załącznik Nr 6 do SIWZ

Nr sprawy: *BZP.271.12.2011*

Szczegółowy opis przedmiotu zamówienia

„Dostawa i instalacja sprzętu komp., sieciowego, serwerów, macierzy, adaptacja pomieszczeń pod serwerownię”
w ramach projektu „e-Ełk: usługi i aplikacje dla przedsiębiorców”

Wdrożenie urządzeń sieciowych LAN/ MPLS, Bezpieczeństwa styku sieci z Internetem oraz systemu klasy Data Center wraz z oprogramowaniem wirtualizacyjnym i systemami operacyjnymi w pomieszczeniu serwerowni.
Wykonanie instalacji teletechnicznych i zabezpieczenia mienia w pomieszczeniu serwerowni.
Dostawę sprzętu do cyfryzacji.

Wymagania ogólne dla dostarczanego sprzętu i oprogramowania (dotyczy wszystkich systemów opisanych w tym dokumencie).

- 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.
- W momencie składania oferty wszystkie elementy architektury muszą być dostępne w sprzedaży przez producenta
- Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie wymaganym w SIWZ . 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 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.
- W wypadku powzięcia wątpliwości co do zgodności oferowanych produktów z umową, w szczególności w zakresie legalności oprogramowania, Zamawiający jest uprawniony do:
    - zwrócenia się do producenta oferowanych produktów o potwierdzenie ich zgodności z umową (w tym także do przekazania producentowi niezbędnych danych umożliwiających weryfikację), oraz

- zlecenia producentowi oferowanych produktów, lub wskazanemu przez producenta podmiotowi, inspekcji produktów pod kątem ich zgodności z umową oraz ważności i zakresu uprawnień licencyjnych

Jeżeli inspekcja, o której mowa powyżej wykaże niezgodność produktów z umową lub stwierdzi, że korzystanie z produktów narusza majątkowe prawa autorskie osób producenta, koszt inspekcji zostanie pokryty przez Wykonawcę, według rachunku przedstawionego przez podmiot wykonujący inspekcję, w kwocie nie przekraczającej 5% wartości zamówienia (ograniczenie to nie dotyczy kosztów poniesionych przez Strony w związku z inspekcją, jak np. konieczność zakupu nowego oprogramowania). Prawo zlecenia inspekcji nie ogranicza ani nie wyłącza innych uprawnień Zamawiającego, w szczególności prawa do żądania dostarczenia produktów zgodnych z umową oraz roszczeń odszkodowawczych

- Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej (tzn. opublikowanej przez producenta nie wcześniej niż 6 miesięcy) na dzień poprzedzający dzień składania ofert
- Serwery i macierze muszą pochodzić od jednego producenta i muszą posiadać Certyfikat „B" (dla obudowy) lub oznakowanie CE produktu albo spełniać normy równoważne.
- Serwery muszą być przygotowane do współpracy z serwerowymi systemami operacyjnymi: Microsoft Windows 2003/2008, Linuks, Sun Solaris lub równoważnymi, w tym muszą umożliwiać używanie systemów operacyjnych 64-bit.
- Zamawiający dopuszcza realizację poszczególnych grup funkcjonalnych przez zespoły urządzeń pod następującymi warunkami:
  - 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),
  - łączna wielkość zestawu nie będzie przekraczać wymaganej wielkości urządzenia,
  - zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zespołu urządzeń,
  - wszystkie elementy zestawu będą spełniały wymagania związane z zarządzaniem,
  - Przed podpisaniem umowy wybrany wykonawca przedstawi szczegółowy opis zespołu, obejmujący schematy połączeń, określenie które elementy zestawu odpowiadają za poszczególne funkcjonalności itp.
- W ofercie należy umieścić szczegółowe konfiguracje oferowanych urządzeń (identyfikatory katalogowe, opisy itp.), pozwalające je jednoznacznie zidentyfikować .
- Wszystkie wymagane funkcjonalności muszą być dostępne w dniu składania oferty. Zamawiający zastrzega sobie możliwość:
  - wystąpienia do Oferenta o wskazanie w publicznie dostępnej dokumentacji producenta (strona WWW) potwierdzenia spełnienia wymogów; nie spełnienie tego warunku w ciągu 5 dni roboczych będzie skutkowało odrzuceniem oferty,
  - wystąpienia do producenta rozwiązania o potwierdzenie spełniania wymogów,
  - przeprowadzenia testów przed wyborem oferty – dostawcy będą na żądanie Zamawiającego zobowiązani do dostarczenia urządzeń testowych w ciągu 30 dni od wezwania.
- Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ±10%, 50 Hz.

- Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej.

Wdrożenie urządzeń sieciowych LAN/ MPLS, Bezpieczeństwa styku sieci z Internetem oraz systemu klasy Data Center wraz z oprogramowaniem wirtualizacyjnym i systemami operacyjnymi.

W ramach rozbudowy infrastruktury sprzętowo-programowej Urzędu Miasta w Ełku, Wykonawca dostarczy i wdroży w serwerowni Urzędu Miasta w Ełku, przy ul. Józefa Piłsudskiego 4 oraz obejmie całość wdrożenia 5-letnim serwisem gwarancyjnym na zasadach ogólnych i szczegółowych przedstawionych dla wszystkich pozycji sprzętowych i oprogramowania, opisanych poniżej.

Wykonawca, w całym okresie gwarancji, jest zobowiązany dostarczać aktualizacje oprogramowania dla wszystkich systemów objętych postępowaniem oraz suporty bezpieczeństwa i oprogramowanie systemowe wymagane przez producentów zaproponowanych technologii.

Zakres realizacji projektu obejmuje dostawę i wdrożenie następujących elementów:

I. System archiwizacji (back up) o pojemności do 5 TB dla dostarczanych serwerów typu blade wraz z niezbędnym sprzętem i oprogramowaniem – 1kpl.
II. UPS 20kVA - 1szt.
III. Zarządzany przełącznik serwerowy z wbudowaną funkcją obsługi BGP wraz systemem zarządzania – 1 kpl.
IV. System szaf 19 - 1szt.
V. Przełącznik szkieletowy MPLS – 1 szt.
VI. Moduł szyfracji HSM z dedykowanym serwerem - 1 kpl.
VII. System personalizacji kart – 1 kpl.
VIII. Serwery do obsługi portali - 1szt. (typ blade)
IX. System operacyjny dla serwerów – 2 licencje (licencje dożywotnie)
X. Serwer relacyjnej bazy danych – 2 licencje (licencje dożywotnie)
XI. Oprogramowanie AV dla serwerów - 10 licencji, w tym 7 licencji dla serwerów wirtualnych, 3 licencje dla serwerów fizycznych
XII. Stacja mobilna zarządzająca - 3szt.
XIII. Instalacja łączy – 2szt.
XIV. Kompletny system zabezpieczeń klasy UTM posiadający m.in. takie mechanizmy jak: AV, IPS, Web filtering, Firewall, IPSEC i SSL VPN – 1 szt.
XV. Podsystem dyskowy kontroler macierzowy – 1 szt.
XVI. System serwerowy Blade – 1 kpl. (półka + 3 serwery typu blade)
XVII. Oprogramowanie monitorujące serwery - 1szt.
XVIII. Stacjonarna stacja zarządzająca KVM – 1 szt.
XIX. Licencje wirtualizacyjne -- Zamawiający wymaga dostarczenia licencji bezterminowych z 5-letnim okresem subskrypcji i wsparcia dla środowiska wirtualizacyjnego, dla dostarczanych w niniejszym postępowaniu **2 szt.** serwerów kasetowych (blade). Pozostałe serwery będą maszynami fizycznymi.
XX. Agregat prądotwórczy

XXI. Klimatyzacja
XXII. Podłoga techniczna
XXIII. Okablowanie LAN
XXIV. Rozbudowa istniejącego systemu kontroli dostępu do pomieszczenia serwerowni, systemu alarmowego i monitoringu
XXV. Dostawa systemu Szaf serwerowych 19" wraz z systemem monitoringu
XXVI. Wdrożenie systemów wczesnej detekcji pożaru w pomieszczeniu serwerowni.
XXVII. Sprzęt do cyfryzacji

I. System archiwizacji o pojemności 5 TB wraz z niezbędnym sprzętem i oprogramowaniem – 1 kpl.

Zamawiający w ramach zadania wymaga zrealizowania systemu archiwizacji o pojemności 5TB, na który mają składać się:
a) serwer typu blade - 1 szt.
b) dedykowana macierz - 1 szt.
c) dedykowane oprogramowanie do backup wraz z wymaganymi licencjami i suportem w całym okresie gwarancji (tj. 5 lat)

Wymaga się, aby dostawa obejmowała:
- 5 –letnią gwarancję producenta na dostarczony sprzęt
- Serwis producenta do końca okresu gwarancji
- Dostarczanie subskrypcji w pełnym zakresie oprogramowania i funkcjonalności wymaganych w tym postępowaniu, aktualizacji oprogramowania do końca okresu gwarancji w całym zakresie wymaganym przez producenta sprzętu i oprogramowania
- Dostarczenie deklaracji zgodności CE na dostarczony sprzęt (wraz z dostawą).

Ad. a) Minimalne wymagania techniczno-funkcjonalne dla serwera backup zostały opisane w **pkt. XVI. 2 Serwery kasetowe Blade**, niniejszego dokumentu.

Ad. b) Zamawiający wymaga dostarczenia macierzy dyskowej do backup o następujących parametrach minimalnych:

1. Macierz dyskowa musi być wyposażona w minimum 5 dysków SAS 6Gb/s 7200 obrotów/min o pojemności co najmniej 1 TB każdy.
2. Obudowa kontrolerów macierzy musi posiadać miejsca na instalacje co najmniej 12 dysków w technologii SAS 2.0 6Gb/s.
3. Macierz musi gwarantować możliwość rozbudowy, do co najmniej 96 dysków.
4. Macierz musi umożliwiać mieszanie w ramach obudowy i półki rozszerzeń dysków o prędkościach 15000, 1000 i 7200 obrotów/min.
5. Macierz musi być wyposażona w dwa kontrolery RAID pracujące w trybie active- active.
6. Macierz musi być wyposażona w minimum 4 (z możliwością rozbudowy do 8) zewnętrzne porty SAS 6Gb/s do podłączenia hostów.
7. Macierz musi być wyposażona w minimum 8 portów FC 8GB/s do podłączenia sieci SAN lub hostów.
8. Macierz musi być wyposażona w minimum 1,5GB pamięci cache przeznaczonej dla danych (sumarycznie dla obu kontrolerów) z możliwością rozbudowy do 3,5 GB.

9. Pamięć *cache* musi być kopiowana pomiędzy kontrolerami i podtrzymywana bateryjnie (wymagane baterie litowo jonowe). Dodatkowo w momencie utraty zasilania musi posiadać specjalne dyski, na które zostanie zapisana zawartość pamięci cache.
10. Awaria dowolnej półki dyskowej nie może powodować przerwania dostępu do dysków w pozostałych półkach dyskowych.
11. Macierz musi jednocześnie obsługiwać wolumeny zabezpieczone następującymi poziomami RAID: RAID 0, RAID 1, RAID 3, RAID 5, RADI 6 i RAID 10.
12. Macierz musi umożliwiać rozbudowę i stworzenie fizycznej grupy RAID-5 na co najmniej 30 dyskach z założeniem, że maksymalnie pojemność jednego dysku przeznaczona jest na informacje o parzystości (np. 29D+1P).
13. Macierz musi zapewnić możliwość wymiany dysków podczas pracy systemu (*Hot-Swap*).
14. Macierz musi wspierać sprzętowe szyfrowanie danych.
15. Rozwiązanie musi umożliwiać dynamiczną zmianę następujących parametrów macierzy dyskowej, bez przerywania dostępu do danych znajdujących się na modyfikowanym wolumenie, lub grupie dysków:
    a. Możliwość dynamicznej zmiany poziomu RAID dla istniejącej grupy RAID.
    b. Możliwość dynamicznego dodawania dysków do istniejących grup RAID.
    c. Możliwość dynamicznego powiększania rozmiaru wolumenów logicznych.
    d. Możliwość dynamicznej zmiany rozmiaru segmentu dla wolumenów logicznych.
    e. Możliwość dodawania kolejnych półek dyskowych oraz dysków bez przerywania pracy macierzy, dla dowolnej konfiguracji macierzy
    f. Możliwość aktualizacji oprogramowania macierzy (*firmware*) w trybie online.
16. Macierz musi umożliwiać rozbudowę o pojedyncze dyski fizyczne i pojedyncze półki rozszerzeń.
17. Macierz dyskowa musi umożliwiać dedykowanie dowolnego dysku fizycznego jako globalny dysk typu *Hot-Spare*. Musi istnieć możliwość definiowania min 5 globalnych dysków typu *Hot-Spare*.
18. Macierz musi mieć możliwość rozbudowy o funkcjonalność wykonywania natychmiastowej kopii danych (*point-in-time copy*). Funkcjonalność ta powinna być realizowana w trybie *copy-on-write*. Licencja na wykonywanie natychmiastowej kopii danych powinna obejmować całą przestrzeń dyskową oferowaną przez macierz.
19. Macierz musi mieć możliwość rozbudowy o funkcjonalność wykonywania pełnej kopii lokalnych wolumenów logicznych z wykorzystaniem jedynie kontrolerów macierzy. Licencja na wykonywanie kopii lokalnego wolumenu powinna obejmować całą przestrzeń dyskową oferowaną przez macierz.
20. Macierz dyskowa musi obsługiwać następujące systemy operacyjne: Microsoft Windows 2003, RedHat, SUSE, VMware, Microsoft Cluster Services, AIX, HP-UX .
21. Macierz dyskowa musi umożliwić redundantne podłączenie bezpośrednio minimum 4 serwerów za pomocą interfejsu FC. Licencje na oprogramowanie do automatycznego przełączania ścieżki dla każdego z 2 serwerów, dla wszystkich wspieranych systemów operacyjnych muszą być dołączone do macierzy bez dodatkowej opłaty.
22. Dane zapisywane w wewnętrznej pamięci *cache* jednego z kontrolerów muszą być także powielane w pamięci *cache* pozostałych kontrolerów, tak aby w przypadku uszkodzenia dowolnego kontrolera zachowana była spójność danych.
23. Wszystkie krytyczne komponenty macierzy takie jak: kontrolery dyskowe, pamięć *cache*, zasilacze i wentylatory muszą być zdublowane, tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu. Komponenty te muszą być wymienialne w trakcie pracy macierzy.
24. Macierz musi mieć możliwość jednoczesnego zasilania z dwóch niezależnych źródeł zasilania. Zanik jednego z nich nie może powodować przerwy w pracy urządzenia ani zmniejszenia jego wydajności lub utraty danych.

25. Macierz musi oferować zarządzanie poprzez sieć LAN oraz port szeregowy.
26. Macierz musi być wyposażona w zestaw do montażu w szafie przemysłowej rack 19". Obudowa z kontrolerami macierzy oraz półki dyskowe muszą mieć wysokość nie większą niż 2U.
27. Na macierz dyskową Oferent musi udzielić 5 lat gwarancji, z gwarantowanym czasem usunięcia awarii 24 godziny.
28. Oprogramowanie do zarządzania musi posiadać funkcjonalność interfejs graficzny oraz CLI (*command-line interface*).

Ad. c) Zamawiający wymaga dostarczenia **oprogramowania backupowego** o następujących parametrach minimalnych**:**

1. Powinno pozwalać na backup (wykonywanie kopii zapasowych) i odtwarzanie danych z dowolnych, konfigurowalnych zasobów dyskowych hostów.

2. Musi umożliwiać wykorzystanie kopii bezpieczeństwa w heterogenicznym środowisku (różne systemy operacyjne).

3. Musi posiadać modularną architekturę ułatwiającą rozbudowę w miarę rozrastania się infrastruktury informatycznej oraz wzrostu wolumenu danych.

4. Musi posiadać możliwość jednoczesnego sekwencyjnego zapisu wielu strumieni danych na pojedynczy napęd taśmowy.

5. Musi umożliwiać backup co najmniej 10 serwerów.

6. Musi umożliwiać obsługę dysku jako nośnika do zapisu kopii bezpieczeństwa w sposób umożliwiający jednoczesny zapis oraz odczyt danych w tym samym czasie o pojemności min. 5TB

7. Musi umożliwiać transfer backupowanych danych przez sieć lokalną (Ethernet) jak również oprogramowanie backupowe powinno wspierać backup przez sieć SAN, tzw. „LAN- free backup".

8. Musi umożliwiać łatwą rozbudowę o licencje umożliwiające odtworzenie serwerów pracujących na platformach Windows 2000 i Windows 2003 w trybie bare- metal-restore czyli bez potrzeby instalowania systemu operacyjnego oraz klienta systemu backupu.

9. Musi mieć możliwość rozszerzenia o moduł zapewniający de-duplikacji danych na źródle.

10. Musi mieć możliwość rozszerzenia o moduł zapewniający Continuos Data Protection .

11. Musi integrować się z mechanizmami Snapshotowymi macierzy jednakże nie jest to przedmiotem niniejszego zamówienia.

12. Musi zapewniać dedykowany moduł zapewniający spójny backup środowiska.

13. Musi być zarządzane z jednego miejsca poprzez jedną centralną konsolę zarządzającą.

14. Musi przechowywać informacje o wykonanych kopiach, harmonogram ich wykonywania oraz informacje o nośnikach używanych do realizacji celów we wbudowanej bazie danych.

15. Musi pozwalać na zapis backupów na taśmach w sposób pozwalający na odtworzenie ich w innym środowisku backupowym poprzez serwer pośredniczący (podłączony do napędu) o innej platformie systemu operacyjnego niż serwer zapisujący.

16. Musi zapewniać długoterminowe przechowywanie informacji o backupach poprzez możliwość przetrzymywania w wewnętrznej bazie danych informacji o całych zadaniach backupowych z pominięciem informacji o pojedynczych plikach minimalizując pojemność wewnętrznej bazy danych.

17. Musi mieć mechanizm regularnego, cyklicznego backupu własnej bazy danych.

18. Musi przechowywać wszystkie informacje o backupach, napędach taśmowych, mediach w centralnym miejscu możliwym do sklonowania na inną maszynę tak by można było na niej uruchomić serwer backupu. Proces klonowania może odbywać się przy wyłączonych procesach backupowych (zapewnienie spójności wewnętrznej bazy danych).

19. Powinno umożliwiać stworzenie polityki backupowej obejmującej pełne i przyrostowe backupy danych, harmonogram ich wykonywania oraz ich czas ważności.

20. Powinno umożliwiać backup więcej niż jednego systemu klienckiego jednocześnie.

21. Musi mieć możliwość ominięcia sieci LAN w celu wykonania backupu danych poprzez wykorzystanie sieci SAN. Licencja oprogramowania backupowego pozwalająca na backup z wykorzystaniem sieci SAN nie jest przedmiotem niniejszego zamówienia.

22. Musi zapewniać możliwość ręcznego uruchomienia backupu (dowolnego typu) danego systemu.

23. Musi umożliwiać odtworzenie danych z dowolnego punktu w czasie, w którym wykonana była kopia zapasowa w ramach zdefiniowanej polityki retencji danych. Dla backupu i odtwarzania oprogramowania backupowego musi zapewniać możliwość automatycznego wznowienia procesów backupu i odtwarzania w przypadku przerwania łączności z hostem.

24. Musi zapewniać współpracę i integrację z oprogramowaniem do de-duplikacji danych na źródle (deduplikacja na backupowanym serwerze) dostarczanym przez producenta oprogramowania backupowego. Integracja musi zapewniać możliwość wyboru backupu z de-duplikacją poprzez proste zaznaczanie odpowiedniego pola w konsoli zarządzającej wspólnej dla backupu tradycyjnego i z de-duplikacją.

25. Moduł do de-duplikacji musi zapewniać de-duplikacje bezpośrednio na zabezpieczonym serwerze (de-duplikacja na źródle) ze zmienna długością bloku minimalizując maksymalnie liczbę przesyłanych danych. Moduł do de-duplikacji nie jest przedmiotem niniejszego postepowania.

26. Operator oprogramowania backupowego powinien mieć możliwość zdefiniowania centralnie polityk backupowych dla grup serwerów/stacji roboczych lub – jeżeli zachodzi taka konieczność – dla dowolnego systemu z osobna (równolegle do zdefiniowanych grup).

27. Harmonogram wykonywania czynności backupowych powinien obejmować datę, godzinę i typ backupu (backup pełny, przyrostowy, różnicowy).

28. Haromonogramy muszą być realizowane automatycznie, bez konieczności ingerencji operatora.

29. Operator powinien mieć możliwość definiowania czasu własności backupu wyrażonego w dniach (ewentualnie miesiącach / latach).

30. Musi zapewnić możliwość wykonywania określonej przez operatora akcji związanej z procesem backupu na danym hoście (np. zatrzymanie procesów, wykonanie backupu i ponowne uruchomienie tych procesów).

31. Musi zapewniać możliwość zdalnego upgrade'u agentów oprogramowania backupowego na zabezpieczanym serwerze wykorzystując bezpieczny protokół SSL uniemożliwiający przejęcie kontroli nad zabezpieczanym serwerze przez osoby trzecie.

32. Powinna istnieć możliwość stworzenia dowolnej liczby puli taśm i przypisania do nich grup hostów i/lub pojedynczych hostów.

33. Musi umożliwiać zapisywanie backupów o tym samym terminie ważności na danej taśmie (zestawie taśm).

34. Powinno korzystać z mechanizmów lokalizacji taśmy - czytnika kodów paskowych zainstalowanego w bibliotece taśmowej.

35. W przypadku awarii fragmentu taśmy, oprogramowanie backupowe musi odtworzyć całość plików, które znajdują się na nieuszkodzonej części nośnika.

36. Musi umożliwić jednoczesne wykorzystanie w procesie zapisu danych wielu napędów biblioteki taśmowej.

37. Musi umożliwiać łączenie strumieni backupowych z wielu zabezpieczanych serwerów w sieci LAN i bezpośredni zapis na napędzie taśmowym (multiplexing).

38. Powinno zapewniać funkcjonalność pozwalającą na wykonanie duplikatów poszczególnych kopii danych oraz całych taśm w ramach biblioteki oraz między bibliotekami podłączonymi do różnych serwerów zarządzanych przez ten sam serwer backupowy – zarówno poprzez LAN jak i SAN.

39. Musi zapewniać różny czas ważności danych na podstawowym nośniku i nośniku zawierającym kopię (klonie).

40. Musi zapewniać możliwość wykonywania i składowania dowolnej ilości pełnych i przyrostowych kopii danych.

41. Musi umożliwiać szyfrowanie danych (plików, baz danych) na zabezpieczanym serwerze z kluczem minimum 256 bitowym.

42. Musi umożliwiać zapis na taśmie szyfrowanych danych oraz pozwalać na zarządzanie kluczami szyfrującymi.

43. Musi dostarczać własne narzędzie do autentykacji użytkowników bądź umożliwiać korzystanie z mechanizmów Active Directory, LDAP.

44. Odzyskiwanie danych musi być możliwe do wykonania w miejscu i na hoście z którego dane zostały pobrane jak również w inne, wskazane przez operatora miejsce i na innego wskazanego hosta.

45. Musi zapewnić mechanizmy bezkolizyjnego współdzielenia napędów taśmowych pomiędzy serwerami.

46. Musi zapewniać możliwość backupu na dysk. W trakcie backupu na dane urządzenie dyskowe musi być możliwość odtworzenia wszystkich dotychczas z backupowanych danych znajdujących się na tym urządzeniu dyskowym.

47. Musi zapewniać możliwość backupu serwerów nie posiadających dostępu do mediów backupowych poprzez dowolną liczbę serwerów pośredniczących (mających dostęp do mediów backupowych). Musi istnieć możliwość swobodnej zmiany serwerów pośredniczących w trakcie użytkowania systemu i oprogramowania backupowego. Całość konfiguracji powinna być zarządzana z pojedynczego serwera – serwera oprogramowania backupowego.
48. Zarządzanie powinno odbywać się z konsoli graficznej, zainstalowanej na komputerze pracującym pod kontrolą systemu Windows (Windows XP, rodzina Windows 2000, rodzina Windows 2003).

49. Informacje dotyczące kopii, harmonogramów backupów, nośników i zdarzeń muszą być dostępne z konsoli operatora systemu.

50. Musi posiadać mechanizm informowania administratorów o wystąpieniu błędów za pośrednictwem automatycznie generowanych wiadomości poczty elektronicznej.

51. Oferta powinna zawierać 5 letnie wsparcie ze strony producenta.

II. <u>System napięcia gwarantowanego UPS (20 kVA).</u>

System napięcia gwarantowanego UPS powinien charakteryzować się następującymi minimalnymi wymaganiami techniczno-funkcjonalnymi:

- Ma zapewniać ciągłe bezprzerwowe zasilanie w trybie TRUE ON-LINE z podwójnym przetwarzaniem przy zupełnych lub chwilowych zanikach napięcia, znacznych spadkach napięcia i wahaniach częstotliwości w sieci energetycznej, przez cały czas pracy urządzenia
- Ma zapewniać możliwość zwiększenia mocy UPS w trakcie jego eksploatacji: -upgrade min. 10 % (upgrade rozumiany jako programowe i sprzętowe zwiększenie mocy wyjściowej, a nie dostawienie następnego urządzenia)
- Musi być fabrycznie nowy tj. data produkcji nie może być wcześniejsza niż 6miesięcy przed datą zapytania ofertowego
- Częstotliwość wejścia i wyjścia zgodne z obowiązującymi w Polskich Normach tj.: 3x400V częstotliwość50 Hz
- Ma posiadać wejście trójfazowe 4-ro lub 5-cio przewodowe (TN- C* lub TN -S*)
- Ma mieć wyjście trójfazowe 5-cio przewodowe
- Minimalny czas pracy automatycznej UPS'a przy obciążeniu odbiorem o współczynniku mocy cos 0,8 musi wynosić 10 min.

- Ma zapewnić napięcie wejściowe 173 – 485 V +/- 2 %
- Współczynnik mocy PF > 0,95
- Ma być wyposażone w dwa bezprzerwowe przełączniki obejściowe, wewnętrzne.
- Ma być wyposażone w zdalny wyłącznik ppoż. (możliwy do wyniesienia na odległość min 50 m i zabezpieczony przed przypadkowym użyciem) umożliwiający wyłączenie napięcia wyjściowego urządzenia UPS w przypadku wystąpienia pożaru lub innych zagrożeń losowych
- Wyłącznik PPOŻ (EPO) wyłącznie przez sieć GSM
- Ma być wyposażone w hermetyczne, bezobsługowe akumulatory o minimalnej żywotności 6-9 lat
- Ma spełniać normy kompatybilności elektromagnetycznej EN 55022, EN 55011, EN 50091 (IEC 62040)
- Ma być wyposażone w osprzęt techniczny i oprogramowanie pozwalające na:
  - kontrolę i zarządzanie pracą urządzenia UPS z wykorzystaniem protokołu SNMP, automatyczne zamknięcie systemu operacyjnego stacji roboczych pracujących pod kontrolą systemu operacyjnego MS WINDOWS xx
- Ma zapewnić następujące parametry pracy: - stabilizacja napięcia wyjściowego przy obciążeniu statycznym , stabilizacja napięcia wyjściowego =<3% przy obciążeniu dynamicznym zmieniającym się od 100% do 0% i odwrotnie w czasie 10ms, stabilizacja częstotliwości napięcia wyjściowego 1% przy pracy z baterii
- Ma zapewnić częstotliwość przebiegu napięcia wyjściowego zgodną z częstotliwością przebiegu napięcia wejściowego przy odchyłkach częstotliwości napięcia 45-55Hz. Urządzenie ma zapewnić regulację tolerancji częstotliwości wejściowej automatycznie lub skokowo co 0,5Hz.
- Ma zapewnić sinusoidalny przebieg napięcia wyjściowego bez względu na charakter obciążenia, współczynnik odkształceń napięcia tzw. THDu<5% dla obciążeń nieliniowych i liniowych oraz współczynnik odkształceń prądu wejściowego THDi < 10% (z filtrem lub poprzez odpowiednią konstrukcję prostownika).
- Prąd zwarciowy wygenerowany przez falownik > 5 In
- Ma zapewnić czas reaktywacji baterii nie dłuższy niż 8 godzin liczony od pełnego rozładowania do 80% pojemności znamionowej baterii
- Praca hybrydowa
- Ma być odporne na przeciążenie przez podany czas do poziomu min: - 120%
- Ma posiadać filtry RFI w celu eliminacji zakłóceń wysokiej częstotliwości zgodnie z normami EN 55022 A lub B, EN 50091-2
- Ma posiadać zabezpieczenie przeciwprzepięciowe wewnętrzne lub zewnętrzne uwzględniające IV poziom ochrony tj. 1,5kV, zgodny z normami EN 50091 i IEC62040
- Ma posiadać zakres synchronizacji częstotliwości napięcia wyjściowego do wejściowego (regulowany skokowo co 0,5Hz)
- Współczynnik szczytu 5:1
- Ma posiadać możliwość pracy z niesymetrycznym obciążeniem poszczególnych faz w zakresie 10 – 100% obciążenia
- Ma posiadać automatyczną diagnostykę parametrów urządzenia na panelach wewnętrznych
- Ma posiadać automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem
- Ma posiadać możliwość wydłużenia czasu podtrzymania napięcia
- Ma posiadać układ „łagodnego startu" i „ zimny start"
- Ma posiadać czujnik temperatury i wilgotności jako zintegrowana część UPS
- Ma zapewniać automatyczne wyłączanie napięcia wyjściowego urządzenia UPS po zamknięciu systemów lub możliwość jego wyłączania poprzez wyniesiony panel
- Dziennik zdarzeń

- Ma być wyposażony we wbudowany lub znajdujący się przy UPS- e panel, który wyświetlałby:

- stan pracy UPS (UPS / praca normalna / Obciążenie odbiorów / Praca bateryjna / Praca w trybie obejściowym / +aktywne alarmy i powiadomienia / + stan baterii)
- ZDARZENIA - Wyświetla listę aktywnych zdarzeń systemowych oraz chronologiczny rejestr zdarzeń systemowych.
- IDENTYFIKACJA - Typ UPS / nr produktu / numer seryjny / wersja oprogramowania
- POMIARY - WYJŚCIE / napięcie / prąd / częstotliwość/ moc; BATERIE / napięcie prąd / czas podtrzymania; WEJŚCIE / napięcie, prąd częstotliwość;

- Ma posiadać opcję wyposażenia w osprzęt techniczny i oprogramowanie (odpowiednia ilość licencji) umożliwiające automatyczne, zdalne zamknięcie
- Wymiary nie większy niż szer. x gł. x wys. 420x930x1100
- Oferta powinna zawierać 5 letnią gwarancję i wsparcie ze strony producenta.

Uwaga: Zamawiający wymaga przeszkolenia personelu eksploatacyjnego / administratora sieci w miejscu instalacji w zakresie pełnej obsługi systemu.

III. Zarządzalny przełącznik serwerowy z wbudowaną funkcją obsługi BGP wraz z systemem zarządzania.

III.1. Zarządzany przełącznik serwerowy z wbudowaną funkcją obsługi BGP powinien charakteryzować się następującymi minimalnymi wymaganiami techniczno-funkcjonalnymi:

1. Przełącznik musi posiadać minimum 48 portów 10/100/1000Base- TX oraz 4 porty 10G-BASE-X Ethernet SFP+.
2. Musi zapewniać przepustowość dla całego systemu przynajmniej 120Gbps.
3. Musi zapewniać poziom wydajności systemu na poziomie przynajmniej 90Mpps.
4. Musi obsługiwać minimum 2 wewnętrzne redundantne zasilacze sieciowe typu hot-swap.
5. Musi obsługiwać standardy PoE 802.3af
6. Musi obsługiwać SNMPv1, SNMPv2c oraz SNMPv3
7. Musi obsługiwać RMON (Statistics, History, Alarms, Events, Host, HostTopN, Matrix, Capture, Filter).
8. Sprzętowa obsługa routingu IPv4 i IPv6
9. Pojemność sprzętowej tablicy routingu min. 250 tys. wpisów
10. Musi obsługiwać funkcje routingu, w tym: trasy statyczne, OSPF v1/v2, RIPv1/RIPv2, IPv4, routing Multicast (IGMP v1/v2/v3, PIM-SM), Policy Based Routing, Route Maps, VRRP.
11. Musi posiadać mapę tras dla obsługi VRF (Virtual Routing and Forwarding), BGP, OSPF.
12. Authentykacja MD5 dla protokołów routing
13. Musi oferować zintegrowane funkcje balansowania ruchu w warstwie L4.
14. Musi obsługiwać wielowarstwową klasyfikacje pakietów.
15. Musi obsługiwać IP Class of Service (COS).
16. Musi obsługiwać wiele mechanizmów kolejkowania (SPQ, WFQ, WRR, Hybrid).
17. Musi obsługiwać kontrolę poziomu pasma wychodzącego i przychodzącego w każdym przepływie.
18. Musi obsługiwać technologię 802.1w, 802.1s
19. Pojemność tablicy MAC minimum 65000.
20. Musi obsługiwać opcje Port/VLAN mirroring (jeden do jednego, jeden do wielu, wielu do wielu)

21. Musi obsługiwać technologię 802.3ad Link Aggregation, 127 grup, 64 porty.
22. Musi obsługiwać ograniczniki poziomu ruchu oparte o pasmo lub liczenie pakietów (pps), z progami pasma pomiędzy 8Kbps i 10Gbps.
23. Musi obsługiwać technologię RADIUS Accounting.
24. Musi obsługiwać technologię TACACS+.
25. Musi mieć możliwość ograniczania liczby nowych lub ustanowionych przepływów lub pakietów, które mogą być zaprogramowane na indywidualnym porcie przełącznika by zwalczyć atak DoS.
26. Musi obsługiwać technologie IEEE 802.1X Port Based Network Access, uwierzytelnianie oparte o adres MAC oraz Port Based Web Authentication.
27. Musi obsługiwać dynamiczne i statyczne blokowanie portów oparte o adresy MAC.
28. Musi mieć możliwość automatycznego ograniczania liczby przepływów na porcie i przypisywania akcji do zdefiniowanych ograniczeń.
29. Musi obsługiwać LLDP oraz LLDP-MED.
30. Musi zapewniać kompletne, niepodzielone, nie samplowane dane NetFlow (v5/v9), lub równoważne, ale nie samplowane.
31. Musi automatycznie śledzić informacje o lokalizacji użytkownika/ urządzenia, zbierając przy tym takie informacje jak adres MAC stacji końcowej, czy dane z warstwy 3 (adres IP, itp.) i przekazuje do aplikacji zarządzającej.
32. Musi mieć możliwość określenia lokalizacji urządzenia końcowego w czasie rzeczywistym, w przypadku wystąpienia zdarzenia.
33. Obsługa zewnętrznego systemu logowania zdarzeń SYSLOG, RMON(9 grup), SMON(RFC 2613) Vlan i statystyki
34. Obsługa synchronizacji czasu w oparciu o zewnętrzny serwer SNTP lub NTP
35. Obsługa SNMP v1/v2/v3
36. Sprzętowa obsługa nie samplowanego NetFlow na każdym porcie bez straty wydajności urządzenia lub równoważne, ale nie samplowane.
37. Obsługa SSH klient i serwer
38. Obsługa Telnet
39. Obsługa TFTP
40. Obsługa TACACS+
41. Obsługa RFC 3580
42. Obsługa RADIUS EAP 802.1x, RFC 2865, RFC 2866

Wymaga się, aby dostawa obejmowała:

- 5 –letnią gwarancję producenta na dostarczony sprzęt
- Serwis producenta do końca okresu gwarancji
- Dostarczanie subskrypcji w pełnym zakresie oprogramowania i funkcjonalności wymaganych w tym postępowaniu, aktualizacji oprogramowania do końca okresu gwarancji w całym zakresie wymaganym przez producenta sprzętu i oprogramowania
- Dostarczenie deklaracji zgodności CE na dostarczony sprzęt (wraz z dostawą).

III.2. System Zarządzania

W ramach zadania Wykonawca dostarczy i wdroży System Zarządzania, o następujących minimalnych wymaganiach:

1. System zarządzania musi mieć architekturę klient-serwer (możliwość instalacji serwera i klienta/ów na oddzielnych maszynach) oraz umożliwiać instalację w wersji *standalone* na jednej maszynie.

2. System zarządzania musi zapewnić możliwość automatycznej wizualizacji mapy urządzeń w sieci wraz z automatycznym wykrywaniem połączeń między tymi urządzeniami (urządzenia wykorzystują LLDP/CDP/STP/VLAN/OSPF).
3. Mapa urządzeń musi zobrazować łącza aktywne i nieaktywne między urządzeniami.
4. System ma umożliwiać tworzenie i zarządzanie VLAN-ami.
5. System musi posiadać narzędzie do łatwego zlokalizowania urządzenia sieciowego: Kojarząc IP z adresem MAC, posiadającego zduplikowany adres MAC lub IP, wyszukanie podanego urządzenia po adresie MAC lub IP i wskazanie, na jakim przełączniku i porcie ono występuje.
6. System ma umożliwiać definiowania i zbierania alarmów. Alarmy muszą mieć możliwość grupowania ze względu na ważność i kategorię.
7. System musi mieć możliwość zainstalowania na systemie operacyjnym Microsoft Windows Server 2003/2008 lub Linuks.
8. System zarządzania musi być zgodny z protokołem SNMP v3.
9. System musi umożliwić zobrazowanie urządzeń w sposób graficzny (widok panelu czołowego urządzeń z zaznaczonymi portami oraz obrazować stany tych portów różnymi kolorami). Umożliwianie blokowania i odblokowywania portów z poziomu aplikacji.
10. System zarządzania musi zapewnić min. 1 licencję serwera, minimum 5 licencji dla klientów podłączonych do serwera w trybie klient-serwer lub minimum 5 licencji na stanowisku samodzielnym w trybie *standalone*. Nie dopuszcza się licencji OEM.
11. Klient systemu zarządzania musi być dostępny z poziomu WWW.
12. System zarządzania siecią musi umożliwiać zbieranie zdarzeń z przełączników.
13. System zarządzania siecią musi umożliwiać pobranie i aktualizację konfiguracji urządzeń.
14. System zarządzania siecią musi umożliwiać aktualizację *firmware*.
15. System zarządzania musi obsłużyć min. 50 urządzeń w sieci, przy czym urządzenia rozumiane są jako jednostki administracyjne/zarządzane (np. stos przełączników).
16. System zarządzania musi umożliwić instalację wtyczek (*plug-in*), które umożliwią np. reagowanie na pojawiające się zagrożenia i w trybie on- line zmienianie odpowiednich polityk/ACL dostępu na urządzeniach sieciowych
17. System zarządzania siecią musi zostać zainstalowany na dostarczanym w ramach zamówienia sprzęcie (serwery wirtualne w ramach serwerów kasetowych, uzgodnione z Zamawiającym) i skonfigurowany tak, aby z opisanej funkcjonalności można było od razu korzystać.
18. Musi posiadać narzędzie do zarządzania z poziomu systemu.
19. Musi pozwalać na operacje z poziomu systemu uruchamiane centralnie, takie jak odkrywanie urządzeń, zarządzanie zdarzeniami, zbieranie logów zdarzeń i obsługa aplikacji.
20. Musi udostępniać możliwości modyfikacji, filtrowania i tworzenia własnych elastycznych obrazów sieci.
21. Musi pozwalać na wyświetlanie danych w postaci tabeli lub grafów oraz na wiele OID wybieralnych przez użytkowników.
22. Musi posiadać narzędzie do szybkiego i łatwego odnajdywania fizycznych lokalizacji użytkowników końcowych i systemów oraz określania sposobów ich podłączenia.
23. Musi umożliwiać realizacje zaplanowanych zdarzeń i zadań wykonywanych przez użytkownika oraz planowanie zdarzeń na przyszłość.
24. Musi mieć możliwość podglądu i wyboru obiektów MIB wyświetlanych w postaci drzewa oraz zawierać kompilator dla nowych MIB lub pochodzących od innych dostawców.
25. Musi umożliwiać pełną konfiguracje sieci VLAN wraz z ich monitoringiem.
26. Musi zapewniać pełne wsparcie dla zdalnego zarządzania wszystkimi urządzeniami sieciowymi, włączając w to urządzenia zarządzane przez SNMP MIB-I lub MIB-II.

Wykonawca w ramach realizacji zamówienia musi dostarczyć aplikację do zarządzania elementami , która będzie:

1. Mieć wbudowaną możliwość definiowania reguł/polis dla wszystkich użytkowników, aplikacji, protokołów, VLAN-ów i portów w danej sieci, przynajmniej o następujących funkcjonalnościach:
    a) Musi mieć zdolność automatycznego egzekwowania raz zdefiniowanych polis na chronionych elementach infrastruktury sieci.
    b) Musi mieć możliwość definiowania polis dotyczących ograniczania pasma, ograniczania szybkości nowych połączeń sieciowych, priorytetyzowania mechanizmów QoS warstw 2 i 3, stosowania etykiet pakietów, izolowania/poddawania kwarantannie wybranego portu lub VLANa oraz uruchamiania predefiniowanych działań.
    c) Musi posiadać możliwość rozprowadzania polis w całej sieci za pomocą jednego kliknięcia.
    d) Musi zapewniać automatyczną funkcjonalność w celu zapewnienia dostępu do odpowiednich usług dla każdego użytkownika, niezależnie od miejsca jego logowania do sieci.
    e) Musi pozwalać na łatwą implementację, administrację i rozwiązywanie problemów.
    f) Musi zapewniać kontrolę zdarzeń (logi).
    g) Musi współpracować z dotychczasowymi metodami uwierzytelniania.
    h) Musi obsługiwać technologie autentykacji: 802.1x, Radius i MAC

2. Miała wbudowane szerokie możliwości inwentaryzacji i zmiany opcji zarządzania, przynajmniej o następujących funkcjonalnościach:
    a) Musi zapewniać możliwość dokładnego katalogowania urządzeń według ich typu.
    b) Musi mieć możliwość pozyskiwania informacji na temat urządzeń takich jak numer seryjny, nadana etykieta, wersja oprogramowania, typ CPU oraz pamięć.
    c) Musi umożliwiać prezentację dokładnych informacji na temat konfiguracji, obejmujących datę i czas zapisu konfiguracji, wersję oprogramowania i rozmiar pliku.
    d) Musi zapisywać dane na temat atrybutów urządzeń i raportować jakiekolwiek zmiany w urządzeniu.
    e) Musi dostarczać informacje na temat jakichkolwiek zmian w oprogramowaniu i konfiguracji urządzenia.
    f) Musi zapewniać zbiór danych na temat operacji związanych z zarządzaniem spisem urządzeń.
    g) Musi mieć możliwość generowania szczegółowych raportów dla celów katalogowania urządzeń sieciowych.
    h) Musi mieć możliwość przesyłania do jednego urządzenia lub kilku jednocześnie:
        1) Firmware
        2) obrazów rozruchowych EPROM
        3) szablonów konfiguracji w postaci tekstowej (ASCII)
    i) Musi mieć możliwość planowania okresowych kopii zapasowych konfiguracji urządzeń.

3. Musi pozwalać nietechnicznym użytkownikom na łatwe aktywowanie/dezaktywowanie predefiniowanych polis, o przynajmniej następującej funkcjonalności:
    a) Musi pozwalać administratorom IT na łatwe definiowanie liczby prekonfigurowanych polis sieciowych i desygnowanie wybranych osób do aktywowania/dezaktywowania tych polis.
    b) Musi mieć możliwość natychmiastowego zezwalania lub blokowania działań sieciowych obejmujących dostęp do sieci Web, pocztę elektroniczną i sieć p2p.
    c) Musi być łatwa do konfiguracji i wdrażania i posiadać prosty, bazujący na sieci Web interfejs aplikacji zarządzającej.

d) Nie może być wymagane jakiekolwiek oprogramowanie klienckie dla końcowych użytkowników lub agenci oprogramowania.

4. Musi w inteligentny sposób współdziałać z zaawansowanymi aplikacjami bezpieczeństwa w celu automatycznej reakcji na zagrożenia bezpieczeństwa sieci i będzie spełniać poniższe minimalne wymagania:
   a) Musi udostępniać dynamiczne i konfigurowalne rozwiązania powstrzymywania zagrożeń z szeroką gamą opcji reagowania, tworzenia logów zdarzeń i oceniania
   b) Musi natychmiastowo zidentyfikować fizyczną lokalizację źródła ataku i profil użytkownika.
   c) Musi mieć możliwość podejmowania działań opartych o wcześniej zdefiniowane reguły postępowania w wypadku zagrożeń, informując o podjętych działaniach system IDS przy wykorzystaniu komunikatu Inform SNMPv3.
   d) Musi mieć możliwość automatycznego wyłączania lub izolowania źródła niedozwolonego lub niewłaściwego ruchu zidentyfikowanego przez system IDS/IPS/SIEM/Firewall w szczególności tymi opisanymi w innych punktach.
   e) Musi zapewniać dokładną kontrolę użytkowników i aplikacji pod względem podejrzanych i nieautoryzowanych działań sieci.
   f) Musi zapewniać dokładną kontrolę na poziomie portów obejmującą wykrywanie zagrożeń i określanie typów zdarzeń
   g) Musi zapewniać gromadzenie logów zdarzeń i raportowanie.
   h) Musi mieć możliwość poddania kwarantannie użytkownika podłączonego do danego portu
   i) Musi mieć możliwość izolowania i poddawania kwarantannie źródła ataku, bez wpływu na pracę innych użytkowników oraz istotnych dla urzędu aplikacji i systemów.
   j) Musi mieć możliwość dynamicznej odmowy, ograniczania lub zmieniania właściwości dostępu użytkownika do sieci.

Wykonawca zabezpieczy wymagany sprzęt pod instalację niezbędnego oprogramowanie zarządczego.

Dodatkowe wymagania:

1. Przełącznik z BGP(zarządzany przełącznik serwerowy (48 portowy) i System Zarządzania muszą pochodzić od tego samego producenta.
2. System Zarządzania musi w inteligentny sposób współdziałać z przełącznikiem z BGP w celu automatycznej reakcji na zagrożenia bezpieczeństwa sieci, a w szczególności bez stosowania dodatkowych skryptów oraz aplikacji Open Source musi umożliwiać: Automatyczne wyłączenie portu, ustanowienie kwarantanny, Rate Limit, zmian VLAN -u, nałożenie/modyfikację ACL, uruchomienie skryptu, , wylogowanie użytkownika (logout - 802.1X), z możliwością zdefiniowanie czasu w jakim wymienione działania mają obowiązywać (minimalny interwał: Minimum 1 minuta, Maximum 24h).

Zamawiający wymaga , aby dostawa obejmowała:

- 5 –letnią gwarancję producenta na dostarczony przełącznik
- Serwis producenta do końca okresu gwarancji
- Dostarczanie subskrypcji w pełnym zakresie oprogramowania i funkcjonalności wymaganych w tym postępowaniu, aktualizacji oprogramowania do końca okresu gwarancji w całym zakresie wymaganym przez producenta
- Dostarczenie deklaracji zgodności CE na dostarczony sprzęt (wraz z dostawą).

IV. System szaf 19” wraz z monitoringiem środowiska – 1 szt.

Założenia:

- niezbędna ochrona urządzeń zainstalowanych w serwerowni Urzędu Miasta Ełk,
- wymagany monitoring wizualny (kamery dzień/noc, rejestracja, zdalny podgląd, minimum dwie kamery w środku serwerowni oraz jedna na zewnątrz obejmująca polem widzenia drzwi wejściowe, podgląd z kamer na stanowisku monitoringu miejskiego zlokalizowanego w tym samym budynku co serwerownia ora zdalnie z dowolnego uprawnionego komputera), temperatury, wilgotności, otwarcia drzwi wejściowych do pomieszczenia, wizualna i dźwiękowa kontrola dostępu do szafy z czytnikiem pastylek, sygnalizacja alarmu, oraz możliwość rozbudowy,
- rejestracja zdarzeń: sygnały i wartości parametrów oraz możliwość nagrywania obrazu z kamer – możliwość obsługi (monitorowanie i konfiguracja) szyfrowanym połączeniem za pomocą aplikacji webowej,
- możliwość nastawiania progów alarmowych dla 5 poziomów alarmów

Wymagane minimalne parametry techniczne systemu szaf 19” (Szafa rackowa z wyposażeniem):

- szafa dystrybucyjna 800x800, drzwi szklane, z cokołem wentylowanym z filtrem
- panel wentylacyjny o wydajności min 350 m3 z możliwością rozbudowy do min 1000m3/h, sterowanym wielopoziomowo z systemu monitorowania
- zamek ryglowany z klawiaturą i czytnikiem pastylek kontrolowany przez system monitoringu środowiska
- panel światłowodowy 24xFO SC
- panel UTP kat 6 24xRJ45
- 2 x listwa zasilająca min 8 gniazd
- panel porządkujący
- wzmocnienia umożliwiające montaż UPS- ów
- możliwa rozbudowa o klimatyzator montowany do ściany bocznej

Monitoring środowiska

W ramach zadania Wykonawca zainstaluje w systemie szaf 19” następujące wyposażenie monitoringu środowiska:

- 2 x kamera IP,
- Czujnik otwarcia drzwi,
- 2 x czujnik temperatury (wewnątrz szafy i na zewnątrz),

- czujnik wilgotności powietrza,

- sygnalizator alarmowy na zewnątrz pomieszczenia.

Monitoring środowiskowy szafy 19" powinien charakteryzować następującymi minimalnymi parametrami:

- minimum 8 sterowanych gniazd zasilających, IEC (230 VAC, 8A), możliwość zdalnego załączania i wyłączania urządzeń,
- sterowanie wyjściami za pomocą progów i parametrów
- kontrola zaniku napięcia zasilania 230V
- kontrola zaniku napięcia sterowania 12V
- oddzielne zasilanie warstwy sterującej umożliwiające zasilanie z UPS
- zapamiętywanie ustawień w przypadku utraty zasilania
- wejście 1-wire RJ12 do pomiaru temperatur i wilgotności
- konfiguracja 5-u progów temperatury, sterownie wentylatorami , grzałkami , klimatyzacją
- kontrola dostępu do szafy dystrybucyjnej oparta na pastylkach i- button, z konfiguracją i zapisem osób otwierających szafę, sterowanie klamką elektromagnetyczną.
- min. 2 wejścia NO/NC z zasilaniem 12V do czujników
- funkcja resetera urządzeń sieciowych
- funkcja przywracania ustawień fabrycznych
- watchdog sprzętowy
- komunikacja z urządzeniem: Ethernet 10Base-T
- wysyłanie informacji o zdarzeniach poprzez e-mail
- aktualizacje oprogramowania on- line
- obserwacja wideo monitorowanych obiektów za pomocą kamer IP

Wycena musi zawierać wszystkie niezbędne do instalacji elementy systemu, w szczególności wszelkie elementy montażowe oraz niezbędne okablowanie i konwertery, oraz oprogramowanie.

Oprogramowanie do centralnego zarządzania monitoringiem środowiska , posiadające co najmniej poniższe cechy:

- nadzoruje połączenie moduły poprzez seryjne odpytywanie wszystkich zdefiniowanych w systemie jednostek, brak komunikacji sygnalizowany jest alarmem
- odbiór informacji typu zdarzenie o alarmach oraz zdefiniowanych przerwaniach i kierowanie ich do poszczególnych komórek bazy danych
- oprogramowanie pozwalające na przełączanie stanu gniazd 230V oraz kontrolę temperatury i innych wartości mierzonych, poprzez sieć lokalną lub internet
- archiwizacja i wizualizacja parametrów środowiskowych, monitorowanie on-line poprzez sieć lokalną oraz Internet
- parametry muszą być zapisywane i przechowywane w bazie danych w celu umożliwienia generowania raportów stanu środowiska
- możliwość zapisu sekwencji video jako opcja
- funkcje zarządzania:

a. definiowanie, dodawanie modułów. Konfiguracja parametrów sieciowych.
b. wideo weryfikacja stanów alarmowych i nadzór wideo.
c. definiowanie wartości progowych wyzwalających odpowiednie wyjścia oraz progów alarmowych

- baza danych zawierająca

a. bazę klientów - zawiera nazwę klienta, poziom dostępu do danych, zakres obsługi poszczególnych szaf , klucze I- button.
b. bazę alarmów - zawiera wszystkie alarmy z systemu pogrupowane według czasu. wystąpienia oraz lokalizacji
c. bazę wartości - przechowuje wszystkie wartości mierzone w zadanym okresie czasu.
d. udostępnianie danych lokalnym systemom zarządzania typu MRTG.

V. Przełącznik szkieletowy MPLS

Przełącznik szkieletowy MPLS (1 szt.) **powinien charakteryzować się następującymi minimalnymi wymaganiami techniczno-funkcjonalnymi:**

- przełącznik modularny lub o zamkniętej konfiguracji, posiadający:
  - porty dostępowe (UNI) - min. 24 porty 1000BaseX ze stykiem definiowanym przez moduły konwerterów SFP lub równoważne, umożliwiające obsługę konwerterów w standardach T, SX, ZX, LX/LH, CWDM, DWDM oraz umożliwiać transmisję dwukierunkową na pojedynczym włóknie światłowodowym
  - porty dołączeniowe (NNI) – min. 2 porty 10GBaseX ze stykiem definiowanym przez moduły konwerterów SFP+ lub równoważne, umożliwiające obsługę konwerterów w standardach SR, LR, CU
- wbudowane redundantne, wymienne zasilacze i panele z wentylatorami, zasilanie 230V AC,
- wydajność przełączania min. 65Mpps / 44Gbps,
- certyfikat Metro Ethernet Forum - MEF9 - (EPL, EVPL, ELAN) i MEF14 (EPL, EVPL, ELAN),
- praca w zakresie temperatur: 0-40°C
- możliwość montażu w szafie 19”, wysokość nie większą niż 3RU,
- funkcjonalności przełączania Ethernet:
  - możliwość obsługi min. 16.000 adresów MAC, 4.000 sieci VLAN i VLAN ID,
  - obsługa tzw. Jumbo Frames (9000 bajtów) na portach Gigabit Ethernet,
  - IEEE 802.1s Rapid Spanning Tree
  - IEEE 802.1w Multi-Instance Spanning Tree
  - możliwość grupowania portów zgodnie ze specyfikacją IEEE 802.3ad (LACP)
  - tworzenie instancji Rapid Spanning Tree per VLAN
  - możliwość zapewnienia redundancji interfejsów warstwy drugiej bez wykorzystania protokołów rodziny STP poprzez skonfigurowanie interfejsu zapasowego
  - obsługa L2PT (L2 Protocol Tunelling).
  - obsługa 802.1Q tunnelling (Q-in-Q tunnelling).
  - mapowanie (translacja) tagów 802.1Q 1:1, 1:2, 2:1
- funkcjonalności routingu IP:
  - możliwość obsługi min. 20.000 tras routingowych unicast i 1000 multicast (dla IPv4),
  - obsługa routingu IPv4: statyczny, RIPv2, ISIS, OSPF, BGPv4
  - możliwość wirtualizacji tablicy routingu – utrzymywania niezależnych, osobnych tablic rutingu dla poszczególnych segmentów sieci, przypisywania interfejsów fizycznych i logicznych (dotyczy routingu unicast i multicast)

    - obsługa Bidirectional Forwarding Detection (BFD)
    - routing multicast:
        - IGMP v1/v2/v3
        - IGMP Snooping v1/v2/v3
        - PIM sparse mode,
        - Source Specific Multicast
    - sprzętowo przygotowany do obsługi IPv6
- funkcjonalności przełączania MPLS
    - obsługa LDP, T-LDP
    - obsługa enkapsulacji VPWS / EoMPLS
    - MPLS L3VPN (IPv4)
    - MPLS TE
    - MPLS FRR
    - MPLS L2 VPN – EoMPLS
- funkcjonalności bezpieczeństwa sieciowego
    - obsługa VRRP, HSRP lub równoważnego protokołu,
    - mechanizmy ochrony drzewa Spanning-Tree,
    - mechanizmy zapobiegania sztormom ruchu rozgłoszeniowego (broadcast storm)
    - mechanizm ograniczania ilości adresów MAC
    - obsługa list kontroli dostępu (ACL):
        - filtracja w warstwach 2-4,
        - ACL dla VLAN, portów (fizycznych i wirtualnych)
- funkcjonalności zapewnienia jakości ruchu (QoS):
    - obsługa hierarchicznego QoS
    - klasyfikacja ruchu w oparciu o: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, VLAN ID (min. dwa poziomy zagnieżdżenia), DSCP, MPLS EXP
    - obsługa kolejki z bezwzględnym priorytetem w stosunku do innych (Strict Priority), z ograniczaniem ruchu w kolejce priorytetowej,
    - możliwość zmiany przez urządzenie pola 802.1p (CoS), IP ToS/DSCP, MPLS EXP
    - możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi (ingress policing, rate limiting) w oparciu o VLAN ID, DSCP, CoS, adres IP, adres MAC, MPLS EXP
    - możliwość kształtowania (shaping) ruchu wyjściowego
    - dynamiczna alokacja kolejek dla interfejsów, dostępne min. 4.000 kolejek per urządzenie
- funkcjonalności związane z zarządzaniem urządzeniem:
    - funkcjonalność zdalnej diagnostyki połączeń optycznych zgodna z SFF-8472 (Digital Diagnostics Monitoring, Digital Optical Monitoring lub równoważne)
    - funkcjonalność monitorowania jakości usług na bazie aktywnych próbników ruchu – pomiar min. dostępności, opóźnienia, jego zmian, strat pakietów,
    - obsługa SNMPv3,

- obsługa SSH,
- obsługa RADIUS,
- zarządzanie poprzez interfejs CLI (konsolę),
- obsługa E-OAM (802.1ag, 802.3ah, E-LMI),
- obsługa MPLS OAM
- obsługa Link Layer Discovery Protocol (LLDP, LLDP-MED),
- możliwość tworzenia makr konfiguracyjnych (zestaw komend konfiguracyjnych, aplikowanych pojedynczym poleceniem),
- min. 5 poziomów dostępu administracyjnego (z możliwością określenia zakresu dostępnych poleceń na poszczególnych poziomach),
- możliwość podłączenie zewnętrznych źródeł sygnałów alarmowych (np. otwarcie drzwi do serwerowni, przekroczenie progowej temperatury w serwerowni) i wysłanie alarmu systemowego w przypadku wystąpienia takich alarmów. Zamawiający dopuszcza rozwiązanie zewnętrzne,
- możliwość tworzenia punktów kontrolnych konfiguracji i ich odtwarzania,
- plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line. Konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się restartów urządzenia po dokonaniu zmian.
- plik konfiguracyjny urządzenia musi być zabezpieczony przed niepowołanym dostępem oraz zmianami – tylko osoby uwierzytelnione powinny posiadać dostęp do pliku konfiguracyjnego,

<u>Warunki serwisu i gwarancji dla przełącznika MPLS</u>

- na dostarczany sprzęt musi być udzielona min. 60-miesięczna gwarancja; Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta
- serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego; usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) ma zostać wykonana w przeciągu następnego dnia roboczego od momentu zdiagnozowania usterki; Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań
- Dostarczenie urządzenia przez producenta na wymianę w ciągu następnego dnia roboczego(usługa w standardzie Next Business Day)
- W przypadku Sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający dopuszcza podstawienie na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 14 dni roboczych od momentu zgłoszenia usterki

- Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego
- Zamawiający uzyska dostęp do stron internetowych producentów rozwiązań, umożliwiający:
    - pobieranie nowych wersji oprogramowania
    - dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej
    - dostęp do pomocy technicznej producentów

Wykonawca zrealizuje Instruktaż z dostarczonych routerów dla 2 osób w wymiarze 40h

Wdrożenie musi być zakończone bezpłatnym instruktażem, który musi się odbyć w siedzibie Zamawiającego. Instruktażu musi dokonać instruktor (certyfikowany przedstawiciel dostawcy sprzętu) lub certyfikowany inżynier wykonawcy posiadający najwyższy poziom certyfikacji (Routing, Swiching) producenta zaoferowanych urządzeń, odpowiadających przedmiotowi zamówienia.

Podczas instruktażu muszą zostać przekazane informacje niezbędne do eksploatacji zaproponowanego rozwiązania.

Minimalny zakres instruktażu:

- Konfiguracja urządzeń typu przełącznik LAN
- Konfiguracja i używanie list kontroli dostępu
- Translacja adresów NAT i PAT
- Konfiguracja routingu:
    - Konfiguracja protokołu OSPF
    - Konfiguracja protokołu RIP
    - Redystrybucja pomiędzy protokołami routingu
    - Konfiguracja protokołu BGP w tym MBGP
- Konfiguracja MPLS
    - L2 VPN
    - L3 VPN
    - Wirtualne tablice routingu na urządzeniach CE
    - Routing pomiędzy urządzeniami PE i CE

VI. Wyposażenie HSM do szyfrowania danych.

Zamawiający wymagana dostarczenia niezbędnego sprzętu i oprogramowania wraz z suportem licencji na okres 5 lat. System musi zapewniać pełną kompatybilność funkcjonalną z systemem wprowadzonym i eksploatowanym przez Urząd Marszałkowski Woj. Warmińsko-Mazurskiego (usługa: Wrota Warmii i Mazur).

Karta HSM powinna zostać zainstalowana i uruchomiona na dedykowanym serwerze typu stojakowego i z odpowiednim systemem operacyjnym (min. klasy Microsoft Windows Sewer 2008 Standard lub równoważnym).

Dedykowany serwer HSM powinien charakteryzować się następującymi parametrami minimalnymi:

Nazwa parametru	minimalne
Obudowa	Obudowa o wysokości maksymalnie 1U, dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.
Architektura serwera	Dwuprocesorowa
Wydajność systemu	Liczba zainstalowanych procesorów: jeden procesor czterordzeniowy, zaprojektowany do pracy w serwerach w układach wieloprocesorowych. Typ architektury: x64 (64-bitowa). Procesory muszą posiadać takie właściwości, aby wynik testu SPECint®_rate2006[1] serwera w konfiguracji z 2 zainstalowanymi procesorami był nie niższy niż 148.
Ilość procesorów	Zainstalowany 1,
Pamięć RAM	Minimum 4 GB DDR3, z technologią ECC, „memory mirroring", Chipkill lub równoważna, możliwość rozszerzenia pamięci do minimum 192 GB dla każdego zainstalowanego procesora.
Płyta główna	Dwuprocesorowa, dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera,
Sloty PCI	Minimum 2 sloty PCI-Express. Serwer musi mieć możliwość adaptacji do uzyskania min 2 slotów PCI-X lub posiadać takie sloty w standardzie.
Dyski HDD	2 x 146 GB SAS, 10000 obrotów na minutę, Hot- Plug 2,5", możliwość zainstalowania minimalnie 8 dysków (SAS/SATA) w wewnętrznych zatokach serwera. Możliwość instalacji dysków w technologii SSD.
Kontroler macierzowy	Kontroler macierzowy SAS/SATA umożliwiający konfigurację dysków w RAID 0/1.
Karta rozszerzeń	Zintegrowane z płytą główną 2x Gigabit Ethernet. Karty sieciowe muszą wspierać load balancing, failover i TCP/IP Offload Engine. Zainstalowane dodatkowe dwa interfejsy GigabitEthernet nie zajmujące slotu PCI-E.
Karta graficzna	Zintegrowana karta graficzna min. 16 MB
Porty	4 porty RJ-45. 1 port RJ-45 dedykowany dla interfejsu zdalnego zarządzania. 5 portów USB (2 z przodu, 2 z tyłu, 1 wewnatrz serwera). 1 port VGA. 1 port szeregowy.
Napęd dysków optycznych	DVD-RW.
Zasilanie	Redundantne zasilacze typu Hot-Plug. Maksymalnie 680 W na zasilacz.
Chłodzenie	Redundantne wiatraki typu Hot-Plug.
Zarządzanie	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu i restartu OS). Serwer musi posiadać możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD i FDD. Rozwiązanie

[1] www.spec.org/cpu2006

Nazwa parametru	minimalne
	sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI.
Bezpieczeństwo	Wbudowany moduł TPM 1,2 do przechowywania kluczy kryptograficznych. Dodatkowo wbudowany panel diagnostyczny umożliwiający identyfikację uszkodzonego elementu serwera, wyposażony także w system przewidywania awarii poszczególnych elementów serwera takich jak: dysków twardych, pamięci RAM, zasilaczy, wiatraków, wraz oprogramowaniem pozwalającym na wysłanie komunikatów alarmowy do administratora.
Serwis	5 lat, z gwarantowanym czasem usunięcia awarii w ciągu 24 godzin

VII. System personalizacji kart - 1szt.

Wykonawca dostarczy system wyposażony w programator, drukarkę do kart, 300 kart, 12 czytników oraz oprogramowanie umożliwiające personalizację (zaprogramowanie i dokonanie kolorowego nadruku na kartach) kart służących do systemu kontroli dostępu oraz systemu logowania do systemów sieciowych UM Ełku.

Ogólne.

- Możliwość utrzymania stałej wysokiej jakości wydruków przy jednoczesnej ochronie głowicy dzięki zastosowaniu wałków czyszczących. Wbudowany w zasobnik wałek czyszczący automatycznie usuwający kurz i zanieczyszczenia z karty przed jej zadrukowaniem, chroniącej głowicę przed potencjalnym uszkodzeniem.
- Oszczędność czasu i kosztów związanych z porwanymi lub zniszczonymi taśmami dzięki zasobnikowi na taśmę.
- Niezawodna technologia DTC (Direct- to- Card) lub równoważna umożliwiająca bezproblemowe wykonywanie trwałych, wysokiej jakości nadruków na kartach plastikowych.
- Szybszy obustronny wydruk kart przy wykorzystaniu opcjonalnego modułu do odwracania karty, umożliwiającego zadruk obu stron karty w jednym przejściu przez drukarkę. Moduł ten musi być instalowany fabrycznie.
- Możliwość natychmiastowego rozpoczęcia drukowania kart dzięki oprogramowaniu dołączonemu do drukarki.
- Zwiększenie funkcjonalności kart dzięki możliwości dodania modułu do kodowania kart magnetycznych.

Specyfikacja techniczna drukarki do drukowania dwustronnego (parametry minimalne):

- Technologia nadruku: termosublimacja
- Rodzaj nadruku: dwustronny
- Rozdzielczość: min. 300dpi (11,8 punktów / mm)
- Kolory: 16,7mln / 256 odcieni szarości
- Szybkość wydruku:
  - Min. 7 sekund na kartę / 514 kart na godzinę (K*)
  - Min. 12 sekund na kartę / 300 kart na godzinę (BO*)
  - Min. 27 sekund na kartę / 144 karty na godzinę (YMCKO*)

    - Min. 35 sekund na kartę / 102 karty na godzinę (YMCKOK* + laminacja)
- Standard rozmiaru karty (obsługiwanej przez drukarkę), przynajmniej:
    - CR-80 (85,6x54mm)
    - CR-79 samoprzylepna (83,9x52,1mm)
- Grubość karty: 0,254-1,27mm
- Pojemność podajnika: min. 90 (zasobnik kart do zadrukowania)
- Pojemność zasobnika: min. 25 szt. kart (zasobnik kart zadrukowanych)
- Czyszczenie karty: rolka czyszcząca jest zintegrowana z zasobnikiem taśmy
- Pamięć: min. 2MB RAM
- Wyświetlacz: panel kontrolny LCD
- Podłączenie komputera: min. USB 1.1 (kompatybilny z USB 2.0)
- Temperatura pracy: 17-27ºC
- Wilgotność otoczenia: 20%-80% (bez kondensacji)
- Wymiary: maksymalne 205x465x210mm
- Certyfikaty: bezpieczeństwo: UL60950-1, CSA C22.2 (60950), CE; emisja: FCC Class A, CRC c1374, CE (EN 55022 Class A, EN 55024, ENG 1000-3-2, ENG 1000-3-3)

VIII. Serwery do obsługi portali - 1szt. (typu blade)

Zamawiający wymaga dostarczenia **1 szt.** serwera kasetowego (blade) zgodnego z oferowaną obudową (opisaną poniżej w niniejszym dokumencie),

Minimalne wymagania techniczno-funkcjonalne dla serwera backup zostały opisane w **pkt. XVI. 2 Serwery kasetowe Blade**, niniejszego dokumentu.

IX. System operacyjny dla serwerów – 2 licencje

Zamawiający wymaga dostarczenia serwerowego systemu operacyjnego klasy Microsoft Windows Serwer 2008 Enterprise lub systemu równoważnego, spełniającego następujące wymagania minimalne. System musi posiadać następujące cechy bez konieczności użycia innych produktów:

1. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych
2. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe
3. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play)
4. Graficzny interfejs użytkownika
5. Obsługa systemów wieloprocesorowych
6. Obsługa platform sprzętowych x86 i x64
7. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu

8. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania):
   a. Podstawowe usługi sieciowe: DNS, DHCP
   b. Usługi katalogowe pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe)
   c. Zdalna dystrybucja oprogramowania na stacje robocze
   d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
   e. PKI (Centrum Certyfikatów, obsługa klucza publicznego i prywatnego)
   f. Szyfrowanie plików i folderów
   g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec)
   h. Możliwość tworzenia systemów wysokiej dostępności (kastry typu fail-over) oraz rozłożenia obciążenia serwerów
   i. Serwis udostępniania stron WWW
   j. Serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management)
   k. Wsparcie dla protokołu IP w wersji 6 (IPv6)
   l. Wbudowane mechanizmy wirtualizacji – Hypervisor
   m. Możliwość uruchomienia (z punktu widzenia praw licencyjnych) do czterech wirtualnych serwerowych systemów operacyjnych zgodnych z opisywanym systemem

Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

X. Oprogramowanie system relacyjnej bazy danych - 2 licencje.

Zamawiający wymaga dostarczenia serwerowego systemu relacyjnej bazy danych klasy Microsoft SQL Serwer 2008 Standard lub systemu równoważnego, spełniającego następujące wymagania minimalne.

1. Możliwość definiowania zasad administracyjnych dla serwera lub grupy serwerów - System RBD powinien mieć możliwość automatyzacji zadań administracyjnych przez definiowanie reguł wymuszanych potem przez system, na przykład uniemożliwienie użytkownikom tworzenia obiektów (np. tabel, procedur, baz danych, widoków) o zdefiniowanych przez administratora nazwach lub ich fragmentach

   Powinna być możliwa rejestracja i raportowanie niezgodności ze wskazanymi regułami działającego systemu bez wpływu na jego funkcjonalność.

Reguły mogą dotyczyć serwera lub grupy serwerów.

2. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - System RBD powinien pozwalać na definiowanie rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych bez ujemnego wpływu na wydajność rozwiązania.
3. Możliwość wywoływania procedur składowanych jako usług sieci Web (Web Services) - System RBD powinien umożliwiać tworzenie procedur składowanych które mogę być udostępnione i wywoływane jako Web Services bez wykorzystania dodatkowego oprogramowania.
4. System raportowania - System RBD powinien posiadać wbudowany system 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). Wymagane jest generowanie raportów w formatach: XML, PDF, XLS (Microsoft Excel), HTML, Microsoft Word
   - mechanizm subskrypcji raportów (np. drogą mailową lub do wybranego folderu) w formacie wybranym przez użytkownika i zgodnie z określonym harmonogramem
   - tworzenie wykresów i wskaźników wydajności

   System raportowy powinien udostępniać narzędzia do tworzenia raportów ad-hoc przez użytkownika (umożliwiające publikację takich raportów na serwerze i udostępnienie innym użytkownikom). Dodatkowo system raportowy powinien pozwalać na tworzenie raportów przez programistów w środowisku deweloperskim (umożliwiającym m.in. na jednoczesne publikowanie grupy raportów na wybranym serwerze raportowym).

   System raportowy powinien umożliwiać rozszerzanie istniejącej funkcjonalności przez dodawanie nowych modułów pozwalających np. na eksport danych w nowym formacie, wizualizację w nowych komponentach lub obsługę nowych (nie istniejących w standardowej wersji) źródeł danych dla raportów.
5. System transformacji danych i przesyłania danych System powinien posiadać wbudowane narzędzie do graficznego projektowania transformacji danych (dla procesów

ekstrakcji, transformacji i ładowania 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. Zestaw standardowych dostępnych transformacji powinien obejmować takie transformacje jak: sortowanie, wyszukiwanie wartości według klucza w tabelach słownikowych, pobranie danych z serwera FTP, wysłanie e-maila. Powinna być także zapewniona możliwość tworzenia własnych transformacji.

Wykonywane transformacje danych powinny mieć możliwość integracji z transakcjami bazy danych RBD, także rozproszonymi (transakcje obejmujące bazy na różnych fizycznych serwerach RBD) bez potrzeby pisania kodu.

Dodatkowo system powinien umożliwiać logowanie procesu wykonywania transformacji do wybranych formatów danych (plik tekstowy, baza danych, plik xml). Zebrane informacje powinny umożliwiać m.in. określenie czasu wykonania transformacji oraz użytkownika, który ją uruchomił.

6. System analityczny - System powinien posiadać wbudowany moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (hurtownia danych) bez konieczności stosowania dodatkowych produktów.

   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.

   System powinien umożliwiać tworzenie i przechowywanie wskaźników wydajności (Key Performance Indicator) powiązanych z wymiarami.

   System powinien 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). System powinien posiadać narzędzie do rejestracji i śledzenia wykonywanych zapytań spójne z analogicznym narzędziem dla systemu RBD.

   System powinien dostarczać narzędzia do projektowania rozwiązań analiz wielowymiarowych (umożliwiające tworzenie takich rozwiązań z wykorzystaniem gotowych kreatorów – dla użytkowników mniej zaawansowanych, jak również od

podstaw bez użycia kreatorów – dla użytkowników zaawansowanych). Narzędzie podczas projektowania powinno kontrolować poprawność tworzonych modeli analiz wielowymiarowych i w przypadku stwierdzenia niezgodności z najlepszymi praktykami projektowania powinno informować o tym użytkownika.

7. Analizy predykcyjne (Data Mining) - System powinien mieć wbudowane modele i algorytmy pozwalające na przygotowywanie i wykonywanie analiz Data Mining (bez konieczności instalacji dodatkowego oprogramowania). System powinien mieć wbudowane m.in. narzędzia do projektowania takich modeli (wbudowane kreatory, narzędzia do budowania zapytań do struktur data mining). System powinien mieć wbudowane m.in. następujące algorytmy data mining: drzewa decyzyjne, algorytm klastrowania, regresja logiczna, regresja liniowa, sieci neuronowe, naiwny klasyfikator Bayesa, reguły asocjacyjne, szeregi czasowe, klastrowanie sekwencyjne.
   Obok narzędzi do projektowanie modeli data mining system powinien dostarczać wbudowane komponenty do wizualizacji tych danych (np. przeglądania drzewa decyzyjnego lub zbioru reguł asocjacyjnych).
8. Wysoka dostępność realizowana programowo z korekcją błędów pamięci masowej
   System RBD powinien 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 RBD)
   - 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.
   - brak limitu odległości miedzy systemami (dopuszczalne są tylko limity w minimalnej wymaganej przepustowości łącza)
   - system automatycznie naprawia błędy pamięci masowej (w przypadku odkrycia błędu fizycznego odczytu danych z pamięci masowej, poprawny fragment danych jest transferowany z drugiego systemu i korygowany).
9. Duplikowanie bazy danych do wielu innych lokalizacji - System RBD powinien posiadać wbudowany mechanizm duplikowania zawartości bazy danych jednocześnie do wielu innych lokalizacji (np. przez mechanizm dostarczania logów transakcyjnych do tych lokalizacji).
10. Definiowanie nowych typów danych w RBD - System RBD powinien 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.

11. Replikacja danych - System RBD powinien pozwalać na transakcyjną replikację wybranych danych z bazy danych między wieloma węzłami. Dodanie lub usunięcie węzła nie powinno wpływać na funkcjonowanie i spójność systemu replikacji ani nie powinno przerywać procesu replikacji.
12. Dedykowana sesja administracyjna - System RBD powinien pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.
13. Wsparcie dla danych przestrzennych - System RBD powinien mieć wbudowane 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,
    - uwzględniać krzywiznę Ziemi w przypadku obliczeń na współrzędnych sferycznych,
    - powinien 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 RBD,
    - 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.).
14. Automatyczne pobieranie poprawek i ulepszeń - System powinien umożliwiać automatyczne pobieranie krytycznych poprawek i ulepszeń (bez konieczności ręcznej instalacji przez administratora).

15. Indeksowanie podzbioru wierszy System powinien umożliwiać utworzenie indeksów, które obejmowałyby jedynie wybrany podzbiór rekordów z tabeli.
16. Natywne przechowywanie typów danych XML - System RBD powinien umożliwiać natywne przechowywanie danych w formacie XML w kolumnach tabeli. Dodatkowo powinien umożliwiać przeszukiwanie takich danych oraz indeksowanie struktur XML (tak, aby przyspieszyć operacje wyszukiwania np. po atrybutach przechowywanych w strukturze XML. Dodatkowo powinien umożliwiać tworzenie zapytań obsługujących również operacje na strukturach XML.
17. Narzędzia do automatycznej optymalizacji bazy danych - System powinien mieć wbudowane narzędzia do automatycznej optymalizacji baz danych. Na podstawie przechwyconych zapytań narzędzia te powinny utworzyć listę rekomendacji dotyczących zmian w strukturze bazy danych pozwalających na optymalizację jej wydajności (np. rekomendacje dotyczące utworzenia lub usunięcia indeksów na wybranych polach tabeli).
18. Narzędzia do monitorowania serwera - System powinien posiadać wbudowane narzędzia pozwalające monitorować stan serwera. W szczególności narzędzia te powinny pozwalać na przechwytywanie i zapisywanie zapytań wysyłanych do serwera (zarówno w przypadku zapytań do baz relacyjnych jak i baz danych dla wielowymiarowych usług analitycznych). Narzędzia te powinny pozwalać na zidentyfikowanie zapytań szczególnie obciążających serwer (np. wykonujących się zbyt długo).
19. Wsparcie dla jednoczesnego wstawiania, aktualizacji i usuwania danych z tabeli - System powinien umożliwiać wykonanie operacji wstawiania, aktualizacji i usuwania rekordów w tabeli za pomocą jednej niepodzielnej operacji.
20. Logowanie dostępu do obiektów zgodne ze standardem C2 - System powinien zapewniać możliwość logowania dostępu do obiektów w bazie danych zgodnie ze standardem C2.
21. Przechowywanie informacji o strefie czasowej w polu z datą - System powinien udostępniać typ danych pozwalający na zapisanie daty wraz z informacją o strefie czasowej.

XI. Oprogramowanie antywirusowe AV dla serwerów - 10 licencji.

Zamawiający wymaga **dostarczenia 3 licencji dla serwerów fizycznych oraz 7 licencji dla serwerów wirtualnych**, objęcia wszystkich licencji suportem i aktualizacją polityk bezpieczeństwa w pełnym zakresie funkcjonalności opisanych poniżej, przez okres 5 lat.
Jednocześnie Zamawiający wymaga dostarczenia oprogramowania centralnego zarządzania bezpieczeństwem AV na serwerach. W tym celu **Wykonawca dostarczy i wdroży**

dedykowany system centralnego zarządzania o funkcjonalności minimalnej przedstawionej poniżej.

Potwierdzenie spełnienia wszystkich wymogów odnośnie funkcjonalności oprogramowania jest warunkiem koniecznym do złożenia oferty przez Wykonawcę.

Z uwagi na krytyczne znaczenie dla bezpieczeństwa systemów IT Zamawiający zastrzega sobie prawo do żądania od Wykonawcy udostępnienia wersji testowej oferowanego produktu/ów
– przed podpisaniem umowy, celem weryfikacji spełnienia poniżej przedstawionych wymagań funkcjonalnych.

A) Minimalne wymagania dla oprogramowania antywirusowego AV **dla serwerów fizycznych,** które musi spełniać dostarczone oprogramowanie:

L.p.	Wymagana minimalna funkcjonalność oprogramowania AV dla serwerów fizycznych:
1	Jeden produkt (plik instalacyjny) na serwery Windows z możliwością tworzenia dokładnych polityk rozdzielnych dla serwerów działający na systemach operacyjnych: Windows 2000, 2003, 2008
2	Przyrostowe aktualizacje z FTP, HTTP, UNC, lokalnych oraz mapowanych dysków.
3	Możliwość korzystania z nowych szczepionek online bez ich ściągania na chroniony komputer.
4	Możliwość wstrzymania przez użytkownika ściągania nowych sygnatur (zdefiniowana ilość potencjalnych i dozwolonych wstrzymań) oraz możliwość wznowienia ściągania od miejsca jego przerwania.
5	Skanowanie pamięci operacyjnej komputera na żądanie
6	Skanowanie plików Cookie komputera na żądanie
7	Skanowanie rejestru komputera na żądanie
8	Możliwość określania konfiguracji skanowania dla różnych procesów (np. email – wysokie, backup niskie)
9	Możliwość określania wykorzystania procesora dla zadań skanowania na żądanie
10	Skanowanie poczty, załączników oraz folderów poczty dla klientów MS Outlook oraz Lotus Notes
11	Ochrona przed atakami buffer overflow na serwisy systemu operacyjnego oraz najczęściej atakowanych aplikacji (np. IExplorer)
12	Możliwość blokowania portów (funkcjonalność desktop firewall)
13	Możliwość definiowania reguł pozwalających na blokowanie dostępu do katalogów, udostępnionych katalogów, tworzenia się określonych plików, itp.
14	Wykrywanie IP komputera infekującego w sieci i raportowanie do serwera zarządzającego
15	Ochrona serwisów oprogramowania antywirusowego przed zatrzymaniem (nawet z uprawnieniami lokalnego administratora)
16	Oprogramowanie antywirusowe musi posiadać zintegrowany moduł antyspyware działający w trybie on-access.
17	Skanowanie na żądanie z możliwością wstrzymania w przypadku wykrycia pracy na baterii.
18	Skanowanie na żądanie z możliwością wstrzymania w przypadku wykrycia pracy w trybie pełnoekranowym (np. prezentacja)

19	System musi chronić usługi, pliki i ustawienia maszyn wirtualnych działających na systemie bazowym.
20	Możliwość ukrycia obecności systemu produktów ochronnych przed użytkownikiem (brak GUI, oraz wpisu w „Dodaj/Usuń Programy w Panelu Sterowania Windows).
21	Możliwość ukrycia oprogramowania w Menu Start.
22	Możliwość ograniczenia opcji konfiguracyjnych programów ochronnych dla użytkowników lub ich zabezpieczenia hasłem.
23	Możliwość stworzenia prekonfigurowanej paczki instalacyjnej z najnowszymi szczepionkami i silnikiem wykrywającym wirusy.

Minimalne wymagania dla oprogramowania antywirusowego AV **dla serwerów wirtualnych,** które musi spełniać dostarczone oprogramowanie

L.p.	Wymagana minimalna funkcjonalność oprogramowania AV dla serwerów wirtualnych
1	Oprogramowanie musi chronić przed złośliwym oprogramowaniem wirtualne desktopy w trakcie ich pracy (przy dostępie)
2	Rozwiązanie do skanowania wirtualnych desktopów musi wykorzystywać nie więcej niż dwa dedykowane skanery antywirusowe na jeden hypervisor.
3	Oprogramowanie musi umożliwiać skanowanie na żądanie wirtualnych maszyn uruchomionych na komputerze z hostującym wirtualne maszyny (hypervisor)
4	Oprogramowanie musi posiadać funkcjonalność wykrywania obciążanie procesora hypervisora i powyżej ustalonego progu automatycznie zatrzymywać proces skanowania
5	Oprogramowanie do skanowanie na żądanie musi mieć możliwość zdefiniowania ilości jednoczesnych zadań skanowania
6	Oprogramowanie musi umożliwiać ustanawianie harmonogramu skanowania w określone dni tygodnia oraz godziny
7	Oprogramowanie musi umożliwiać tryb pracy niewidoczny dla użytkownika.

B) Minimalne wymagania dla oprogramowania serwera zarządzającego oprogramowaniem antywirusowym AV dla serwerów.

L.p.	Wymagana minimalna funkcjonalność oprogramowania zarządczego:
1	Jeden serwer zarządzający dla wszystkich produktów, które zostały zdefiniowane wymaganymi funkcjonalnościami powyżej (dla serwerów fizycznych i wirtualnych) zarządzanych nodów ze spójną polityką dla dowolnie i elastycznie definiowanych grup komputerów lub użytkowników zarządzanych z tej samej konsoli administracyjnej i pojedynczego serwera.
2	Zarządzanie powinno odbywać się poprzez standardową przeglądarkę WWW i połączenie https.
3	Funkcjonalność wymuszania konfiguracji przez serwer zarządzający w przypadku, gdy użytkownik zmieni cokolwiek w konfiguracji (jeżeli zmiana taka jest dozwolona), co zdefiniowany interwał czasowy.
4	Funkcjonalność zdalnej instalacji systemu komponentów ochronnych oraz centralne zarządzanie i raportowanie bezpośrednio od klienta do serwera bez podsystemów pośredniczących. Komunikacja ściąga dane dotyczące wszystkich zainstalowanych produktowa na stacji za jednym razem i jest spójna dla wszystkich produktów.
5	Możliwość automatycznego zainstalowania nowych silników AV, service paków oraz hot-fixow z serwera zarządzającego.
6	Możliwość zbudowania architektury rozproszonej – w celu zminimalizowania

	ruchu związanego ze ściąganiem nowych szczepionek, instalacji nowych wersji oprogramowania, hot-fixow, Service paków, etc. Klient instaluje nowe produkty z lokalnego repozytorium a raportuje bezpośrednio serwera zarządzającego.
7	Możliwość skonfigurowania automatycznego wyboru najszybszego/najbliższego repozytorium do ściągnięcia nowych szczepionek/produktów (po czasie odpowiedzi na polecenie ping, adresacji IP lub stałej listy).
8	System musi wykryć obecność w sieci nowego, niechronionego komputera bez zainstalowanych produktów ochronnych.
9	System musi posiadać możliwość powiadamiania o wszystkich zdarzeniach za pomocą poczty elektronicznej, wiadomości SNMP lub wywołania komendy.
10	System zarządzający musi mieć możliwość działania w klastrze HA.
11	System musi umożliwiać tworzenie profili administratorów o różnych stopniach uprawnień dla różnych komputerów lub grup komputerów oraz oprogramowania do którego administrator ma mieć dostęp przy uwzględnieniu praw dostępu: tylko odczyt lub edycja.
12	System zarządzający musi mieć możliwość integracji z Active Directory zarówno w rozumieniu powielenia struktury komputerów jak i autentykacji administratorów i dynamicznego przypisywania uprawnień w serwerze zarządzającym w zależności od przynależności do odpowiedniej grupy w Active Directory.
13	Tworzenie struktury zarządzanych komputerów musi być również możliwe poprzez określenie adresacji IP komputera który podlega zarządzaniu.
14	Tworzenie struktury i przypisywanie polityk musi być możliwe ze względu na parametry samego komputera takie jak: nazwa, domena, parametry sprzętowe, rodzaj systemu operacyjnego, komputer jest przenośny czy stacjonarny.
15	System zarządzający musi umożliwiać tworzenie struktury repozytoriów oraz umożliwiać ich aktualizacje w zaplanowany sposób oraz automatycznie powiadamiać o statusie takiej aktualizacji za pomocą zdefiniowanego mechanizmu (SNMP, email).
16	System musi być przygotowany do pracy w strefie DMZ tak aby było możliwe zarządzanie komputerami znajdującymi się poza siecią korporacyjną.
17	System musi prezentować dane w formie graficznej w panelu głównym z możliwością ich automatycznego generowania i wysyłania w wybranym formacie (minimum PDF i html) pod wskazane adresy email wg harmonogramu.

XII. Stacja mobilna zarządzająca – 3 szt.

Stacja mobilna zarządzająca powinna charakteryzować się następującymi minimalnymi wymaganiami techniczno-funkcjonalnymi:

L.p.	**Opis wymagań minimalnych**	
1	Ekran	Matryca 15.6" WXGA o rozdzielczości 1366x768.
2	Procesor	Procesor klasy x86 dedykowany do pracy w komputerach przenośnych zaprojektowany do pracy w układach jednoprocesorowych, o wydajności pozwalającej na osiągnięcie wartości „PassMark CPU Mark" min. 1615 w testach CPU opublikowanych przez niezależną firmę PassMark Software na stronie http://www.cpubenchmark.net/cpu_list.php,(dot. tylko wydajności procesora bez względu na testowaną konfiguracje komputera). Wyniki

		testów procesorów mają być aktualne z dniem opublikowania specyfikacji przez zamawiającego. Ponadto Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testu może zwrócić się do Wykonawcy z prośbą o dostarczenie w ciągu 3 dni oprogramowania testującego, zaoferowanego sprzętu komputerowego oraz dokładnego opisu przeprowadzonego testu wraz z uzyskanymi wynikami. Niedostarczenie sprzętu do testu będzie skutkować odrzuceniem oferty jako nie spełniającej wymagań postawionych przez Zamawiającego.
3	Płyta główna	Wspomagająca technologię wielowątkowości oraz dwurdzeniowości z obsługa pamięci DDR3-SDRAM 1066MHz.
4	Chipset	Zaprojektowany i wykonany do pracy w komputerach przenośnych rekomendowany przez producenta procesora.
5	BIOS	- w pamięci Flash, możliwość odczytania z BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych, informacji na temat: zainstalowanego procesora, pamięci operacyjnej RAM - możliwość wyłączenia/włączenia zintegrowanej karty sieciowej. - możliwość włączenia/wyłączenia portów USB.
6	Obudowa	Obudowa wyposażona w diody informujące użytkownika o: - włączonym lub wyłączonym module Wifi. - stopniu naładowania baterii: kontrolka LED wyłączona (bateria naładowana), kontrolka LED włączona (ładowanie), kontrolka LED miga (słaba bateria)
7	Pamięć RAM	1x2048MB DDR3 1066Mhz z możliwością rozbudowy do 8GB DDR3
8	Dysk twardy	Min. 320 GB SATA, prędkość obrotowa 5400 obr./min.
9	Karta graficzna	Zintegrowana z możliwością dynamicznego przydziału pamięci do 512MB RAM z pamięci operacyjnej z obsługą DirectX 10, Shader Model 4.0, OpenGL 2.0.
10	Karta dźwiękowa	Zintegrowana karta dźwiękowa zgodna ze standardem High Definition Audio, wsparcie dla efektów 3D i trybu pełnego dupleksu (wbudowane głośniki stereo 2 x 2W + mikrofon)
11	Łączność przewodowa	- wbudowana karta sieciowa 10/100/1000 Mb/s ze złączem RJ45.
12	Łączność bezprzewodowa	- wbudowana bezprzewodowa karta sieciowa z obsługą standardu 802.11 b/g/n
13	Porty/złącza	min. 1 x Złącze RJ-45 (podłączenie sieci lokalnej) min. 1 x Czytnik kart pamięci 4 w 1 min. 3 x USB (2.0) min. 1 x VGA (D-Sub) min. 1 x Gniazdo mikrofonowe min. 1 x Gniazdo słuchawkowe min. 1 x HDMI
14	Klawiatura	Pełnowymiarowa z wydzielonymi pełnowymiarowymi klawiszami numerycznymi w prawej części klawiatury, w układzie US- QWERTY, polskie znaki zgodne z układem MS Windows "polski programistyczny", klawiatura musi być wyposażona w 2 klawisze ALT (prawy i lewy).
15	Urządzenie wskazujące	- Touch Pad (płytka dotykowa) - Wielodotykowy, umożliwia powiększanie i pomniejszanie zdjęć oraz przewijanie stron. - Wyposażony w technologię analizującą różnice pomiędzy dotykiem nadgarstka i palca zapobiegającą przypadkowemu przemieszczeniu kursora w czasie pisania.
16	Kamera	Wbudowana kamera o rozdzielczości 0.3Mpix.
17	Napęd optyczny	8x DVD +/- RW Super Multi Dual Layer wewnętrzny (z oprogramowaniem do nagrywania płyt DVD oraz odtwarzania płyt DVD Video).
18	Bateria	Bateria litowo-jonowa 6 komorowa o pojemności 4400mAh Bateria musi być wyposażona w system zapewniający jej naładowanie do

		poziomu min. 90% pojemności w czasie 120 minut.
19	Zasilacz	Dedykowany do notebooka.
20	System operacyjny	W polskiej wersji umożliwiający pełną integrację i pracę w domenie opartej o Windows 2008 PL, 64 bit (system operacyjny z licencją, sterowniki do wszystkich podzespołów zainstalowanych w notebooku) dostarczony przez producenta notebooka.
21	Dodatkowe oprogramowanie	- Zainstalowane oprogramowanie producenta komputera zarządzające wydajnością oraz poziomem poboru mocy w czasie pracy na bateriach oraz przy zasilaniu zewnętrznym. - Oprogramowanie producenta umożliwiające szybką konfigurację ustawień sieciowych notebooka oraz łatwe przełączanie się pomiędzy różnymi otoczeniami sieciowymi. Wyposażone w kreator pozwalający na edycję ustawień oraz diagnozę ewentualnych problemów w nich występujących. - Notebook musi być wyposażony w oprogramowanie zabezpieczające przed nieautoryzowanym kopiowaniem znajdujących się na dysku danych. Przy ustawieniu blokady, zawartość pamięci masowej notebooka nie będzie mogła być wypalona na płytę CD/DVD, nagrana na dyskietkę, karty pamięci, czy zewnętrzny napęd, ani też na dysk sieciowy.
22	Ciężar	Waga maksymalna do 2650g z baterią
23	Bezpieczeństwo	- Zabezpieczenie BIOS hasłem użytkownika. - Zabezpieczenie dysku twardego hasłem użytkownika. - Złącze typu Kensington Lock.
24	Gwarancja	5 lata w systemie door- to- door na notebooka; 1 rok gwarancji na baterie, Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta - wymagany stosownych dokument potwierdzający autoryzację.
25	Wsparcie techniczne	Dostęp do najnowszych sterowników i uaktualnień na stronie producenta notebooka realizowany poprzez podanie na dedykowanej stronie internetowej producenta nazwy platformy notebooka . Możliwość konsultacja poprzez infolinię w sprawie instalacji systemu operacyjnego oraz dołączonego oprogramowania,
26	Certyfikaty i standardy	- Deklaracja zgodności CE).

I. Instalacja łączy

Wykonawca wykona przyłącze internetowe umożliwiające doprowadzenie sygnału od operatorów zewnętrznych w formie szafy telekomunikacyjnej umiejscowionej na zewnątrz serwerowni i patch paneli umiejscowionych w serwerowi. W szafie przyłącze po obu stronach ma się składać z panela światłowodowego 6 włókien wielomodowych i 12 włókien jednomodowych oraz kabla UTP 12 portów na panelu RJ45.

XIV. Kompletny system zabezpieczeń klasy UTM

Na potrzeby tego projektu muszą zostać uruchomione następujące mechanizmy:

- Firewall z kontrolą stanu sesji,
- Mechanizmy zarządzania pasmem oraz kolejkowanie ruchu zgodnie z założonymi dla poszczególnych usług priorytetytami,
- Mechanizmy ochrony przed atakami – IPS – w tym ochronę przed Dos, D Dos i trady-cyjnymi atakami,

- Możliwość wykrywania i blokowania aplikacji, z opcją określenia maksymalnej wielkości ruchu generowanego w ramach pojedynczych aplikacji lub ich grupy,
- Konfigurację szyfrowanych tuneli IP Sec VPN,
- Kontrolę treści WWW w oparciu o kategoryzację i klasyfikację w celu blokowania i limitowania dostępu do niepożądanych treści (bardzo istotnym jest, aby realizowana kontrola treści http pozwalała blokować dostęp do serwerów określanych mianem „proxy avoidance")

Platforma sprzętowa powinna być przygotowana do uruchomienia usługi AV (uruchomienie AV nie jest w zakresie tego postępowania)
Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łączy dla poszczególnych lokalizacji. Integralność systemu musi być zapewniona także w przypadku różnych dostawców dla poszczególnych lokalizacji. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

A. Dla elementów systemu bezpieczeństwa obsługujących centralny punkt sieci w lokalizacji centralnej serwerowni Urzędu Miasta Ełk Wykonawca zapewni wszystkie poniższe funkcjonalności:

A.1 System powinien być zaprojektowany w taki sposób aby możliwa była jego rozbudowa w celu wyeliminowania pojedynczego punktu awarii. W tym celu powinien zapewnić co najmniej:

a) Możliwość łączenia w klaster Active-Active lub Active- Passive każdego z elementów systemu.

b) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

c) Monitoring stanu realizowanych połączeń VPN z możliwością implementacji mechanizmów redundancji

B. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.

C. System realizujący funkcję Firewall powinien dysponować minimum 18 portami Ethernet 10/100/1000Base- TX oraz powinien mieć możliwość rozbudowy o 4 dodatkowe interfejsy typu Ethernet 10/100/1000Base- TX lub SFP

D. Możliwość tworzenia min 230 interfejsów wirtualnych definiowanych jako VLAN y w oparciu o standard 802.1Q.

E. W zakresie Firewall'a obsługa nie mniej niż 1 milion jednoczesnych połączeń oraz 25 tys. nowych połączeń na sekundę

F. Przepustowość Firewall'a: nie mniej niż 15 Gbps

G. Wydajność szyfrowania AES lub 3DES: nie mniej niż 3 Gbps.

H. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności:

- kontrola dostępu - zapora ogniowa klasy Stateful Inspection
- ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
- poufność danych - IPSec VPN oraz SSL VPN
- ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
- kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
- kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) oraz ich wersji szyfrowanych z wykorzystaniem SSL
- kontrola pasma oraz ruchu [QoS, Traffic shaping]
- Kontrola aplikacji oraz rozpoznawanie ruchu P2P
- Możliwość analizy ruchu szyfrowanego SSL'em
- Możliwość cachowania obiektów dla protokołu http
- Ochrona przed wyciekiem poufnej informacji (DLP)

I. Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączonymi funkcjami: Stateful Firewall, Antivirus, WebFilter, min. 250 Mbps

J. Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min. 500 Mbps

K. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:

- Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
- Dostawca musi dostraczyć nielimitowanego klienta VPN współpracującego z proponowanym rozwiązaniem.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
- Praca w topologii Hub and Spoke oraz Mesh
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth

L. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.

M. Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.

N. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.

O. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)

P. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ

Q. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)

R. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 4000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.

S. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP

T. Baza filtra WWW o wielkości co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne (np. spyware, malware, spam). Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.

U. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.

V. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:

- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
- haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
- haseł dynamicznych (RADIUS, RSA Secure ID) w oparciu o zewnętrzne bazy danych
- Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania a kontrolerze domeny.

W. Funkcje bezpieczeństwa oferowanego systemu powinny posiadać certyfikaty:

- ICSA dla funkcjonalności IPSec VPN, IPS, Antywirus
- ICSA lub EAL4 dla funkcjonalności Firewall

X. Elementy systemu powinny być zarządzane lokalnie za pomocą protokołów co najmniej: HTTPS, SSH jak i mieć możliwość współpracy z dedykowanymi do centralnego zarządzania i monitorowania platformami.

Y. W przypadku awarii systemu powinna istnieć możliwość podmiany systemy w ciągu jednej godziny.

Z. Oferent powinien dostarczyć oświadczenie autoryzowanego dystrybutora na terenie Polski, iż urządzenia objęte oferowanymi usługami serwisowymi, wprzypadku korzystania z tych usług, zostaną przyjęte do naprawy w autoryzowanym punkcie serwisowym producenta na terenie Polski.

AA. Dostawca musi dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres 5 lat, w całym zakresie usług opisanym powyżej i wymaganym przez Zamawiającego. System powinien być objęty serwisem gwarancyjnym producenta przez okres 5 lat.

BB. Serwis powinien być realizowany przez Producenta rozwiązania lub Autoryzowanego Dystrybutora Producenta, mającego swoją lokalizację serwisową na terenie Polski. Zgłoszenia serwisowe przyjmowane w trybie 8x5 przez dedykowany serwisowy moduł internetowy (należy podać adres WWW). W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania, Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz. U. z 2004, Nr 229, poz. 2315 z późna. zm).

Wymaga się, aby dostawa obejmowała:

- 5 –letnią gwarancję producenta na dostarczony sprzęt
- Serwis producenta do końca okresu gwarancji
- Dostarczanie subskrypcji w pełnym zakresie oprogramowania i funkcjonalności wymaganych w tym postępowaniu, aktualizacji oprogramowania do końca okresu gwarancji w całym zakresie wymaganym przez producenta sprzętu i oprogramowania
- Dostarczenie deklaracji zgodności CE na dostarczony sprzęt (wraz z dostawą).

XV. Podsystem dyskowy (macierz)

W ramach zamówienia Wykonawca dostarczy **1 zestaw macierzy dyskowej.**

Macierz dyskowa powinna charakteryzować się następującymi minimalnymi wymaganiami techniczno-funkcjonalnymi:

1. Macierz dyskowa musi być wyposażona w minimum 16 dysków FC o pojemności każdego dysku co najmniej 300 GB i minimum 14 dysków SATA-2 o pojemności każdego dysku co najmniej 1TB.
2. Obudowa kontrolerów macierzy musi posiadać miejsca na instalację co najmniej 16 dysków w technologii FC i SATA-2.
3. Macierz musi gwarantować możliwość rozbudowy do co najmniej 112 dysków.
4. Macierz musi umożliwiać rozbudowę o dyski FC i SATA 2 i SSD.
5. Macierz musi umożliwiać rozbudowę o dyski FC 4Gbit o pojemnościach 300 GB; 450 GB; 600 GB oraz o dyski SATA-2 o pojemnościach 1 TB; 2 TB.
6. Macierz musi umożliwiać mieszanie dysków FC i SATA2 w obrębie obudowy z kontrolerami macierzy, a także w obrębie półki dyskowej.
7. Prędkość obrotowa pojedynczego dysku musi wynosić minimum 15 000 obr./min dla dysków FC i minimum 7200 obr/min dla dysków SATA.
8. Każdy z dysków macierzy typu FC musi być wykonany w technologii 4 Gbit/s Fibre Channel. Macierz musi pracować w trybie 4 Gbit/s FC przy połączeniach do dysków. Wszystkie komponenty służące do rozbudowy macierzy muszą być także wykonane w technologii 4 Gbit/s FC (nie dotyczy samych dysków SATA).
9. Macierz musi wspierać sprzętowe szyfrowanie danych.
10. Macierz musi umożliwiać zapis danych na wszystkich dyskach.
11. Macierz musi zapewniać połączenia typu punkt-punkt do dysków twardych, musi istnieć możliwość jednoczesnego transferu danych z co najmniej 2 dysków.
12. Macierz musi być wyposażona w dwa kontrolery RAID pracujące w trybie active - active.
13. Macierz musi być wyposażona w minimum 8 zewnętrznych portów 8 Gbit/s Fibre Channel umożliwiające bezpośrednie podłączenie serwerów lub skomunikowania macierzy z siecią SAN.
14. Macierz musi być wyposażona w dodatkowe porty 1 GbE – min. 4 sztuki.
15. Macierz musi być wyposażona w minimum 4GB pamięci cache przeznaczonej dla danych (sumarycznie dla obu kontrolerów).
16. Macierz musi pozwalać na stworzenie min. 2 storage partycji. Dodatkowo macierz musi pozwolić na stworzenie min. 128 partycji logicznych (odseparowanych od siebie przestrzeni dyskowych).
17. Pamięć *cache* musi być podtrzymywana bateryjnie (wymagane baterie litowo-jonowe) oraz musi posiadać pamięć typu SSD, na którą zostanie zapisana zawartość pamięci cache w momencie utraty zasilania zewnętrznego.
18. Awaria dowolnej półki dyskowej nie może powodować przerwania dostępu do dysków w pozostałych półkach dyskowych.
19. Macierz musi jednocześnie obsługiwać wolumeny zabezpieczone następującymi poziomami RAID: RAID 0, RAID 1, RAID 3, RAID 5, RAID 6, RAID 10. Poziomy RAID muszą być generowane na drodze sprzętowej – macierz musi być wyposażona w dedykowany układ elektroniczny.
20. Macierz musi umożliwiać stworzenie konfiguracji odpornej na awarię pojedynczej półki bez utraty danych przy zastosowaniu RAID-5. Taka konfiguracja musi być możliwa dla zestawu kontrolera i dwóch półek dyskowych.
21. Macierz musi umożliwiać stworzenie fizycznej grupy RAID 5 na co najmniej 30 dyskach z założeniem, że maksymalnie pojemność jednego dysku przeznaczona jest na informacje o parzystości (np. 29D+1P)

22. Macierz musi umożliwiać stworzenie fizycznej grupy RAID 6 na co najmniej 30 dyskach z założeniem, że maksymalnie pojemność dwóch dysków przeznaczona jest na informacje o parzystości (np. 28D+2P)
23. Macierz musi umożliwić stworzenie fizycznej grupy RAID 0 lub RAID 10 na co najmniej 112 dyskach.
24. Macierz musi zapewnić możliwość wymiany dysków podczas pracy systemu (*hot-swap*).
25. Rozwiązanie musi umożliwiać dynamiczną zmianę następujących parametrów macierzy dyskowej, bez przerywania dostępu do danych znajdujących się na modyfikowanym wolumenie, lub grupie dysków:
- Możliwość dynamicznej zmiany poziomu RAID dla istniejącej grupy RAID.
- Możliwość dynamicznego dodawania dysków do istniejących grup RAID.
- Możliwość dynamicznego powiększania rozmiaru wolumenów logicznych.
- Możliwość dynamicznej zmiany rozmiaru segmentu dla wolumenów logicznych.
- Możliwość dodawania kolejnych półek dyskowych oraz dysków bez przerywania pracy macierzy, dla dowolnej konfiguracji macierzy
- Możliwość aktualizacji oprogramowania macierzy (*firmware*) w trybie online.

26. Macierz musi umożliwiać rozbudowę o pojedyncze dyski fizyczne i pojedyncze półki rozszerzeń.
27. Macierz musi umożliwiać utworzenie co najmniej 1024 niezależnych wolumenów logicznych.
28. Macierz dyskowa musi umożliwiać dedykowanie dowolnego dysku fizycznego jako globalny dysk typu *hot- spare*. Musi istnieć możliwość definiowania min 5 globalnych dysków typu *hot- spare*.
29. Macierz musi mieć możliwość rozbudowy o funkcjonalność wykonywania natychmiastowej kopii danych (*point- in- time copy*). Funkcjonalność ta musi być realizowana w trybie *copy-on- write*. Licencja na wykonywanie natychmiastowej kopii danych musi obejmować całą przestrzeń dyskową oferowaną przez macierz. Musi posiadać możliwość równoczesnego istnienia co najmniej 500 takich kopii w obrębie macierzy.
30. Macierz musi mieć możliwość rozbudowy o replikację danych z druga macierzą w sposób synchroniczny i asynchroniczny z wykorzystaniem jedynie kontrolerów macierzy. Musi istnieć możliwość dynamicznej zmiany trybu i kierunku replikacji, bez potrzeby ponownej pełnej synchronizacji Licencja na wykonywanie zdalnej replikacji musi obejmować całą przestrzeń dyskową oferowaną przez macierz.
31. Macierz musi mieć możliwość rozbudowy o funkcjonalność wykonywania pełnej kopii lokalnych wolumenów logicznych z wykorzystaniem jedynie kontrolerów macierzy. Licencja na wykonywanie kopii lokalnego wolumenu musi obejmować całą przestrzeń dyskową oferowaną przez macierz.
32. Macierz dyskowa musi obsługiwać następujące systemy operacyjne: Windows 2003/2008x, Linuks, IBM AIX, HP-UX, Sun Solaris oraz oprogramowanie VMware.
33. Macierz dyskowa musi umożliwić redundantne podłączenie minimum 2 serwerów. Licencje na oprogramowanie do automatycznego przełączania ścieżki dla każdego z 2 serwerów, dla wszystkich wspieranych systemów operacyjnych muszą być dołączone do macierzy bez dodatkowej opłaty.
34. Dane zapisywane w wewnętrznej pamięci cache jednego z kontrolerów muszą być także powielane w pamięci cache pozostałych kontrolerów, tak aby w przypadku uszkodzenia dowolnego kontrolera zachowana była spójność danych.
35. Wszystkie krytyczne komponenty macierzy takie jak: kontrolery dyskowe, pamięć cache, zasilacze i wentylatory muszą być zdublowane, tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu. Komponenty te muszą być wymienialne w trakcie pracy macierzy.
36. Macierz musi mieć możliwość jednoczesnego zasilania z dwóch niezależnych źródeł zasilania. Zanik jednego z nich nie może powodować przerwy w pracy urządzenia ani zmniejszenia jego wydajności lub utraty danych.

37. Macierz musi być wyposażona w funkcjonalność replikacji danych (synchronicznej i asynchronicznej) pomiędzy dwoma macierzami tego samego typu. Replikacji musi być wykonywana sprzętowo na poziomie kontrolerów macierzowych.
38. Macierz musi posiadać zarządzanie poprzez sieć SAN i LAN. Oba tryby zarządzania muszą działać niezależnie od siebie, co oznacza, że musi istnieć możliwość zarządzania macierzą w przypadku awarii (całkowitej niedostępności) sieci SAN, jak i w przypadku awarii (całkowitej niedostępności) sieci LAN. Podsystem zarządzania macierzą nie może posiadać pojedynczego punktu awarii.
39. Macierz musi posiadać zarządzanie poprzez port szeregowy.
40. Macierz musi być wyposażona w zestaw do montażu w szafie przemysłowej rack 19". Obudowa z kontrolerami macierzy oraz półki dyskowe muszą mieć wysokość nie większą niż 3U.
41. Oprogramowanie do zarządzania musi posiadać funkcjonalność interfejs graficzny oraz CLI (*command-line interface*) wraz ze wsparciem technicznym do końca okresu gwarancji w cenie macierzy.
42. Macierz musi posiadać możliwość zdalnego nadzorowania przez Serwis producenta bez dodatkowej opłaty serwisowej.
43. Producent macierzy musi posiadać na terenie Polski podmiot serwisowy.
44. Deklaracja zgodności CE na dostarczony sprzęt (wraz z dostawą).
45. Gwarancja 5 lat, świadczona w miejscu instalacji z gwarancją usunięcia awarii w ciągu 24 godzin.

XVI. System serwerowy – 4 szt. (Półka + 3 serwery typu blade)

XVI.1. Obudowa do serwerów kasetowych (blade)

Zamawiający wymaga dostarczenia **1 szt. obudowy do serwerów kasetowych (blade)** o następujących minimalnych parametrach i minimalnym wyposażeniu:

Typ obudowy	Do montażu w szafie 19" z wymaganym zestawem montażowym Dostępny na przednim panelu: USB, DVD- ROM Musi umożliwiać wyposażenie jej w minimum dwie wydajne dmuchawy
Rozmiary obudowy	Wysokość maksymalnie 7U, głębokość maksymalnie 28" (712 mm) Możliwość instalacji do 6 obudów kasetowych w standardowej szafie 42U
Liczba montowanych serwerów i modułów	Możliwość zamontowania w ramach jednej obudowy min. 14 serwerów o różnym typie architektury procesorów (wymagane x86 i RISC) Możliwość instalacji min. 4 modułów przełączników LAN/SAN
Rodzaj obsługiwanych serwerów	Możliwość umieszczania w ramach jednej obudowy wszystkich typów serwerów kasetowych producenta dostarczanego rozwiązania
Sposób wyprowadzeń sygnałów LAN	Obudowa musi być wyposażona w minimum dwa przełączniki Ethernet 1 Gbit/s, montowane w modułach w obudowie kasetowej w układzie pracy nadmiarowej, z minimum 4 portami zewnętrznymi w standardzie 1 Gbit/s każdy. Przełączniki muszą umożliwiać zastosowanie technologii VLAN

Sposób wyprowadzeń sygnałów Fibre Channel	Obudowa musi być wyposażona w minimum dwa moduły przełącznika SAN umożliwiające komunikację Fibre Channel (wewnętrzną) z wszystkimi slotami serwerów kasetowych, przy czym zamawiający dopuszcza uaktywnienie redundantnej komunikacji z minimum 7 slotami serwerów kasetowych w obudowie (z możliwością późniejszego rozszerzenia aktywnych portów FC dla wszystkich serwerów w obudowie). Przełączniki muszą umożliwiać podłączenie zewnętrznych urządzeń Fibre Channel 8 Gbit/s za pomocą minimum 2x3 portów wyposażonych we wkładki SFP Short Wave (multimod)
Zasilanie i chłodzenie	Zasilanie doprowadzone do serwerów przez dwie niezależne magistrale i dwa niezależne łącza w serwerach bez pojedynczego punktu awarii. Zasilanie redundantne o konstrukcji modularnej z możliwością dokładania i wymiany modułów na gorąco. System zasilania zainstalowany wewnątrz obudowy zdolny do dostarczenia mocy, jaką może potrzebować obudowa obsadzona serwerami i opcjami w zamawianej konfiguracji. Wymagane zastosowanie minimum jednej wydajnej dmuchawy.
Zarządzanie	Zintegrowany, modułowy system umożliwiający zdalną administrację wszystkimi elementami infrastruktury poprzez sieć LAN. Obudowa musi mieć możliwość zainstalowania drugiego redundantnego systemu umożliwiającego zdalną administrację.
Certyfikaty	Obudowa musi znajdować się na liście kompatybilności producenta serwerów kasetowych
Gwarancja	5lat, świadczona w miejscu instalacji, z gwarancją usunięcia awarii w ciągu 24 godzin

XVI.2. Serwery kasetowe (blade)

Zamawiający wymaga dostarczenia **3 szt. identycznych serwerów kasetowych (blade**) zgodnych z oferowaną obudową, każdy o następujących parametrach minimalnych:

Architektura serwera	Dwuprocesorowa
Procesory	Liczba zainstalowanych procesorów: dwa procesory czterordzeniowe, zaprojektowane do pracy w serwerach w układach wieloprocesorowych Typ architektury: x64 (64-bitowa) Procesory muszą posiadać takie właściwości, aby wynik testu SPECint_rate2006[2] serwera w konfiguracji z 2 zainstalowanymi procesorami był nie niższy niż 127 (przykładowa klasa procesora: Intel Xeon E5504)
Pamięć RAM	DDR3 zainstalowane 16 GB, z możliwością rozszerzenia do 192 GB 12 gniazd DIMM
Kontroler dyskowy	Obsługujący RAID1
Dyski twarde	Zainstalowane w serwerze minimum 2 dyski o pojemności 146 GB, 10 000 obr./min. typu SAS HotSwap (możliwy montaż/demontaż dysków bez wyjmowania serwera z obudowy kasetowej)

[2] www.spec.org/cpu2006

Karta sieciowa	Dwa redundantne porty sieciowe zintegrowane z płytą główną 10/100/1000 Gigabit NIC lub na osobnej karcie. Wsparcie: IPv4 i IPv6, IPMI 2.0, TOE, Wake On LAN, Failover, Load Balancing, Preboot Execution Environment
Karta Fibre Channel	Dwa redundantne porty FC zintegrowane z płytą główną lub na osobnej karcie
Zasilanie i chłodzenie	Zasilanie realizowane przez redundantne i hot-swapowe zasilacze. Chłodzenie realizowane przez redundantne wentylatory
Obudowa	Typu kasetowego (blade)
Złącza USB	Minimum jedno złącze USB zintegrowane z płytą główną
Monitorowanie i diagnostyka	Serwer musi posiadać podsystem umożliwiający kontrolę poprawności działania elementów serwera, diagnostykę oraz narzędzie sprzętowe ułatwiające lokalizację uszkodzenia (np. świetlny lub ekranowy wskaźnik uszkodzonego elementu). System musi umożliwiać przewidywanie awarii podstawowych elementów oraz możliwość pełnej zdalnej administracji serwerem (przejęcie konsoli) oraz montowania zdalnych zasobów dyskowych
Oprogramowanie	Nośniki CD lub DVD z oprogramowaniem wspomagającym instalację i konfigurację systemu operacyjnego oraz oprogramowaniem monitorująco – zarządzającym obsługujące zarówno dostarczane serwery, jak i obecnie posiadane przez Zamawiającego serwery i stacje robocze
Nośniki ratunkowe	Komplet nośników, dyskietek, CD lub DVD, umożliwiających odtworzenie stanu serwera (ustawień, kontrolera macierzy, oprogramowania), jak w momencie dostawy serwera do użytkownika
Gwarancja	5 lat, świadczona w miejscu instalacji z gwarancją usunięcia awarii w ciągu 24 godzin

XVII. Oprogramowanie monitorujące serwery - 1szt.

Zamawiający wymaga dostarczenia oprogramowania do zarządzania infrastrukturą serwerową, które musi wspierać następujące minimalne funkcjonalności:

1. Oprogramowanie musi zapewniać funkcjonalności obejmujące: sterowanie sprzętem, zdalne zatrzymywanie, uruchamianie i restartowanie systemów,
2. Oprogramowanie musi zapewniać dystrybucję oprogramowania w celu instalowania nowych aplikacji lub aktualizacji w skali całego środowiska,
3. Oprogramowanie musi realizować monitorowanie zasobów krytycznych z automatycznym powiadamianiem lub działaniami w reakcji na określone stany.
4. Oprogramowanie musi dawać możliwość zarządzania procesami, pozwalającymi na uruchamianie, zatrzymywanie, planowanie i monitorowanie zadań.
5. Oprogramowanie musi dawać możliwość zarządzania w oparciu o grupy pozwalające ograniczyć liczbę błędów i przeoczeń, przy czym możliwe jest automatyczne tworzenie i utrzymywanie grup na podstawie cech systemów.)
6. Oprogramowanie musi być dostępne dla systemów AIX 5L, Linux i Windows.

Oprogramowanie zostanie zainstalowane na zasobach sprzętowych dostarczanych w ramach niniejszego postępowania.

XVIII. Stacjonarna stacja zarządzająca KVM – 1 szt.

W ramach zamówienia Wykonawca dostarczy do Centrum Zarządzania Siecią zestaw przełącznika KVM z konsolą LCD, spełniający poniższe wymagania minimalne:

1. Konsola LCD musi być przystosowana do instalacji w szafie serwerowej rack 19" i mieć wysokość nie wyższą niż 1U.
2. Konsola LCD powinna umożliwiać zamontowanie z tyłu przełącznika tego samego producenta w tym samym 1U.
3. Konsola LCD powinna zapewniać wyświetlanie 16,7 mln kolorów, mieć przekątną wyświetlacza nie mniejszą niż 17" i rozdzielczości 1280x1024 pikseli, kącie widzenie 80 stopni w pionie/poziomie/lewo/prawo, współczynniku kontrastu 1000:1 oraz jasności 250cd/m2.
4. Konsola LCD powinna mieć klawiaturę wysuwaną w standardzie QWERTY z 82 klawiszami oraz touchpad.
5. Przełącznik KVM powinien pozwalać na podłączenie do 8 komputerów, być przystosowany do instalacji w szafie serwerowej rack 19" i mieć wysokość nie wyższą niż 1U.
6. Przełącznik KVM powinien zapewniać menu ekranowe do wyboru urządzenia lub za pośrednictwem skrótu klawiaturowego.
7. Przełącznik KVM powinien mieć dołączone 4 kable o długości 2,1 metra do podłączenia komputerów za pomocą złącz VGA/USB.
8. Przełącznik KVM powinien mieć dołączone 4 przejściówek na RJ45 do podłączenia komputerów za pomocą złącz VGA/USB
9. Urządzenia powinny posiadać deklarację zgodności CE.

Wymaga się, aby dostawa obejmowała:

- 5 –letnią gwarancję producenta na dostarczony sprzęt
- Serwis producenta do końca okresu gwarancji
- Dostarczanie subskrypcji w pełnym zakresie oprogramowania i funkcjonalności wymaganych w tym postępowaniu, aktualizacji oprogramowania do końca okresu gwarancji w całym zakresie wymaganym przez producenta sprzętu i oprogramowania
- Dostarczenie deklaracji zgodności CE na dostarczony sprzęt (wraz z dostawą).

XIX. Licencje wirtualizacyjne dla dostarczanych 2 serwerów typu blade.

Licencje wirtualizacyjne powinny charakteryzować się następującymi minimalnymi wymaganiami techniczno-funkcjonalnymi:

1) Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
2) Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.

3) Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w maksymalnie dwanaście rdzeni.
4) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-4 procesorowych.
5) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 255GB pamięci operacyjnej RAM.
6) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-10 wirtualnych kart sieciowych.
7) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć co najmniej 3 porty szeregowe i 3 porty równoległe i 10 urządzeń USB.
8) Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
9) Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
10) Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM.
11) Rozwiązanie musi wspierać następujące systemy operacyjne: MS-DOS 6.22, Windows 3.1, Windows 95, Windows 98, Windows XP, Windows Vista , Windows NT 4.0, Windows 2000, Windows Server 2003, Windows Server 2008, Windows 7, SLES 10, SLES9, SLES8, Ubuntu 7.04, RHEL 5, RHEL 4, RHEL3, RHEL 2.1, Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, NetWare 6.5, NetWare 6.0, NetWare 6.1, Debian, CentOS, FreeBSD, Asianux, Ubuntu 7.04, SCO OpenServer, SCO Unixware, FreeBSD
12) Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
13) Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
14) Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.
15) Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
16) Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
17) Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.

18) Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
19) Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (np. wgrywania krytycznych poprawek) bez potrzeby wyłączania wirtualnych maszyn.
20) Rozwiązanie musi zapewniać taki mechanizm bezpiecznego uaktualniania aplikacji i systemów operacyjnych wirtualnych maszyn, poprzez który można wprowadzać poprawki na pojedyncze wirtualne maszyny jak i na całe grupy wirtualnych maszyn. Dla bezpieczeństwa wspomniany mechanizm musi pozwalać na automatyczne wykonywanie kopii migawkowych przed aktualizacją.
21) Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z kilku dostępnych ścieżek.
22) Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi na których pracują. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
23) Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
24) Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny które na nim pracowały były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym.
25) System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
26) Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia Ethernet w razie awarii karty sieciowej.
27) Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN)

Uwaga: Wymagany okres subskrypcji wszystkich licencji oprogramowania wirtualizacyjnego – do końca okresu gwarancji (5 lat)

Zakres wykonawstwa instalacji teletechnicznych w pomieszczeniu serwerowni .

Zakres realizacji obejmuje:

1. Dostawę i wdrożenie agregatu prądotwórczego wraz z instalacją wydechową i kompletem dokumentacji.
2. Dostawę i wdrożenie klimatyzacji typu SPLIT wraz z kompletną instalacją i dokumentacją.
3. Wykonanie podłogi technicznej.
4. Wykonanie instalacji LAN i elektrycznej.
5. Rozbudowa istniejącego systemu kontroli dostępu do pomieszczenia serwerowni, systemu alarmowego i monitoringu.
6. Dostawa systemu Szaf serwerowych 19" wraz z systemem monitoringu została opisana w część A. niniejszego dokumentu.
7. Wykonanie instalacji systemu wczesnej detekcji.

Dla wszystkich instalacji przedstawiony poniżej minimalne wymagania techniczno-funkcjonalne.

Wymagania techniczno-funkcjonalne dla systemów teletechnicznych serwerowni e-Portal.

XX. Agregat prądotwórczy.

Zamawiający wymaga dostarczenia i wdrożenia do pracy: agregatu dla serwerowni **UM Ełk** w wersji stacjonarnej, obudowie wyciszonej, zainstalowany na betonowym fundamencie z dylatacja obrzeżową.
Dostarczony sprzęt musi być **objęty 2-letnim serwisem** producenckim/ lub autoryzowanego dystrybutora proponowanego rozwiązania.

Wykonawca w ramach zadania wykona:
- dokumentację wykonawczą z niezbędnym projektem budowlanym
- projekt powykonawczy
- instruktaż eksploatacyjny
- układ wydechowy z rury dwu płaszczowej nierdzewnej o długości min. 20 mb wyprowadzoną po elewacji ponad dach budynku UM Ełk

Agregat prądotwórczy o parametrach nie gorszych niż:
1) **Moc** – ciągła PRP min. 100kVA, moc dorywcza LTP min. 110kVA
2) **Moc czynna przy cos fi = 0,8** wynosi 80 KW dla PRP i 88 KW dla dorywczej
3) **Zbiornik paliwa** – min. 180l
4) **Konstrukcja** - Stalowa, spawana rama z układem tłumienia drgań - Silent bloki. Stalowy zbiornik paliwa zintegrowany w ramie. Tłumiki wydechu: min. 9dB(A) - Compact. Złączka kompensacyjna wydechu dla wersji Compact.
5) **Silnik** - rzędowy, chłodzony cieczą, spełnia normy: przynajmniej: ISO 3046 / DIN 6271, BS 5514
6) Ilość gazów spalinowych maksymalnie 16,3 m3/min
7) Temperatura gazów spalinowych maksymalnie 550 °C
8) Średnica układu wydechowego min. 4,5 ''
9) Wielkość akumulatorów rozruchowych min. 12 V 80 Ah
1) **Regulator obrotów** - regulator elektroniczny 1.500rpm +/- 1%
2) **Maksymalne spalanie (praca ciągła PRP)**: procent obciążenia – spalanie: 25% - 5,5l, 50% - 12l, 75% - 17,5l, 100% - 23l
3) **Układ ogrzewania bloku silnika** – grzałka w bloku silnika min. 1000W.
4) **Start** - akumulator rozruchowy wraz z automatyczną ładowarką.

5) **Prądnica** - alternator synchroniczny 4 biegunowy z automatycznym regulatorem napięcia +/- 0,5%. Klasa Izolacji – co najmniej H, stopień ochrony IP 23. Alternator spełniający normy: IEC 34.1, NEMA MG 21, BS 4999.

6) **Konstrukcja** - jednołożyskowa, z samocentrującym sprzęgłem mocowanym w kole zamachowym silnika diesla.

7) **Głośność** – maks. 70 dB@7m, obudowa akustyczna odporna na warunki atmosferyczne.

8) **Tablica automatyki** – Mikroprocesorowy system sterowania i kontroli z komunikatami w języku polskim

- moduł AMF / automatyczny start
- sygnalizacja LED
- ekran LCD / parametry pracy, komunikaty
- przyciski funkcjonalne AUTO/RECZNY/TEST/Start / Stop/Reset
- sterowanie grzałką bloku silnika
- automatyczna ładowarka baterii akumulatora
- współpraca z układem SZR' a
- ręczne sterowanie układem SZR
- możliwość zdalnej kontroli i monitoringu agregatu przez sieć Ethernet
- możliwość podłączenia modemu GSM
- port USB do programowania automatyki
- monitorowanie przy pomocy: RS 485 (Modbus RTU).
- rejestr alarmów i zdarzeń
- autentykacja alarmów: min. następujących: nieudany rozruch, nadobroty, przeciążenie, brak ładowania akumulatora, wyłączenie awaryjne, niski poziom chłodziwa, niski poziom paliwa, wysoka temperatura silnika)
- programator cyklicznego uruchamiania

9) **Zdalny panel sterowania LCD** z możliwością zdalnego uruchamiania (identyczne funkcje jak główny panel sterowania)

10) **Układ SZR** – 160 A – zbudowany w oparciu o przełącznik z napędem elektrycznym z możliwością ręcznego przełączania w sytuacji awarii napędu elektrycznego. Możliwość konfigurowania progów zadziałania SZR i czasów przełączania.

11) Masa sucha zespołu prądotwórczego – maks. 1750 kg netto.

12) Wymiary zespołu prądotwórczego: maks. (D x S x W) 280x110x160cm.

13) **Certyfikat –** CE

XXI. Klimatyzacja.

Założenia instalacyjne dla klimatyzacji do serwerowni e-Portal UM Ełk:
Moc chłodnicza przewidywanych klimatyzatorów – ok. 7,5 kW. Dodając zyski ciepła od urządzeń typu UPS, zasilaczy oraz uwzględniając kubaturę pomieszczenia o powierzchni 24 m^2 należy dobrać urządzenia o nominalnej mocy chłodniczej min. 7,9 kW.
Zamawiający wymaga dostarczenia urządzeń, które będą dobrane w systemie N+1.
Ze względu na brak dokładnego projektu, oraz nie wystarczającą przestrzeń w podłodze technicznej (20cm) należy dostarczyć urządzenia SPLIT typu ściennego. Urządzenia muszą pracować w trybie ON- OFF.

Zamawiający wymaga dostarczenia systemu klimatyzacji przy powyższych założeniach oraz minimalnych wymaganiach wydajnościowych:

1. Wydajność chłodnicza – min. 7,9kW
2. Wydajność grzewcza – min. 8,4kW
3. Zasilanie – 230/1/50 (V/Ø/Hz)
4. Osuszanie – min. 3 l/h
5. Poziom ciśnienia akustycznego jedn. wew. – maks. 40,5dB(A)
6. Poziom ciśnienia akustycznego jedn. zew. – maks. 54dB(A)

7. Wydajność powietrza – min. 1 040 m^3/h
8. Pobór prądu – maks. 13 A
9. Prąd rozruchowy – 70 A
10. Pobór mocy – maks. 2,75kW
11. Współczynnik EER – przynajmniej 2,86
12. Czynnik chłodniczy – R410A

Urządzenie musi być wyposażone w tzw. zestaw pracy całorocznej tj. regulator obrotów wentylatora oraz grzałkę karteru sprężarki, co pozwoli na poprawną pracę urządzenia w trybie chłodzenia przy ujemnych temperaturach powietrzna na zewnątrz.
Dodatkowo urządzenia musi być wyposażone w zestaw pracy naprzemiennej, co pozwoli na równomierną pracę obu urządzeń oraz w przypadku awarii któregoś z nich, drugie sprawne przejmie rolę głównego urządzenia.

Kompletna instalacja klimatyzacji oraz wszystkie użyte urządzenia, muszą być objęte **2 letnim serwisem gwarancyjnym.**

Zakres zadania dla systemu klimatyzacji obejmuje:
- wykonanie projektów wykonawczego, budowlanego (jeżeli niezbędny) i projektu powykonawczego
-dostawę wraz z kompleksom montażem, włącznie w wszelkimi niezbędnymi pracami budowlanymi
-pełną instalację rozprowadzenia powierza w pomieszczeniu
- szkolenie eksploatacyjne

Wymagania w zakresie obsługi gwarancyjnej klimatyzacji:
- niezbędne przeglądy w ciągu całego okresu obowiązywania gwarancji
-czas reakcji na zgłoszenie awarii maks. 48h,
-czas usunięcia awarii nie wymagającej wymiany i naprawy osprzętu technicznego nie przekraczający 48h.
-usunięcie awarii wymagającej wymiany i naprawy osprzętu technicznego w czasie nie przekraczającym 14 dni od daty zlecenia naprawy

XXII. <u>Podłoga techniczna.</u>

Zamawiający wymagania wybudowania w pomieszczeniu serwerowym podłogi podniesionej na powierzchni około 24 m kw., składającej się z płyt typu W38BS-P lub równoważnych o właściwościach antyelektrostatycznych, na wysokości około 20 cm ponad poziom posadzki. Tak niski poziom dla podłogi technicznej podyktowany jest parametrami lokalu.

W ramach wykonawstwa Zamawiający wymaga:
- przystosowania podłogi do uziemienia
- wykończenia podłogi listwą przyścienną z PVC
- objęcia całości realizacji 5 –letnią gwarancją

Minimalne parametry techniczne dla podłogi:
- podłoga wykonana ze sprasowanej płyty wiórowej o gęstości przynajmniej 720 kg/m^3, silnie sprasowanej
- spód płyty wykonany z blachy stalowej ocynkowanej o grubości przynajmniej 0,5 mm
- wierzch płyty wyłożony wykładziną PVC antyelektrostatyczną np. Gerflor Robust lub Fatra Antistatik

- Konstrukcja wsporcza podłogi: wykonana z profilu min. C40/40/2, wsparta na płynnie regulowanych wspornikach stalowych ocynkowanych, klejonych do podłoża.

- Ramy pod urządzenia wykonane z profilu przynajmniej C82/40/2, wkomponowane w podłogę podniesioną, klejone.
- Dopuszczalne obciążenie punktowe min. 6,0 kN
- Dopuszczalne obciążenie powierzchniowe min. 25 kN/m^2
- opór elektryczny upływu podłogi Ru [Ω] $5 \cdot 10^4 \leq Ru \leq 1 \cdot 10^9$
- współczynnik bezpieczeństwa min. 2
- klasyfikacja ogniowa: wyrób niezapalny – od strony spodniej, trudno-zapalny - od strony wierzchniej
    - odporność ogniowa REI30
    - klasa ugięcia A (2,5 mm)

Minimalne parametry techniczne dla wykładziny:
- opór elektryczny upływu R_u [Ω] $\leq 1 \cdot 10^6$
- klasyfikacja ogniowa w zakresie stopnia palności: wyrób trudno-zapalny.

Niezbędne certyfikaty dla podłogi:
- Certyfikat Zgodności Nr ITB-1558/W– zgodny z europejską normą PN-EN 12825:2002
- Atest Higieniczny PZH Nr HK/B/0030/01/2006

UWAGA!

Pomieszczenia do montażu podłogi podniesionej w serwerowni UM Ełk spełnia następujące warunki:
- temperatura nie niższa niż + 5^0C,
- wilgotność względna nie większa niż 70%,
- pomieszczenia zakryte, zadaszone, zabezpieczone przed dostępem wody,
- podłoże stabilne, niekruszące.

W pomieszczeniu serwerowni wykonawca wykona **prace remontowo-adaptacyjne** oraz prace związane z instalacją elektryczną.

XXIII. Okablowanie LAN

Wykonawca zaprojektuje i wykona instalację logiczną (FTP kat co najmniej kat 6) oraz instalację zasilającą, w korycie ułożonym w pomieszczeniu na ścianach serwerowni. Wybuduje w pomieszczeniu serwerowni 20 modułów złożonych z gniazda 2xRJ45, i 4 gniazd elektrycznych z czego 2 dedykowane dla urządzeń IT.

XXIV. Rozbudowa istniejącego systemu kontroli dostępu do pomieszczenia serwerowni, systemu alarmowego i monitoringu

Wykonawca zrealizuję rozbudowę istniejących systemów będących w posiadaniu Zamawiającego.
Wykonawca dostarczy i zainstaluje i zabezpieczy okno oraz drzwi antywłamaniowe. Drzwi wyposaży w kontrolę dostępu.

XXV. Dostawa systemu Szaf serwerowych 19” wraz z systemem monitoringu

Zakres realizacji dostaw sprzętu i usług został opisany w powyższej części niniejszego dokumentu.

XXVI. Wdrożenie systemów wczesnej detekcji pożaru w pomieszczeniu serwerowni.

Systemy wczesnej detekcji pożaru zostaną zainstalowane w pomieszczeniu serwerowni.

Wymagania dla systemów wczesnej detekcji pożaru:
Minimalne wymagania dla systemu wczesnej detekcji pożaru:

- Parametry zastosowanych czujek zasysających muszą być podane w sposób zgodny z normą EN 54-20
- Klasa zabezpieczenia obiektu musi być zgodna z przykładami aplikacji podanymi w tabeli 7 normy EN 54-20 albo lepsza – klasa min B
- Należy stosować czujki, które umożliwiają śledzenie rozwoju pożaru i realizację różnych scenariuszy w zależności od stopnia zadymienia.
- Dla umożliwienia śledzenia rozwoju pożaru zakres użytecznych nastaw czujki powinien wynosić co najmniej: od 0,06% zaciemnienia na metr do 6.5% zaciemnienia na metr.
- Dla umożliwienia realizacji różnych scenariuszy w zależności od stopnia zadymienia czujka powinna posiadać co najmniej 2 progi alarmowe dowolnie programowalne w całym zakresie podanym wyżej.
- Należy stosować czujki, dla których zostały opracowane specjalizowane metodologie obliczeń istotnych parametrów przepływowych i czułościowych, w szczególności komputerowe programy obliczeniowe dedykowane dla poszczególnych typów czujek.
- Projektant systemu sygnalizacji pożaru wykorzystującego zasysającą czujkę dymu obowiązany jest podać metodykę obliczeń istotnych parametrów czujki umożliwiających określenie klasy systemu właściwej dla zastosowania będącego przedmiotem projektu, a w szczególności:
    - obliczeń przepływów powietrza przez detektor, rury oraz poszczególne otwory próbkujące,
    - obliczeń czasów transportu dla najdalszych otworów próbkujących,
    - obliczeń czułości poszczególnych otworów próbkujących,
    - obliczeń stopnia zrównoważenia czułości wszystkich otworów próbkujących.

Akceptowalne są obliczenia wykonane przy użyciu:

- programów dostarczanych przez producenta danego sprzętu dedykowanych dla użytych detektorów,
- metod powszechnie stosowanych w mechanice płynów. W tym przypadku projektant musi przedstawić stosowaną metodologię (wzory i założenia - w szczególności upraszczające).

Zastosowane metodologia musi umożliwić ponowne przeliczenie systemu w przypadku konieczności wprowadzenia zmian na etapie wykonywania instalacji.

- Instalator systemu sygnalizacji pożaru wykorzystującego zasysającą czujkę dymu powinien przestawić:
    - autoryzację producenta lub dystrybutora,
    - zalecaną przez producenta lub dystrybutora metodykę uruchomienia systemu (formularz, check list, lub podobny dokument),

raport z uruchomienia na formularzu producenta lub dystrybutora.

- System zasysający z rurarzem PCV i jednostką detekcyjną z wbudowanym wentylatorem zasysającym powietrze.
- Kompletny rurarz PCV systemu wraz z trójnikami, kolanami, zaślepkami i uchwytami. Montaż rurarzu stały przez sklejenie części i osadzenie w uchwytach montażowych.
- monitorowanie przepływu powietrza, sygnalizacja usterki przy zmianie jego bilansu zgodnie z PN EN 54-20.
- Zasilanie systemu z certyfikowanego zasilacza buforowego. Czas podtrzymania zasilania min. 30h w stanie dozoru i 30 min w stanie alarmu.
- Nadzorowanie stanu alarmu i usterki systemu zasysającego przez nadrzędny system sygnalizacji pożaru.

XXVII. Sprzęt do cyfryzacji

Wymagania dla stanowisk roboczych

a)Minimalne wymagania techniczno-funkcjonalne dla komputera klasy PC wraz z oprogramowaniem (system operacyjny, oprogramowanie antywirusowe, pakiet biurowy, oprogramowanie OCR).

W zadaniu należy dostarczyć - 2 szt.

Procesor	Procesor dwurdzeniowy klasy x86, umożliwiający osiągnięcie przez komputer, w zaoferowanej konfiguracji sprzętowej, w teście SysMark2007, Preview Rating wyniku minimum 168pkt, testowany przy rozdzielczości ekranu 1280x1024 pikseli z paletą minimum 32 bit. Wymaga się załączenia wydruków z przeprowadzonych testów.
Pamięć RAM	4GB (DDR3 SDRAM 1333MHz) - możliwość rozbudowy do 16GB, dwa gniazda na pamięci wolne
Dysk twardy	250 GB (min. SATA II; min. 7200rpm, NCQ/3Gbit, 8mb cache)
Napęd dyskietek	brak
Napęd optyczny	DVD- RW SATA z oprogramowaniem do odtwarzania i nagrywania płyt DVD
Płyta główna	Producenta komputera, opatrzona trwałym jego Logo z niezamazywaną informacją w BIOS zawierającą nazwę oraz nr seryjny komputera, z wbudowanym kontrolerem dysków obsługującym konfiguracje RAID 0, 1, 5. Wyposażona w złącza: 2 x PCI-Express x 16, 1 x PCI

Bezpieczeństwo	1.BIOS musi posiadać możliwość - skonfigurowania hasła „Power On”, - ustawienia hasła dostępu do BIOSu (administratora), - blokadę portów USB, COM i Centronics; - możliwość wyłączenia w BIOS-ie portów USB; - możliwość wyłączenia w BIOS-ie portu szeregowego; - możliwość wyłączenia w BIOS-ie portu równoległego; - możliwość wyłączenia slotów PCI-E/PCI - kontrola sekwencji boot-ącej; - możliwość wyłączenia funkcji bootowania z urządzeń USB 2. Komputer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v 1.2); 3. Możliwość zapięcia linki typu Kensington
Karta dźwiękowa	-Zintegrowana -w standardzie High Definition -oparta o układ sprzętowy ALC663 lub nowszy -możliwość wyłączenia karty muzycznej w BIOS
Karta sieciowa	10/100/1000 Mbps WoL, PXE, -możliwość wyłączenia karty sieciowej w BIOS, -możliwość odczytania adresu MAC karty z BIOS komputera
Karta graficzna	Zintegrowana z płytą główną ze współdzieloną pamięcią karta dwumonitorowa z możliwością obsługi monitora do 2560 x 1600 pikseli, zgodna ze standardem DIRECTX 10.0,
Porty I/O	2 x PS/2 1 x Serial, 10 x USB 2.0 (w tym 4 z przodu obudowy), 1 x DB-15, 1 x Display Port 1 x RJ45, 1 x wejście audio 1 x wyjście audio, 1 x wejście mikrofonowe -nie dopuszcza się możliwości zasłonięcia złączy USB znajdujących się na panelu przednim jakimikolwiek zaślepkami, maskownicami utrudniającymi wzrokową weryfikację ich użycia – np. obecności klucza USB czy innego urządzenia podłączonego do złączy na panelu przednim obudowy komputera
Oprogramowanie	- system operacyjny w polskiej wersji umożliwiający pełną integrację i pracę w domenie opartej o Windows 2008 PL 64 bit - Preinstalowany fabrycznie na dysku twardym. - Dostarczony nośnik pozwalający na ponowną instalację systemu niewymagającą wpisywania klucza rejestracyjnego lub rejestracji poprzez Internet czy telefon - dostawa oprogramowania antywirusowego - dostawa pakietu biurowego zawierającego arkusz kalkulacyjny, edytor tekstu, program do prezentacji, klient pocztowy z kalendarzem) w pełni obsługujące dokumenty bez utraty jakichkolwiek ich parametrów i cech użytkowych (korespondencja seryjna, arkusze kalkulacyjne zawierające makra i formularze, itp.)

	- Oprogramowanie OCR o minimalnych funkcjonalnościach: - rozpoznawanie kodów jedno, jak i dwuwymiarowych, oferując opcję traktowania kodów paskowych jak grafiki lub rozpoznawania ich i wyświetlania ich wartości - zapisanie rozpoznanego tekstu w jednym z wielu formatów pliku, takich jak PDF, PDF/A, HTML, Microsoft Word XML, DOC/DOCX, RTF, XLS/ XLSX, PPTX, CSV i TXT - rozpoznawanie tekstu, w różnorodnych językach posługujących się alfabetem łacińskim, cyrylicą, greckim, ormiańskim, hebrajskim, chińskim, japońskim, tajskim i koreańskim - automatycznej identyfikacji języków - możliwość pracy z dokumentami wielojęzycznymi zawierającymi dowolną kombinację języków - przetwarzanie plików PDF - otwieranie plików graficznych: bmp, jpeg, jpeg 2000, tiff, jbig2, dcx, pcx, png, xps,dib,wdp, eksport do różnych formatów, w tym: rtf, txt, doc, xls, csv, dbf, html, pdf, ppt, docx, xlsx, pptx, html, scv - rozpoznawanie: pisma drukowanego i tabel, języków formalnych (C++, Pascal, etc.), tekstu w pionie, hiperłącz, nagłówków i stopek oraz numeracji stron oraz pieczątek - przetwarzanie zdjęć dokumentów wykonanych aparatem cyfrowym lub telefonem komórkowym -zachowanie koloru tekstu
Obudowa	Obudowa typu Tower, trwale oznaczona logo producenta, metalowa, umożliwiająca pracę w pionie jak i w poziomie oraz **montaż min. 2 napędów zewnętrznych 5.25**. Opcjonalny montaż dwóch dodatkowych dysków wewnętrznych. Obudowa musi umożliwiać serwisowanie komputera bez użycia narzędzi. Obudowa wyposażona w **czujnik otwarcia obudowy oraz fizyczne zabezpieczenie otwarcia obudowy w postaci kłódki z kluczem indywidualnym i serwisowym (master key) lub zamka elektromagnetycznego** -zasilacz o mocy maksymalnej 320W z aktywnym filtrem PFC, o gwarantowanej sprawności co najmniej 89% -licencja na system operacyjny oraz numer seryjny komputera umieszczony na górnej części obudowy -slot Kensington
Klawiatura	-Klawiatura USB/PS2 w układzie US -trwałe oznaczenie klawiatury logo producenta komputera
Mysz	-Mysz optyczna 800 dpi -USB -dwu-przyciskowa, rolka (scroll) jako trzeci przycisk
Inwentaryzacja i diagnostyka	1.Oprogramowanie wyprodukowane i wspierane przez producenta komputera wraz z licencją do zarządzania w sieci, pozwalające minimum na: -pracę w architekturze serwer-klient - licencja musi pozwalać na pełne wykorzystanie aplikacji w wymaganym zakresie -możliwość zdalnego przypisania dla jednego, lub grupy komputerów unikalne-

	go numeru inwentarzowego widocznego zdalnie dla administratora jak i bezpośrednio w BIOS maszyny - monitoring systemu i przekazywanie informacji o zdarzeniach na stację administratorską (konsola graficzna na stacji zarządzającej, konsola tekstowa, email, sms) -możliwość konfiguracji i weryfikacji zakresu i stopnia szczegółowości alertów przekazywanych na stację administratorską oraz wybór sposobu informacji o zdarzeniu -monitoring komponentów takich jak: dysku twardy (SMART), pamięci, wentylatorów, stanu czujnika otwarcia obudowy, monitoring temperatury wewnętrznej komputera -zdalne zarządzanie BIOS: wprowadzanie i zmiana haseł BIOS, archiwizacja i aktualizacja BIOSu dla pojedynczego komputera i grupy komputerów jednocześnie; modyfikacja sekwencji bootowania; -generowanie raportów dot. pojedynczych komputerów lub grup komputerów, w zakresie zainstalowanych komponentów, systemu operacyjnego oraz aplikacji - inwentaryzacja szczegółowa komputera: -odczyt modelu, numeru seryjnego i numer inwentarzowego komputera - wersja i model płyty głównej, wersja BIOS; - model, wersja firmware i numer seryjny dysku twardego, - model, wersja firmware i numer seryjny napędu optycznego - sposób obsadzenia kości pamięci wraz z informacją o zainstalowanych kościach (pojemność, oznaczenie, numer seryjny kości) 2. Oprogramowanie wyprodukowane i wspierane przez producenta komputera pozwalające minimum na: - praca w środowisku Windows 7, Vista, XP, DOS - pełną diagnostykę sprzętową komputera (praca dysku twardego, płyty głównej i jej układów, karty muzycznej, praca podsystemu pamięci, karty graficznej),pozwalającą na wykrycie usterki z wyprzedzeniem lub jej weryfikację -odczyt informacji o systemie: numer seryjny, numer inwentarzowy -eksport informacji do plików danych -automatyczne pobieranie z sieci Internet i instalację/aktualizację sterowników dla wszystkich komponentów sprzętowych notebooka dla systemów Windows 7, Vista i XP (aplikacja musi rozpoznawać automatycznie typ i model komputera, na którym pracuje, brak konieczności wprowadzania jakichkolwiek informacji na temat sprzętu przez użytkownika) -automatyczne pobieranie krytycznych dla pracy komputera poprawek systemowych (niezależnie od narzędzi systemu operacyjnego) 3. Wbudowana w płytę główną technologia zarządzania i monitorowania, która niezależnie od obecności systemu operacyjnego, powinna umożliwiać: a) monitorowanie konfiguracji komponentów komputera - CPU, pamięć, HDD, wersje BIOS płyty głównej;

	b) zdalną konfigurację BIOSu, zdalne uaktualnienie BIOSu; c) zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; d) zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej.
Gwarancja	**Gwarancja 36 miesięcy, na części i robociznę.** Realizowana w serwisie, transport w obie strony na koszt producenta.

b) Minimalne wymagania dla monitora 22 cali. Wymagana ilość dostawy: 2 szt.

Przekątna ekranu, rozdzielczość	Min. 22 cali o rozdzielczości natywnej minimum 1680x1050 pikseli, maksymalny rozmiar piksela 0.282 mm
Parametry obrazu	Odwzorowanie 16,7 miliona kolorów, kontrast min. 800:1, jasność min. 250cd/m^2 ,czas reakcji matrycy max.5ms, kąty widzenia minimum 160 stopni, częstotliwość pozioma 31,5-83kHz, częstotliwość pionowa 50-76 Hz (weryfikacja na podstawie dokumentacji technicznej producenta monitora)
Wejścia wideo	Przynajmniej: 1x DVI (HDCP), 1x VGA
Obudowa i regulacja monitora	Obudowa ekranu w kolorze czarnym lub siwym, pochylenie ekranu w zakresie -5° / +15° (tzw. tilt), zintegrowany zasilacz i głośniki stereo o mocy minimum 1W każdy, przynajmniej 1xzłącze Kensington Lock, 1xzłącze montażu na ścianie w standardzie VESA 100 (100 mm),
Kable	Kabel analogowy VGA o długości minimum 1,8m, kabel DVI o długości minimum 1,8m, kabel audio stereo - analogowy
Gwarancja	Gwarancja 36 miesięcy w systemie door- to- door
Menu OSD	TAK
Certyfikaty i normy, dokumentacja	Przynajmniej -Energy Star (EPA 4.1), zużycie energii max.33W wg standardów EPA -CE -ISO13406-2 (klasa II) -RoHS lub WEEE -Instrukcja obsługi monitora

Urządzenie wielofunkcyjne do cyfryzacji – szt. 1 - o funkcjonalności kopiarki, drukarki, skanera o parametrach:

Proces kopiowania elektrograficzny, laserowy
Szybkość kopiowania/druku A4: do 28 kopii/min A3: do 17 kopii/min
Automatyczna praca w trybie dwustronnym A4 do 28 kopii/min
Czas oczekiwania na pierwszą kopię/wydruk do 7 s
Czas przygotowania do pracy do 25 s
Rozdzielczość kopii 600 x 600 dpi
Skala szarości w zakresie kopiarki256 odcieni

Wielokrotność kopiowania 1 - 999, możliwość wstrzymania wykonywanego zadania
Format dokumentów oryginalnych do A3
Powiększanie 25 - 400% w odstępach co 0,1% , automatyczna zmiana rozmiarów
Język opisu stron: PCL 6 (PostScript 3)
Systemy operacyjne wspierane: Windows NT4.0/2000/XP/XP64/Vista/Vista64
Windows Server 2000/2003/2003 x64/Server2008 Macintosh OS 9.2 lub wersja
późniejsza
Macintosh OS 10.2,3,4/10.4 Unix/Linux/Citrix
Czcionki drukowane : 80x PCL Latin, 136x PostScript 3 Emulation Latin
Szybkość skanowania do 70 stron oryginału/min (200dpi, podawanie przez
automatyczny podajnik dokumentów), do 41 stron oryginału/min (600dpi, podawanie
przez automatyczny podajnik dokumentów) Rozdzielczość skanowania maks. 600 x 600
dpi
Formaty plików PDF, TIFF
Pamięć wewnętrzna minimum 192 MB
Interfejs 10Base-T/100Base-TX Ethernet, USB 2.0
Protokoły sieciowe: TCP/IP, IPX/SPX, AppleTalk (EtherTalk), SMB, LPD, IPP, SNMP,
HTTP
Format papieru A6 - A3
Gramatura papieru 50 - 210 g/m2
Wydajność tonera powyżej 15000 stron
Trwałość bębna/startera powyżej 70.000 stron

Serwerownia	**XX, XXI, XXII, XXIII, XXIV, XXVI**
Back Office	**I, II, III XXV, IV, V, VI, VII, IX, X, XII, XIII**
Płatności - sprzęt	**VIII, XI, XIV, XV, XVI, XVII, XVIII, XIX**
Sprzęt do cyfryzacji	**XXVII**