość pracy w formie sensorów sieci – pracujących w pełnym lub niepełnym wymiarze czasu.
W przypadku awarii punktu dostępowego, sąsiednie punkty dostępowe muszą rozszerzyć swój zasięg by wyeliminować niepokryte obszary, nawet w sytuacji, gdy punkt dostępowy nie może uzyskać dostępu do kontrolera. Wybór optymalnego kanału musi także być rekonfigurowany dynamicznie i bez interwencji użytkownika.
Punkt dostępowy musi zapewniać rozproszone zarządzanie łącznością radiową RF (Radio Frequency) Management niezależne od kontrolera - poza tylko wstępną konfiguracją. Po utracie połączenia z kontrolerem, punkt dostępowy musi być zdolny do zapewnienia ciągłości operacji związanych z szyfrowaniem, tworzeniem czarnych list, filtrowaniem, QoS oraz zarządzaniem łącznością radiową, zarówno dla swoich potrzeb, jak i lokalnie mostowanego ruchu.
Zarządzanie łącznością radiową RF Management musi dostosowywać się do nowych kanałów w oparciu o wartości stosunku sygnału do szumu (SNR) i zajętości kanału, które mogą być ustalane przez użytkownika.
Możliwość konfiguracji zapewniającej równoważenie obciążenia i sterowanie pasmem w celu pozwolenia punktom dostępowym na równoważenie/sterowanie ruchem klientów pomiędzy obiema częstotliwościami na jednym punkcie dostępowym i/lub pomiędzy wieloma punktami dostępowymi w ramach domeny łączności radiowej,
Punkty dostępowe muszą mieć możliwość wdrożenia w konfiguracji kratowej, tworzącej bezprzewodowe, wzajemne połączenia pomiędzy poszczególnymi punktami dostępowymi,
Możliwość stworzenia i jednoczesnego uruchomienia minimum 16 profili sieci bezprzewodowych WLAN,
Każdy profil wirtualny sieci bezprzewodowej powinien posiadać możliwość przypisania do sieci VLAN,
Połączenie pomiędzy AP, a kontrolerem musi być szyfrowane przy pomocy technologii AES minimum 128 bit,
Punkty dostępowe muszą obsługiwać suplikanta 802.1x, by chronić swoje połączenia przewodowe przed nieautoryzowanym dostępem innych urządzeń,
Obsługa standardów uwierzytelniania i szyfrowania, w tym: WEP, WPA (TKIP), WPA2 (AES), 802.11i, 802.1x,
Punkt dostępowy musi wspierać szyfrowanie, tworzenie czarnych list, filtrowanie oraz QoS, niezależnie od kontrolera,
Możliwość pracy w architekturze bezpieczeństwa opartej na rolach, zapewniając ciągłe zarządzanie tożsamością wraz z opartymi na rolach funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma, aplikowane względem użytkownika i aplikacji,
Funkcje egzekwowania przypisanych ról i ograniczania przepustowości muszą być osiągalne na poziomie punktu dostępowego,
Przypisywanie ról klientom musi odbywać się bez konieczności segmentacji przez dedykowane SSID.
Oprogramowanie działające na punktach dostępowych powinno umożliwiać oddzielną specyfikację częstotliwości dla każdego z modułów radia,

Wykonawca uruchomi zapasowy kontroler sieci o parametrach:

System zarządzania siecią		
Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Funkcjonalność	• Musi zapewniać narzędzie do zarządzania na poziomie systemowym - umożliwiające implementacje dowolnej funkcjonalności wynikającej z karty katalogowej zarządzanego urządzenia • Musi umożliwiać centralne wykonywanie operacji systemowych, takich jak wykrywanie urządzeń, zarządzanie zdarzeniami, rejestrowanie zdarzeń i utrzymanie aplikacji • Musi zapewnić narzędzie umożliwiające szybkie i łatwe określenie fizycznej lokalizacji systemów i użytkowników końcowych oraz miejsca ich podłączenia do sieci • Musi zapewniać możliwości monitorowania całego systemu i wdrażania w nim konfiguracji VLAN • Musi zapewniać kompleksowe wsparcie zdalnego zarządzania dla wszystkich proponowanych urządzeń sieciowych, jak również wszystkich urządzeń zarządzanych przez SNMP MIB-I oraz MIB-II • Do obsługi zdalnej nie może wymagać stosowania żadnych klientów użytkowników końcowych lub oprogramowania typu agent • Musi umożliwiać śledzenie atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania *firmware*, typ CPU i pamięć
2.	Architektura	• Musi zapewniać scentralizowane zarządzanie wszystkimi urządzeniami sieci przewodowej. • Musi zawierać zintegrowane aplikacje typu *plug-in*, separujące poszczególne komponenty i uzupełniające możliwości systemu zarządzania. • Musi mieć możliwość instalacji, jako maszyna wirtualna • Musi obsługiwać możliwość automatycznego egzekwowania raz zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej • Rozwiązanie musi integrować się ze środowiskiem wirtualnym VMware ESX i ESXi

3.	Raportowanie	• Musi zapewniać możliwości modyfikacji, filtrowania i tworzenia własnych, elastycznych widoków sieci • Musi umożliwiać prezentowanie danych w formie wykresów lub tabelarycznej i pozwalać użytkownikowi na wybór wielu unikatowych identyfikatorów obiektów (*OID*) • Musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń) • Musi mieć możliwość generowania szczegółowego wykazu produktów zainstalowanych w sieci, zorganizowany według typu urządzenia • Musi rejestrować dane historyczne o atrybutach urządzenia i raportować jakiekolwiek zmiany w urządzeniu • Musi zapewniać dane historyczne o zmianach w konfiguracji i oprogramowaniu *firmware* urządzenia • Musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania, spisem urządzeń • Musi umożliwiać generowanie szczegółowych raportów dla potrzeb związanych z planowaniem spisu urządzeń sieciowych • Musi zapewniać możliwości analiz na poziomie portu • Musi oferować możliwość tworzenia własnych, dostosowanych do potrzeb raportów przez tworzenie indywidualnych szablonów • Możliwość raportowania do elementu zarządzającego maszynami wirtualnymi (vSphere oraz XenCenter), informacji o rzeczywistym położeniu maszyny wirtualnej w sieci- fizyczny port i przełącznik
4.	Narzędzia administracyjne	• Musi pozwalać użytkownikowi na generowanie w tle zaplanowanych zdarzeń i zadań oraz planowanie terminu ich wykonania • Musi zapewnić narzędzie do podglądu i wyboru obiektów MIB *(Management Information Base)* z reprezentacji opartej na drzewie, oraz zawierać kompilator dla nowych lub pochodzących od innych dostawców MIB • Musi pozwalać administratorom IT na desygnowanie wybranego personelu do aktywowania/dezaktywowania wcześniej skonfigurowanych polityk w razie potrzeby • Musi umożliwiać prezentowanie szczegółowych informacji konfiguracyjnych, w tym datę i godzinę zapisów konfiguracji, wersję oprogramowania *firmware* i wielkość pliku konfiguracyjnego • Musi posiadać możliwość pobierania oprogramowania *firmware* do jednego urządzenia lub do wielu urządzeń jednocześnie • Musi mieć możliwość pobierania obrazów *boot PROM* do jednego urządzenia lub do wielu urządzeń jednocześnie • Musi posiadać zdolność do przeprowadzania zaplanowanych, rutynowych kopii zapasowych konfiguracji urządzeń • Musi mieć możliwość pobierania szablonów konfiguracyjnych w formacie tekstowym (ASCII) do jednego lub większej liczby urządzeń • Musi zapewniać interfejs sieci Web zawierający narzędzia do raportowania, monitorowania, rozwiązywania problemów i panele zarządzania • Musi zapewniać oparte o sieć Web elastyczne widoki, widoki urządzeń oraz dzienniki zdarzeń dla całej infrastruktury • Musi umożliwiać diagnozowanie problemów sieciowych i wydajności poprzez analizy danych NetFlow w czasie rzeczywistym

5.	Bezpieczeństwo	• Musi obsługiwać uwierzytelnianie RADIUS i LDAP dla użytkowników aplikacji • Musi obsługiwać bezpieczne zarządzanie przełącznikiem przez https. Musi mieć możliwość definiowania polityk: o ograniczających poziom pasma, o ograniczających liczbę nowych połączeń sieciowych, o ustalających pierwszeństwo ruchu w oparciu o mechanizmy QoS warstw 2 i 3, o nadających tagi pakietom, poddających kwarantannie poszczególne porty lub sieci VLAN i/lub uruchamiających wcześniej zdefiniowane działania • Musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej aplikacji, poprzez wykonanie jednej czynności, dzięki której polityki zostaną rozesłane do wszystkich urządzeń • Musi funkcjonować automatycznie gwarantując, że odpowiednie usługi są dostępne dla każdego użytkownika. Niezależnie od miejsca jego logowania do sieci • Musi współpracować z istniejącymi w danej sieci metodami uwierzytelniania, w szczególności z musi obsługiwać uwierzytelnianie oparte o 802.1X, Radius oraz MAC • Musi mieć możliwość natychmiastowego blokowania lub dopuszczania różnych aktywności sieciowych, w tym dostępu do sieci Web, poczty elektronicznej lub wymiany plików p2p • Musi zapewniać dynamiczne, konfigurowalne rozwiązanie powstrzymywania zagrożeń z szeroką gamą opcji reagowania, rejestrowania i audytowania • Musi natychmiastowo identyfikować fizyczną lokalizację i profil użytkownika źródła ataku • Musi mieć możliwość podejmowania działań w oparciu o wcześniej określone polityki bezpieczeństwa, włączając w to zdolność do powiadamiania systemu IDS o podjętych działaniach poprzez komunikat SNMPv3 *Trap* (*Inform*) • Musi umożliwiać automatyczne odłączanie lub izolowanie źródła nielegalnego lub nieodpowiedniego ruchu zidentyfikowanego przez system IDS

III. PIAPY

Wykonawca dostarczy, skonfiguruje i uruchomi 2 szt. PIAP'ów o minimalnych wymaganiach techniczno-funkcjonalnych:

PIAPy należy wykonać - dwa PIAPy w następujących lokalizacjach:
1. Szkoła Podstawowa nr 5, ul. Św. M.M. Kolbego 11 pomieszczenie numer 33
2. Zespół Szkół Samorządowych, ul. Suwalska 15 pomieszczenie numer 209

Na wyposażenie każdego pojedynczego PIAP składają się:
a) Komputer wraz z klawiaturą, myszą, monitorem i oprogramowaniem (15 kompletów)
b) Urządzenie drukujące (1 szt.)
c) Zestaw biurko i krzesło (15 kompletów)
d) Switch, System projekcyjny, system kontroli i bezpieczeństwa

e) Adaptacja pomieszczenia

f) Laptop typ 1 (1 szt.)

Minimalne wymagania techniczno-funkcjonalne dla elementów wyposażenia PIAP:

a. Komputer wraz z klawiaturą, myszą, monitorem i oprogramowaniem:

Komputer typu 2

b. Urządzenie drukujące:

Opis	**Wymagania minimalne**
Typu urządzenia	druk/kopiowanie/skanowanie/faksowanie
Rodzaj/technologia wydruku	druk laserowy monochromatyczny
Prędkość druku (czerń, normalna jakość, A4)	min. 31 (stron /minutę)
Czas wydruku pierwszej strony (format A4)	Max 6,5 sekundy
Jakość druku (czerń, najwyższa jakość)	1200 x 1200 dpi
Język drukarki (emulacje)	PCL 6, Postscript level 3
Interfejs	2 porty USB (1x Hi-Speed USB 2.0 Host type A, 1x Hi-Speed USB2.0 typ B), Ethernet 10/100/1000BaseTX
Procesor	600 MHz
Pamięć / możliwość rozbudowy do:	min. 256 MB / min. 768 MB
Podajniki papieru	Podajnik nr 1 - uniwersalny podajnik na min. 50 arkuszy o gramaturze 80 g/m2, obsługa od min. 60 do 220 g/m2, podajnik nr 2 - podajnik na min. 250 arkuszy obsługujący nośniki o gramaturze od min. 60 do 163 g/m2,
Rozmiar nośników	A4, A5, B5, Letter, Legal
Wydajność /dopuszczalne obciążenie	50 000 (stron /miesiąc)
Średnie obciążenie miesięczne	4 000 stron
Druk dwustronny	automatyczny
Podajnik dokumentów	tak, na 50 ark. 80 g/m2, umożliwiający automatyczne dwustronne kopiowanie/skanowanie
Miejsce docelowe skanowania	SMB, FTP, USB, e-mail
Optyczna rozdzielczość skanowania	1200 x 1200 dpi
Pamięć faksu	Min. 6 MB
Obsługiwane systemy operacyjne	min. Microsoft Windows 2000, Microsoft Windows XP Professional, Microsoft Windows 7, Server 2003

Materiały eksploatacyjne	Toner zintegrowany z bębnem, wydajność materiałów dostarczonych wraz z urządzeniem min. 2 tys. stron A4 (ISO 19752)
Druk ekonomiczny	druk ekonomiczny (oszczędność tonera), druk dwustronny oraz druk kilku zmniejszonych stron na jednym arkuszu (oszczędność papieru)
Gwarancja	Min. 24 miesięcy, door- to door

Wykonawca skonfiguruje drukarkę do pracy w sieci w zakresie druku i skanowania przez każdy z komputerów w PIAP. Wykonawca dodatkowo dostarczy jedno biurko opisane w punkcie c. na którym umieści urządzenie drukujące.

c. Zestaw biurko i krzesło

Biurko:

Biurko wykonane z płyty wiórowej o grubości min. 18mm, oklejonej taśmą PCV/ABS o grubości min. 2 mm w kolorze blatu. Obrzeża zaokrąglone oklejone – o promieniu min. 2mm. Wymiary biurka: szerokość min. 820, głębokość min 500mm, wysokość min. 750mm. Wysuwana półka na prowadnicach rolkowych służąca do przechowywania i korzystania z klawiatury i myszy.
Materiały, z których wykonane jest biurko powinny posiadać atesty higieniczne opuszczające od stosowania na terenie Polski.

Krzesło:

Krzesło obrotowe, odznaczające się dużą wytrzymałością
podstawa pięcioramienna
- oparcie i siedzisko miękkie
- regulacja wysokości (góra-dół)
- regulowany kąt nachylenia oparcia z blokadą w dowolnej pozycji
- regulacja odległości siedziska od oparcia krzesła

d. Switch, System projekcyjny, system kontroli i bezpieczeństwa

Wykonawca do każdego PIAP'a dostarczy i zainstaluje przełącznik sieciowy Typu 1, laptopa Typ 1 system projekcyjny złożony z projektora wraz z ekranem elektrycznym, Wykonawca projektor zamocuje za pomocą uchwytu sufitowego o konstrukcji metalowej z możliwością teleskopowej regulacji odległości projektora od sufitu, możliwością prowadzenia kabli sygnałowych wewnątrz uchwytu. Wykonawca wszystkie kable sygnałowe VGA, HDMI, Audio i USB od projektora zakończy w gnieździe sygnałowym, które umieści w okolicach biurka na którym zainstaluje dostarczonego laptopa, Wykonawca dostarczy wszystkie niezbędne elementy w tym w szczególności okablowanie, Wykonawca dostarczy i zamontuje ekran o parametrach umożliwiających odtwarzanie obrazu w formacie zgodnym z

dostarczonym projektorem i o minimalnej wielkości 250 cm x 160 cm. Wykonawca dostarczy, i podłączy do SZBME kamerę IP o rozdzielczości minimum 2,0 MP i szybkości 25 kl/s.

e. Adaptacja pomieszczenia

W ramach adaptacji Wykonawca dostarczy i zamontuje w pomieszczeniu PIAP drzwi wewnętrzne antywłamaniowe zgodne z obowiązującymi normami, na oknach zamontuje rolety kasetonowe (PIAP Szkoła Podstawowa nr 5 – 3 okna o wymiarach 195 cm x 170 cm każde, Zespół Szkół Samorządowych – 4 okna o wymiarach 244 cm x 210 cm każde) umożliwiające skuteczne zaciemnienie zarówno całego PIAP jak i poszczególnych elementów okien.
Wykonawca kolorystykę drzwi i rolet uzgodni z Zamawiającym.
Poprzez adaptację pomieszczenia Zamawiający rozumie dodatkowo wykonanie prac adaptacyjnych polegających na montażu uchwytów do instalacji projektora i ekranu, wykonaniu kanału kablowego ułożeniu kabla, a następnie usunięciu ubytków ściennych wraz z pomalowaniem, wykonaniu zabezpieczenia elektrycznego obwodu do którego będą podłączane urządzenia komputerowe.

Do obsługi PIAP Wykonawca wykona sieć LAN.
Całość okablowania logicznego powinna zostać wykonana za pomocą nie ekranowanego 4 parowego kabla UTP Cat.6 (klasa E) 4x2x23AWG LSOH.
Podwójne gniazda logiczne i elektryczne montować na wysokości uzgodnionej z Zamawiającym.
W pomieszczeniu wytypowanym pod lokalizację PIAP-u dodatkowo należy wykonać instalację zasilającą 230V, dla każdego stanowiska z osobna.
Dla okablowania strukturalnego przeznaczonego na obwody zasilające stacje robocze przewidziano wykorzystanie kabla YDYżo o minimalnym przekroju 3x2,5mm w izolacji PCV przystosowanego do instalacji na jak i podtynkowych. Na podstawie planowanych przez Wykonawcę do instalacji urządzeń (Komputer + monitor, tablica multimedialna, urządzenie wielofunkcyjne) Wykonawca dokona wszelkich niezbędnych wyliczeń i na ich podstawie dokona ostatecznego doboru parametrów podzespołów instalacji elektrycznych.
Na każde stanowisko komputera przypadać będzie 1 Punkt PEL (Punkt Elektryczno-Logiczny), w skład którego wchodzą: jeden podwójny moduł RJ-45 oraz jedno podwójne gniazdo elektryczne 230V (2x2P+Z). Łącznie należy wybudować w sali komputerowej 17 punktów PEL.
Do każdego PEL powinno się doprowadzić jedną linie okablowania strukturalnego w skład której wchodzą dwie linie okablowania logicznego oraz linia elektryczna.
Okablowanie logiczne należy prowadzić z punktu GPD.
Zamawiający informuje iż GPD w Szkoła Podstawowa nr 5 ul. Św. M.M. Kolbego 11 znajduje w odległości ok. 50 m w stosunku do pomieszczenia PIAP, a w Zespole Szkół Samorządowych ul. Suwalska 15 w pomieszczeniu przylegającym.

Wykonawca dostarczy wszystkie, wymagane zastosowaną technologią, typy licencji gwarantujące poprawne uruchomienie usług domenowych w oparciu o serwerowy system operacyjny.

Uwaga: Liczby tych licencji muszą umożliwiać uruchomienie wszystkich użytkowników usług domenowych jednocześnie.

Oprogramowanie antywirusowe:

Wykonawca dostarczy zainstaluje i skonfiguruje oprogramowanie antywirusowe na wszystkich dostarczonych komputerach i zainstalowanych serwerowych systemach operacyjnych z subskrypcją na okres min. 60 miesięcy Wykonawca zainstaluje i skonfiguruje konsolę umożliwiającą centralne zarządzanie oprogramowaniem antywirusowym.

Wykonawca jest zobowiązany dostarczyć i wdrożyć system antywirusowy dla wszystkich stacji roboczych i serwerów objętych projektem, o następujących wymaganiach minimalnych:

System musi wspierać min. następujące systemy operacyjne	Windows XP SP2 lub nowszy Windows Vista 32 i 64bit Windows 7 32 i 64bit Windows 8 32 I 64bit Windows Server 2003 SP2 lub nowszy Windows Server 2008 32 i 64bit Windows Server 2008 R2 32 i 64bit Windows SBS Server 2011 32 i 64bit Windows Server 2012
System musi wspierać min. następujące aplikacje	MS SharePoint Services 2.0/3.0 MS SharePoint Server 2003/2007/2010 MS Exchange 2003/2007/2010 (tylko Internet Security Business)
System musi realizować ochronę przed zagrożeniami wspierając następujące minimalne funkcjonalności:	- ochrona przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem (w tym Java i ActiveX); - wykrywanie oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich; - skanowanie skryptów napisanych w językach VB Script i Java Script wykonywane przez system operacyjny Windows; - wykrywanie rootkitów - moduł oceny wyników wyszukiwania w głównych wyszukiwarkach w czasie rzeczywistym - monitorowanie adresów URL w czasie rzeczywistym - funkcja inteligentnego skanowania automatycznie przełączająca tryb skanowania w wyższy lub niższy priorytet odpowiednio do wykorzystania zasobów przez użytkownika - ochrona przed phishingiem; - ochrona przed dialerami; - możliwość zdefiniowania portów, które będą monitorowane lub wykluczone z monitorowania przez moduły skanujące ruch sieciowy (z wyłączeniem zapory ogniowej); - monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera działający nieprzerwanie do momentu zamknięcia systemu operacyjnego; - dedykowany moduł ochrony tożsamości, który posiada własną, wyspecjalizowaną bazę sygnatur do wykrywania keyloggerów - moduł ochrony tożsamości powinien dodatkowo oferować funkcjonalność

	monitorowania zachowań podejrzanych aplikacji i blokować próby przejęcia danych logowania użytkownika
Skanowanie w czasie rzeczywistym	- uruchamianych, otwieranych, kopiowanych, przenoszonych lub tworzonych plików; - pobieranej z Internetu poczty elektronicznej (wraz z załącznikami) po protokołach POP3, SMTP, IMAP (także szyfrowanych z wykorzystaniem SSL/TLS) - możliwość zmiany nazwy lub usuwania określonych typów załączników; - Opcja modyfikowania tematu wiadomości jeśli zostanie w niej wykryty wirus.
Wyszukiwanie heurystyczne	- wyszukiwanie heurystyczne bazujące na analizie kodu potencjalnego wirusa;
Archiwa	- leczenie i usuwanie plików z archiwów następujących formatów: ZIP, RAR, 7z, CAB; - skanowanie archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia;
Działanie programu po wykryciu infekcji	- podejmować zalecane działanie - próbować leczyć, a jeżeli nie jest to możliwe pytać użytkownika o działanie; - rejestrować w pliku raportu informację o wykryciu wirusa; - powiadamiać administratora przy użyciu poczty elektronicznej; - poddać kwarantannie podejrzany obiekt;
Zapora ogniowa (firewall)	- możliwość ustawienia predefiniowanych poziomów ochrony, w tym poziomu zapewniającego interakcję z użytkownikiem po wykryciu nowego połączenia (tryb uczenia zapory) oraz trybu automatycznego; - możliwość ręcznego tworzenia i modyfikacji reguł dostępu dla zainstalowanych aplikacji; - zdefiniowania reguł zezwalających na komunikację na określonym porcie niezależnie od reguł dla aplikacji; - zdefiniowania zaufanych podsieci, dla których nie będą stosowane żadne reguły zapory(sieci zaufane); - ochrony przed atakami sieciowymi; - oferować białą i czarną listę adresów IP dla których nie będą stosowane reguły, a ruch dla tych adresów będzie w całości dozwolony lub blokowany.
Płyta ratunkowa	- możliwość utworzenia płyty ratunkowej lub nośnika USB lub płyty CD w oparciu o obraz w formacie ISO pobierany z serwerów producenta, umożliwiającego przeskanowanie dysków komputera bez uruchamiania systemu zainstalowanego na dysku; - płyta ratunkowa musi posiadać opcję aktualizacji sygnatur z Internetu, dysku lokalnego oraz innego nośnika np. usb. - płyta ratunkowa powinna oferować możliwość zarządzania kwarantanną utworzoną przez program na komputerze i pozwalać na przywracanie obiektów, które są niezbędne do poprawnego uruchomienia systemu - nośnik powinien zawierać również dodatkowe narzędzia naprawcze jak na przykład edytor rejestru
Wykorzystywanie zasobów systemowych	- możliwość dynamicznej zmiany użycia zasobów systemowych w zależności od obciążenia systemu przez aplikacje użytkownika;
Język	- polski, również dla konsoli zdalnej administracji; - dodatkowo powinien być instalowany również język angielski niezależnie od

	języka wybranego podczas instalacji; - możliwość łatwego przełączania interfejsu pomiędzy zainstalowanymi wersjami językowymi
Harmonogram	- umożliwiający modyfikowanie oraz tworzenie zadań aktualizacji komponentów programu, - sygnatur, - skanowania cyklicznego, Każde z tych zadań musi posiadać własne zadanie harmonogramu.
Blokowanie ustawień programu	- blokowanie dostępu do ustawień programu dla użytkowników w tym: zatrzymywania skanowania, wyłączania ochrony, dostępu do przywracania bądź usuwania obiektów z kwarantanny, przerywania aktualizacji; - możliwość całkowitego zablokowania dostępu do ustawień zaawansowanych lub interfejsu programu;
Wysyłanie podejrzanych obiektów	- możliwość wysyłania podejrzanych obiektów do producenta oprogramowania w celu przeprowadzenia analizy;
Informowanie użytkownika	- program powinien umożliwić administratorowi wyłączenie niektórych lub wszystkich powiadomień wyświetlanych na stacjach roboczych; - możliwość wyłączenia powiadomień o stanie składnika;
Aktualizacja	- antywirusowe bazy danych na serwerach producenta aktualizowane nie rzadziej niż raz na cztery godziny; - pobieranie uaktualnień w trybie przyrostowym;
Zdalne zarządzanie	- program (poprzez funkcjonalność w niego wbudowaną lub z wykorzystaniem dodatkowego modułu/ aplikacji) powinien umożliwiać zdalne zarządzanie oprogramowaniem i jego funkcjami. - przechowywać ustawienia w relacyjnej bazie danych MS SQL Server 2005/2008 również wersje Express, MySQL 5, Oracle 10/11, Firebird 2.0/2.5 - umożliwiać automatyczne i regularne tworzenie kopii zapasowej serwera zarządzającego, która umożliwi przywrócenie w pełni działającego systemu zarządzania; - powinien dostarczać własny silnik bazodanowy - umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych odpowiadających strukturze sieci (grupy robocze sieci Microsoft Windows i/lub struktura Active Directory) również w oparciu o zdefiniowane reguły; - umożliwiać tworzenie hierarchicznej struktury serwerów administracyjnych; - umożliwiać zarządzanie komputerami położonymi w różnych podsieciach; - umożliwiać zdalne zarządzanie o obiektami poddanymi kwarantannie oraz podejmowanie odpowiednich działań (np. przywracanie, usuwanie itp.); - umożliwiać przeglądanie informacji o obiektach, które zostały wykryte ale program nie podjął względem nich żadnego działania wraz z możliwością wymuszenia przez administratora odpowiedniego działania; - konsola administracyjna posiada możliwość zdalnego inicjowania skanowania antywirusowego na stacjach roboczych włączonych do sieci komputerowych w całej firmie (wszystkich podsieciach); - Konsola zdalnej administracji musi oferować możliwość zdalnego zarządzania konfiguracją komputerów, grup komputerów oraz całej sieci - musi ofertować funkcjonalność raportowania i powiadamiania mailem oraz generowania raportów i statystyk z pracy systemu antywirusowego na stacjach

	roboczych - raporty te powinny być dostarczane mailem zgodnie ze zdefiniowanym ręcznie harmonogramem - musi oferować opcję zdalnego restartowania i zamykania komputera na którym zainstalowany jest program - umożliwiać automatyczne aktualizacje licencji na stacjach roboczych; - system centralnej dystrybucji i instalacji aktualizacji oprogramowania, umożliwiający automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowego oprogramowania; - system centralnej dystrybucji i instalacji aktualizacji bibliotek sygnatur wirusów, umożliwiający automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowej wersji biblioteki - system administracji zdalnej nie może wymagać do działania żadnego serwera www (Apache, IIS itp.) - posiadający mechanizmy raportowania i dystrybucji oprogramowania oraz polityk antywirusowych w sieciach korporacyjnych;
Wsparcie	- w całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej, realizowanej w języku polskim; - pomoc techniczna telefonicznie, mailowo oraz w razie potrzeby z użyciem połączeń zdalnych
Licencjonowanie	- w całym okresie trwania subskrypcji użytkownik ma możliwość pobierania i instalacji nowszych wersji oprogramowania i konsoli zarządzającej; - w razie konieczności producent ma obowiązek dostarczyć nowe numery licencji jeśli dotychczasowe nie będą zgodne z nową wersją programu mimo ważnej licencji - licencja musi zagwarantować ochronę
Czas trwania subskrypcji	min. 60 miesięcy

Wszystkie komputery dostarczone w ramach PIAP zostaną skonfigurowane do pracy domenowej. Dla każdego PIAP zostanie założona osobna jednostka organizacyjna z użytkownikiem o prawach administratora przypisany tylko do danego PIAP. W każdym Piap zostaną założeni unikalni użytkownicy. W każdym PIAP zostaną założeni unikalni użytkownicy, tzn. jeden unikalny na każdy PIAP. Zostanie założony współdzielony katalog w każdym PIAP z dostępem dla użytkowników tego PIAP. W całej domenie zostanie zaimplementowany system dystrybucji aktualizacji dla Systemu operacyjnego , system dystrybucji oprogramowania systemu operacyjnego stacji roboczych.
Wykonawca skonfiguruje do pracy sieciowej dostarczone urządzenia wielofunkcyjne. w poszczególnych PIAP tak, aby mogły ich używać zainstalowane tam komputery.

Wykonawca podłączy i skonfiguruje laptopa do współpracy z projektorem.

Wykonawca dostarczy, skonfiguruje i uruchomi 1 szt piapa rodzinnego o ninimalnych wymaganiach techniczno-funkcjonalnych:

PIAPa należy wykonać w następującej lokalizacji: sala młodzieżowa przy Parafii Św Tomasza ul Tuwima w Ełku w miejscu instalacji węzła optycznego GPD

Na wyposażenie PIAP składają się:

g) Komputer wraz z klawiaturą, myszą, monitorem i oprogramowaniem (5 kompletów)
h) Zestaw biurko i krzesło (5 kompletów)
i) Switch, , system kontroli i bezpieczeństwa
j) Adaptacja pomieszczenia

Minimalne wymagania techniczno-funkcjonalne dla elementów wyposażenia PIAP:

Komputer wraz z klawiaturą, myszą, monitorem i oprogramowaniem: Komputer typu 2

Zestaw biurko i krzesło

Biurko:
Biurko wykonane z płyty wiórowej o grubości min. 18mm, oklejonej taśmą PCV/ABS o grubości min. 2 mm w kolorze blatu. Obrzeża zaokrąglone oklejone – o promieniu min. 2mm. Wymiary biurka: szerokość min 820, głębokość min 500mm, wysokość min. 750mm. Wysuwana półka na prowadnicach rolkowych służąca do przechowywania i korzystania z klawiatury i myszy.
Materiały z których wykonane jest biurko powinny posiadać atesty higieniczne dopuszczające od stosowania na terenie Polski.

Krzesło:
Krzesło obrotowe, odznaczające się dużą wytrzymałością
podstawa pięcioramienna
- oparcie i siedzisko miękkie
- regulacja wysokości (góra-dół)
- regulowany kąt nachylenia oparcia z blokadą w dowolnej pozycji
- regulacja odległości siedziska od oparcia krzesła

Switch, System projekcyjny, system kontroli i bezpieczeństwa, adaptacja

Wykonawca dostarczy i zainstaluje przełącznik sieciowy, system projekcyjny złożony z projektora wraz z ekranem elektrycznym, Wykonawca projektor zamocuje za pomocą uchwyt sufitowego o konstrukcji metalowej z możliwością teleskopowej regulacji odległości projektora od sufitu, możliwością prowadzenia kabli sygnałowych wewnątrz uchwytu. Wykonawca wszystkie kable sygnałowe VGA, HDMI, Audio i USB od projektora zakończy w gnieździe sygnałowym które umieści w okolicach dodatkowego biurka które wykonawca dostarczy w raz z krzesłem a które ma służyć do ustawienia i podłaczenia laptopa, Wykonawca dostarczy wszystkie niezbędne elementy w tym w szczególności okablowanie, Wykonawca dostarczy i zamontuje ekran o parametrach umożliwiających odtwarzanie obrazu w formacie zgodnym z dostarczonym projektorem i o minimalnej wielkości 250 cm x 160 cm. Wykonawca dostarczy, i podłączy do SZBME kamerę IP o rozdzielczości minimum 2,0 MP i szybkości 25 kl/s.

Adaptacja pomieszczenia

Do obsługi PIAP Wykonawca wykona sieć LAN
Całość okablowania logicznego powinna zostać wykonana za pomocą nie ekranowanego 4 parowego kabla UTP Cat.6 (klasa E) 4x2x23AWG LSOH.
Podwójne gniazda logiczne i elektryczne montować na wysokości uzgodnionej z Zamawiającym.
Wykonawca dokona adaptacji pomieszczenia polegającą na odmalowaniu pomieszczenia, wstawieniu wewnętrznych drzwi antywłamaniowych, wykonaniu sufitu podwieszanego wraz z oświetleniem, wyrównaniu podłogi i ułożeniu wykładziny podłogowej. Kolorystykę zastosowanych elementów Wykonawca uzgodni z Zamawiającym na etapie realizacji.
W pomieszczeniu wytypowanym pod lokalizację PIAP-u dodatkowo należy wykonać instalację zasilającą 230V, dla każdego stanowiska z osobna.
Dla okablowania strukturalnego przeznaczonego na obwody zasilające stacje robocze przewidziano wykorzystanie kabla YDYżo o minimalnym przekroju 3x2,5mm w izolacji PCV przystosowanego do instalacji na jak i podtynkowych. Na podstawie planowanych przez Wykonawcę do instalacji urządzeń (Komputer + monitor, tablica multimedialna, urządzenie wielofunkcyjne) Wykonawca dokona wszelkich niezbędnych wyliczeń i na ich podstawie dokona ostatecznego doboru parametrów podzespołów instalacji elektrycznych.
Na każde stanowisko komputera przypadać będzie 1 Punkt PEL (Punkt Elektryczno-Logiczny), w skład którego wchodzą: jeden podwójny moduł RJ-45 oraz jedno podwójne gniazdo elektryczne 230V (2x2P+Z). Łącznie należy wybudować w sali komputerowej 6 punktów PEL.
Do każdego PEL powinno się doprowadzić jedną linie okablowania strukturalnego w skład której
wchodzą dwie linie okablowania logicznego oraz linia elektryczna.
Okablowanie logiczne należy prowadzić z punktu GPD

Wykonawca dostarczy wszystkie, wymagane zastosowaną technologią, typy licencji gwarantujące poprawne uruchomienie usług domenowych w oparciu o serwerowy system operacyjny
Uwaga: Liczby tych licencji muszą umożliwiać uruchomienie wszystkich użytkowników usług domenowych jednocześnie.

Oprogramowanie antywirusowe:

Wykonawca dostarczy zainstaluje i skonfiguruje oprogramowanie antywirusowe na wszystkich dostarczonych komputerach i zainstalowanych serwerowych systemach operacyjnych z subskrypcją na okres min. 60 miesięcy Wykonawca zainstaluje i skonfiguruje konsolę umożliwiającą centralne zarządzanie oprogramowaniem antywirusowym.

Wykonawca jest zobowiązany dostarczyć i wdrożyć system antywirusowy dla wszystkich stacji roboczych i serwerów objętych projektem, o następujących wymaganiach minimalnych:

System musi wspierać min. następujące systemy operacyjne	Windows XP SP2 lub nowszy Windows Vista 32 i 64bit Windows 7 32 i 64bit Windows 8 32 I 64bit Windows Server 2003 SP2 lub nowszy Windows Server 2008 32 i 64bit Windows Server 2008 R2 32 i 64bit

	Windows SBS Server 2011 32 i 64bit Windows Server 2012
System musi wspierać min. następujące aplikacje	MS SharePoint Services 2.0/3.0 MS SharePoint Server 2003/2007/2010 MS Exchange 2003/2007/2010 (tylko Internet Security Business)
System musi realizować ochronę przed zagrożeniami wspierając następujące minimalne funkcjonalności:	- ochrona przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem (w tym Java i ActiveX); - wykrywanie oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich; - skanowanie skryptów napisanych w językach VB Script i Java Script wykonywane przez system operacyjny Windows; - wykrywanie rootkitów - moduł oceny wyników wyszukiwania w głównych wyszukiwarkach w czasie rzeczywistym - monitorowanie adresów URL w czasie rzeczywistym - funkcja inteligentnego skanowania automatycznie przełączająca tryb skanowania w wyższy lub niższy priorytet odpowiednio do wykorzystania zasobów przez użytkownika - ochrona przed phishingiem; - ochrona przed dialerami; - możliwość zdefiniowania portów, które będą monitorowane lub wykluczone z monitorowania przez moduły skanujące ruch sieciowy (z wyłączeniem zapory ogniowej); - monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera działający nieprzerwanie do momentu zamknięcia systemu operacyjnego; - dedykowany moduł ochrony tożsamości, który posiada własną, wyspecjalizowaną bazę sygnatur do wykrywania keyloggerów - moduł ochrony tożsamości powinien dodatkowo oferować funkcjonalność monitorowania zachowań podejrzanych aplikacji i blokować próby przejęcia danych logowania użytkownika
Skanowanie w czasie rzeczywistym	- uruchamianych, otwieranych, kopiowanych, przenoszonych lub tworzonych plików; - pobieranej z Internetu poczty elektronicznej (wraz z załącznikami) po protokołach POP3, SMTP, IMAP (także szyfrowanych z wykorzystaniem SSL/TLS) - możliwość zmiany nazwy lub usuwania określonych typów załączników; - Opcja modyfikowania tematu wiadomości jeśli zostanie w niej wykryty wirus.
Wyszukiwanie heurystyczne	- wyszukiwanie heurystyczne bazujące na analizie kodu potencjalnego wirusa;
Archiwa	- leczenie i usuwanie plików z archiwów następujących formatów: ZIP, RAR, 7z, CAB; - skanowanie archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia;
Działanie programu po wykryciu infekcji	- podejmować zalecane działanie - próbować leczyć, a jeżeli nie jest to możliwe pytać użytkownika o działanie; - rejestrować w pliku raportu informację o wykryciu wirusa; - powiadamiać administratora przy użyciu poczty elektronicznej;

	- poddać kwarantannie podejrzany obiekt;
Zapora ogniowa (firewall)	- możliwość ustawienia predefiniowanych poziomów ochrony, w tym poziomu zapewniającego interakcję z użytkownikiem po wykryciu nowego połączenia (tryb uczenia zapory) oraz trybu automatycznego; - możliwość ręcznego tworzenia i modyfikacji reguł dostępu dla zainstalowanych aplikacji; - zdefiniowania reguł zezwalających na komunikację na określonym porcie niezależnie od reguł dla aplikacji; - zdefiniowania zaufanych podsieci, dla których nie będą stosowane żadne reguły zapory(sieci zaufane); - ochrony przed atakami sieciowymi; - oferować białą i czarną listę adresów IP dla których nie będą stosowane reguły, a ruch dla tych adresów będzie w całości dozwolony lub blokowany.
Płyta ratunkowa	- możliwość utworzenia płyty ratunkowej lub nośnika USB lub płyty CD w oparciu o obraz w formacie ISO pobierany z serwerów producenta, umożliwiającego przeskanowanie dysków komputera bez uruchamiania systemu zainstalowanego na dysku; - płyta ratunkowa musi posiadać opcję aktualizacji sygnatur z Internetu, dysku lokalnego oraz innego nośnika np. usb. - płyta ratunkowa powinna oferować możliwość zarządzania kwarantanną utworzoną przez program na komputerze i pozwalać na przywracanie obiektów, które są niezbędne do poprawnego uruchomienia systemu - nośnik powinien zawierać również dodatkowe narzędzia naprawcze jak na przykład edytor rejestru
Wykorzystywanie zasobów systemowych	- możliwość dynamicznej zmiany użycia zasobów systemowych w zależności od obciążenia systemu przez aplikacje użytkownika;
Język	- polski, również dla konsoli zdalnej administracji; - dodatkowo powinien być instalowany również język angielski niezależnie od języka wybranego podczas instalacji; - możliwość łatwego przełączania interfejsu pomiędzy zainstalowanymi wersjami językowymi
Harmonogram	- umożliwiający modyfikowanie oraz tworzenie zadań aktualizacji komponentów programu, - sygnatur, - skanowania cyklicznego, Każde z tych zadań musi posiadać własne zadanie harmonogramu.
Blokowanie ustawień programu	- blokowanie dostępu do ustawień programu dla użytkowników w tym: zatrzymywania skanowania, wyłączania ochrony, dostępu do przywracania bądź usuwania obiektów z kwarantanny, przerywania aktualizacji; - możliwość całkowitego zablokowania dostępu do ustawień zaawansowanych lub interfejsu programu;
Wysyłanie podejrzanych obiektów	- możliwość wysyłania podejrzanych obiektów do producenta oprogramowania w celu przeprowadzenia analizy;
Informowanie użytkownika	- program powinien umożliwić administratorowi wyłączenie niektórych lub wszystkich powiadomień wyświetlanych na stacjach roboczych; - możliwość wyłączenia powiadomień o stanie składnika;

Aktualizacja	- antywirusowe bazy danych na serwerach producenta aktualizowane nie rzadziej niż raz na cztery godziny; - pobieranie uaktualnień w trybie przyrostowym;
Zdalne zarządzanie	- program (poprzez funkcjonalność w niego wbudowaną lub z wykorzystaniem dodatkowego modułu/ aplikacji) powinien umożliwiać zdalne zarządzanie oprogramowaniem i jego funkcjami. - przechowywać ustawienia w relacyjnej bazie danych MS SQL Server 2005/2008 również wersje Express, MySQL 5, Oracle 10/11, Firebird 2.0/2.5 - umożliwiać automatyczne i regularne tworzenie kopii zapasowej serwera zarządzającego, która umożliwi przywrócenie w pełni działającego systemu zarządzania; - powinien dostarczać własny silnik bazodanowy - umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych odpowiadających strukturze sieci (grupy robocze sieci Microsoft Windows i/lub struktura Active Directory) również w oparciu o zdefiniowane reguły; - umożliwiać tworzenie hierarchicznej struktury serwerów administracyjnych; - umożliwiać zarządzanie komputerami położonymi w różnych podsieciach; - umożliwiać zdalne zarządzanie o obiektami poddanymi kwarantannie oraz podejmowanie odpowiednich działań (np. przywracanie, usuwanie itp.); - umożliwiać przeglądanie informacji o obiektach, które zostały wykryte ale program nie podjął względem nich żadnego działania wraz z możliwością wymuszenia przez administratora odpowiedniego działania; - konsola administracyjna posiada możliwość zdalnego inicjowania skanowania antywirusowego na stacjach roboczych włączonych do sieci komputerowych w całej firmie (wszystkich podsieciach); - Konsola zdalnej administracji musi oferować możliwość zdalnego zarządzania konfiguracją komputerów, grup komputerów oraz całej sieci - musi ofertować funkcjonalność raportowania i powiadamiania mailem oraz generowania raportów i statystyk z pracy systemu antywirusowego na stacjach roboczych - raporty te powinny być dostarczane mailem zgodnie ze zdefiniowanym ręcznie harmonogramem - musi oferować opcję zdalnego restartowania i zamykania komputera na którym zainstalowany jest program - umożliwiać automatyczne aktualizacje licencji na stacjach roboczych; - system centralnej dystrybucji i instalacji aktualizacji oprogramowania, umożliwiający automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowego oprogramowania; - system centralnej dystrybucji i instalacji aktualizacji bibliotek sygnatur wirusów, umożliwiający automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowej wersji biblioteki - system administracji zdalnej nie może wymagać do działania żadnego serwera www (Apache, IIS itp.) - posiadający mechanizmy raportowania i dystrybucji oprogramowania oraz polityk antywirusowych w sieciach korporacyjnych;
Wsparcie	- w całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej, realizowanej w języku polskim; - pomoc techniczna telefonicznie, mailowo oraz w razie potrzeby z użyciem połączeń zdalnych

Licencjonowanie	- w całym okresie trwania subskrypcji użytkownik ma możliwość pobierania i instalacji nowszych wersji oprogramowania i konsoli zarządzającej; - w razie konieczności producent ma obowiązek dostarczyć nowe numery licencji jeśli dotychczasowe nie będą zgodne z nową wersją programu mimo ważnej licencji - licencja musi zagwarantować ochronę
Czas trwania subskrypcji	min. 60 miesięcy

Wszystkie komputery dostarczone w ramach PIAP zostaną skonfigurowane do pracy domenowej. Dla każdego PIAP zostanie założona osobna jednostka organizacyjna z użytkownikiem o prawach administratora przypisany tylko do danego PIAP. W każdym Piap zostaną założeni unikalni użytkownicy. W każdym PIAP zostaną założeni unikalni użytkownicy, tzn. jeden unikalny na każdy PIAP. Zostanie założony współdzielony katalog w każdym PIAP z dostępem dla użytkowników tego PIAP. W całej domenie zostanie zaimplementowany system dystrybucji aktualizacji dla Systemu operacyjnego , system dystrybucji oprogramowania systemu operacyjnego stacji roboczych.
Wykonawca skonfiguruje do pracy sieciowej dostarczone urządzenia wielofunkcyjne. w poszczególnych PIAP tak, aby mogły ich używać zainstalowane tam komputery.

Wykonawca dostarczy, skonfiguruje i uruchomi 2 szt. PIAP'ów multimedialnych o minimalnych wymaganiach techniczno-funkcjonalnych:

PIAPy należy wykonać w następujących lokalizacjach:
1. Szkoła Artystyczna ul Armii Krajowej 21 w Ełku
2. Salka młodzieżowa przy parafii NSJ w Ełku

Na wyposażenie każdego z powyższych PIAP składają się:
a) Komputer wraz z klawiaturą, myszą, monitorem i oprogramowaniem (3 kompletów)
b) Zestaw biurko i krzesło (3 kompletów)
c) Switch, system kontroli i bezpieczeństwa
d) kamera
e) Adaptacja pomieszczenia

Minimalne wymagania techniczno-funkcjonalne dla elementów wyposażenia PIAP:

Komputer wraz z klawiaturą, myszą, monitorem i oprogramowaniem: Komputer typu 2

Zestaw biurko i krzesło

Biurko:

Biurko wykonane z płyty wiórowej o grubości min. 18mm, oklejonej taśmą PCV/ABS o grubości min. 2 mm w kolorze blatu. Obrzeża zaokrąglone oklejone – o promieniu min. 2mm.

Wymiary biurka: szerokość min 820, głębokość min 500mm, wysokość min. 750mm. Wysuwana półka na prowadnicach rolkowych służąca do przechowywania i korzystania z klawiatury i myszy.
Materiały z których wykonane jest biurko powinny posiadać atesty higieniczne dopuszczające od stosowania na terenie Polski.

Krzesło:

Krzesło obrotowe, odznaczające się dużą wytrzymałością
podstawa pięcioramienna
- oparcie i siedzisko miękkie
- regulacja wysokości (góra-dół)
- regulowany kąt nachylenia oparcia z blokadą w dowolnej pozycji
- regulacja odległości siedziska od oparcia krzesła

Switch, System projekcyjny, system kontroli i bezpieczeństwa

Wykonawca do każdego piapa dostarczy i zainstaluje przełącznik sieciowy, Wykonawca dostarczy, i podłączy do SZBME kamerę IP o rozdzielczości minimum 2,0 MP i szybkości 25 kl/s.

Adaptacja pomieszczenia

W ramach adaptacji Wykonawca dostarczy i zamontuje w pomieszczeniu PIAP drzwi wewnętrzne antywłamaniowe zgodne z obowiązującymi normami, na oknach zamontuje rolety kasetonowe.
Do obsługi PIAP Wykonawca wykona sieć LAN
Całość okablowania logicznego powinna zostać wykonana za pomocą nie ekranowanego 4 parowego kabla UTP Cat.6 (klasa E) 4x2x23AWG LSOH
Podwójne gniazda logiczne i elektryczne montować na wysokości uzgodnionej z Zamawiającym.
W pomieszczeniu wytypowanym pod lokalizację PIAP-u dodatkowo należy wykonać instalację zasilającą 230V, dla każdego stanowiska z osobna.
Dla okablowania strukturalnego przeznaczonego na obwody zasilające stacje robocze przewidziano wykorzystanie kabla YDYżo o minimalnym przekroju 3x2,5mm w izolacji PCV przystosowanego do instalacji na jak i podtynkowych. Na podstawie planowanych przez Wykonawcę do instalacji urządzeń (Komputer + monitor, tablica multimedialna, urządzenie wielofunkcyjne) Wykonawca dokona wszelkich niezbędnych wyliczeń i na ich podstawie dokona ostatecznego doboru parametrów podzespołów instalacji elektrycznych.
Na każde stanowisko komputera przypadać będzie 1 Punkt PEL (Punkt Elektryczno-Logiczny), w skład którego wchodzą: jeden podwójny moduł RJ-45 oraz jedno podwójne gniazdo elektryczne 230V (2x2P+Z). Łącznie należy wybudować w sali komputerowej 5 punktów PEL.
Do każdego PEL powinno się doprowadzić jedną linie okablowania strukturalnego w skład której
wchodzą dwie linie okablowania logicznego oraz linia elektryczna.
Okablowanie logiczne należy prowadzić z punktu GPD

Wykonawca dostarczy wszystkie, wymagane zastosowaną technologią, typy licencji gwarantujące poprawne uruchomienie usług domenowych w oparciu o serwerowy system operacyjny
Uwaga: Liczby tych licencji muszą umożliwiać uruchomienie wszystkich użytkowników usług domenowych jednocześnie.

Oprogramowanie antywirusowe:
Wykonawca dostarczy zainstaluje i skonfiguruje oprogramowanie antywirusowe na wszystkich dostarczonych komputerach i zainstalowanych serwerowych systemach operacyjnych z subskrypcją na okres min. 60 miesięcy Wykonawca zainstaluje i skonfiguruje konsolę umożliwiającą centralne zarządzanie oprogramowaniem antywirusowym.

Wykonawca jest zobowiązany dostarczyć i wdrożyć system antywirusowy dla wszystkich stacji roboczych i serwerów objętych projektem, o następujących wymaganiach minimalnych:

System musi wspierać min. następujące systemy operacyjne	Windows XP SP2 lub nowszy Windows Vista 32 i 64bit Windows 7 32 i 64bit Windows 8 32 I 64bit Windows Server 2003 SP2 lub nowszy Windows Server 2008 32 i 64bit Windows Server 2008 R2 32 i 64bit Windows SBS Server 2011 32 i 64bit Windows Server 2012
System musi wspierać min. następujące aplikacje	MS SharePoint Services 2.0/3.0 MS SharePoint Server 2003/2007/2010 MS Exchange 2003/2007/2010 (tylko Internet Security Business)
System musi realizować ochronę przed zagrożeniami wspierając następujące minimalne funkcjonalności:	- ochrona przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem (w tym Java i ActiveX); - wykrywanie oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich; - skanowanie skryptów napisanych w językach VB Script i Java Script wykonywane przez system operacyjny Windows; - wykrywanie rootkitów - moduł oceny wyników wyszukiwania w głównych wyszukiwarkach w czasie rzeczywistym - monitorowanie adresów URL w czasie rzeczywistym - funkcja inteligentnego skanowania automatycznie przełączająca tryb skanowania w wyższy lub niższy priorytet odpowiednio do wykorzystania zasobów przez użytkownika - ochrona przed phishingiem; - ochrona przed dialerami; - możliwość zdefiniowania portów, które będą monitorowane lub wykluczone z monitorowania przez moduły skanujące ruch sieciowy (z wyłączeniem zapory ogniowej); - monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera działający nieprzerwanie do momentu zamknięcia systemu operacyjnego;

	- dedykowany moduł ochrony tożsamości, który posiada własną, wyspecjalizowaną bazę sygnatur do wykrywania keyloggerów - moduł ochrony tożsamości powinien dodatkowo oferować funkcjonalność monitorowania zachowań podejrzanych aplikacji i blokować próby przejęcia danych logowania użytkownika
Skanowanie w czasie rzeczywistym	- uruchamianych, otwieranych, kopiowanych, przenoszonych lub tworzonych plików; - pobieranej z Internetu poczty elektronicznej (wraz z załącznikami) po protokołach POP3, SMTP, IMAP (także szyfrowanych z wykorzystaniem SSL/TLS) - możliwość zmiany nazwy lub usuwania określonych typów załączników; - Opcja modyfikowania tematu wiadomości jeśli zostanie w niej wykryty wirus.
Wyszukiwanie heurystyczne	- wyszukiwanie heurystyczne bazujące na analizie kodu potencjalnego wirusa;
Archiwa	- leczenie i usuwanie plików z archiwów następujących formatów: ZIP, RAR, 7z, CAB; - skanowanie archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia;
Działanie programu po wykryciu infekcji	- podejmować zalecane działanie - próbować leczyć, a jeżeli nie jest to możliwe pytać użytkownika o działanie; - rejestrować w pliku raportu informację o wykryciu wirusa; - powiadamiać administratora przy użyciu poczty elektronicznej; - poddać kwarantannie podejrzany obiekt;
Zapora ogniowa (firewall)	- możliwość ustawienia predefiniowanych poziomów ochrony, w tym poziomu zapewniającego interakcję z użytkownikiem po wykryciu nowego połączenia (tryb uczenia zapory) oraz trybu automatycznego; - możliwość ręcznego tworzenia i modyfikacji reguł dostępu dla zainstalowanych aplikacji; - zdefiniowania reguł zezwalających na komunikację na określonym porcie niezależnie od reguł dla aplikacji; - zdefiniowania zaufanych podsieci, dla których nie będą stosowane żadne reguły zapory(sieci zaufane); - ochrony przed atakami sieciowymi; - oferować białą i czarną listę adresów IP dla których nie będą stosowane reguły, a ruch dla tych adresów będzie w całości dozwolony lub blokowany.
Płyta ratunkowa	- możliwość utworzenia płyty ratunkowej lub nośnika USB lub płyty CD w oparciu o obraz w formacie ISO pobierany z serwerów producenta, umożliwiającego przeskanowanie dysków komputera bez uruchamiania systemu zainstalowanego na dysku; - płyta ratunkowa musi posiadać opcję aktualizacji sygnatur z Internetu, dysku lokalnego oraz innego nośnika np. usb. - płyta ratunkowa powinna oferować możliwość zarządzania kwarantanną utworzoną przez program na komputerze i pozwalać na przywracanie obiektów, które są niezbędne do poprawnego uruchomienia systemu - nośnik powinien zawierać również dodatkowe narzędzia naprawcze jak na przykład edytor rejestru
Wykorzystywanie zasobów	- możliwość dynamicznej zmiany użycia zasobów systemowych w zależności od obciążenia systemu przez aplikacje użytkownika;

systemowych	
Język	- polski, również dla konsoli zdalnej administracji; - dodatkowo powinien być instalowany również język angielski niezależnie od języka wybranego podczas instalacji; - możliwość łatwego przełączania interfejsu pomiędzy zainstalowanymi wersjami językowymi
Harmonogram	- umożliwiający modyfikowanie oraz tworzenie zadań aktualizacji komponentów programu, - sygnatur, - skanowania cyklicznego, Każde z tych zadań musi posiadać własne zadanie harmonogramu.
Blokowanie ustawień programu	- blokowanie dostępu do ustawień programu dla użytkowników w tym: zatrzymywania skanowania, wyłączania ochrony, dostępu do przywracania bądź usuwania obiektów z kwarantanny, przerywania aktualizacji; - możliwość całkowitego zablokowania dostępu do ustawień zaawansowanych lub interfejsu programu;
Wysyłanie podejrzanych obiektów	- możliwość wysyłania podejrzanych obiektów do producenta oprogramowania w celu przeprowadzenia analizy;
Informowanie użytkownika	- program powinien umożliwić administratorowi wyłączenie niektórych lub wszystkich powiadomień wyświetlanych na stacjach roboczych; - możliwość wyłączenia powiadomień o stanie składnika;
Aktualizacja	- antywirusowe bazy danych na serwerach producenta aktualizowane nie rzadziej niż raz na cztery godziny; - pobieranie uaktualnień w trybie przyrostowym;
Zdalne zarządzanie	- program (poprzez funkcjonalność w niego wbudowaną lub z wykorzystaniem dodatkowego modułu/ aplikacji) powinien umożliwiać zdalne zarządzanie oprogramowaniem i jego funkcjami. - przechowywać ustawienia w relacyjnej bazie danych MS SQL Server 2005/2008 również wersje Express, MySQL 5, Oracle 10/11, Firebird 2.0/2.5 - umożliwiać automatyczne i regularne tworzenie kopii zapasowej serwera zarządzającego, która umożliwi przywrócenie w pełni działającego systemu zarządzania; - powinien dostarczać własny silnik bazodanowy - umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych odpowiadających strukturze sieci (grupy robocze sieci Microsoft Windows i/lub struktura Active Directory) również w oparciu o zdefiniowane reguły; - umożliwiać tworzenie hierarchicznej struktury serwerów administracyjnych; - umożliwiać zarządzanie komputerami położonymi w różnych podsieciach; - umożliwiać zdalne zarządzanie o obiektami poddanymi kwarantannie oraz podejmowanie odpowiednich działań (np. przywracanie, usuwanie itp.); - umożliwiać przeglądanie informacji o obiektach, które zostały wykryte ale program nie podjął względem nich żadnego działania wraz z możliwością wymuszenia przez administratora odpowiedniego działania; - konsola administracyjna posiada możliwość zdalnego inicjowania skanowania antywirusowego na stacjach roboczych włączonych do sieci komputerowych w całej firmie (wszystkich podsieciach);

	- Konsola zdalnej administracji musi oferować możliwość zdalnego zarządzania konfiguracją komputerów, grup komputerów oraz całej sieci - musi ofertować funkcjonalność raportowania i powiadamiania mailem oraz generowania raportów i statystyk z pracy systemu antywirusowego na stacjach roboczych - raporty te powinny być dostarczane mailem zgodnie ze zdefiniowanym ręcznie harmonogramem - musi oferować opcję zdalnego restartowania i zamykania komputera na którym zainstalowany jest program - umożliwiać automatyczne aktualizacje licencji na stacjach roboczych; - system centralnej dystrybucji i instalacji aktualizacji oprogramowania, umożliwiający automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowego oprogramowania; - system centralnej dystrybucji i instalacji aktualizacji bibliotek sygnatur wirusów, umożliwiający automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowej wersji biblioteki - system administracji zdalnej nie może wymagać do działania żadnego serwera www (Apache, IIS itp.) - posiadający mechanizmy raportowania i dystrybucji oprogramowania oraz polityk antywirusowych w sieciach korporacyjnych;
Wsparcie	- w całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej, realizowanej w języku polskim; - pomoc techniczna telefonicznie, mailowo oraz w razie potrzeby z użyciem połączeń zdalnych
Licencjonowanie	- w całym okresie trwania subskrypcji użytkownik ma możliwość pobierania i instalacji nowszych wersji oprogramowania i konsoli zarządzającej; - w razie konieczności producent ma obowiązek dostarczyć nowe numery licencji jeśli dotychczasowe nie będą zgodne z nową wersją programu mimo ważnej licencji - licencja musi zagwarantować ochronę
Czas trwania subskrypcji	min. 60 miesięcy

Wszystkie komputery dostarczone w ramach PIAP zostaną skonfigurowane do pracy domenowej. Dla każdego PIAP zostanie założona osobna jednostka organizacyjna z użytkownikiem o prawach administratora przypisany tylko do danego PIAP. W każdym PIAP zostaną założeni unikalni użytkownicy. W każdym PIAP zostaną założeni unikalni użytkownicy, tzn. jeden unikalny na każdy PIAP. Zostanie założony współdzielony katalog w każdym PIAP z dostępem dla użytkowników tego PIAP. W całej domenie zostanie zaimplementowany system dystrybucji aktualizacji dla Systemu operacyjnego, system dystrybucji oprogramowania systemu operacyjnego stacji roboczych.
Wykonawca skonfiguruje do pracy sieciowej dostarczone urządzenia wielofunkcyjne. w poszczególnych PIAP tak, aby mogły ich używać zainstalowane tam komputery.

Kamery: w ramach PIAP multimedialnych wykonawca ma dostarczyć łącznie dwie kamery o minimalnych parametrach:
Jedna kamera:

Umożliwiająca nagrywanie i odtwarzanie obrazu 3840x2160, zapis obrazu HD o przepływności minimum 50 Mb/s, wyposażona w złącza XLR i funkcje ręcznego wyboru ustawień, zapis w formacie XAVC S ,dwa gniazda na karty pamięci XQD współpracujące z nośnikami XQD z serii S i N, złącze HDMI, zoom optyczny 20 x,wejście mikrofonowe, wyjście słuchawkowe, przysłona minimalna 1.6Matryca CMOS - 1/2,3, przekątna wizjera LCD 0.45 cm. Do powyższej kamery Wykonawca dostarczy sztywną torbę ochronną naramienną na kamerę oraz na akcesoria, statyw umożliwiający stabilny montaż kamery wyposażony w rozpórkę z gumowymi stopkami o udźwigu: 4 kg, o zakresie temperatur: -20°C do +60°C o minimalnej wysokości 160 cm. wykonawca dostarczy jedną zewnętrzna lampę oświetleniową LED przystosowaną do współpracy z kamerą.Wykonawca dostarczy minimum dwie kary pamięci do kamery o pojemności minimum 32 Gb każda wraz z czytnikiem do podłączenia ich do komputera klasy PC, Wykonawca do kamery dostarczy jeden mikrofon zewnętrzny kypu klip, wszystkie niezbędne do podłączenia kamery okablowanie i akcesoria.
Jedna kamera:
Umożliwiająca nagrywanie i odtwarzanie obrazu 3840x2160, zoom optyczny 12 x, format nagrywania AVCHD/MP4, wbudowany mikrofon, stabilizator obrazu, wyjście AV, wejście mikrofonowe, microUSB, cyfrowe wyjście HDMI. Do powyższej kamery Wykonawca dostarczy sztywną torbę ochronną naramienną na kamerę oraz na akcesoria, statyw umożliwiający stabilny montaż kamery o udźwigu: 4 kg. wykonawca dostarczy jedną zewnętrzna lampę oświetleniową LED przystosowaną do współpracy z kamerą. Wykonawca dostarczy minimum dwie kary pamięci do kamery o pojemności minimum 32 Gb każda wraz z czytnikiem do podłączenia ich do komputera klasy PC, Wykonawca do kamery dostarczy jeden mikrofon zewnętrzny kypu klip, wszystkie niezbędne do podłączenia kamery okablowanie i akcesoria.

Wykonawca dostarczy, skonfiguruje i uruchomi jeden PIAP małego pacjenta o minimalnych wymaganiach techniczno-funkcjonalnych:

PIAP należy wykonać w następującej lokalizacji: świetlica na oddziale dziecięcym szpitala miejskiego w Ełku zlokalizowanego przy ulicy Baranki 24 w Ełku.

Na wyposażenie PIAP składają się:
a) Komputer wraz z klawiaturą, myszą, monitorem i oprogramowaniem (3 kompletów)
b) Zestaw biurko i krzesło (3 kompletów)
c) Switch, system kontroli i bezpieczeństwa
d) Adaptacja pomieszczenia

Minimalne wymagania techniczno-funkcjonalne dla elementów wyposażenia PIAP:

Komputer wraz z klawiaturą, myszą, monitorem i oprogramowaniem: Komputer typu 2

Zestaw biurko i krzesło

Biurko:

Biurko wykonane z płyty wiórowej o grubości min. 18mm, oklejonej taśmą PCV/ABS o grubości min. 2 mm w kolorze blatu. Obrzeża zaokrąglone oklejone – o promieniu min. 2mm. Wymiary biurka: szerokość min 820, głębokość min 500mm, wysokość min. 750mm. Wysuwana półka na prowadnicach rolkowych służąca do przechowywania i korzystania z klawiatury i myszy.
Materiały z których wykonane jest biurko powinny posiadać atesty higieniczne dopuszczające od stosowania na terenie Polski.

Krzesło:

Krzesło obrotowe, odznaczające się dużą wytrzymałością
podstawa pięcioramienna
- oparcie i siedzisko miękkie
- regulacja wysokości (góra-dół)
- regulowany kąt nachylenia oparcia z blokadą w dowolnej pozycji
- regulacja odległości siedziska od oparcia krzesła

Switch, System projekcyjny, system kontroli i bezpieczeństwa

Wykonawca zainstaluje przełącznik sieciowy, Wykonawca dostarczy, i podłączy do SZBME kamerę IP o rozdzielczości minimum 2,0 MP i szybkości 25 kl/s.

Adaptacja pomieszczenia

W ramach adaptacji Wykonawca dostarczy i zamontuje w pomieszczeniu PIAP drzwi wewnętrzne antywłamaniowe zgodne z obowiązującymi normami, na oknach zamontuje rolety kasetonowe
Do obsługi PIAP Wykonawca wykona sieć LAN
Całość okablowania logicznego powinna zostać wykonana za pomocą nie ekranowanego 4 parowego kabla UTP Cat.6 (klasa E) 4x2x23AWG LSOH
Podwójne gniazda logiczne i elektryczne montować na wysokości uzgodnionej z Zamawiającym.
W pomieszczeniu wytypowanym pod lokalizację PIAP-u dodatkowo należy wykonać instalację zasilającą 230V, dla każdego stanowiska z osobna.
Dla okablowania strukturalnego przeznaczonego na obwody zasilające stacje robocze przewidziano wykorzystanie kabla YDYżo o minimalnym przekroju 3x2,5mm w izolacji PCV przystosowanego do instalacji na jak i podtynkowych. Na podstawie planowanych przez Wykonawcę do instalacji urządzeń (Komputer + monitor, tablica multimedialna, urządzenie wielofunkcyjne) Wykonawca dokona wszelkich niezbędnych wyliczeń i na ich podstawie dokona ostatecznego doboru parametrów podzespołów instalacji elektrycznych.
Na każde stanowisko komputera przypadać będzie 1 Punkt PEL (Punkt Elektryczno-Logiczny), w skład którego wchodzą: jeden podwójny moduł RJ-45 oraz jedno podwójne gniazdo elektryczne 230V (2x2P+Z). Łącznie należy wybudować w sali komputerowej 5 punktów PEL.
Do każdego PEL powinno się doprowadzić jedną linie okablowania strukturalnego w skład której wchodzą dwie linie okablowania logicznego oraz linia elektryczna.
Okablowanie logiczne należy prowadzić z punktu GPD

Wykonawca dostarczy wszystkie, wymagane zastosowaną technologią, typy licencji gwarantujące poprawne uruchomienie usług domenowych w oparciu o serwerowy system operacyjny
Uwaga: Liczby tych licencji muszą umożliwiać uruchomienie wszystkich użytkowników usług domenowych jednocześnie.

Oprogramowanie antywirusowe:

Wykonawca dostarczy zainstaluje i skonfiguruje oprogramowanie antywirusowe na wszystkich dostarczonych komputerach i zainstalowanych serwerowych systemach operacyjnych z subskrypcją na okres min. 60 miesięcy Wykonawca zainstaluje i skonfiguruje konsolę umożliwiającą centralne zarządzanie oprogramowaniem antywirusowym.

Wykonawca jest zobowiązany dostarczyć i wdrożyć system antywirusowy dla wszystkich stacji roboczych i serwerów objętych projektem, o następujących wymaganiach minimalnych:

System musi wspierać min. następujące systemy operacyjne	Windows XP SP2 lub nowszy Windows Vista 32 i 64bit Windows 7 32 i 64bit Windows 8 32 I 64bit Windows Server 2003 SP2 lub nowszy Windows Server 2008 32 i 64bit Windows Server 2008 R2 32 i 64bit Windows SBS Server 2011 32 i 64bit Windows Server 2012
System musi wspierać min. następujące aplikacje	MS SharePoint Services 2.0/3.0 MS SharePoint Server 2003/2007/2010 MS Exchange 2003/2007/2010 (tylko Internet Security Business)
System musi realizować ochronę przed zagrożeniami wspierając następujące minimalne funkcjonalności:	- ochrona przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem (w tym Java i ActiveX); - wykrywanie oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich; - skanowanie skryptów napisanych w językach VB Script i Java Script wykonywane przez system operacyjny Windows; - wykrywanie rootkitów - moduł oceny wyników wyszukiwania w głównych wyszukiwarkach w czasie rzeczywistym - monitorowanie adresów URL w czasie rzeczywistym - funkcja inteligentnego skanowania automatycznie przełączająca tryb skanowania w wyższy lub niższy priorytet odpowiednio do wykorzystania zasobów przez użytkownika - ochrona przed phishingiem; - ochrona przed dialerami; - możliwość zdefiniowania portów, które będą monitorowane lub wykluczone z monitorowania przez moduły skanujące ruch sieciowy (z wyłączeniem zapory ogniowej); - monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera działający nieprzerwanie do momentu

	zamknięcia systemu operacyjnego; - dedykowany moduł ochrony tożsamości, który posiada własną, wyspecjalizowaną bazę sygnatur do wykrywania keyloggerów - moduł ochrony tożsamości powinien dodatkowo oferować funkcjonalność monitorowania zachowań podejrzanych aplikacji i blokować próby przejęcia danych logowania użytkownika
Skanowanie w czasie rzeczywistym	- uruchamianych, otwieranych, kopiowanych, przenoszonych lub tworzonych plików; - pobieranej z Internetu poczty elektronicznej (wraz z załącznikami) po protokołach POP3, SMTP, IMAP (także szyfrowanych z wykorzystaniem SSL/TLS) - możliwość zmiany nazwy lub usuwania określonych typów załączników; - Opcja modyfikowania tematu wiadomości jeśli zostanie w niej wykryty wirus.
Wyszukiwanie heurystyczne	- wyszukiwanie heurystyczne bazujące na analizie kodu potencjalnego wirusa;
Archiwa	- leczenie i usuwanie plików z archiwów następujących formatów: ZIP, RAR, 7z, CAB; - skanowanie archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia;
Działanie programu po wykryciu infekcji	- podejmować zalecane działanie - próbować leczyć, a jeżeli nie jest to możliwe pytać użytkownika o działanie; - rejestrować w pliku raportu informację o wykryciu wirusa; - powiadamiać administratora przy użyciu poczty elektronicznej; - poddać kwarantannie podejrzany obiekt;
Zapora ogniowa (firewall)	- możliwość ustawienia predefiniowanych poziomów ochrony, w tym poziomu zapewniającego interakcję z użytkownikiem po wykryciu nowego połączenia (tryb uczenia zapory) oraz trybu automatycznego; - możliwość ręcznego tworzenia i modyfikacji reguł dostępu dla zainstalowanych aplikacji; - zdefiniowania reguł zezwalających na komunikację na określonym porcie niezależnie od reguł dla aplikacji; - zdefiniowania zaufanych podsieci, dla których nie będą stosowane żadne reguły zapory(sieci zaufane); - ochrony przed atakami sieciowymi; - oferować białą i czarną listę adresów IP dla których nie będą stosowane reguły, a ruch dla tych adresów będzie w całości dozwolony lub blokowany.
Płyta ratunkowa	- możliwość utworzenia płyty ratunkowej lub nośnika USB lub płyty CD w oparciu o obraz w formacie ISO pobierany z serwerów producenta, umożliwiającego przeskanowanie dysków komputera bez uruchamiania systemu zainstalowanego na dysku; - płyta ratunkowa musi posiadać opcję aktualizacji sygnatur z Internetu, dysku lokalnego oraz innego nośnika np. usb. - płyta ratunkowa powinna oferować możliwość zarządzania kwarantanną utworzoną przez program na komputerze i pozwalać na przywracanie obiektów, które są niezbędne do poprawnego uruchomienia systemu - nośnik powinien zawierać również dodatkowe narzędzia naprawcze jak na przykład edytor rejestru
Wykorzystywanie	- możliwość dynamicznej zmiany użycia zasobów systemowych w zależności

zasobów systemowych	od obciążenia systemu przez aplikacje użytkownika;
Język	- polski, również dla konsoli zdalnej administracji; - dodatkowo powinien być instalowany również język angielski niezależnie od języka wybranego podczas instalacji; - możliwość łatwego przełączania interfejsu pomiędzy zainstalowanymi wersjami językowymi
Harmonogram	- umożliwiający modyfikowanie oraz tworzenie zadań aktualizacji komponentów programu, - sygnatur, - skanowania cyklicznego, Każde z tych zadań musi posiadać własne zadanie harmonogramu.
Blokowanie ustawień programu	- blokowanie dostępu do ustawień programu dla użytkowników w tym: zatrzymywania skanowania, wyłączania ochrony, dostępu do przywracania bądź usuwania obiektów z kwarantanny, przerywania aktualizacji; - możliwość całkowitego zablokowania dostępu do ustawień zaawansowanych lub interfejsu programu;
Wysyłanie podejrzanych obiektów	- możliwość wysyłania podejrzanych obiektów do producenta oprogramowania w celu przeprowadzenia analizy;
Informowanie użytkownika	- program powinien umożliwić administratorowi wyłączenie niektórych lub wszystkich powiadomień wyświetlanych na stacjach roboczych; - możliwość wyłączenia powiadomień o stanie składnika;
Aktualizacja	- antywirusowe bazy danych na serwerach producenta aktualizowane nie rzadziej niż raz na cztery godziny; - pobieranie uaktualnień w trybie przyrostowym;
Zdalne zarządzanie	- program (poprzez funkcjonalność w niego wbudowaną lub z wykorzystaniem dodatkowego modułu/ aplikacji) powinien umożliwiać zdalne zarządzanie oprogramowaniem i jego funkcjami. - przechowywać ustawienia w relacyjnej bazie danych MS SQL Server 2005/2008 również wersje Express, MySQL 5, Oracle 10/11, Firebird 2.0/2.5 - umożliwiać automatyczne i regularne tworzenie kopii zapasowej serwera zarządzającego, która umożliwi przywrócenie w pełni działającego systemu zarządzania; - powinien dostarczać własny silnik bazodanowy - umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych odpowiadających strukturze sieci (grupy robocze sieci Microsoft Windows i/lub struktura Active Directory) również w oparciu o zdefiniowane reguły; - umożliwiać tworzenie hierarchicznej struktury serwerów administracyjnych; - umożliwiać zarządzanie komputerami położonymi w różnych podsieciach; - umożliwiać zdalne zarządzanie o obiektami poddanymi kwarantannie oraz podejmowanie odpowiednich działań (np. przywracanie, usuwanie itp.); - umożliwiać przeglądanie informacji o obiektach, które zostały wykryte ale program nie podjął względem nich żadnego działania wraz z możliwością wymuszenia przez administratora odpowiedniego działania; - konsola administracyjna posiada możliwość zdalnego inicjowania skanowania antywirusowego na stacjach roboczych włączonych do sieci komputerowych w

	całej firmie (wszystkich podsieciach); - Konsola zdalnej administracji musi oferować możliwość zdalnego zarządzania konfiguracją komputerów, grup komputerów oraz całej sieci - musi ofertować funkcjonalność raportowania i powiadamiania mailem oraz generowania raportów i statystyk z pracy systemu antywirusowego na stacjach roboczych - raporty te powinny być dostarczane mailem zgodnie ze zdefiniowanym ręcznie harmonogramem - musi oferować opcję zdalnego restartowania i zamykania komputera na którym zainstalowany jest program - umożliwiać automatyczne aktualizacje licencji na stacjach roboczych; - system centralnej dystrybucji i instalacji aktualizacji oprogramowania, umożliwiający automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowego oprogramowania; - system centralnej dystrybucji i instalacji aktualizacji bibliotek sygnatur wirusów, umożliwiający automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowej wersji biblioteki - system administracji zdalnej nie może wymagać do działania żadnego serwera www (Apache, IIS itp.) - posiadający mechanizmy raportowania i dystrybucji oprogramowania oraz polityk antywirusowych w sieciach korporacyjnych;
Wsparcie	- w całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej, realizowanej w języku polskim; - pomoc techniczna telefonicznie, mailowo oraz w razie potrzeby z użyciem połączeń zdalnych
Licencjonowanie	- w całym okresie trwania subskrypcji użytkownik ma możliwość pobierania i instalacji nowszych wersji oprogramowania i konsoli zarządzającej; - w razie konieczności producent ma obowiązek dostarczyć nowe numery licencji jeśli dotychczasowe nie będą zgodne z nową wersją programu mimo ważnej licencji - licencja musi zagwarantować ochronę
Czas trwania subskrypcji	min. 60 miesięcy

Wszystkie komputery dostarczone w ramach PIAP zostaną skonfigurowane do pracy domenowej. Dla każdego PIAP zostanie założona osobna jednostka organizacyjna z użytkownikiem o prawach administratora przypisany tylko do danego PIAP. W każdym PIAP zostaną założeni unikalni użytkownicy. W każdym PIAP zostaną założeni unikalni użytkownicy, tzn. jeden unikalny na każdy PIAP. Zostanie założony współdzielony katalog w każdym PIAP z dostępem dla użytkowników tego PIAP. W całej domenie zostanie zaimplementowany system dystrybucji aktualizacji dla Systemu operacyjnego, system dystrybucji oprogramowania systemu operacyjnego stacji roboczych.
Wykonawca skonfiguruje do pracy sieciowej dostarczone urządzenia wielofunkcyjne. w poszczególnych PIAP tak, aby mogły ich używać zainstalowane tam komputery.

Wykonawca dostarczy, skonfiguruje i uruchomi dwa PIAP'y mobilne o minimalnych wymaganiach techniczno-funkcjonalnych:

PIAP mobilny złożony z rozkładanego masztu, z access pointa oraz systemu bezpieczeństwa

wizyjnego zabezpieczającego PIAPa przed kradzieżą, okablowania podłączającego. PIAP mobilny musi obsługiwać standardy minimum 802.11a/b/g. Maszt na którym ma być instalowany PIAP musi być rozkładany w sposób pneumatyczny, teleskopowy, musi gwarantować stabilność konstrukcji i wysokość minimum 4 m. Jego montaż i demontaż musi być możliwy przez maksymalnie 2 osoby. Na maszcie musi być zamocowany hotspot oraz kamera o minimalnych parametrach:

Przeznaczenie do zastosowań zewnętrznych,
Przeznaczenie do pracy w trybie ciągłym 24/7/365,
Przetwornik CMOS nie mniejszy niż 1/2,8”,
Czułość nie gorsza niż kolor: 0,8 Lux, B-W: 0,04 Lux (dla 30 IRE),
Transmisja obrazu w formie cyfrowej poprzez siec IP,
Sterowanie PTZ w formie cyfrowej poprzez sieć IP,
Co najmniej 20x zoom optyczny,
Co najmniej 12x zoom cyfrowy,
Kodowanie obrazu co najmniej H.264 oraz MJPEG,
Rozdzielczości HDTV 1080p (1920x1080) przy 25 klatkach na sekundę,
Możliwość generowania 3 strumieni wizyjnych w pełniej rozdzielczości HDTV 1080p,
Możliwość generowania 3 strumieni wizyjnych o różnych parametrach obrazu,
Możliwość zdefiniowania co najmniej 99 presetów (pozycji),
Kąt obrotu (PAN) 360° bez punktu końcowego,
Kąt pochylenia (TILT) 220°,
Szybkość obrotu w poziomie co najmniej 450°/s,
Możliwość nakładania tekstu na wyświetlany obraz,
Złącze Ethernet 10 BaseT / 100 BaseTX,
Wsparcie co najmniej dla następujących protokołów sieciowych:
IPv4, IPv6, HTTP, HTTPS, QoS l.3, FTP, SMTP, SNMPv3, DNS, DynDNS,
NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP,
Transmisja unicast oraz multicast,
Możliwość ustawienia transmisji Constant Bit Rate (CBR),
Możliwość ustawienia transmisji Variable Bit Rate (VBR),
Możliwość rejestracji trasy PTZ,
Możliwość ustawienia co najmniej 8 stref prywatności,
Możliwość filtrowania adresów IP,
Możliwość ochrony dostępu hasłem,
Kamera wraz z elementami grzewczymi i wentylatorami powinna być zasilana za pomocą pojedynczego kabla sieciowego wpiętego do kamery,
Obudowa co najmniej IP66,
Pracę w zakresie temperatur co najmniej od -40 °C do +50 °C,
Waga urządzenia: nie więcej niż 5kg.

Do PIAPa wykonawca dostarczy przenośne okablowanie wraz z zabezpieczeniami umożliwiające zasilenie logiczne i elektryczne PIAPa z założeniem odległości minimum 120 metrów od najbliższego optycznego punktu styku z siecią optyczną. Wykonawca dostarczy

szafkę przyłączeniową mobilną złożoną z zabezpieczeń elektrycznych, panela optycznego oraz switcha umożliwiającego podłączenie do sieci optycznej kamery oraz hotspota.

Wykonawca dostarczy, skonfiguruje i uruchomi 13 PIAP'ów typu hotspot o minimalnych wymaganiach techniczno-funkcjonalnych:

Wykonawca dostarczy i zamontuje 13 PIAP'ów typu hotspot o parametrach: Obsługa standardu a/b/n kompatybilne z ZSBME, wykonane w obudowie zewnętrznej odpornej na warunki atmosferyczne. Do zadań Wykonawcy należy dostarczenie wszystkich niezbędnych elementów i uruchomienie hotspotów w poniższych lokalizacjach:

1. 3 szt. Wykonawca zainstaluje na terenie Parku wodnego w Ełku przy ulicy Marsz. J. Piłsudskiego 29
2. 1 szt. Wykonawca zainstaluje na terenie parku linowego położonego przy ulicy Grunwaldzkiej.
3. 1 szt. Wykonawca zainstaluje na budynku UM przy ulicy Piłsudskiego 8
4. 2 szt. Wykonawca zainstaluje na budynku UM przy ulicy Piłsudskiego 4
5. 1 szt. Wykonawca zainstaluje na terenie skweru miejskiego na skrzyżowaniu ul W. Polskiego z Zamkową.
6. 1 szt. Wykonawca zainstaluje na terenie amfiteatru w ECK przy ulicy W. Polskiego 47
7. 1 szt. Wykonawca zainstaluje na Punkcie bezpieczeństwa wizyjnego nr 2 - zlokalizowanym na skrzyżowaniu ulicy Jana Pawła II z ulicą Grajewską
8. 1 szt. Wykonawca zainstaluje obok punktu wizyjnego zlokalizowanego na promenadzie Jeziora Ełckiego w okolicach pomostu.
9. 2 szt. Wykonawca zainstaluje w Szkole Podstawowej numer 5 przy ulicy św. M.M. Kolbego 11.

Zamawiający informuje, iż we wszystkich powyższych lokalizacjach dysponuje infrastrukturą, do której można podłączyć hotspoty.

IV. Zapasowe Centrum Zarządzania Siecią

Wykonawca w ramach niniejszego zadania dokona adaptacji pomieszczenia kontenera telekomunikacyjnego znajdującego się w pobliżu komina PEC w Ełku przy ulicy Ciepłej i dostosuje go do pełnienia funkcji Zapasowego Centrum Zarządzania Siecią (ZCZS) poprzez:
- wykonanie adaptacji budowlanej polegającej na usunięciu ubytków i pomalowaniu wewnętrznej części kontenera o zewnętrznych wymiarach: 235cm x 375 cm i wysokości 265 cm;
- wykonanie systemu zabudowy 19" złożonego z dwóch szaf serwerowych 19" o wysokości 42 u każda i głębokości 1000 mm;
- wykonanie systemu zasilania (rozdzielnia elektryczna) przystosowanej do zasilania ZCZS z uwzględnieniem podłączenia UPS oraz zewnętrznego generatora prądu;
- wykonaniu oświetlenia wnętrza kontenera, złożonego z minimum 2 źródeł światła;
- wykonanie systemu klimatyzacyjnego złożonego z dwóch klimatyzatorów przystosowanych do pracy w serwerowni o mocy chłodzącej min. 3 KW każdy; klimatyzatory muszą być spięte ze sobą i pracować zamiennie, naprzemiennie i razem;

- wykonanie systemu alarmowego kompatybilnego z używanym systemem w Zintegrowanym Systemem Bezpieczeństwa Miasta Ełku (ZSBME) złożonego z centrali, modułu powiadamiania GSM, i minimum 2 czujek.
- wykonanie systemu monitoringu złożonego z minimum dwóch kamer IP z czego jedna musi być umieszczona wewnątrz kontenera, a druga na zewnątrz. System musi być kompatybilny z Zintegrowanym Systemem Bezpieczeństwa Miasta Ełku (ZSBME).
- Wykonanie kontroli dostępu poprzez wymianę zamków na zamki patentowe oraz instalację systemu KD kompatybilnego z ZSBME
- dostawa i montaż czterech listew 8 portowych przystosowana do zabudowy w szafie serwerowej typu rack 19". Listwa 1U wysokości. Wyposażona jest w złącza sieciowe 10/100 Mbit, umożliwiające zdalny monitoring poboru mocy oraz alarmowanie w wypadku przekroczenia zadanych stanów poprzez wysyłanie e-mail lub SNMP. Możliwe zdalne (przez interfejs www) włączenie/ wyłączenie każdego gniazda oddzielnie oraz dokonywanie pomiaru parametrów zasilania, w tym także łącznego poboru mocy (na całej listwie). Minimalne obciążenie 16 A dla całej listwy. Kontrola gniazda - możliwość kontrolowania każdego gniazda osobno (włącz./wyłącz.), możliwość definiowania sekwencyjnego włączania/wyłączania zasilania, kontrola obciążenia: łączna dla całego urządzenia, 8 x IEC 320 C13, złącze sieciowe - 1 x RJ45 Ethernet, napięcie pracy - 230 V

V. Link radiowy

Zadaniem Wykonawcy jest dostarczenie, zamontowanie i uruchomienie linku radiowego umożliwiającego podłączenie cmentarza komunalnego w Bartoszach do sieci szerokopasmowej jako węzeł dostępowy. Stacja bazowa systemu radiowego zainstalowana zostanie na kominie żelbetowym PEC zlokalizowanym w Ełku przy ulicy Ciepłej. Komin o wysokości 120 m jest własnością Miasta Ełku. W celu mocowania anten na kominie należy zaprojektować konstrukcje wsporcze dla anten spełniające wymogi prawa budowlanego. Konstrukcje podantenowe nie mogą ingerować w poszycie komina. Kable sygnałowe łączące urządzenia zewnętrzne i wewnętrzne mocowane będą do istniejącej drabiny kablowej zainstalowanej na kominie. Kable należy układać w peszlu odpornym na warunki atmosferyczne oraz mocować za pomocą opasek stalowych. Peszel należy trwale oznaczyć w celu identyfikacji właściciela. Mocowania do drabiny co ok. 0,5m, aż do podstawy komina. Pomiędzy kominem a ZCZS, kable należy prowadzić pod ziemią w rurze arota o średnicy min 100 mm. Rura musi być zabezpieczona przed wnikaniem wody. Wejście do szafy telekomunikacyjnej za pomocą otworu w fundamencie. Konstrukcje wsporcze dla anten, nadajniki oraz urządzenia wewnętrzne należy uziemić do istniejącej instalacji odgromowej. Dodatkowo należy użyć zabezpieczeń przeciwprzepięciowych na kablach sygnałowych zabezpieczających zarówno urządzenia wewnętrzne jak i zewnętrzne. Oznaczenia kabli powinny się znajdować wewnątrz jak i na zewnątrz szafy zewnętrznej, a także na dole komina oraz przy nadajnikach. Druga końcówka linku zostanie zainstalowana na maszcie na cmentarzu komunalnym w Bartoszach. Zamawiający posiada przygotowane miejsce do montażu masztu, w miejscu tym jest doprowadzony od GPD światłowód oraz zasilanie elektryczne, Wykonawca dostarczy maszt w formie masztu reklamowego z dwoma tablicami w kształcie V o wysokości umożliwiającej osiągnięcie widoczności optycznej pomiędzy masztem a kominem PEC (instalacja zgodnie z przepisami prawa budowlanego – uzyskanie wszelkich zgód i pozwoleń należy do Wykonawcy).
Wykonawca ma obowiązek zbudować link radiowy składający się urządzeń, dla których określono następujące minimalne wymagania techniczno-funkcjonalne oraz objąć system 48 miesięczną gwarancją.

Minimalne wymagania techniczne dla systemu radiowego punkt-punkt:
Minimalna sumaryczna przepustowość 200Mb/s
Obsługiwane pasmo częstotliwości 5.4-5.7GHz ETSI;
Dostęp czasowy TDD (Time Division Duplex);
Zwielokrotnienie OFDM (Orthogonal Frequency Division Multiplexing);
Wykorzystanie technik antenowych MIMO 2x2 oraz Diversity;
Obsługiwane modulacje BPSK/QPSK/16QAM/64QAM;
Obsługiwane szerokości kanałów 10, 20, 40MHz;
Adaptacyjna modulacja i kodowanie;
Efektywność spektralna co najmniej 5 bit/s/Hz @ 10MHz;
Automatyczny wybór kanałów
Automatyczne żądanie retransmisji
Symetryczny i asymetryczny przydział ruchu co najmniej 90% w dowolnym kierunku;
Automatyczny przydział ruchu uplink i downlink w zależności od natężenia ruchu;
Maksymalne opóźnienia End-to-End <3ms;
Korekcja błędów min. FEC k= 1/2, 2/3, 3/4, 5/6;
Maksymalna szerokość ramki 2048 bajtów;
Wydajność sprzętowa co najmniej 360.000 PPS (Packets Per Second);
Sprzętowe szyfrowanie AES 128;
Możliwość synchronizacji czasu za pomocą GPS (Global Positioning System) oraz zegara wewnętrznego;
Możliwość konfigurowania QoS 4-go poziomu zgodnie z 802.1p i Diffserv;
Możliwość konfigurowania VLAN zgodnie z 802.1Q, 802.1P, QinQ;
Możliwość konfigurowania MIR (Maximum Information Rate) ze skokiem co najmniej 1kbps;
Wbudowany analizator widma;
Wspierana protekcja usług Ethernet 1+1 oraz Ring;
Dostępne interfejsy sieciowe Ethernet 10/100BaseT, 1000BaseT;
Możliwość lokalnej i zdalnej aktualizacji oprogramowania;
Zarządzanie radiolinią za pomocą dedykowanego oprogramowania, przeglądarki internetowej oraz protokołów SNMP (wersja 2c lub wyższa) i Telnet;
Zasilanie poprzez zasilacz sieciowy PoE (Power over Ethernet) -20-60VDC lub 230VAC;
Pobór mocy <35W (IDU+ODU);
Klasa szczelności urządzeń radiowych ODU IP67;
Zintegrowana antena panelowa o zysku co najmniej 23dBi;
Temperaturowy zakres pracy od -30 st C do 60st C;
Deklaracja zgodności CE;

VI. Sprzęt komputerowy.

Wykonawca dostarczy 16 szt. komputerów typu 1 wraz z pakietem biurowym, który musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:
1.Wymagania odnośnie interfejsu użytkownika:
a. Pełna polska wersja językowa interfejsu użytkownika.
2. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
a. posiada kompletny i publicznie dostępny opis formatu,

b. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526),
3. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców.
4.W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
5. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
6. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
a. Edytor tekstów
b. Arkusz kalkulacyjny
c. Narzędzie do przygotowywania i prowadzenia prezentacji
d. Narzędzie do tworzenia drukowanych materiałów informacyjnych
e. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
f. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.
7. Edytor tekstów musi umożliwiać:
a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
b. Wstawianie oraz formatowanie tabel.
c. Wstawianie oraz formatowanie obiektów graficznych.
d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
f. Automatyczne tworzenie spisów treści.
g. Formatowanie nagłówków i stopek stron.
h. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
i. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
j. Określenie układu strony (pionowa/pozioma).
k. Wydruk dokumentów.
l. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
m. Pełna zgodność z dokumentami utworzonymi przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
o. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
p. 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.

8. Arkusz kalkulacyjny musi umożliwiać:
a. Tworzenie raportów tabelarycznych
b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
g. Wyszukiwanie i zamianę danych
h. Wykonywanie analiz danych przy użyciu formatowania warunkowego
i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
k. Formatowanie czasu, daty i wartości finansowych z polskim formatem
l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
m. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
9. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
a. Przygotowywanie prezentacji multimedialnych, które będą:
b. Prezentowanie przy użyciu projektora multimedialnego
c. Drukowanie w formacie umożliwiającym robienie notatek
d. Zapisanie jako prezentacja tylko do odczytu.
e. Nagrywanie narracji i dołączanie jej do prezentacji
f. Opatrywanie slajdów notatkami dla prezentera
g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
j. Możliwość tworzenia animacji obiektów i całych slajdów
k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.
10. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:
a. Tworzenie i edycję drukowanych materiałów informacyjnych
b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.
c. Edycję poszczególnych stron materiałów.
d. Podział treści na kolumny.
e. Umieszczanie elementów graficznych.
f. wykorzystanie mechanizmu korespondencji seryjnej

g. Płynne przesuwanie elementów po całej stronie publikacji.
h. Eksport publikacji do formatu PDF oraz TIFF.
i. Wydruk publikacji.
j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.
11. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego
b. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców
c. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną
d. Automatyczne grupowanie poczty o tym samym tytule
e. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy
f. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia
g. Zarządzanie kalendarzem
h. Udostępnianie kalendarza innym użytkownikom
i. Przeglądanie kalendarza innych użytkowników
j. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach
k. Zarządzanie listą zadań
l. Zlecanie zadań innym użytkownikom
m. Zarządzanie listą kontaktów
n. Udostępnianie listy kontaktów innym użytkownikom
o. Przeglądanie listy kontaktów innych użytkowników
p. Możliwość przesyłania kontaktów innym użytkownikom.

Wykonawca dostarczy 3 komputery o parametrach:

Komputer stacjonarny. Komputer będzie wykorzystywany dla potrzeb obróbki grafiki, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
Procesor minimum czterordzeniowy
Pamięć operacyjna RAM 16 GB DDR3 1600MHz możliwość rozbudowy do min 32GB
Parametry pamięci masowej dysk systemowy SSD min 240 GB, Min. 2000 GB SATA 7200 obr./min
Dedykowana karta graficzna posiadająca własną pamięć RAM min.: 1GB umożliwiająca obsługę pełnej rozdzielczości monitora:
Zasilacz o mocy max. 390W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 90% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 87% przy obciążeniu zasilacza na poziomie 100%,
Zainstalowany system operacyjny umożliwiający podłączenie i pełna integrację z posiadaną przez Zamawiającego domeną AD opartą o Windows Server 2012.
Wykonawca dostarczy pakiet biurowy o parametrach opisanych w niniejszym punkcie tj punkcie „sprzęt komputerowy”
- Wbudowane porty:
min. 1 x RS232,
min. 1 x VGA,
min. 2 x PS/2,
min. 2 x DisplayPort v1.1a;

min. 10 portów USB wyprowadzonych na zewnątrz komputera w tym min 4 porty USB 3.0; min. 4 porty z przodu obudowy w tym 2 porty USB 3.0 i 6 portów na tylnim panelu w tym min 2 porty USB 3.0, wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy.
- Możliwość podłączenia dwóch pracujących równolegle dodatkowych zewnętrznych kart graficznych.
- Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL

Uwaga jeden z powyższych zestawów musi mieć zainstalowane minimum dwie karty graficzne umożliwiające łącznie podłączenie minimum 8 monitorów HD.

Monitor tego samego producenta co jednostka centralna o parametrach:
Monitor o minimalnych parametrach:
rodzaj matrycy TN
rodzaj podświetlenia LED
rozdzielczość nominalna 3840 x 2160 piksele
jasność 300 cd/m²
wielkość plamki 0.16 mm
czas reakcji plamki max5 ms
kąt widzenia pionowy 160 °
kąt widzenia poziomy 170 °
porty wejścia/wyjścia: mini DisplayPort, HDMI, 4 x USB 3.0, DisplayPort
spełniane normy jakościowe
kontrast: 1000:1
VESA 100 x 100 mm
Monitor musi posiadać trwałe oznaczenie logo producenta jednostki centralnej.
Na cały powyższy zestaw komputer wraz z monitorem gwarancja 3 lata na miejscu u Zamawiającego, czas reakcji serwisu - do końca następnego dnia roboczego w przypadku monitora gwarancja zero martwych pikseli.

Wykonawca dostarczy komputer o parametrach:

Komputer stacjonarny. Komputer będzie wykorzystywany dla potrzeb obróbki grafiki, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
Procesor minimum czterordzeniowy
Pamięć operacyjna RAM 16 GB DDR3 1600MHz możliwość rozbudowy do min 32GB
Parametry pamięci masowej dysk systemowy min 240 GB SSD, Min. 2000 GB SATA 7200 obr./min
Dedykowana karta graficzna posiadająca własną pamięć RAM min.: 1GB umożliwiająca obsługę pełnej rozdzielczości monitora:
Zasilacz o mocy max. 390W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 90% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 87% przy obciążeniu zasilacza na poziomie 100%,
Zainstalowany system operacyjny umożliwiający podłączenie i pełna integrację z posiadaną przez Zamawiającego domeną AD opartą o Windows Server 2012.

Zainstalowany pakiet biurowy o parametrach opisanych w niniejszym punkcie tj punkcie „sprzęt komputerowy”
- Wbudowane porty:
min. 1 x RS232,
min. 1 x VGA,
min. 2 x PS/2,
min. 4 x HDMI (zamawiający dopuszcza użycie przejściówek)
min. 10 portów USB wyprowadzonych na zewnątrz komputera w tym min 4 porty USB 3.0; min. 4 porty z przodu obudowy w tym 2 porty USB 3.0 i 6 portów na tylnim panelu w tym min 2 porty USB 3.0, wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy.
- Możliwość podłączenia dwóch pracujących równolegle dodatkowych zewnętrznych kart graficznych.
- Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL

Monitor o minimalnych parametrach:
Rodzaj panelu: Matryca AH-IPS z podświetleniem GB-R LED
Wielkość ekranu 24.1”
Proporcje obrazu 16:10
Rozmiar plamki [mm]: 0.270
Jasność [cd/m²]: 340
Kontrast: 1000:1
Kąty widzenia [°]: 178 poziomo / 178 pionowo
Kolory [miliard]: 1,074 (10 bitów na kolor)
Rozmiar Gamutu Barwowego/ Pokrycie: 108.6% / 99.3% Adobe RGB
Częstotliwość pozioma [kHz]: 31.5 - 93.8 and 118.4 (analog); 31.5 - 91.1 and 118.4 (digital)
Częstotliwość pionowa [Hz]: 50 – 85
Wbudowany czujnik autokorekcji RGB
ROZDZIELCZOŚĆ
Rozdzielczość optymalna: 1920 x 1200 przy 60 Hz
Mocowanie VESA [mm]: 100 x 100 (4 otwory)
Złącze Kensington: tak
Advanced Non-Touch-Auto-Adjustment
sześcioosiowa kontrola koloru
regulacja poziomu czerni
regulacja temperatury barwowej
reprodukcja zakresy barwne: 100% ISO Coated v2, 100% sRGB, 99,3% AdobeRGB, 94% ECI-RGB v2.0.
Na cały powyższy zestaw komputer wraz z monitorem gwarancja 3 lata na miejscu u Zamawiającego, czas reakcji serwisu - do końca następnego dnia roboczego w przypadku monitora gwarancja zero martwych pikseli.

Wykonawca dostarczy, skonfiguruje i uruchomi dwa urządzenia wielofunkcyjne o parametrach:
specyfikacja kopiarki:
Prędkość druku / kopiowania A4 w czerni 35 str./min.
Prędkość druku / kopiowania A4 w kolorze 35 str./min.

Prędkość druku / kopiowania A3 w czerni 15 str./min.
Prędkość druku / kopiowania A3 w kolorze 15 str./min.
Prędkość w dupleksie A4 w czerni 30 str./min.
Prędkość w dupleksie A4 w kolorze 33 str./min.
Czas pierwszej kopii / wydruku w czerni max 8 sek.
Czas pierwszej kopii / wydruku w kolorze max 8 sek.
Rozdzielczość kopiowania (dpi) 600 x 600
Skala szarości 256 odcieni
Kopiowanie wielokrotne 1-9999
Format oryginału A5-A3
Skalowanie 25-400%
Specyfikacja drukarki:
Rozdzielczość drukowania (dpi) 1800 x 600
Język opisu strony PostScript 3
Specyfikacja skanera:
Rozdzielczość skanowania (dpi): 600 x 600
Skanowanie do email
Skanowanie do SMB/LAN
Skanowanie do FTP
Skanowanie do Skrzynki Użytkownika
Skanowanie do USB
Skanowanie sieciowe TWAIN
Formaty plików JPEG; TIFF; PDF; PDF
obsługa LDAP
Specyfikacja systemu:
Standardowa pamięć systemu (MB) 2,048
Standardowy dysk twardy (GB) 250
Standardowe interfejsy 10-Base-T/100-Base-T/1000-Base-T Ethernet
USB 2.0
Protokoły sieciowe TCP/IP (IPv4 / IPv6); IPX/SPX; NetBEUI; AppleTalk (EtherTalk); SMB; LPD; IPP; SNMP; HTTP
Rodzaje ramek Ethernet 802.2; Ethernet 802.3; Ethernet II; Ethernet SNAP
Automatyczny podajnik dokumentów 100 oryginałów; A6-A3; 35-163 g/m²
Rozmiar papieru A6-A3,
Gramatura papieru (g/m²) 52-300 g/m²
Urządzenie wyposażone w wyświetlacz dotykowy o przekątnej minimum 7”
Pojemniki papieru:
Taca 1: 500 arkuszy, A5-A3, 52-256 g/m²
Taca 2: 500 arkuszy, A5-SRA3, 52-256 g/m²
Taca 3: 500 arkuszy, A5-A3, 52-256 g/m²
Podstawa pod urządzenie.
Automatyczny dupleks A5-SRA3; 52-256 g/m²
Pobór energii 220-240 V / 50/60 Hz
szyfrowanie danych na dysku twardym (AES 128);
automatyczne usuwanie danych z pamięci; odbieranie poufnych faksów; szyfrowanie danych druku użytkownika;
minimum 2500 kont użytkowników; obsługa Active Directory
Definiowanie dostępu funkcji użytkownika
Gwarancja na urządzenie 36 miesięcy.

Wykonawca dostarczy 10 szt. laptopów w tym
6 szt. laptopów typu 1,
2 szt. laptopów o parametrach minimalnych:
Procesor wielowątkowy minimum czterordzeniowy 2.8 GHz, 6MB Cache
Monitor 39.6cm (15.6") FHD (1920x1080)
RAM: 16GB (2x8GB) 1600MHz DDR3L Memory
HDD: 512GB SSD 2.5 - SATA 6Gb/s,
DVD +/-RW
Dedykowana karta graficzna z własną pamięcią 2GB GDDR5
Obsługa 802.11n
Zainstalowany system operacyjny typu 1.
dwa laptopy wykonawca ma dostarczyć w ramach PIAPów.

VII. Modernizacja centrum zarządzania siecią

W ramach modernizacji centrum zarządzania siecią Wykonawca wykona zamaskowania zewnętrznych modułów agregatów systemu klimatyzacyjnego serwerowni znajdującego się na stojaku umieszczonym przy elewacji budynku UM przy ulicy Piłsudskiego 4, Wykonawca umieści stelaż a na nim siatkę typu reklamowego z nadrukiem przypominającym elewację budynku tak aby zamaskować agregaty i jednocześnie nie utrudnić warunków ich pracy.
Wykonawca dostarczy dla Zamawiającego 4 serwerowe dedykowane moduły 16GB RAM do posiadanych przez Zamawiającego serwerów IBM Blade hs22 2x xeon e5507 2,27 Ghz, oraz 4 serwerowe dedykowane moduły 16GB RAM do posiadanych przez Zamawiającego serwerów IBM Blade hs23 2x xeon E5-2403 1,8 Ghz
Wykonawca rozbuduje posiadany przez zamawiającego serwer wizyjny Eyevis NPX-4800 o kartę sprzętową posiadającą minimum wejścia 2x RGB/ DVI/HDMI o rozdzielczości minimum 1920x1200.

Wykonawca dostarczy następujące oprogramowanie:

2 licencje systemu relacyjnych baz danych z licencją do zastosowania w edukacji: serwer relacyjnej bazy danych (SRB) musi spełniać następujące wymagania poprzez wbudowane mechanizmy:
1. Możliwość wykorzystania SRB jako silnika relacyjnej bazy danych, wielowymiarowej bazy danych oraz platformy bazodanowej dla wielu aplikacji, narzędzi raportowania i analiz biznesowych,
2. Kompresja kopii zapasowych - SRB musi pozwalać na kompresję kopii zapasowej danych (backup) od razu w czasie jej tworzenia. Powinna to być cecha SRB niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.
3. Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników lub zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników).
4. Możliwość definiowania zasad administracyjnych dla serwera lub grupy serwerów - SRB musi mieć możliwość automatyzacji zadań administracyjnych przez definiowanie reguł wymuszanych potem przez system. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów (np. tabel, procedur, baz danych, widoków) o

zdefiniowanych przez administratora nazwach lub ich fragmentach. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności ze wskazanymi regułami działającego systemu bez wpływu na jego funkcjonalność.
5. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - SRB musi pozwalać na definiowanie rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych bez ujemnego wpływu na wydajność rozwiązania. Między innymi wymagane są:
- odczyt lub zapis danych na dysku dla wyszczególnionego zapytania (w celu wychwytywania zapytań znacząco obciążających system),
- wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur),
- para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy takim jak np. tabela (w celu wychwytywania długotrwałych blokad obiektów bazy).
6. Rejestracja zdarzeń powinna pozwalać na selektywne ich wychwytywanie (rejestrowanie tylko zdarzeń spełniających zdefiniowane warunki filtrujące, np. dotyczących tylko wskazanego obiektu).
7.Zarządzanie serwerem za pomocą skryptów - SRB musi udostępniać mechanizm zarządzania silnikiem bazy danych za pomocą skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.
8. Możliwość wywoływania procedur składowanych, jako usług sieci Web (WebServices) - SRB musi umożliwiać tworzenie procedur składowanych, które mogę być udostępnione i wywoływane, jako WebServices bez wykorzystania dodatkowego oprogramowania.
9. Wysoka dostępność - SRB musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech:
- bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SRB),
- niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe),
- klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,
- czas przełączenia na system zapasowy poniżej 10 sekund.
10. SRB musi umożliwiać tworzenie klastrów niezawodnościowych.
11. Wykonywanie typowych zadań administracyjnych w trybie on-line - SRB musi umożliwiać wykonywanie typowych zadań administracyjnych (indeksowanie, backup, odtwarzanie danych) bez konieczności przerywania pracy systemu lub przechodzenia w tryb jednoużytkownikowy (operacje w trybie on-line).
12. Możliwość automatycznej aktualizacji systemu - SRB musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).
13. Definiowanie nowych typów danych - SRB musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków” obiektu, „rodzica” itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Dostawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji.
14. Wsparcie dla technologii XML - SRB musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML.
W szczególności musi:

- udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,
- udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD,
- udostępniać język zapytań do struktur XML,
- udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML),
- udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.

15. Obsługa błędów w kodzie zapytań - język zapytań i procedur w SRB musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.
16. Możliwość tworzenia rekursywnych zapytań do bazy danych - SRB musi udostępniać wbudowany mechanizm umożlwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny.
17. Dedykowana sesja administracyjna - SRB musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.
18. Wsparcie dla danych przestrzennych SRB musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności:
- zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów,
- oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp.,
- obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SRB,
- typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja (punkt), seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.).

19. Raportowanie zależności między obiektami SRB musi udostępniać obiekty systemowe do raportowania zależności między obiektami baz danych. Mechanizm ten powinien umożliwiać m.in. uzyskanie informacji o referencjach między obiektami, czyli które obiekty bazy danych odwołują się do innych obiektów.
20. Mechanizm blokowania planów wykonania zapytań do bazy danych SRB musi udostępniać mechanizm pozwalający na zablokowanie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Mechanizm ten ma umożliwiać przenoszenie systemów między serwerami (środowisko testowe i produkcyjne), migrację do innych wersji SRB lub wprowadzanie zmian sprzętowych w serwerach. Mechanizm ma umożliwiać przewidywalność czasu odpowiedzi na zapytania.
21. Zarządzanie pustymi wartościami w bazie danych - SRB musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci.
22. System transformacji danych SRB musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą

operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.
- mechanizm debuggowania tworzonego rozwiązania,
- mechanizm stawiania „pułapek" (breakpoints),
- mechanizm logowania do pliku wykonywanych przez transformację operacji,
- możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu),
- możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo)
- mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli),
- mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach),
- mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego,
- mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiany źródła danych.

23. Wbudowany system analityczny SRB musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (kostki OLAP). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina.
24. SRB musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail).
25. SRB musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki).
26. System powinien posiadać narzędzie do rejestracji i śledzenia wykonywanych zapytań .
27. System powinien obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).
28. Wbudowany system analityczny musi udostępniać rozwiązania Data Mining (m.in. algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system powinien udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli.
29. System analityczny powinien pozwalać na dodawanie własnych algorytmów oraz modułów wizualizacji modeli Data Mining.

30. Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators) - SRB musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu.
31. System raportowania - SRB musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki) bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania powinien obsługiwać:
- raporty parametryzowane,
- cache raportów (generacja raportów bez dostępu do źródła danych),
- cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych z różnymi wartościami parametrów),
- współdzielenie predefiniowanych zapytań do źródeł danych,
- wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File),
- możliwość opublikowania elementu raportu (wykresu, tabeli) do współdzielonej biblioteki, z której mogą korzystać inni użytkownicy, tworząc nowy raport ze znajdujących się w bibliotece elementów raportowych,
- możliwość wizualizacji wskaźników KPI,
- możliwość wizualizacji danych w postaci obiektów sparkline.
32. Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).
33. Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel (od wersji 1997 do 2010), Microsoft Word (od wersji 1997 do 2010), HTML, TIFF. Dodatkowo raporty powinny być eksportowane w formacie Atom data feeds, które można będzie wykorzystać jako źródło danych w innych aplikacjach.
34. SRB musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów.
35. SRB musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja).
36. Wbudowany system raportowania powinien posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.
37. Zintegrowanie narzędzia do zarządzania systemem – SRB musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia i wykonywania skryptów zarządzających SRB oraz silnikiem baz wielowymiarowych OLAP.
38. Możliwość tworzenia funkcji i procedur w innych językach programowania - SRB musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego SRB. System powinien umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo powinien udostępniać środowisko do debugowania.

2 licencje sieciowych systemów operacyjnych typu 2 z licencją do zastosowań edukacyjnych.

Bezpieczna Platforma Modułów Aplikacyjnych

4 licencje Oprogramowanie wirtualizacyjne o parametrach:
Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych.
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.
Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
- Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
- Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
- Obsługi 4-KB sektorów dysków
- Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
- Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
- Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model)
Zamawiający dopuszcza możliwość iż jeżeli powyższe wymagania w zakresie oprogramowania wirtualizacyjnego spełnią dostarczone systemy operacyjne to Wykonawca zwolniony jest z konieczności dostarczania dodatkowego oprogramowania wirtualizacyjnego.

Oprogramowanie graficzne o minimalnych właściwościach:
Możliwości pakietu:
- edycja grafiki wektorowej z układem stron
- edycja zdjęć
- przekształcanie map bitowych w grafiki wektorowe
- narzędzia do przechwytywania zawartości ekranu
Licencja dla szkół podstawowych, średnich i gimnazjów umożliwiająca uruchomienie pakietu w 12 piapach złożonych z minimum 15 komputerów każdy.
Pełna zgodność z plikami crd.

Oprogramowanie antywirusowe. O minimalnych wymaganiach:

System musi wspierać min. następujące systemy operacyjne	Windows XP SP2 lub nowszy Windows Vista 32 i 64bit Windows 7 32 i 64bit Windows 8 32 I 64bit Windows Server 2003 SP2 lub nowszy Windows Server 2008 32 i 64bit Windows Server 2008 R2 32 i 64bit Windows SBS Server 2011 32 i 64bit Windows Server 2012
System musi wspierać min. następujące aplikacje	MS SharePoint Services 2.0/3.0 MS SharePoint Server 2003/2007/2010 MS Exchange 2003/2007/2010 (tylko Internet Security Business)
System musi realizować ochronę przed zagrożeniami wspierając następujące minimalne funkcjonalności:	- ochrona przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem (w tym Java i ActiveX); - wykrywanie oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich; - skanowanie skryptów napisanych w językach VB Script i Java Script wykonywane przez system operacyjny Windows; - wykrywanie rootkitów - moduł oceny wyników wyszukiwania w głównych wyszukiwarkach w czasie rzeczywistym - monitorowanie adresów URL w czasie rzeczywistym - funkcja inteligentnego skanowania automatycznie przełączająca tryb skanowania w wyższy lub niższy priorytet odpowiednio do wykorzystania zasobów przez użytkownika - ochrona przed phishingiem; - ochrona przed dialerami; - możliwość zdefiniowania portów, które będą monitorowane lub wykluczone z monitorowania przez moduły skanujące ruch sieciowy (z wyłączeniem zapory ogniowej); - monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera działający nieprzerwanie do momentu zamknięcia systemu operacyjnego; - dedykowany moduł ochrony tożsamości, który posiada własną, wyspecjalizowaną bazę sygnatur do wykrywania keyloggerów - moduł ochrony tożsamości powinien dodatkowo oferować funkcjonalność monitorowania zachowań podejrzanych aplikacji i blokować próby przejęcia danych logowania użytkownika
Skanowanie w czasie rzeczywistym	- uruchamianych, otwieranych, kopiowanych, przenoszonych lub tworzonych plików; - pobieranej z Internetu poczty elektronicznej (wraz z załącznikami) po protokołach POP3, SMTP, IMAP (także szyfrowanych z wykorzystaniem SSL/TLS) - możliwość zmiany nazwy lub usuwania określonych typów załączników; - Opcja modyfikowania tematu wiadomości jeśli zostanie w niej wykryty wirus.
Wyszukiwanie heurystyczne	- wyszukiwanie heurystyczne bazujące na analizie kodu potencjalnego wirusa;
Archiwa	- leczenie i usuwanie plików z archiwów następujących formatów: ZIP, RAR, 7z, CAB;

	- skanowanie archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia;
Działanie programu po wykryciu infekcji	- podejmować zalecane działanie - próbować leczyć, a jeżeli nie jest to możliwe pytać użytkownika o działanie; - rejestrować w pliku raportu informację o wykryciu wirusa; - powiadamiać administratora przy użyciu poczty elektronicznej; - poddać kwarantannie podejrzany obiekt;
Zapora ogniowa (firewall)	- możliwość ustawienia predefiniowanych poziomów ochrony, w tym poziomu zapewniającego interakcję z użytkownikiem po wykryciu nowego połączenia (tryb uczenia zapory) oraz trybu automatycznego; - możliwość ręcznego tworzenia i modyfikacji reguł dostępu dla zainstalowanych aplikacji; - zdefiniowania reguł zezwalających na komunikację na określonym porcie niezależnie od reguł dla aplikacji; - zdefiniowania zaufanych podsieci, dla których nie będą stosowane żadne reguły zapory(sieci zaufane); - ochrony przed atakami sieciowymi; - oferować białą i czarną listę adresów IP dla których nie będą stosowane reguły, a ruch dla tych adresów będzie w całości dozwolony lub blokowany.
Płyta ratunkowa	- możliwość utworzenia płyty ratunkowej lub nośnika USB lub płyty CD w oparciu o obraz w formacie ISO pobierany z serwerów producenta, umożliwiającego przeskanowanie dysków komputera bez uruchamiania systemu zainstalowanego na dysku; - płyta ratunkowa musi posiadać opcję aktualizacji sygnatur z Internetu, dysku lokalnego oraz innego nośnika np. usb. - płyta ratunkowa powinna oferować możliwość zarządzania kwarantanną utworzoną przez program na komputerze i pozwalać na przywracanie obiektów, które są niezbędne do poprawnego uruchomienia systemu - nośnik powinien zawierać również dodatkowe narzędzia naprawcze jak na przykład edytor rejestru
Wykorzystywanie zasobów systemowych	- możliwość dynamicznej zmiany użycia zasobów systemowych w zależności od obciążenia systemu przez aplikacje użytkownika;
Język	- polski, również dla konsoli zdalnej administracji; - dodatkowo powinien być instalowany również język angielski niezależnie od języka wybranego podczas instalacji; - możliwość łatwego przełączania interfejsu pomiędzy zainstalowanymi wersjami językowymi
Harmonogram	- umożliwiający modyfikowanie oraz tworzenie zadań aktualizacji komponentów programu, - sygnatur, - skanowania cyklicznego, Każde z tych zadań musi posiadać własne zadanie harmonogramu.
Blokowanie ustawień programu	- blokowanie dostępu do ustawień programu dla użytkowników w tym: zatrzymywania skanowania, wyłączania ochrony, dostępu do przywracania bądź usuwania obiektów z kwarantanny, przerywania aktualizacji; - możliwość całkowitego zablokowania dostępu do ustawień zaawansowanych lub interfejsu programu;

Wysyłanie podejrzanych obiektów	- możliwość wysyłania podejrzanych obiektów do producenta oprogramowania w celu przeprowadzenia analizy;
Informowanie użytkownika	- program powinien umożliwić administratorowi wyłączenie niektórych lub wszystkich powiadomień wyświetlanych na stacjach roboczych; - możliwość wyłączenia powiadomień o stanie składnika;
Aktualizacja	- antywirusowe bazy danych na serwerach producenta aktualizowane nie rzadziej niż raz na cztery godziny; - pobieranie uaktualnień w trybie przyrostowym;
Zdalne zarządzanie	- program (poprzez funkcjonalność w niego wbudowaną lub z wykorzystaniem dodatkowego modułu/ aplikacji) powinien umożliwiać zdalne zarządzanie oprogramowaniem i jego funkcjami. - przechowywać ustawienia w relacyjnej bazie danych MS SQL Server 2005/2008 również wersje Express, MySQL 5, Oracle 10/11, Firebird 2.0/2.5 - umożliwiać automatyczne i regularne tworzenie kopii zapasowej serwera zarządzającego, która umożliwi przywrócenie w pełni działającego systemu zarządzania; - powinien dostarczać własny silnik bazodanowy - umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych odpowiadających strukturze sieci (grupy robocze sieci Microsoft Windows i/lub struktura Active Directory) również w oparciu o zdefiniowane reguły; - umożliwiać tworzenie hierarchicznej struktury serwerów administracyjnych; - umożliwiać zarządzanie komputerami położonymi w różnych podsieciach; - umożliwiać zdalne zarządzanie o obiektami poddanymi kwarantannie oraz podejmowanie odpowiednich działań (np. przywracanie, usuwanie itp.); - umożliwiać przeglądanie informacji o obiektach, które zostały wykryte ale program nie podjął względem nich żadnego działania wraz z możliwością wymuszenia przez administratora odpowiedniego działania; - konsola administracyjna posiada możliwość zdalnego inicjowania skanowania antywirusowego na stacjach roboczych włączonych do sieci komputerowych w całej firmie (wszystkich podsieciach); - Konsola zdalnej administracji musi oferować możliwość zdalnego zarządzania konfiguracją komputerów, grup komputerów oraz całej sieci - musi ofertować funkcjonalność raportowania i powiadamiania mailem oraz generowania raportów i statystyk z pracy systemu antywirusowego na stacjach roboczych - raporty te powinny być dostarczane mailem zgodnie ze zdefiniowanym ręcznie harmonogramem - musi oferować opcję zdalnego restartowania i zamykania komputera na którym zainstalowany jest program - umożliwiać automatyczne aktualizacje licencji na stacjach roboczych; - system centralnej dystrybucji i instalacji aktualizacji oprogramowania, umożliwiający automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowego oprogramowania; - system centralnej dystrybucji i instalacji aktualizacji bibliotek sygnatur wirusów, umożliwiający automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowej wersji biblioteki - system administracji zdalnej nie może wymagać do działania żadnego serwera www (Apache, IIS itp.) - posiadający mechanizmy raportowania i dystrybucji oprogramowania oraz

	polityk antywirusowych w sieciach korporacyjnych;
Wsparcie	- w całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej, realizowanej w języku polskim; - pomoc techniczna telefonicznie, mailowo oraz w razie potrzeby z użyciem połączeń zdalnych
Licencjonowanie	- w całym okresie trwania subskrypcji użytkownik ma możliwość pobierania i instalacji nowszych wersji oprogramowania i konsoli zarządzającej; - w razie konieczności producent ma obowiązek dostarczyć nowe numery licencji jeśli dotychczasowe nie będą zgodne z nową wersją programu mimo ważnej licencji
Czas trwania subskrypcji	min. 60 miesięcy

VIII. Archiwum backupów

W ramach modernizacji CZS do zadań Wykonawcy należy wykonanie archiwum backupu które zostanie zlokalizowane w piwnicy Parku Naukowo-Technologicznego w Ełku. W ramach zadania wykonawca dostarczy:
I. Sejf do przechowywania nośników informatycznych magnetycznych i optycznych o wymiarach wysokość: 1850, szerokość: 675, głębokość: 616, pojemność dm3: 400 i minimalnych wymaganiach:

- I klasa odporności na włamanie zgodnie z normą EN 1143-1
- ognioodporność 60 P zgodny z normą NT Fire017
- zamek kluczowy klasy A. Natomiast w opcji, sejf można wyposażyć w zamek elektroniczny lub szyfrowy mechaniczny lub dwa zamki jednocześnie.
- przystosowany do przechowywania nośników magnetycznych i optycznych.
- wyposażony w 4 półki

II. Szafy na nośniki danych 4 szt o wymiarach: wysokość: 1900, szerokość: 1000, głębokość: 400, pojemność dm3: 800 i minimalnych wymaganiach:

- Korpus wykonany z blachy 1,0 mm, płaszcz zewnętrzny drzwi z blachy stalowej grubości 0,8 mm.
- Szafa wyposażona w rygle pionowe i poziome (po 2 sztuki),
- Korpus i drzwi wykonane z blachy stalowej o grubości 0,8 mm, nadającej odpowiednią sztywność oraz zabezpieczonej przed korozją.
- Wyposażone w zamek
- 4 półki

III. Adaptacja pod kątem bezpieczeństwa w ramach których Wykonawca wykona adaptację budowlaną polegającą na pomalowaniu pomieszczenia, wstawieniu drzwi antywłamaniowych wraz z zamkami, wykona połączenie logiczne złożone z 2 x 2xRJ46 od serwerowni zlokalizowanej w odległości ok. 10 m do której jest wykonany trakt kablowy z tegoż

pomieszczenia. Wykonawca umieści i podłączy do SZBME kamerę IP 2MP przy odświeżaniu 30 kl/s wyposażoną w podświetlacz podczerwieni.

IX. Serwery, serw. telekom wraz z oprogramowaniem

Wykonawca dostarczy cztery serwery o minimalnych wymaganiach
1 szt. serwera o minimalnych parametrach:

Obudowa typu Rack o wysokości maksymalnie 2U z możliwością instalacji minimum 48TB w wewnętrznej pamięci masowej typu Hot Plug 7.2k RPM.
Obudowa wraz z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem kabli.
Płyta główna z możliwością instalacji minimum dwóch fizycznych procesorów, posiadająca minimum 24 sloty na pamięci z możliwością zainstalowania do minimum 1.5TB pamięci RAM, możliwe zabezpieczenia pamięci: ECC, SDDC, Memory Mirroring Rank Sparing, SBEC. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
Dwa procesory min. sześciordzeniowe dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku łącznie minimum 230,40 Gflops w trybie standardowej pracy
Minimum 48 GB pamięci RAM typu RDIMM o częstotliwości taktowania minimum 2133 MHz
- minimum trzy sloty x16 generacji 3 o prędkości x8 niskoprofilowe
- minimum trzy sloty x16 generacji 3 o prędkości x8
- minimum jeden slot x16 generacji 3 o prędkości x16 pełnej długości i wysokości
Minimum 5 portów USB 2.0 z czego min. 2 w technologii 3.0 (porty nie mogą zostac osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń) 1x RS-232, 2x VGA D-Sub
Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Minimum dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseT, interfejsy sieciowe nie mogą zajmować żadnego z dostępnych slotów PCI Express. Wsparcie dla protokołów iSCSI Boot oraz IPv6. Możliwość instalacji wymiennie modułów udostępniających:
- dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+
- cztery interfejsy sieciowe 1Gb Ethernet w standarcie BaseT
- cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+

Kontroler dyskowy, umożliwiający obsługę dysków z prędkościami transferu 3, 6 oraz 12Gb/s obsługujący do 128 dysków, posiadający nieulotną pamięć cache min. 1GB, możliwość konfiguracji poziomów RAID :0, 1, 5,6,10,50,60.
Możliwość instalacji dysków SATA, NearLine SAS, SAS, SSD i SED dostępnych w ofercie producenta serwera.
Zainstalowane 2 dyski twarde o pojemności min. 300GB SAS 10k RPM każdy skonfigurowane fabrycznie w RAID 1
Możliwość instalacji wewnętrznej pamięci masowej typu flash, dedykowanej dla hypervisora wirtualizacyjnego, umożliwiającej konfigurację zabezpieczenia typu "mirror" lub RAID 1 z

poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wymaganych wnęk wnęk na dyski twarde.
Zainstalowany wewnętrzny napęd umożliwiający odczyt i zapis nośników DVD
Bezpieczeństwo i system diagnostyczny - Elektroniczny panel informacyjny umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze, adresach MAC kart sieciowych, numerze serwisowym serwera, aktualnym zużyciu energii, nazwie serwera, modelu serwera.
-Fabryczne oznaczenie urządzenia, wykonane przez producenta serwera informujące Zamawiającego m.in. o numerze serwisowym serwera, pełnej nazwie podmiotu Zamawiającego, modelu serwera; gwarantujące Zamawiającemu dostawę nowego, nieużywanego i nie pochodzącego z innych projektów sprzętu.
- Zintegrowany z płytą główną moduł TPM
- Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
- Fizyczne zabezpieczenie dedykowane przez producenta serwera uniemożliwiające wyjęcie dysków twardych umieszczonych na froncie obudowy przez nieuprawnionych użytkowników.
System operacyjny Zainstalowany fabrycznie Microsoft Windows Server 2012 R2 Standard wraz z nośnikiem DVD.
Chłodzenie i zasilanieMinimum sześć wewnętrznych redundantnych wentylatorów typu Hot Plug
Dwa redundantne zasilacze Hot Plug o mocy minimum 750 Wat każdy wraz z kablami o dł. min. 2 m.
Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu,
W przypadku awarii dyski twarde pozostają własnością Zamawiającego.

Zainstalowany Sieciowy system operacyjny typu 2

2 szt. serwerów o minimalnych parametrach:

Obudowa typu rack o wysokości maksymalnie 2U z możliwością instalacji minimum 48TB w wewnętrznej pamięci masowej typu Hot Plug 7.2k RPM.
Obudowa wraz z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem kabli.
Płyta główna z możliwością instalacji minimum dwóch fizycznych procesorów, posiadająca minimum 24 sloty na pamięci z możliwością zainstalowania do minimum 1.5TB pamięci RAM, możliwe zabezpieczenia pamięci: ECC, SDDC, Memory Mirroring Rank Sparing, SBEC. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
Dwa procesory min. ośmiordzeniowe dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku łącznie minimum 332,80 Gflops w trybie standardowej pracy
Pamięć RAM Minimum 192 GB pamięci RAM typu RDIMM o częstotliwości taktowania minimum 2133 MHz
- minimum trzy sloty x16 generacji 3 o prędkości x8 niskoprofilowe
- minimum trzy sloty x16 generacji 3 o prędkości x8
- minimum jeden slot x16 generacji 3 o prędkości x16 pełnej długości i wysokości
Minimum 5 portów USB 2.0 z czego min. 2 w technologii 3.0 (porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń) 1x RS-232, 2x VGA D-Sub

Karta graficzna Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
Minimum dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseT, interfejsy sieciowe nie mogą zajmować żadnego z dostępnych slotów PCI Express. Wsparcie dla protokołów iSCSI Boot oraz IPv6. Możliwość instalacji wymiennie modułów udostępniających:
- dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+
- cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
- cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+
Kontroler dyskowy Kontroler dyskowy, umożliwiający obsługę dysków z prędkościami transferu 3, 6 oraz 12Gb/s obsługujący do 128 dysków, , posiadający nieulotną pamięć cache min. 1GB, możliwość konfiguracji poziomów RAID :0, 1, 5,6,10,50,60.
Wewnętrzna pamięć masowa Możliwość instalacji dysków SATA, NearLine SAS, SAS, SSD i SED dostępnych w ofercie producenta serwera.
Zainstalowane 2 dyski twarde o pojemności min. 300GB SAS 10k RPM każdy skonfigurowane fabrycznie w RAID 1
Możliwość instalacji wewnętrznej pamięci masowej typu flash, dedykowanej dla hypervisora wirtualizacyjnego, umożliwiającej konfigurację zabezpieczenia typu "mirror" lub RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wymaganych wnęk wnęk na dyski twarde.
Zainstalowany wewnętrzny napęd umożliwiający odczyt i zapis nośników DVD
Bezpieczeństwo i system diagnostyczny - Elektroniczny panel informacyjny umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze, adresach MAC kart sieciowych, numerze serwisowym serwera, aktualnym zużyciu energii, nazwie serwera, modelu serwera.
-Fabryczne oznaczenie urządzenia, wykonane przez producenta serwera informujące Zamawiającego m.in. o numerze serwisowym serwera, pełnej nazwie podmiotu Zamawiającego, modelu serwera; gwarantujące Zamawiającemu dostawę nowego, nieużywanego i nie pochodzącego z innych projektów sprzętu.
- Zintegrowany z płytą główną moduł TPM
- Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
- Fizyczne zabezpieczenie dedykowane przez producenta serwera uniemożliwiające wyjęcie dysków twardych umieszczonych na froncie obudowy przez nieuprawnionych użytkowników.
Dwa redundantne zasilacze Hot Plug o mocy minimum 750 Wat każdy wraz z kablami o dł. Min. 2m
Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu
W przypadku awarii dyski twarde pozostają własnością Zamawiającego.

Na powyższych serwerach zainstalowany sieciowy system operacyjny typu 1

Wykonawca dostarczy i wdroży kompletną konsola KVM umożliwiająca podłączenie 16 serwerów.
Charakterystyka konsoli:
zdalny dostęp po TCP/IP do 16 przełączników w wersji podstawowej
Panel Array Mode - jednoczesny widok wszystkich 16 portów na jednym ekranie
Możliwość podłączenia minimum 16 serwerów
zintegrowana konsola LCD 17"
Konstrukcja pozwala na niezależne złożenie klawiatury i monitora

Dostosowany do standardu 19", wysokość 1U
Podłączenie 16 serwerów
Minimalna odległość do serwerów 40m przy rozdzielczości 1280x1024 @ 60Hz
Możliwość podłączanie komputerów bez konieczności wyłączania przełączników
Dwa poziomy haseł - 4 użytkowników + administratora z osobnym profilem
Wylogowanie manualne lub automatyczne po określonym czasie bezczynności
Emulacja myszy i klawiatury PS/2
Możliwość aktualizacji oprogramowania
Obsługa IPv6
Konsola kompletna ze wszystkimi modułami, kablami i licencjami umożliwiająca podłączenie 16 serwerów USB.

Bezpieczna Platforma Uruchomieniowa Modułów Aplikacyjnych:
Wykonawca dostarczy licencje i skonfiguruje aplikacje wraz z możliwością pracy licencji dla jednostek edukacyjnych UM Ełk w ramach IT edu secure Server: modułów z zakresu finansowo-księgowego, kadrowo-płacowego i wszystkich innych które zapewnia integrację z posiadanym przez Zamawiającego systemem dziedzinowym wdrożonym w ramach projektu realizowanego przez Urząd Marszałkowski województwa warmińsko-mazurskiego - „Wrota Warmii i Mazur – elektroniczna platforma funkcjonowania administracji publicznej i świadczenia usług publicznych" Wykonawca powyższe moduły zainstaluje i skonfiguruje w sposób bezpieczny, zapewniający należyte zabezpieczenie danych wrażliwych przechowywanych w powyższych aplikacjach.

Na powyższych dostarczonych serwerach wykonawca wdroży:

1. Przygotowanie projektu systemu Private Cloud dla wdrażanego systemu wirtualizacji serwerów wraz z opracowaniem polityk dostępu do zasobów.
2. Wdrożenie zaprojektowanej przez zespół wdrożeniowy usługi w oparciu o zamówione oprogramowanie i dostarczony przez wykonawcę sprzęt.
3. Przed przystąpieniem do konfiguracji wykonawca zobowiązany jest do przygotowania projektu technicznego oraz planu wdrożenia.
4. Podłączenia serwerów do istniejącej infrastruktury sieciowej zgodnie z wytycznymi Zamawiającego.
5. Po zaakceptowaniu projektu rozwiązania uwzględniającego wymagania Zamawiającego, oraz zaakceptowaniu planu wdrożenia Wykonawca zobowiązany jest do instalacji i konfiguracji serwerów zgodnie z przyjętym projektem i harmonogramem.
6. Instalacji fizycznej urządzeń w szafie RACK w miejscach wskazanych przez Zamawiającego.
7. Konfiguracji systemu przełączająco-zarządzającego w tym:
•Konfiguracji Klastra Wysokiej Dostępności
•Konfiguracji zarządzania;
8. Przygotowania procedur testowych potwierdzających zgodność zainstalowanych serwerów z wymaganiami SIWZ
9. Opracowanie, instalacja i konfiguracja systemu do wirtualizacji serwerów mającego na celu podniesienie wydajności środowiska przy zachowaniu najwyższego poziomu dostępności usług zainstalowanych w tym środowisku. Wykonawca ma za zadanie:
• Zainstalowanie i skonfigurowanie na dostarczonych serwerach systemu opecyjnego.
• Instalacja platformy wirtualizacji na dostarczonych serwerów.

• Przygotowanie projektu infrastruktury wirtualizacji serwerów, z zapewnieniem mechanizmów wysokiej dostępności środowiska.
• Przygotowanie schematu połączeń platformy wirtualizacji z elementami sieci Ethernet, sieci SAN.
• Przygotowanie projektu integracji z systemami macierzowymi.
• Zainstalowanie i skonfigurowania serwera zarządzającego platformą wirtualizacji.
• Przygotowanie projektu systemu zarządzania platformą wirtualizacji zintegrowanego z wdrażaną usługą katalogową.
• Przygotowanie wzorcowych obrazów systemów wirtualnych „template".
• Przygotowanie projektu systemu monitoringu stabilności i wydajności systemu platformy wirtualizacji.
• Przygotowanie projektu systemu Private Cloud dla wdrażanego systemu wirtualizacji serwerów wraz z opracowaniem polityk dostępu do zasobów.
• Wdrożenie zaprojektowanej przez zespół wdrożeniowy usługi w oparciu o zamówione oprogramowanie i dostarczony przez wykonawcę sprzęt.
• Przeprowadzenie wdrożenia infrastruktury wirtualizacji należy przeprowadzić zgodnie z opracowanym w zespole schematem wdrożenia Wirtualizacji Serwerów.
• Przygotowanie i integracja wybranych przez Zamawiającego elementów systemu z rozwiązaniem Microsoft Office 365 wraz z migracją wskazanych danych i synchronizacją użytkowników.
• Po wdrożeniu wymagane jest opracowanie dokumentacji powykonawczej wszystkich wdrożonych elementów zamówienia oraz zaleceń powdrożeniowych. Dokumentacja musi zawierać:
a. Opis procesu instalacji i konfiguracji środowiska;
b. Schematy wdrożonego środowiska (połączenia między komponentami, połączenia fizyczne);
c. Procedury eksploatacyjne środowiska (tworzenie VM, obsługa kopii migawkowych, live migration, backup);
d. Procedury ratunkowe;
e. Procedury testowe.
• Po wdrożeniu systemu przeprowadzone zostaną testy funkcjonalne mające na celu zweryfikowanie poprawności konfiguracji środowiska zgodnie z założeniami projektowymi.
• Opracowanie i konfiguracja architektury dla usługi katalogowej w oparciu o dostarczone przez Wykonawcę oprogramowanie i urządzenia. Dla proponowanego rozwiązania na etapie wdrażania należy opracować następujące elementy:
a. Stworzenie projektu infrastruktury usług katalogowych zawierającego plan utworzenia od zera usług katalogowych, z zapewnieniem mechanizmów wysokiej dostępności. Awaria pojedynczego elementu nie może mieć negatywnego wpływu na dostępność zasobów dla użytkowników i usług.
b. Stworzenie projektu nazewnictwa obiektów w usługach katalogowych.
c. Projekt wewnętrznego DNS (intranet). Struktura wewnętrznego DNS zintegrowana z usługą usług katalogowych.
d. Projekt centralnego zarzadzania aktualizacjami zintegrowany z usługa katalogową.
• Dla wdrażanej usługi katalogowej wymagane jest opracowanie planu zawierającego diagram jednostek organizacyjnych.
• Wymagane jest przygotowanie projektu migracji stacji roboczych i istniejących serwerów do nowo wdrożonej usługi katalogowej:
a. Migrację zasobów z istniejących grup roboczych do usługi katalogowej
b. Migrację lokalnych profili użytkowników z stacji roboczych do usługi katalogowej

c. Migrację serwerów plików, wydruku i innych usług do struktur usługi katalogowej
d. Dla migrowanych zasobów należy nadać odpowiedne uprawnienia zgodnie z istniejącą polityką
• Projekt obejmuje wdrożenie spójnych polityk zabezpieczeń mających na celu podniesienie poziomu bezpieczeństwa systemu, oraz centralne sterowanie ustawieniami systemów włączonych do usług katalogowych
• Wdrożenie zaprojektowanej przez zespół wdrożeniowy usługi w oparciu o zamówione oprogramowanie i dostarczony przez Wykonawcę sprzęt.
• Przeprowadzenie wdrożenia infrastruktury usług katalogowych należy przeprowadzić zgodnie z opracowanym w zespole schematem wdrożenia.
• Po wdrożeniu niezbędne będzie opracowanie dokumentacji powykonawczej wszystkich wdrożonych elementów zamówienia oraz zaleceń powdrożeniowych. Dokumentacja musi zawierać:
a. Opis procesu instalacji i konfiguracji środowiska
b. Procedury eksploatacyjne środowiska w tym: migracji, modyfikacji (w tym zmian, dodawania, odblokowywania, tworzenia, przejmowania), konwersji, dystrybucji, odtwarzania, testowania, backupu oraz procedury ratunkowe
c. Procedury testowe
• Po wdrożeniu systemu zostaną przeprowadzone testy funkcjonalne mające na celu zweryfikowanie poprawności konfiguracji środowiska zgodnie z założeniami projektowymi.

Wykonawca zapewni instruktarz dla minimum pięciu wskazanych przez Zamawiającego osób w wymiarze 40 godzin zegarowych składające się z części teoretycznej i praktycznej, obejmującej tematykę instalacji i administracji oferowanym systemem operacyjnym, instruktarz musi być przeprowadzony przez certyfikowanego trenera dostarczanego oprogramowania. Instruktarz musi obejmować w szczególności tematykę:

- Zarządzanie dyskami przy wykorzystaniu zaoferowanych systemów operacyjnych
- Zarządzanie woluminami przy wykorzystaniu zaoferowanych systemów operacyjnych
- Zabezpieczanie dysków i woluminów
- Podstawowe topologie magazynowania i komponenty serwerowe
- Topologie magazynowania
- Technologie magistrali i protokoły
- Konfiguracja współdzielenia
- Implementacja deduplikacji danych
- Wysoka dostępność zaoferowanego środowiska serwerowego
- Definiowanie poziomów dostępności
- Wysoka dostępność i odzyskiwanie awaryjne z wykorzystaniem maszyn wirtualnych
- Wysoka dostępność i klaster pracy awaryjnej
- Implementacja klastra pracy awaryjnej
- Planowanie klastra
- Tworzenie nowego klastra
- Zarządzanie rolami serwerowymi i zasobami klastrowymi
- Konfiguracja aplikacji i usług wysokiej dostępności na klastrze

- Zarządzanie i utrzymanie klastra
- Rozwiązywanie problemów dotyczących klastra
- Implementacja wysokiej dostępności z wieloma klastrami
- Implementacja klastra pracy bezawaryjnej przy wykorzystaniu zaoferowanych systemów operacyjnych
- Omówienie aspektów integracji wirtualizacji z klastrem
- Zarządzanie i utrzymanie maszyn wirtualnych na klastrach
- Magazynowanie i wysoka dostępność w oparciu o chmurę
- Planowanie i implementacja strategii wirtualizacji serwera
- planowanie i implementacja środowiska utrzymania wirtualizacji serwera.
- Planowanie i implementacja wirtualizacji magazynów i sieci
- planowanie wirtualizacji dla infrastruktury magazynu
- implementacja wirtualizacji dla infrastruktury magazynu
- planowanie i implementacja wirtualizacji dla infrastruktury sieciowej.
- Planowanie i wdrażanie maszyn wirtualnych
- planowanie konfiguracji maszyny wirtualnej
- planowanie infrastruktury klastrów pracy awaryjnej
- implementacja klastrów pracy awaryjnej
- integracja klastrów pracy awaryjnej z wirtualizacją serwera
- planowanie klastrów pracy awaryjnej w środowisku wielolokacyjnym.
- Planowanie i implementacja infrastruktury aktualizacji serwera
- Planowanie i implementacja strategii ciągłości biznesowej
- planowanie i implementacja strategii kopii zapasowych
- planowanie i implementacja odtwarzania danych
- planowanie i implementacja kopii zapasowych maszyn wirtualnych i ich odtwarzania.
- Planowanie i implementacja infrastruktury kluczy publicznych
- planowanie i implementacja wdrażania urzędu certyfikatów
- planowanie i implementacja szablonów certyfikatów
- planowanie i implementacja dystrybucji i odwoływania certyfikatów
- planowanie i implementacja archiwizacji kluczy i ich odtwarzania.
- Planowanie i implementacja infrastruktury federacją tożsamości
- Planowanie i implementacja infrastruktury zarządzania prawami.

W celu realizacji zadania Wykonawca zapewni:

1. Licencje dostępowe muszą zapewniać dostęp minimum 135 klientów do oferowanych systemów serwerowych (łącznie) dla licencjonowania instytucji rządowych

2. Licencje dostępowe muszą zapewniać dostęp minimum 2400 klientów do oferowanych systemów serwerowych (łącznie) dla licencjonowania instytucji edukacyjnych

W ramach wdrożenia Zamawiający wymaga dokonania:

1. Migracji 10 serwerów do wdrażanej chmury prywatnej
2. Migracji 10 serwerów do istniejącego środowiska VMWare

W ramach wdrożenia Zamawiający wymaga wdrożenia usług certyfikacji:
W ramach wdrożenia infrastruktury klucza publicznego opartej na dostarczonym oprogramowaniu Wykonawca musi zrealizować:

1. Analizę i audyt polityki bezpieczeństwa oraz aktualnej konfiguracji infrastruktury informatycznej Zamawiającego, niezbędnych do prawidłowego funkcjonowania wdrażanego rozwiązania.

2. Projekt techniczny wdrażanej infrastruktury klucza publicznego obejmujący przynajmniej:
   • Architekturę i opis techniczny systemu
   • Szczegółowy opis konfiguracji usług
   • Dokumentację wdrożeniową
   • Opis ról administracyjnych

3. Opracowanie procedur operacyjnych, zgodnych z obowiązującą u Zamawiającego Polityką Bezpieczeństwa obejmujących:
   • Procedury tworzenia kopii zapasowych z wykorzystaniem procedury systemu posiadanego przez Zamawiającego
   • Procedury Disaster-Recovery
   • Procedury administracyjne, w tym procedury wydawania i unieważnienia certyfikatów oraz procedurę funkcjonowania punktów rejestracji
   • Procedury polityki bezpieczeństwa obejmujące Politykę Certyfikacji i Kodeks Postępowania Certyfikacyjnego oaz ewentualne rekomendacje dotyczące Polityki Bezpieczeństwa Zamawiającego

4. Wdrożenie infrastruktury klucza publicznego, obejmujące:

• Wdrożenie komponentów PKI
• instalacja serwera Root CA
• konfiguracja serwera Root CA
• instalacja serwera Subordinate CA
• konfiguracja serwera Subordinate CA
• Konfigurację szablonów certyfikatów i usług publikacji (w tym repozytorium certyfikatów, listy CRL i usługę OCSP)
• Konfigurację mechanizmów Smartcard
• Konfigurację i uruchomienie 2 stacji zarządzających
• Konfigurację i uruchomienie punktu personalizacji
• Wdrożenie systemu umożliwiającego zarządzanie wydanymi certyfikatami
• Testy funkcjonalne
• Testy procedur

• instruktarz dla administratorów w wymiarze 16 godzin zegarowych składające się z części teoretycznej i praktycznej, obejmującej tematykę:
• wdrożenie PKI – części teoretyczna,
• w zakresie wydawania, unieważnienia i odnawiania certyfikatów – część teoretyczna i praktyczna
• obsługę punktu rejestracji i personalizacji – cześć teoretyczna

Wykonawca dostarczy i skonfiguruje oprogramowanie serwera streamingu umożliwiającego przeprowadzanie transmisji w czasie rzeczywistym minimum 25 jednoczesnych strumieni wideo z zachowaniem jakości HD – rozdzielczości i płynności (ilości klatek).

Serwer telekomunikacyjny:

Wykonawca w ramach zadania dostarczy serwer telekomunikacyjny złożony z:
• Serwer telekomunikacyjny redundantny.
• Moduł wyniesiony serwera telekomunikacyjnego, analog, 16 portowy 10 szt.
• Moduł wyniesiony serwera telekomunikacyjnego, analog, 8 portowy 10 szt.
Redundantny moduł sterujący pracujący w systemie gorącej rezerwy (hot swap):
• obudowa typu rack 19"
• zasilanie 230V AC
• minimum 4 łącza E1-PRA (EDSS1 NT/TE) z możliwością rozbudowy do minimum 8 E1-PRA (EDSS1 NT/TE) bez rozszerzania o kolejne moduły
• obsługa minimum 300 kont abonenckich VoIP (minimum SIPv2) z możliwością rozszerzenia do 500 bez rozbudowy o kolejne moduły
• obsługa minimum 30 kont typu SIP-trunk
obsługa minimum SIPv2
możliwość rozszerzenia do 100 kont SIP-trunk bez rozbudowy o kolejne moduły
każde łącze SIP-trunk musi obsługiwać minimum 10 kanałów głosowych jednocześnie
obsługa kodeków minimum: G.711a, G.711u, GSM, G722.
• bsługa faxow zgodna z T.38 oraz G.711 passthrough
• obsługa dowolnych urządzeń końcowych (bram FXO/FXS, terminali VoIP) zgodnych z SIPv2
• możliwość tworzenia wielopoziomowego interaktywnego systemu kierowania ruchem - IVR
• możliwość monitorowania wybranych/wszystkich połączeń (rejestrowania połączenia)
• możliwość tworzenia wirtualnych PABX w ramach systemu minimum 50 PABX
• możliwość tworzenia wydzielonej numeracji w ramach każdego PABX
• możliwość definiowania klas ruchu dla każdego PABX oraz każdego konta (abonent / trunk)
o uprawnienia
o ograniczenia
• możliwość zdefiniowania minimum 100 poziomów wybierania ("dial planów") opisujących kierowanie ruchem - możliwość kierowania ruchem przez określone E1, SIP-trunk, konta SIP w zależności od wymagań

moduły wyniesione serwera telekomunikacyjnego FXS
• obudowa rack 19" 1U
• zasilanie 230V AC
• obsługa minimum SIPv2
• obsługa kodeków minimum: G.711a, G.711u, G.729AB, G.723
• obsługa T.38 lub G.711 bypass

• obsługa VAD (Voice Activity Detection)
• obsługa eliminacji echa G.168
• obsługa CLIP (FSK), CW, CFB, CFU, CFNR, hotline, reverse polarity
• obsługa minimum 2 serwerów proxy/rejestracji (podstawowy / zapasowy) w jednym czasie na każde konto
Pełna integracja systemu taryfikacji z istniejącym oprogramowaniem UM w Ełku.
Wymagania Zamawiającego odnośnie wdrożenia systemu:
• dostawca uruchomi wszystkie dostarczone moduły w oparciu o sieć IP Zamawiającego
• dostawca uruchomi moduł sterujący serwera telekomunikacyjnego
• dostawca uruchomia wszystkie moduły wyniesione serwera telekomunikacyjnego w lokalizacjach podanych przez Zamawiającego
• dostawca skonfiguruje sprzęt zgodnie z wymaganiami Zamawiającego
• dostawca udzieli bezterminowej licencji na użytkowanie całości dostarczonego sprzętu, oprogramowania

Wykonawca uruchomi w szczególności poniższe funkcjonalności:
- możliwość wysyłania przez serwer telekomunikacyjny sms o nieodebranych połączeniach.
- oddzwanianie alarmowe - użytkownik dzwoni na wskazany numer Zamawiającego i po chwili system oddzwania do niego,
- głosowy system powiadamiania grupowego - czyli komunikat głosowy i system obdzwania listę numerów i odtwarza nagrana wcześniej informację,
- głosowy system powiadamiania - czyli nagrany komunikat, który jest odtwarzany po dodzwonieniu się na wskazany numer,
- rejestracja połączeń - każdy użytkownik mógłby zalogować się i włączyć/wyłączyć rejestracje połączeń na swoim numerze.

Dostawca udzieli 48-miesiecznej gwarancji

Wykonawca dostarczy dla powyższych serwerów system backupowy o minimalnych parametrach:

• Oprogramowanie powinno współpracować z infrastrukturą VMware w wersji 4.0, 4.1, 5.0, 5.1, 5.5 oraz Microsoft Hyper-V 2008 R2 SP1, 2012 I 2012 R2
• Oprogramowanie powinno wpółpracować z hostami zarządzanymi przez VMware vCenter oraz Microsoft Virtual Machine Manger oraz z hostami niezarządzanymi
• Oprogramowanie powinno zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V
• Oprogramowanie powinno być licencjonowanie w modelu “per-CPU”. Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpiecznony TB, dodatkowo platna deduplikacja) nie jest dozwolone
• Oprogramowanie powinno być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
• Oprogramowanie powinno tworzyć “samowystarczalne” archiwa to odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
• Oprogramowanie powinno mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów

• Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu
• Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej
• Oprogramowanie powinno zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia
• Oprogramowanie powinno zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP
• Oprogramowanie powinno mieć możliwość uruchamiania skryptów przed i po zadaniu backupowym
• Oprogramowanie powinno zapewniać bezpośrednią integrację z VMware vCloud Director 5.1 i archiwizować również metadane vCD. Powinno też umożliwiać odtwarzanie tych metadanych do vCD
• Oprogramowanie powinno mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
• Oprogramowanie powinno mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej.
• Oprogramowanie powinno oferować zarządzanie kluczami w przypadku utraty podstawowego klucza
• Oprogramowanie powinno wspierać backup maszyn wirtualych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
• Oprogramowanie powinno wykorzystywać VMware vStorage API for Data Protection i używać mechanizmów Change Block Tracking
• Oprogramowanie powinno oferować podobne rozwiązanie jak CBT również dla platformy Hyper-V
• Oprogramowanie powinno oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji
• Oprogramowanie powinno automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu
• Oprogramowanie powinno wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
• Oprogramowanie powinno mieć możliwość wydzielenia osobnej roli typu tape server
• Oprogramowanie powinno mieć możliwość kopiowania backupów do lokalizacji zdalnej
• Oprogramowanie powinno mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
• Oprogramowanie powinno umieć korzystać z protokołu DDBOOST w przypadku gdy repozytorium backupów jest umiejscowione na EMC DataDomain
• Oprogramowanie powinno mieć możliwość kopiowania
• Oprogramowanie powinno mieć możliwość replikacji wirtualnych maszyn pomiędzy lokalizacjiami
• Funkcjonalność ta powinna być zapewniona dla vSphere i Hyper-V
• Oprogramowanie powinno dawać możliwość użycia wcześniej wykonanego backupu jako źródła do zadania replikacji
• Oprogramowanie powinno wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
• Oprogramowanie powinno dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere

• Oprogramowanie powinno przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)

X. Macierz

Obudowa do instalacji w standardowej szafie RACK 19". Wysokość maksymalnie 4U.
Możliwość instalacji min. 60 dysków Hot Plug oraz rozbudowy do min. 180 dysków poprzez dodatkowe półki dyskowe.
Dodatkowy panel zamykany na klucz chroniący dyski twarde przed nieuprawnionym wyjęciem z macierzy.
Dwa kontrolery posiadające łącznie minimum cztery aktywne porty iSCSI 10Gb w standardzie BaseT do podłączenia serwerów. Obsługa zabezpieczeń RAID: 0,1,5,6,10.
Możliwość rozszerzenia pamięci cache poprzez rozbudowę dyskami SSD.
Cache 4GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, z opcją zapisu na dysk lub inna pamięć nieulotną lub podtrzymywana bateryjnie przez min. 72h w razie awarii
Zainstalowane dyski w ramach jednego urządzenia:
24 sztuki dysków o pojemności 4 TB NearLine SAS 7.2k RPM każdy
Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych, możliwość obsługi łącznie minimum 180 dysków, wydajnych dysków SAS, SATA (lub NearLine SAS), samoszyfrujących dysków SED dostępnych w aktualnej ofercie producenta macierzy dyskowej, możliwość mieszania typów dysków w obrębie macierzy.
Zarządzające macierzą w tym powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków. Możliwość tworzenia kopii migawkowych oraz funkcjonalność wykonywania pełnych kopii dysków logicznych (licencja dostarczona wraz z macierzą).
Macierz musi posiadać możliwość przydzielania większej ilości zasobów dyskowych dla hostów niż pojemność zainstalowana – Thin Provisioning.
Licencja macierzy powinna umożliwiać podłączanie minimum 32 hostów bez konieczności zakupu dodatkowych licencji.
Macierz musi posiadać możliwość zarządzania z poziomu aplikacji zarządzającej producenta serwerów oraz być z nim kompatybilna.
Wsparcie dla systemów operacyjnych MS Windows 2003/ 2008, RedHat Enterprise Linux, SUSE Linux.
Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.
Pięć lat gwarancji.
W przypadku awarii dyski twarde pozostają własnością Zamawiającego.

XI. System bezpieczeństwa wiz., KD

Wykonawca zaprojektuje wykona, skonfiguruje i uruchomi w ramach zadania System bezpieczeństwa wizyjnego złożony z ośmiu punktów bezpieczeństwa wizyjnego (PBW) zlokalizowanych w poniższych miejscach:

Punkt bezpieczeństwa wizyjnego nr 1 – zlokalizowany na skrzyżowaniu ulicy Gdańskiej z ulicą gen. Władysława Sikorskiego
Punkt bezpieczeństwa wizyjnego nr 2 - zlokalizowany na skrzyżowaniu ulicy Jana Pawła II z ulicą Grajewską

Punkt bezpieczeństwa wizyjnego nr 3 - zlokalizowany obok przystanku autobusowego na pętli autobusowej w okolicach ulicy Dobrzańskiego 9
Punkt bezpieczeństwa wizyjnego nr 4 - zlokalizowany na skrzyżowaniu z przejazdem kolejowym gen. Władysława Sikorskiego z ulicą Wincentego Witosa oraz z ulicą Słoneczną.
Punkt bezpieczeństwa wizyjnego nr 5 - zlokalizowany na skrzyżowaniu ulicy Suwalskiej z ulicą Józefa Bema
Punkt bezpieczeństwa wizyjnego nr 6 – zlokalizowany na skrzyżowaniu ulicy Tadeusza Kościuszki z ulicą Chopina
Punkt bezpieczeństwa wizyjnego nr 7 - zlokalizowany na skrzyżowaniu ulicy mjr Piwnika Ponurego z ulicą gen Bora-Komorowskiego
Punkt bezpieczeństwa wizyjnego nr 8 – Punkt na ulicy Juliana Tuwima na wysokości bloku numer 18 i 10.

Dokładną lokalizację oraz punkty styku z istniejącą siecią wykonawca przedstawi Zamawiającemu do akceptacji i zatwierdzenia.

W ramach zadania Wykonawca dodatkowo zaprojektuje, dostarczy i zamontuje 8 słupów, 8 przełączników sieciowych, 8 kamer szybkoobrotowych HD, tj. wykona 8 kompletnych punktów kamerowych oraz dostarczy system rejestracji oparty na systemie w pełni kompatybilnym z Zintegrowanym Systemem Bezpieczeństwa Miasta Ełku (ZSBME) z kluczem licencyjnym na 32 kanały wideo. System – aplikację serwerową kompatybilną z ZSBME - należy zainstalować na serwerze, dostarczanym w ramach niniejszego postępowania.
W zakres zadania wchodzi także zaprojektowanie, wykonanie i uruchomienie przyłączy teletechnicznych dla tych kamer (szczegółowy zakres przyłączy teletechnicznych został przedstawiony poniżej).

Opis kompletnego punktu kamerowego:

Kamerę należy zamontować na dostarczonym słupie Do montażu użyć adapter nasłupowy. Okablowanie (transmisja i zasilanie PoE) prowadzić od kamery do szafki, Wykonawca zamontuje szafę wraz z niezbędnym wyposażeniem. Szafka wraz z wyposażeniem dostarczona przez Wykonawcę wyposażona powinna być w zasilanie, zabezpieczenia oraz połączona powinna być ze światłowodową siecią szerokopasmową. Rurę do słupa mocować opaskami metalowymi, natomiast w ziemi układać na głębokości zgodnej z obowiązującymi normami. Po wykonanych pracach należy doprowadzić teren do stanu pierwotnego, m. in. wykonać odtworzenie nawierzchni. Transmisję pomiędzy kamerą, a szafką wykonać za pomocą żelowanego kabla 4 x UTP kat. 6.
W każdym punkcie należy zainstalować przemysłowy przełącznik sieciowy (switch), do którego należy podłączyć kabel transmisyjny (skrętkę) od kamery oraz pathcord światłowodowy (SFP) do przełącznicy światłowodowej. Transmisja od przełącznika sieciowego do studia monitoringu przebiegać będzie poprzez istniejącą światłowodową sieć szerokopasmową poprzez węzeł światłowodowy. W węźle należy zainstalować konwertery światłowodowe i wpiąć je do istniejącego przełącznika światłowodowego.
Obraz z kamer będzie wyświetlany w studiu monitoringu w budynku Urzędu Miasta. W ramach prac należy dostarczyć klucz licencyjny na 32 kanały wideo.

Zamawiający określa minimalne wymagania techniczno-funkcjonalne

Dla kamer:
Przeznaczenie do zastosowań zewnętrznych,
Przeznaczenie do pracy w trybie ciągłym 24/7/365,
Przetwornik CMOS nie mniejszy niż 1/2,8”,
Czułość nie gorsza niż kolor: 0,8 Lux, B-W: 0,04 Lux (dla 30 IRE),
Transmisja obrazu w formie cyfrowej poprzez siec IP,
Sterowanie PTZ w formie cyfrowej poprzez sieć IP,
Co najmniej 20x zoom optyczny,
Co najmniej 12x zoom cyfrowy,
Kodowanie obrazu co najmniej H.264 oraz MJPEG,
Rozdzielczości HDTV 1080p (1920x1080) przy 25 klatkach na sekundę,
Możliwość generowania 3 strumieni wizyjnych w pełniej rozdzielczości HDTV 1080p,
Możliwość generowania 3 strumieni wizyjnych o różnych parametrach obrazu,
Możliwość zdefiniowania co najmniej 99 presetów (pozycji),
Kąt obrotu (PAN) 360° bez punktu końcowego,
Kąt pochylenia (TILT) 220°,
Szybkość obrotu w poziomie co najmniej 450°/s,
Możliwość nakładania tekstu na wyświetlany obraz,
Złącze Ethernet 10 BaseT / 100 BaseTX,
Wsparcie co najmniej dla następujących protokołów sieciowych:
IPv4, IPv6, HTTP, HTTPS, QoS l.3, FTP, SMTP, SNMPv3, DNS, DynDNS,
NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP,
Transmisja unicast oraz multicast,
Możliwość ustawienia transmisji Constant Bit Rate (CBR),
Możliwość ustawienia transmisji Variable Bit Rate (VBR),
Możliwość rejestracji trasy PTZ,
Możliwość ustawienia co najmniej 8 stref prywatności,
Możliwość filtrowania adresów IP,
Możliwość ochrony dostępu hasłem,
Kamera wraz z elementami grzewczymi i wentylatorami powinna być zasilana za pomocą pojedynczego kabla sieciowego wpiętego do kamery,
Obudowa co najmniej IP66,
Pracę w zakresie temperatur co najmniej od -40 °C do +50 °C,
Waga urządzenia: nie więcej niż 5kg.

Dla przyłączy teletechnicznych:

Do budowy przyłączy telekomunikacyjnych należy zastosować rurę fi 110 jako rurę podstawową.
Należy zastosować kanalizację wtórna minimum trzy rury HDPE fi25 lub HDPE fi32.
Szafa zewnętrzna telekomunikacyjna z przełącznicami optycznymi ze złączami typu SC/PC do których zostanie doprowadzony i zakończony światłowód o profilu nie mniejszym niż 12 włókien, przy założeniu wykonania spawów na pełnych profilach. Wykonawca zaprojektuje i wykona przyłącze elektryczne do każdej szafy zewnętrznej.
Do budowy przyłączy telekomunikacyjnych należy zastosować studnie kablowe typu SKO-2 (SKO-2x) lub odpowiedniki jako podstawową oraz studnie przelotowe, rozgałęźne i końcowe
Zamawiający dopuszcza stosowanie studni typu SK-1 (SK-1x) w przypadku braku miejsca na umieszczenie studni SK-2 po uzyskaniu pisemnej zgody Zamawiającego

Należy zastosować pokrywy jednoelementowe
Studnie muszą być wyposażone w zamknięcia na zamki
Betonowy korpus studni może składać się z nie więcej niż dwóch części
W miejscach występowania ruchu kołowego (np. parking, wjazd, pobocze) należy zastosować ramy i pokrywy o konstrukcji wzmocnionej (nakrywa jednoelementowa)
Studnie kablowe powinny być usytuowane w następujących miejscach kanalizacji teletechnicznej:
- na odcinkach przebiegu prostoliniowego - jako studnie przelotowe dla zachowania dopuszczalnych długości przelotów między sąsiednimi studniami do 100m
- w miejscach przyszłego odgałęzienia kanalizacji - jako studnie odgałęźne
- na zakończeniach ciągu kanalizacji - jako studnie końcowe
Wykonawca zastosuje rury HDPE lub RHDPE Lub DVR lub PCV o grubości ścianki minimum 4 mm w zależności od miejsca instalacji. Do kanalizacji teletechnicznej należy zaciągnąć rurę HDPE32 lub HDPE25 a następnie do niej kable optyczne zakańczając je na projektowanych przełącznicach optycznych złączami. Kabel należy zaciągać do kanalizacji teletechnicznej, zakańczając na projektowanej przełącznicy optycznej złączami typu SC/PC w projektowanej szafie telekomunikacyjnej we wskazanych lokalizacjach.
Wykonawca dostarczy i zamontuje kompletne szafy telekomunikacyjne zewnętrzne które wyposaży we wszystkie niezbędne elementy w tym w szczególności w panele światłowodowe, osprzęt elektryczny, osprzęt zabezpieczający elektryczny.
Wszystkie szafy opisane w tym punkcie wykonawca zabezpieczy kłódkami patentowymi z kluczem typu master-key.
Zastosować kabel optyczny jednomodowy o przekroju minimum 12j.
Każdy kabel zakończyć na przełącznicy w pełnym profilu.
Jeżeli punkt bezpieczeństwa wizyjnego znajduje się w pobliżu istniejącego przełącznika sieciowego to Zamawiający dopuszcza możliwość podłączenia do przełącznika PBW, w przeciwnym razie Wykonawca dostarczy przełącznik przemysłowy o parametrach identycznych jak przełącznik przemysłowy opisany w punkcie dotyczącym masztów hotspotowych.

Switch przemysłowy 8 szt. o minimalnych parametrach:

Zamawiający wymaga dostarczenia urządzeń w wykonaniu przemysłowym odpornych na warunki atmosferyczne w tym w szczególności na temperaturę. Switche muszą pracować w temperaturze od -30 do +70 st Celsjusza. Dostarczone switche muszą pracować w układzie pierścieniowym co oznacza iż muszą posiadać obsługę oraz konfigurację ringów optycznych wraz z minimum dwoma odpornymi na warunki przemysłowe wkładkami SFP 1000 Mb/s, Wszystkie switche muszą obsługiwać VLAN, POE oraz być zarządzalne.
Switch musi obsługiwać poniższe standardy:
802.3i, 802.3u, 802.3z, 802.3ab, 802.3x, 802.3ac, 802.3af, 802.1D, 802.1Q, 802.1p, 802.1w, RFC 791, RFC 826, RFC 792, RFC 2131.
Wykonawca dostarczy, skonfiguruje i uruchomi ring w ramach dostawy Switchy przemysłowych.

Szczegółowy opis punktów bezpieczeństwa wizyjnego:

Punkt bezpieczeństwa wizyjnego nr 1 – Wykonawca wykona przyłącze optyczne z węzła optycznego zlokalizowanego w Zespole Szkół Nr 2 im. K.K. Baczyńskiego położonej przy

ulicy gen. Władysława Sikorskiego. Zamawiający informuje iż wzdłuż ulicy gen. Władysława Sikorskiego dysponuje kanalizacja teletechniczną fi 110 którą Wykonawca może wykorzystać do prowadzenia kabli optycznych i zasilania.

Punkt bezpieczeństwa wizyjnego nr 2 – Zamawiający informuje, że obok planowanego punktu posiada wykonaną szafę optyczną wyposażoną w złącze optyczne i zasilanie.

Punkt bezpieczeństwa wizyjnego nr 3 – Zamawiający informuje, że obok planowanego punktu posiada wykonaną szafę optyczną wyposażoną w złącze optyczne i zasilanie.

Punkt bezpieczeństwa wizyjnego nr 4 – Zamawiający informuje, że wzdłuż ulicy gen. Władysława Sikorskiego dysponuje kanalizacją teletechniczną fi 110, którą Wykonawca może wykorzystać do prowadzenia kabli optycznych i zasilania. Jednocześnie Zamawiający informuje, iż w pobliżu planowanego punktu dysponuje złączem optycznym wraz z zasilaniem zlokalizowanym obok szafy oświetleniowej S-629.

Punkt bezpieczeństwa wizyjnego nr 5 – Zamawiający informuje, że wzdłuż ulicy Suwalskiej dysponuje kanalizacją teletechniczną fi 110, którą Wykonawca może wykorzystać do prowadzenia kabli optycznych i zasilania. Najbliższy węzeł optyczny zlokalizowany jest w pobliskiej jednostce Powiatowej Państwowej Straży Pożarnej.

Punkt bezpieczeństwa wizyjnego nr 6 – Zamawiający informuje, że wzdłuż ulicy Tadeusza Kościuszki dysponuje kanalizacją teletechniczną fi 110, którą Wykonawca może wykorzystać do prowadzenia kabli optycznych i zasilania.

Punkt bezpieczeństwa wizyjnego nr 7 – zlokalizowany na skrzyżowaniu ulicy mjr Piwnika Ponurego z ulicą gen Bora-Komorowskiego.

Punkt bezpieczeństwa wizyjnego nr 8 – Zamawiający informuje, że wzdłuż ulicy Juliana Tuwima dysponuje kanalizacją teletechniczną fi 110 wraz ze złączem optycznym, którą Wykonawca może wykorzystać do prowadzenia kabli optycznych i zasilania.

Wykonawca dostarczy i skonfiguruje do pracy z powyższymi punktami kontroler punktów wizyjnych optycznych o minimalnych parametrach:
Obudowa typu rack 19”
Zainstalowane 7 dysków dedykowanych do zastosowania raidowego (NAS) o minimalnej pojemności 6 TB każdy. Dyski spięte w RAID min 5.
Dwa sześciordzeniowe procesory o minimalnej częstotliwości 2000 MHz każdy.
Zainstalowana pamięć RAM min 16 GB.
Zainstalowany system operacyjny w wersji 64 bitowej umożliwiający pełna integrację z posia-damym przez zamawiającego oprogramowaniem domenowym opartym na Windows Server 2012. Oprogramowanie musi obsługiwać usługi katalogowe oraz wirtualizację, musi również umożliwiać uruchomienie zapasowego AD
Na powyższy kontroler Wykonawca udzieli 60 miesięcznej gwarancji.

XII. Modernizacja systemu zasilania

Wykonawca zamontuje na dwóch mobilnych agregatach zasilających serwerownie urządzenia namierzające GPS tak by można było zdalnie zlokalizować pozycję agregatu. Wykonawca wyposaży jeden mobilny agregat w szybkozłącze przemysłowe do podłączania i rozłączania wszystkich kabli logicznych, sygnałowych i zasilających tak by odłączenie i rozruch agregatu w zakresie kabli sterujących i sygnałowych mogło nastąpić bez konieczności używania jakichkolwiek narzędzi. Wykonawca dostarczy system obciążeniowy agregatu prądotwórczego umożliwiający obciążenie agregatu w zakresie 20-22, 40-44, 60-66 i 80-88 KW, system obciążeniowy musi być wyposażony w odpowiednie kable oraz być podłączany bez konieczności użycia narzędzi.

XIII. Modernizacja sprzętu aktywnego

Wykonawca zaktualizuje oprogramowanie na przełącznikach rdzeniowych, dokona konfiguracji dostarczonych przełączników oraz Wykonawca przeprowadzi szereg testów penetracyjnych mających na celu optymalizację bezpieczeństwa w sieci komputerowej Zamawiającego. Skanowanie będzie polegało na zdalnej enumeracji otwartych portów oraz weryfikacji bezpieczeństwa oprogramowania na nich nasłuchującego. Skanowanie obejmie:

1. urządzenia dedykowane (embeded), na przykład routerów i przełączniki;
2. punkty styku z sieciami obcymi;
3. zbadanie podatności systemów Zamawiającego na ataki przeprowadzane z zewnątrz.

Ponadto Wykonawca przeprowadzi badanie bezpieczeństwa sieci systemów komputerowych, które pozwoli na:

1. określenie błędów w konfiguracji skutkujących powstaniem podatności na atak;
2. wskazanie nadmiernych uprawnień, niezgodnych z zasadami dobrych praktyk;
3. wskazanie potencjalnie niebezpiecznego oprogramowania znajdującego się w badanym systemie.

Badaniu będą podlegały następujące systemy:

rodzina Microsoft Windows Server (do poziomu weryfikacji poprawek Windows Update włącznie);
Linux 2.4.x, 2.6.x, 3.x.x;
IBM AIX;
CISCO IOS;
Microsoft SQL;
MySQL;

Badanie zostanie zakończone raportem. Forma i zakres raportu musi być zaakceptowany przez Zamawiającego przed zakończeniem projektu.

Konfiguracja dodatkowych funkcjonalności istniejącego systemu Zarządzania siecią i NAC

Zamawiający wymaga, aby Wykonawca wykonał:

1. Przygotowanie projektu konfiguracji zawierającego:
   - ustaloną przez dział informatyki hierarchię polityk bezpieczeństwa
   - proponowaną strukturę VLAN
   - proponowane reguły ACL
   - hierarchię użytkowników w podziale na role
   - dokładną definicję ról i uprawnień w systemie

2. Konfigurację systemu zawierającą:
   - ustalone przez dział informatyki polisy bezpieczeństwa
   - dodatkowe sieci VLAN
   - dodatkowe reguły ACL
   - wdrożenie scenariuszy (802.1x, MAC), profili (Gość, Pracownik, Drukarka itp.) i polityk bezpieczeństwa/ACL-VLAN (uprawnienia dostępu/QoS dla L2-L4
   - konfigurację wybranych przełączników sieciowych zgodnie z ustaloną składnią CLI.
   - diagnostykę i usunięcie znalezionych problemów sieciowych
   - testy
   - weryfikacja i usunięcie błędów
   - strojenie

Konfiguracja dodatkowych funkcjonalności istniejącego systemu Wireless

Zamawiający wymaga, aby Wykonawca wykonał:

1. Przygotowanie projektu konfiguracji zawierającego:
   - ustaloną przez dział informatyki hierarchię polityk bezpieczeństwa
   - proponowaną strukturę VLAN
   - proponowane reguły ACL
   - hierarchię użytkowników w podziale na role
   - dokładną definicję ról i uprawnień w systemie

2. Konfigurację systemu zawierającą:
   - ustalone przez dział informatyki polisy bezpieczeństwa
   - dodatkowe sieci VLAN
   - dodatkowe reguły ACL
   - diagnostykę i usunięcie znalezionych problemów sieci bezprzewodowej
   - wdrożenie scenariuszy (802.1x, MAC), profili (Gość, Pracownik, Drukarka itp.) i polityk bezpieczeństwa/ACL-VLAN (uprawnienia dostępu/QoS dla L2-L4
   - diagnostykę i usunięcie znalezionych problemów sieciowych
   - testy
   - weryfikacja i usunięcie błędów
   - strojenie

Testy funkcjonalne

Zamawiający wymaga, aby Wykonawca wykonał:

1. Wygenerowanie kont testowych użytkowników – Wykonawca wygeneruje około 15 przykładowych kont użytkowników zgodnie z przyjętym scenariuszem.

2. Testy – system powinien zostać przetestowany pod kątem zabezpieczeń I uprawnień dla każdej grupy użytkowników zgodnie z przyjętym scenariuszem
3. Weryfikacja i usunięcie błędów konfiguracji – całość konfiguracji powinna zostać przetestowana. W przypadku znalezienia błędów konfiguracyjnych należy je natychmiast poprawić
4. Strojenie systemu – Wykonawca zoptymalizuje pracę systemu do warunków panujących w sieci komputerowej Zamawiającego.

Wykonawca udziela usług gwarancji na dostarczony sprzęt i działanie systemu zgodnie z wymaganiami Umowy, SIWZ, SST i Projektem Technicznym na okres jednego roku.
W ramach obsługi gwarancyjnej Zamawiający stworzy i wystawi Wykonawcy zdalne bezpieczne łącze VPN, za pomocą którego możliwa będzie zdalna pomoc techniczna świadczona przez Wykonawcę.
Zamawiający będzie zgłaszać usterkę/awarię, drogą telefoniczną lub poprzez e-mail na wskazane w umowie dane kontaktowe.

XIV. Przyłącza teletechniczne

Wykonawca zaprojektuje i wykona następujące przyłącza teletechniczne:

Przyłącze 1: od węzła zlokalizowanego w Miejskim Zakładzie Komunikacji Sp. z o. o. znajdującego się w Ełku przy ulicy ul. Łukasiewicza 8 do szafy oświetleniowej S-636 zlokalizowanej na ulicy Słonecznej. Zamawiający informuje, iż posiada wybudowaną kanalizację teletechniczną wraz z kablem optycznym wzdłuż ulicy Łukasiewicza, którą Wykonawca może wykorzystać, przy szafie oświetleniowej Wykonawca umieści szafkę ze złączem optycznym.

Przyłącze 2 – od szafy zewnętrznej zlokalizowanej przy ulicy A. Krajowej 33 do szafy zewnętrznej zlokalizowanej na rogu ulicy A. Krajowa z ulicą J. Dąbrowskiego.

Przyłącze 3 – do ronda Jerzego Cichowicza znajdującego się na ulicy Suwalskiej, gdzie Wykonawca dostarczy i zamontuje szafę zewnętrzną, do której doprowadzi napięcie z szafy oświetleniowej S-665 lub S-667 oraz kabel optyczny minimum 24j z węzła optycznego zlokalizowanego w serwerowni Parku Naukowo-Technologicznego przy ulicy Podmiejskiej 5. Zamawiający informuję iż posiada kanalizację teletechniczną na odcinku od ronda do serwerowni Parku Naukowo-Technologicznego

Przyłącze 4 – Do punktu kamerowego zlokalizowanego na elewacji budynku przy ulicy Dąbrowskiego 10. Zamawiający dysponuje punktem styku na rogu ulicy A. Krajowa z ulicą J. Dąbrowskiego oraz w pobliżu szafy oświetleniowej S-615.

Przyłącze 5 - przyłącze od szafy zlokalizowanej na skrzyżowaniu ulicy Jana Kilińskiego z ulicą Koszykową do szafy zewnętrznej, którą wykonawca dostarczy i zamontuje w okolicach szafy oświetleniowej S-654 na ulicy Emilii Plater. Zamawiający informuje, iż posiada wybudowaną kanalizację teletechniczną wzdłuż ulicy Kilińskiego, do zadań Wykonawcy należeć będzie uzupełnić kanalizację na odcinku od ulicy Kilińskiego do S-654, oraz umieścić w kanalizacji wtórnik wraz z kablem optycznym 24j.

Przyłącza należy wykonać zgodnie z poniższymi wytycznymi:

1. Zleceniobiorca zobowiązuje się do wykonania prac projektowych oraz robót budowlanych w oparciu o umowę zgodnie z:
- ustawą Prawo Budowlane,
- warunkami technicznymi (zestawionymi poniżej),
- warunkami zabudowy i zagospodarowania terenu,
- zasadami współczesnej wiedzy technicznej,
- obowiązującymi w tym zakresie przepisami,
- Polskimi Normami,
- Normami Branżowymi TP S.A.

2. Zleceniobiorca zapewni udział w pracach nad projektem i budową osób dysponujących uprawnieniami do projektowania oraz kierowania robotami bez ograniczeń z przynależnością do izby budowlanej właściwej specjalności.

3. Zleceniobiorca jest zobowiązany do:
- opracowanie szczegółowej koncepcji projektowanych sieci i przyłączy telekomunikacyjnych zgodnych z warunkami technicznymi i przedstawienie jej do akceptacji Zleceniodawcy,
- wykonania na podstawie zaakceptowanej koncepcji kompletnej dokumentacji projektowej i wybudowania na terenie miasta Ełk sieci i przyłączy telekomunikacyjnych z wykorzystaniem rur ∅ 110,
- pozyskania aktualnych map do celów projektowych,
- uzyskania właściwych dla danego projektu opinii, uzgodnień i sprawdzeń rozwiązań, projektowych oraz dla lokalizacji tego wymagających prawomocnych pozwoleń na budowę projektowanych elementów,
- opracowanie dokumentacji budowlanej dla projektowanych przyłączy telekomunikacyjnych,
- opracowanie dokumentacji wykonawczej na potrzeby budowy kablowych przyłączy optotelekomunikacyjnych w oparciu o ww. projekt przyłączy telekomunikacyjnych a następnie wybudowanie go zgodnie z opracowaną dokumentacją,
- dostarczenia w celu sprawdzenia i zatwierdzenia przez Zleceniodawcę opracowań projektowych w terminach zgodnych z umową,
- opracowania koncepcji logicznej sieci.
- wszystkie kable optyczne muszą być zakańczane w pełnym profilu na przełącznicach optycznych (dopuszcza się zakończenie kabli w pełnym profilu na złączu optycznym)
- poprzez zewnętrzne złącze optyczne Zamawiający rozumie iż Wykonawca dostarczy i wykona złącze optyczne zewnętrzne w którym: umieści panel optyczny, dokona rozszycia minimum 12 włókien.

Szafkę instalacyjną zewnętrzną o minimalnych parametrach:
Szafa zewnętrzna 19” o wysokości minimum 18U
Zamykana na zamek ryglowy 3- punktowy, wkładka patentowa,
Dodatkowe zamknięcie na kłódkę
Wejście do szaf zabezpieczyć przed dostaniem się gryzoni.
Wykonawca dostarczy kłódkę z kluczem MasterKey włókna należy rozszyć na panelu optyczny.
-Do budowy należy zastosować studnie kablowe typu SKO-2 (SKO-2x, SK-2X) lub odpowiedniki jako podstawową oraz studnie przelotowe, rozgałęźne i końcowe. Betonowy

korpus studni może składać się z nie więcej niż dwóch części. Dostęp do studni należy zabezpieczyć dodatkowo zasłoną metalową zabezpieczoną kłódką z kluczem MasterKey
- Wykonawca trwale oznaczy wybudowany kabel optyczny w każdej studni.
- W miejscach występowania ruchu kołowego (np. parking, wjazd, pobocze) należy zastosować ramy i pokrywy o konstrukcji wzmocnionej (nakrywa jednoelementowa). Studnie powinny być zabezpieczone farbą antykorozyjną (pomalowane wszystkie elementy metalowe/żeliwne) oraz powinny być zabezpieczone przed dostępem osób nieuprawnionych. Studnie kablowe powinny być usytuowane w następujących miejscach kanalizacji teletechnicznej:
- na odcinkach przebiegu prostoliniowego - jako studnie przelotowe dla zachowania dopuszczalnych długości przelotów między sąsiednimi studniami do 100m,
- w miejscach przyszłego odgałęzienia kanalizacji - jako studnie odgałęźne,
- na zakończeniach ciągu kanalizacji - jako studnie końcowe.
- Wykonawca zastosuje rury fi 110 lub 160 HDPE lub RHDPE lub DVR lub PCV. Wykonawca zastosuje kanalizację wtórną nie większa niż HDPE fi32 w zależności od rodzaju kabli światłowodowych.
- Na całej długości przebiegu ziemnego nad rurociągiem należy ułożyć taśmę ostrzegawczą z wkładką stalową z napisem „UWAGA ! KABEL OPTOTELEKOMUNIKACYJNY” na głębokości 0,5m. Wkładka metalowa powinna mieć ciągłość elektryczna na całej długości, a miejsca jej łączeń powinny być chronione przed korozją.

4. W związku z wykonaniem w ramach inwestycji miejskich nowych ciągów pieszych (chodniki z kostki polbrukowej) w pasach drogowych na terenie miasta Ełk, Zleceniobiorca zobowiązany jest w przypadku prowadzenia prac ziemnych metodą wykopu otwartego do odbudowy chodnika oraz przejęcia gwarancji z tytułu nieprawidłowego odtworzenia nawierzchni w ciągach pieszych w momencie zakończenia prowadzenia robót budowlanych w pasach drogowych ww. ulic związanych z realizacją przedmiotu zamówienia.

Koszty zajęcia pasa drogowego, innych terenów/gruntów oraz nadzorów (archeolog, PKP, GDDKiA, konserwator zabytków, przyrody, ZMiUW itp.) na czas prowadzenia robót obciążają wykonawcę.

Wykonawca dokona inwentaryzacji wykonanej sieci w aplikacji posiadanej przez Zamawiającego

WYMAGANIA DOTYCZĄCE PROJEKTU I BUDOWY KABLA OPTOTELEKOMUNIKACYJNEGO

Na podstawie opracowanej dokumentacji projektowej na budowę sieci oraz przyłączy teletechnicznych należy opracować dokumentację projektową wykonawczą dotyczącą budowy sieci wraz z kablem optycznym oraz kablowych przyłączy optotelekomunikacyjnych.

Zapasy technologiczne kabla optotelekomunikacyjnego (nie mniej niż 20m) należy zaprojektować i zainstalować w studniach na stelażach/skrzynkach zapasu w punktach początkowych i końcowych linii oraz w punktach istotnych (tj. studnie odgałęźne, budynki) na terenie miasta Ełk.

Do kanalizacji teletechnicznej należy zaciągnąć rury kanalizacji wtórnej, a następnie do niej kable optyczne zakańczając je pełnym profilem na projektowanych przełącznicach optycznych złączami typu SC/APC w projektowanych szafach.

Kabel należy zaciągać do kanalizacji teletechnicznej, zakańczając na projektowanej przełącznicy optycznej złączami typu SC/APC w projektowanej szafie telekomunikacyjnej we wskazanych lokalizacjach.

Wykonawca zastosuje światłowód o przekroju minimum 12j.

Na całej długości przebiegu ziemnego nad rurociągiem należy ułożyć taśmę ostrzegawczą z wkładką stalową z napisem „UWAGA ! KABEL OPTOTELEKOMUNIKACYJNY" na głębokości 0,5m. Wkładka metalowa powinna mieć ciągłość elektryczna na całej długości, a miejsca jej łączeń powinny być chronione przed korozją.

Wykonawca oznaczy w sposób trwały kabel optyczny.

WYMAGANIA DOTYCZĄCE DOKUMENTACJI PROJEKTOWEJ

1. Zleceniobiorca jest zobowiązany przygotować dokumentację projektową w niżej wymienionych ilościach egzemplarzy:

- projekty budowlane – 5 egz. z czego 1 egz. z możliwością ingerencji w zawartość,
- projekty wykonawcze - 5 egz. z czego 1 egz. z możliwością ingerencji w zawartość,
- przedmiar robót wraz z kosztorysem inwestorskim w formacie zgodnym z formatem programu NORMA – 3 egz. oraz wersja elektroniczna na płycie CD-R,
- oprócz dokumentacji w formie papierowej Zamawiający wymaga dostarczenia również dokumentacji w formie elektronicznej edytowalnej na nośniku w postaci płyty CD-R.

2. Zleceniobiorca zaopatrzy dokumentację w wykaz opracowań oraz pisemne Oświadczenia:

- że dokumentacja została wykonana zgodnie z umową, zasadami współczesnej wiedzy technicznej, obowiązującymi w tym zakresie przepisami oraz zgodnie z Polskimi Normami i Normami Branżowymi TP S.A., oraz że zostaje wydana w stanie kompletnym ze względu na cel oznaczony w umowie,
- o prawie dysponowania gruntem na cele inwestycyjne dotyczącego opracowania,

3. Zakres czynności Zleceniobiorcy przy wykonywaniu prac projektowych:

- pozyskanie niezbędnych map do celów projektowych,
- pozyskanie wszystkich niezbędnych zgód i pozwoleń,
- wykonanie projektów budowlanych, wykonawczych budowy studni kablowych oraz kabla optotelekomunikacyjnego,
- opracowanie przedmiarów robót i kosztorysów inwestorskich wg podanych przez Zleceniodawcę w formacie Norma,
- uzyskanie na rzecz Zleceniodawcy od właściciela nieruchomości lub innych posiadaczy prawa do dysponowania gruntem na cele budowlane wg odpowiednich wzorów umów i druków oświadczeń zatwierdzonych przez Zleceniodawcę.

4. Zawartość dokumentacji projektowej:

Dokumentacja projektowa powinna składać się z następujących części:
- projektu budowlanego,
- projektu wykonawczego,
- przedmiaru robót,
- kosztorysu inwestorskiego.

Do zadań Wykonawcy należy w szczególności:
- pozyskanie map do celów projektowych,
- pozyskanie wymaganych prawem uzgodnień (min. Wojewódzki Konserwator Zabytków, PKP, GDDKiA, ZMiUW) i pozwoleń, o ile wymagają tego aktualne przepisy,
- pozyskanie prawa do dysponowania gruntami na cele budowlane tj. wszystkich wymaganych przepisami prawa uzgodnień z właścicielami gruntów na budowę i umieszczenie na danej działce infrastruktury teletechnicznej,
- pozyskanie pozytywnej opinii Zespołu Uzgadniania Dokumentacji Projektowej,
- opracowanie kompletnej dokumentacji budowlano – wykonawczej,
- uzyskanie prawomocnej decyzji pozwolenia na budowę dla lokalizacji tego wymagających.

Projekt budowlany powinien zawierać co najmniej:
- stronę tytułową (tytuł, branża, dane inwestora, data wykonania, dane Wykonawcy projektu, nazwiska projektantów, opracowujących i sprawdzających projekt z podpisami i pieczątkami, liczba egzemplarzy/numer egzemplarza),
- informacje o podstawie prawnej opracowania,
- decyzję o warunkach zabudowy i zagospodarowania terenu dla lokalizacji tego wymagających,
- uzgodnienia branżowe i specjalistyczne z protokołami ZUDP,
- pozwolenie na budowę dla lokalizacji tego wymagających,
- ogólny opis techniczny przedmiotu projektu,
- symbolikę i oznaczenia wykorzystane w projekcie budowlanym,
- spis rysunków i schematów zawartych w projekcie budowlanym,
- ogólny pogląd sytuacyjny na mapie w skali 1:10000,
- szczegółową lokalizację projektowanych studni kablowych przedstawiony na mapach geodezyjnych dopuszczonych na danym terenie do projektowania w skali 1:500,
- wypisy z ewidencji gruntów działek, których dotyczy dokumentacja potwierdzone przez właściwy urząd,
- komplet oryginałów zgód właścicieli gruntów i nieruchomości na wykonanie robót budowlanych w oparciu o przedmiotową dokumentację.

Projekt wykonawczy powinien zawierać co najmniej:
- stronę tytułową (tytuł, branża, dane inwestora, data wykonania, dane Wykonawcy projektu, nazwiska projektantów, opracowujących i sprawdzających projekt z podpisami i pieczątkami, liczba egzemplarzy/numer egzemplarza),
- informacje o podstawie prawnej opracowania,
- nr projektu budowlanego na podstawie, którego został wykonany projekt wykonawczy,
- szczegółowy opis techniczny projektowanej linii tj. charakterystykę:
    - zastosowanych materiałów,
    - budowanej kanalizacji teletechnicznej wraz ze studniami kablowymi,
    - budowanej sieci światłowodowej,
    - uszczelniania kanalizacji,
    - układania i montażu zapasów kabla,
    - oznakowania kabla,
    - wykonania przecisków i przewiertów sterowanych pod nawierzchnią ulic,
    - pomiarów optycznych kabli,
    - przebiegu i zakończeń kabli;
- symbolikę i oznaczenia wykorzystane w projekcie wykonawczym,

- spis rysunków i schematów zawartych w projekcie wykonawczym,
- szczegółowy przebieg trasowy linii optotelekomunikacyjnej przedstawiony na mapach do celów projektowych wraz ze wszystkimi elementami składowymi linii,
- schemat rozwinięty kanalizacji teletechnicznej,
- schemat budowy kabli światłowodowych,
- schemat optyczny linii światłowodowej,
- przedmiar robót.

Wykonawca dostarczy dokumentację logiczną kabla i przyłączy światłowodowych wraz z pomiarami torów światłowodowych, schematami połączeń oraz szaf dystrybucyjnych.

Wykonawca dokona pomiarów torów światłowodowych, co udokumentuje w dokumentacji.

WYMAGANIA DOTYCZĄCE ROBÓT BUDOWLANYCH

1. Kierownik budowy

Kierownikiem budowy powinna być osoba posiadająca uprawnienia budowlane bez ograniczeń z przynależnością do izby budowlanej właściwej specjalności, posiadająca doświadczenie w procesie budowania właściwej branży który będzie osobiście nadzorował budowę i przebywał na terenie budowy – Ełk. Kierownik budowy powinien uzyskać wszelkie zezwolenia i decyzje na prowadzenie robót w pasach drogowych dróg publicznych oraz prowadzić roboty pod nadzorem gestorów sieci z zachowaniem zapisów i uzgodnień opinii ZUDP oraz uzgodnień branżowych i dyspozycji Zamawiającego.

Po zrealizowaniu procesu budowy kierownik budowy powinien przeprowadzić badania i pomiary kontrolne, opracować dokumentację powykonawczą oraz zgromadzić i przekazać Zamawiającemu komplet dokumentów związanych z zakończeniem budowy.

2. Roboty tymczasowe i prace towarzyszące.

Koszty wykonania robót tymczasowych , czasowego zajęcia terenów oraz prac towarzyszących obciążają Wykonawcę. Wykonawca zobowiązany jest uwzględnić te koszty w cenie oferty. Zakres i charakter robót tymczasowych zależeć będzie od przyjętej przez Wykonawcę organizacji robót budowlanych, zastosowanych konkretnych technologii, organizacji zaplecza budowy. Do robót tymczasowych należy zaliczyć ponadto:
- organizację zaplecza socjalnego i zaplecza budowy, montaż zasileń tymczasowych i urządzeń pomiarowych,
- stosowanie tymczasowych ogrodzeń, zabezpieczeń i oznakowań wykopów,
- stosowanie osłon i zabezpieczeń ochrony zieleni,
- stosowanie osłon i zabezpieczeń pomieszczeń przed skutkami prowadzonych prac.

W trakcie realizacji przedmiotu zamówienia Wykonawca zobowiązany jest:
- stosować środki ochrony istniejącej zieleni (drzewa i krzewy) w celu zabezpieczenia przed zniszczeniem i uszkodzeniem,
stosować stabilne ogrodzenia (zabezpieczenia) przy wykonywaniu wykopów dla montażu studni kablowych,
- oznakować zgodnie z przepisami BHP wykopy liniowe kanalizacji,
- zasypki wykopów prowadzić warstwami z zagęszczeniem warstwami,
- w miejscach wykopów odtworzyć nawierzchnię trawników z uzupełnieniem czarnoziemu i dosianiem trawy,

- wykonać tablice informacyjne o realizowanym projekcie i umieści na czas robót budowlanych, a następnie oznaczy wykonane prace zgodnie z zestawem znaków graficznych zgodnie z załącznikiem nr 1 do Strategii Komunikacji Funduszy Europejskich w Polsce w ramach Narodowej Strategii Spójności na lata 2007-2013: Księga Identyfikacji Wizualnej Narodowej Strategii Spójności.

3. Zastosowane materiały, dobór sprzętu oraz inne obowiązki Wykonawcy

Wykonawca ma prawo dowolnego wyboru materiałów pod warunkiem, że są to materiały fabrycznie nowe oraz posiadają co najmniej wymagane w wytycznych do budowy właściwości i parametry, są dopuszczone do stosowania w budownictwie polskim, gwarantują poprawność wykonania robót i całości przedmiotu zamówienia. W przypadku gdy Wykonawca nie udokumentuje poprawności wyboru materiału Zamawiający ma prawo odmówić odbioru elementu robót lub ich całości. Udokumentowanie następuje na podstawie właściwych dokumentów odniesienia (FV źródłowe, deklaracje zgodności, certyfikaty, atesty).

Decyzja w zakresie doboru i stosowania sprzętu, maszyn lub środków transportu w celu realizacji przedmiotu zamówienia w terminie oraz poprawnej jakości należy do Wykonawcy. Zastosowany sprzęt, maszyny lub środki transportu nie mogą stwarzać zagrożenia dla ludzi, ich mienia lub mienia Zamawiającego.

Wykonawca zobowiązany będzie do utrzymania w należytym porządku terenu prowadzonych prac, ich otoczenia oraz zaplecza budowy. Wykonawca zobowiązany jest do sukcesywnego wywozu na wysypisko wszystkich odpadów powstałych w wyniku realizowania przez niego przedmiotu zamówienia.

Wykonawca zobowiązany jest na swój koszt zapewnić obsługę geodezyjną oraz dołączyć oświadczenie geodety uprawnionego o długościach zgłoszonej - wybudowanej kanalizacji do Powiatowego Ośrodka Dokumentacji Geodezyjnej w Ełku.

Wykonawca dostarczy dokumentację logiczną kabla i przyłączy światłowodowych wraz z pomiarami torów światłowodowych, schematami połączeń oraz szaf dystrybucyjnych.

4. Warunki techniczne i normy.

Wszystkie roboty objęte niniejszym projektem należy wykonać zgodnie z obowiązującymi normami i przepisami, w szczególności normami zakładowymi TP S.A.:

- Instrukcja T-01. Odbiór i utrzymanie kablowych linii telekomunikacyjnych.
- ZN-96/TPSA-002. Linie optotelekomunikacyjne. Ogólne wymagania techniczne.
- ZN-96/TPSA-004. Zbliżenia i skrzyżowania z innymi urządzeniami uzbrojenia terenowego-Ogólne wymagania techniczne.
- ZN-96/TPSA-005. Kable optotelekomunikacyjne jednomodowe dalekosiężne. – Wymagania i badania.
- ZN-96/TPSA-006. Linie optotelekomunikacyjne. Złącza spajane światłowodów jednomodowych.
- ZN-96/TPSA-007. Linie optotelekomunikacyjne. Złączki światłowodowe i kable stacyjne.-Wymagania i badania.
- ZN-96/TPSA-008. Linie optotelekomunikacyjne. Osłony złączowe.-Wymagania i badania.
- ZN-96/TPSA-009. Kablowe linie optotelekomunikacyjne. Przełącznice światłowodowe-Wymagania i badanie.

- ZN-96/TPSA-011. Telekomunikacyjna kanalizacja kablowa-Ogólne wymagania techniczne.
- ZN-96/TPSA-012. Kanalizacja kablowa pierwotna-Wymagania i badania.
- ZN-96/TPSA-013. Kanalizacja wtórna i rurociągi kablowe-Wymagania i badania.
- ZN-96/TPSA-014. Rury z polichlorku winylu (RPCW)-Wymagania i badania.
- ZN-96/TPSA-015. Rury polipropylenowe RPP i polietylenowe RPE kanalizacji pierwotnej- Wymagania i badania.
- ZN-96/TPSA-016. Rury polietylenowe karbowane dwuwarstwowe (RHDPEk)-Wymagania i badania.
- ZN-96/TPSA-017. Rury kanalizacji wtórnej i rurociągu kablowego (RHDPE)-Wymagania i badania.
- ZN-96/TPSA-018. Rury polietylenowe (RHDPEp) przepustowe-Wymagania i badania.
- ZN-96/TPSA-019. Rury trudnopalne (RHDPEt)-Wymagania i badania.
- ZN-96TPSA-020. Złączki rur kanalizacji kablowej-Wymagania i badania.
- ZN-96/TPSA-021. Uszczelki końców rur kanalizacji kablowej-Wymagania i badania.
- ZN-96/TPSA-022. Przywieszka identyfikacyjna-Wymagania i badania.
- ZN-96/TPSA-023. Studnie kablowe-Wymagania i badania.
- ZN-96/TPSA-024. Zasobnik złączowy- Wymagania i badania.
- ZN-96/TPSA-025. Taśmy ostrzegawcze i ostrzegawczo-lokalizacyjne-Wymagania i badania.
- ZN-96/TPSA-026. Słupki oznaczeniowe i oznaczeniowo-pomiarowe- Wymagania i badania.
- Zn-96/TPSA-041. Zabezpieczone pokrywy studni kablowych, dodatkowe (wewnętrzne)- Wymagania i badania.

XV. Sprzęt aktywny

Wykonawca dostarczy 15 sztuk sprzętu aktywnego, w tym:

10 szt. przełączników, z których każdy musi spełniać minimum:
Musi być wyposażony w minimum 48 portów 10/100/1000 RJ45, 4 porty SFP oraz 1 port konsolowy
Musi obsługiwać łączenie w jeden przełącznik wirtualny pod kątem zarządzania dowolnego typu kombinacji przełączników tej samej serii, umożliwiając podłączanie do sieci przełączników z 24 i 48 portami 10/100/1000, z portami 100Base-FX i Power-over-Ethernet, poprzez media miedziane, światłowody wielomodowe i jednomodowe.
Musi zapewniać przepustowość przełączania na poziomie minimum 100 Gbps
Musi obsługiwać pojedynczy adres IP do zarządzania wieżą.
Musi obsługiwać redundantne zarządzanie wieżą.
Musi obsługiwać opcjonalnie zapasowe źródło zasilania.
Musi obsługiwać technologię zamkniętej pętli w stosie.
Musi obsługiwać technologie IEEE 802.1D (MAC Bridges) i IEEE 802.1t (802.1D Maintenance)
Musi obsługiwać technologię IEEE 802.1s Multiple Spanning Tree.
Musi obsługiwać technologię IEEE 802.1w Rapid Reconfiguration of Spanning Tree.
Musi obsługiwać do 16,000 adresów MAC.

Musi zapewniać 8 przypisanych do użytkowników kolejek o określonych priorytetach na każdy port.
Musi obsługiwać technologię Link Aggregation (IEEE 802.3ad).
Musi obsługiwać technologie Many-to-One Port Mirroring oraz One-to-One Port Mirroring
Musi obsługiwać technologię IGMP Snooping v1, v2i v3.
Musi obsługiwać technologie Weighted Round Robin Queuing (WRR) i Strict Priority Queuing.
Musi obsługiwać jednocześnie do 4,094 ID sieci VLAN oraz do 255 dynamicznych VLAN w jednym przełączniku.
Musi mieć możliwość obsługi statycznego routingu
Musi obsługiwać sieci VLAN IEEE 802.1Q oparte na portach i tagach z pełnym wsparciem protokołów GARP i GVRP.
Musi obsługiwać uwierzytelnianie IEEE 802.1X na wszystkich portach.
Musi obsługiwać uwierzytelnianie wykorzystujące adres MAC
Musi być w pełni zarządzany przy pomocy standardowych interfejsów z wierszami poleceń (CLI), wbudowanych interfejsów webowych z SSL, technologii Telnet z SSH i dowolnej aplikacji zarządzającej SNMP oraz po http.
Musi obsługiwać następujące grupy RMON: Statistics, History, Alarms, Events.
Musi obsługiwać protokół SNMP v1/2 i v3
Musi działać w temperaturze otoczenia do 50°C
Musi posiadać gwarancję obejmującą aktualizację oprogramowania firmware i łaty naprawiające błędy oprogramowania (bug fixes), wsparcie telefoniczne oraz zaawansowaną wymianę sprzętu (wysyłka następnego dnia roboczego).
Musi być w pełni kompatybilny z posiadanym przez Zamawiającego systemem zarządznia infrastrukturą aktywną.

3 szt. przełączników, z których każdy musi spełniać minimum:

Przełączniki muszą mieć możliwość łączenia w stosy/wieże do 8 przełączników lub budowę modularną, zapewniając możliwość rozbudowy liczby portów w poszczególnych punktach dystrybucyjnych,
Połączenie urządzeń w stos/wieżę powinno zapewniać redundancję - połączenie przełączników w pętlę zwrotną,
Zarządzanie stosem/wieżą poprzez 1 adres IP.
Minimum 48 portów 10/100/1000 BASE-T RJ45, z technologią auto-sensing, auto-negotiating MDI/MDI-X
Minimum 4 porty uplink 1000Base-X SFP – dopuszcza się wykorzystanie portów podwójnego zastosowania (COMBO),
Minimum 2 dedykowane porty do łączenia w stos/wieżę nie ograniczające liczby portów dostępowych,
Minimum 1 port konsolowy do zarządzania przełącznikiem.
Standardowy stelaż teletechniczny 19” typu Rack o wysokości nie większej niż 1 U.
Minimalna wielkość pamięci SDRAM: 512 MB,
Minimalna wielkość pamięci FLASH: 32 MB.
Minimalna przepustowość: 70 Mpps,
Minimalna przepustowość przełączania: 90 Gbps na przełącznik,
Minimalna wydajność połączenia w stosie: 48 Gbps, a w urządzeniach modularnych minimum 48 Gbps pomiędzy modułami,
Przełącznik musi zapewniać przełączanie z pełną prędkością łącza w obie strony.

Przełączniki muszą mieć możliwość doposażenia w system redundantnego zasilania zapewniając zasilanie dla wszystkich portów.
Minimalna liczba adresów: 32 000.
Obsługa sieci VLAN zgodnych ze standardem IEEE 802.1Q z pełnym wsparciem dla protokołów GARP i GVRP,
Obsługa minimum 4 000 ID sieci VLAN oraz minimum 1 000 sieci VLAN aktywnych jednocześnie w pojedynczym stosie.
Przełącznik musi obsługiwać następujące funkcjonalności:
- SNMP v1/v2c/v3,
- Standardowy interfejs wiersza poleceń CLI,
- Secure Shell (SSHv2),
- Secured Socket Layer (SSL),
- RFC 2865 RADIUS,
- RFC 2866 RADIUS Accounting,
- TACACS+, przy czym TACACS+ musi zapewniać obsługę zarządzania AAA (uwierzytelniania, autoryzacja i audytowanie).
- Obsługa wielu obrazów oprogramowania z funkcją odtwarzania,
- Obsługa wielu plików konfiguracyjnych,
- Plik konfiguracyjny w formie tekstowej,
- Telnet,
- Syslog,
- Secure Copy oraz Secure FTP,
- Simple Network Time Protocol (SNTP) lub NTP,
- RMON – wsparcie dla 6 różnych grup,
- Port mirroring (jeden do jednego, wiele do jednego),
- Monitorowanie źródła zasilania i układu chłodzenia poprzez SNMP,
- Redundantne zarządzanie stosem.

Przełącznik musi obsługiwać następujące protokoły i technologie:
LLDP/LLDP-MED
802.3ad Link Aggregation
802.1D MAC Bridges
802.1s Multiple Spanning Tree
802.1t Path Cost Amendment to 802.1D
802.1w Rapid re-convergence of Spanning Tree
802.3x Flow Control
IP Multicast (IGMPv1,v2,v 3)
IGMP v1/v2/v3 Snooping
Ramki Jumbo Frames (minimum 9 kB)
Standardowe listy ACL
Rozszerzone listy ACL
RIPv1 i RIPv2,
Trasy statyczne
DHCP/BootP Relay
Musi mieć możliwość pracy w architekturze bezpieczeństwa opartej na rolach. Zapewniając ciągłe zarządzanie tożsamością wraz z opartymi na rolach funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma,
Ochrona przed atakami typu DHCP/ARP Spoof Protection
Obsługa MAC Port Locking (dynamiczne i statyczne).
Przełącznik musi obsługiwać następujące funkcjonalności:

Obsługa priorytetów zgodna z IEEE 802.1p,
Możliwość klasyfikacji pakietów w warstwach L2-L4 według:
ID portu fizycznego,
Adresie MAC,
Podsieci IP,
Adresie IP,
Typie protokołu IP,
IP ToS (Type of Service),
DSCP (Differentiated Services Code Point),
Porcie TCP/UDP,
Sprzętowo realizowana obsługa minimum 8 kolejek priorytetów na każdym porcie,
Obsługa wielu mechanizmów kolejkowania (SPQ, WRR oraz ich kombinacji),
Obsługa kontroli poziomu pasma wychodzącego i przychodzącego w każdym przepływie, rate-limit dla ruchu wchodzącego i wychodzącego,
Możliwość przypisania ruchu do różnych sieci VLAN zgodnie z kryteriami L2-L4, nawet jeśli nie jest skonfigurowany protokół 802.1Q VLAN Tagging.
Urządzenie musi obsługiwać następujące metody uwierzytelniania:
poprzez IEEE 802.1x,
wykorzystujące adres MAC,
wykorzystujące przeglądarkę internetową,
Uwierzytelnianie wielu użytkowników jednocześnie przez 802.1X, portal i/lub adres MAC, dla minimalnie 4 użytkowników/urządzeń na port,
Obsługa Dynamic VLAN Assignment (RFC 3580),
Obsługa wielu użytkowników RFC-3580 na jednym porcie Gigabit Ethernet (minimum 4).

Gwarancja 5 lat.

2 szt. przełączników, z których każdy musi spełniać minimum:

Przełączniki muszą mieć możliwość łączenia w stosy/wieże do 8 przełączników lub budowę modularną, zapewniając możliwość rozbudowy liczby portów w poszczególnych punktach dystrybucyjnych,
Połączenie urządzeń w stos/wieżę powinno zapewniać redundancję - połączenie przełączników w pętlę zwrotną,
Zarządzanie stosem/wieżą poprzez 1 adres IP.
Minimum 48 portów 10/100/1000 BASE-T RJ45 PoE (zgodnych ze standardami 802.3.af oraz 802.3.at), z technologią auto-sensing, auto-negotiating MDI/MDI-X
Minimum 4 porty uplink 1000Base-X SFP – dopuszcza się wykorzystanie portów podwójnego zastosowania (COMBO),
Minimum 2 dedykowane porty do łączenia w stos/wieżę nie ograniczające liczby portów dostępowych,
Minimum 1 port konsolowy do zarządzania przełącznikiem.
Standardowy stelaż teletechniczny 19” typu Rack o wysokości nie większej niż 1 U.
Minimalna wielkość pamięci SDRAM: 512 MB,
Minimalna wielkość pamięci FLASH: 32 MB.
Minimalna przepustowość: 70 Mpps,
Minimalna przepustowość przełączania: 90 Gbps na przełącznik,
Minimalna wydajność połączenia w stosie: 48 Gbps,
Przełącznik musi zapewniać przełączanie z pełną prędkością łącza w obie strony.

Przełączniki muszą być wyposażone w zasilanie PoE niezbędne do zasilania punktów dostępowych WLAN, kamer oraz innych urządzeń PoE w standardzie 802.3at oraz 802.3af,
Przełączniki dodawane do stosu/wieży muszą zapewniać moc do 375W dla funkcjonalności PoE,
Przełączniki muszą mieć możliwość doposażenia w system redundantnego zasilania zapewniając zasilanie dla wszystkich portów PoE zgodnie ze standardami 802.3af oraz 802.3at.
Minimalna liczba adresów: 32 000.
Obsługa sieci VLAN zgodnych ze standardem IEEE 802.1Q z pełnym wsparciem dla protokołów GARP i GVRP,
Obsługa minimum 4 000 ID sieci VLAN oraz minimum 1 000 sieci VLAN aktywnych jednocześnie w pojedynczym stosie.
Funkcje zarządzania Przełącznik musi obsługiwać następujące funkcjonalności:
SNMP v1/v2c/v3,
Standardowy interfejs wiersza poleceń CLI,
Secure Shell (SSHv2),
Secured Socket Layer (SSL),
RFC 2865 RADIUS,
RFC 2866 RADIUS Accounting,
TACACS+, przy czym TACACS+ musi zapewniać obsługę zarządzania AAA (uwierzytelniania, autoryzacja i audytowanie).
Obsługa wielu obrazów oprogramowania z funkcją odtwarzania,
Obsługa wielu plików konfiguracyjnych,
Plik konfiguracyjny w formie tekstowej,
Telnet,
Syslog,
Secure Copy oraz Secure FTP,
Simple Network Time Protocol (SNTP) lub NTP,
RMON – wsparcie dla 6 różnych grup,
Port mirroring (jeden do jednego, wiele do jednego),
Monitorowanie źródła zasilania i układu chłodzenia poprzez SNMP,
Redundantne zarządzanie stosem.
Przełącznik musi obsługiwać następujące protokoły i technologie:
LLDP/LLDP-MED,
802.3ad Link Aggregation,
802.1D MAC Bridges,
802.1s Multiple Spanning Tree,
802.1t Path Cost Amendment to 802.1D,
802.1w Rapid re-convergence of Spanning Tree,
802.3x Flow Control,
IP Multicast (IGMPv1,v2,v 3),
IGMP v1/v2/v3 Snooping,
Ramki Jumbo Frames (minimum 9 kB),
Standardowe listy ACL,
Rozszerzone listy ACL,
RIPv1 i RIPv2,
Trasy statyczne,
DHCP/BootP Relay.
Przełącznik musi obsługiwać następujące funkcjonalności:

Musi mieć możliwość pracy w architekturze bezpieczeństwa opartej na rolach. Zapewniając ciągłe zarządzanie tożsamością wraz z opartymi na rolach funkcjami uwierzytelniania, autoryzacji, QoS i ograniczania pasma,
Ochrona przed atakami typu DHCP/ARP Spoof Protection
Obsługa MAC Port Locking (dynamiczne i statyczne).
QoS Przełącznik musi obsługiwać następujące funkcjonalności:
Obsługa priorytetów zgodna z IEEE 802.1p,
Możliwość klasyfikacji pakietów w warstwach L2-L4 według:
ID portu fizycznego,
Adresie MAC,
Podsieci IP,
Adresie IP,
Typie protokołu IP,
IP ToS (Type of Service),
DSCP (Differentiated Services Code Point),
Porcie TCP/UDP,
Sprzętowo realizowana obsługa minimum 8 kolejek priorytetów na każdym porcie,
Obsługa wielu mechanizmów kolejkowania (SPQ, WRR oraz ich kombinacji),
Obsługa kontroli poziomu pasma wychodzącego i przychodzącego w każdym przepływie, rate-limit dla ruchu wchodzącego i wychodzącego,
Możliwość przypisania ruchu do różnych sieci VLAN zgodnie z kryteriami L2-L4, nawet jeśli nie jest skonfigurowany protokół 802.1Q VLAN Tagging.
Urządzenie musi obsługiwać następujące metody uwierzytelniania:
poprzez IEEE 802.1x,
wykorzystujące adres MAC,
wykorzystujące przeglądarkę internetową,
Uwierzytelnianie wielu użytkowników jednocześnie przez 802.1X, portal i/lub adres MAC, dla minimalnie 4 użytkowników/urządzeń na port,
Obsługa Dynamic VLAN Assignment (RFC 3580),
Obsługa wielu użytkowników RFC-3580 na jednym porcie Gigabit Ethernet (minimum 4).
Gwarancja 5 lat.