**Załącznik nr 1 do SIWZ**

Wykonawca w ramach dostawy dokona instalacji i konfiguracji wszystkich dostarczonych elementów.

Wykonawca zainstaluje na komputerach i serwerze dostarczone oprogramowanie.

Wykonawca dokona uruchomienia domeny w oparciu o dostarczony system operacyjny serwera.

W ramach uruchomienia domeny Wykonawca dokona wraz z pracownikami Zamawiającego:

- usystematyzowania nazewnictwa komputerów,
- usystematyzowania numeracji IP
- podziału przestrzeni dyskowej na komputerach i serwerze
- utworzy listę użytkowników domeny wraz podziałem na grupy
- utworzy strukturę katalogów sieciowych.

W trakcie wykonywania prac Wykonawca ma dokonać szkolenia pracowników Zamawiającego, umożliwiające samodzielne późniejsze administrowanie zasobami.

W celu wykonania powyższego Wykonawca musi dysponować minimum 2 osobami posiadającymi aktualny status Microsoft Certified Trainer, w tym minimum 1 posiadający certyfikat Microsoft Certified Solutions Expert.

W celu potwierdzenia spełnienia powyższych wymogów do oferty należy dołączyć wykaz osób wraz z numerem certyfikatu i linkiem do strony www gdzie można potwierdzić jego aktualny status.

Do oferty należy przedłożyć referencje z podaniem danych kontaktowych instytucji/firmy w celu weryfikacji poprawności wykonanych usług.

Ilekroć w treści SIWZ, w tym w opisie przedmiotu zamówienia, użyte są znaki towarowe, patenty lub pochodzenie, a także normy, Zamawiający dopuszcza rozwiązanie równoważne i zastrzega sobie prawo (np. w przypadku oferowania produktu równoważnego) do przeprowadzenia testów zgodności.

W przypadku wątpliwości dotyczących spełniania przez oferowany produkt wymagań określonych w SIWZ (np. w przypadku oferowania produktu równoważnego), Zamawiający zastrzega sobie możliwość wezwania, na etapie badania i oceny ofert, każdego z Wykonawców do dostarczenia produktu będącego przedmiotem zamówienia do siedziby wskazanej przez Zamawiającego, w celu wykonania stosownych testów. Wykonawca będzie zobowiązany, na pisemne żądanie Zamawiającego, do bezpłatnego wypożyczenia w ciągu 2 tygodni na okres co najmniej 2 tygodni zestawu sprzętu zaoferowanego w ofercie przez Wykonawcę.

Zamawiający przeprowadzi stosowne testy według niżej przedstawionych warunków:

- Testowanie zaoferowanych zestawów przeprowadzone będzie przez pracowników Zamawiającego lub przez osobę trzecią (np. osobę/osoby firmy zewnętrznej) wybraną przez Zamawiającego (biegłego w rozumieniu art. 21 ust 4 ustawy);

- Zamawiający zastrzega sobie prawo do testowania, przewożenia, powierzania sprzętu osobom trzecim celem dokonania stosownych testów, jeśli uzna to za niezbędne do prawidłowej oceny przedmiotu oferty;

- Przedmiotem testów będzie kompletny zestaw sprzętu, identyczny z zaoferowany w przetargu. Zestaw ten będzie w dalszym postępowaniu traktowany jako wzorcowy,

- Sprzęt dostarczony do testów musi mieć sprawne wszystkie elementy wymienione w specyfikacji. Niesprawność któregokolwiek elementu podczas testów dyskwalifikuje sprzęt. W tej sytuacji przedmiot zamówienia zostanie uznany za niespełniający warunków SIWZ.

Wykonawca zapewni serwis dostarczonego sprzętu w siedzibie Zamawiającego. Wykonawca zapewni wsparcie techniczne dotyczące systemu teleinformatycznego Zamawiającego opartego na dostarczonym sprzęcie w ilości 8 godzin miesięcznie w okresie trwania gwarancji. Do oferty należy dołączyć dane kontaktowe - email , nr telefonu- działu serwisowego Wykonawcy.

**Wykaz sprzętu:**

**Telefony stacjonarne – 20 szt.**

- CLIP - identyfikacja numerów przychodzących w systemie DTMF i FSK
- Pamięć 10 połączeń przychodzących
- Książka telefoniczna 20 wpisów
- Powtarzanie 5 ostatnich numerów
- Funkcja głośno mówiąca
- Paging - przywołanie słuchawki
- GAP - możliwość zalogowania do 5 słuchawek
- Wyświetlanie czasu połączenia
- Blokada klawiszy
- Czas czuwania około 100 h

**Centrala telefoniczna – 1 szt.**

- Pojemność:
    - do 24 telefonów analogowych
    - do 100 abonentów IP (w tym 18 abonentów telefonów systemowych IP)
    - do 12 cyfrowych telefonów systemowych

- Cechy sprzętowe:
    - wewnętrzna brama IP - bezpieczeństwo, niezawodność, gwarancja wysokiej jakości rozmów - obsługa protokołów SIP oraz IAX2 (kodeki G.711, G.729)
    - wewnętrzna brama GSM obsługująca małe karty SIM dowolnego operatora GSM (900/1800) - optymalizacja kosztów połączeń oraz wsparcie dla pracy mobilnej, obsługa sms
    - współpraca z ISDN-BRA (2B+D) i POTS (Clip-FSK, wybieranie tonowe i impulsowe)
    - zintegrowany system nagrywania - Embedded Recording - do 8 kanałów nagrywania
    - modem zdalnego zarządzania serwerem
    - monitoring i zarządzanie poprzez firmową sieć LAN lub zdalnie - poprzez modem lub Internet
    - współpraca z cyfrowymi telefonami systemowymi oraz systemowymi telefonami IP
- Cechy funkcjonalne:
    - wsparcie dla protokołów TAPI (integracja z MS Outlook), CTIP (rozwiązania CRM), HOTELP (aplikacje hotelowe)
    - aplikacja do obsługi połączeń oraz innych funkcji centrali, obsługa sms i odsłuchiwanie nagrań za pomocą komputera
    - aplikacja do zarządzania ruchem telefonicznym oraz konferencjami z poziomu ekranu dotykowego monitora
    - inteligentna dystrybucja połączeń
    - wsparcie dla pracy mobilnej - telefon stacjonarny i komórkowy dostępny pod jednym numerem
    - program taryfikacyjny - informacja o kosztach i strukturze połączeń
    - do 99 zapowiedzi łącznie oraz możliwość odtwarzania do 4 jednoczesnych zapowiedzi na Infoliniach
    - TELEKONFERENCJE - do 32 uczestników konferencji
    - system Poczty Głosowej
    - redukcja kosztów - funkcja LCR (LeastCost Routing) - automatyczny wybór najtańszej drogi połączenia

**Szafa serwerowa – 1 szt.**

- Wysokość minimum 199 cm, głębokość minimum 107cm, szerokość minimum 60 cm. Drzwi przednie i tylne perforowane, zdejmowane, zamykane na klucz. Boczne ściany dzielone,

zdejmowane. Szafa powinna mieć możliwość łączenia z innymi szafami tego samego modelu. Szafa powinna być wyposażona w elementy stabilizujące.

- Szafa musi być kompatybilna ze wszystkimi zaoferowanymi urządzeniami
- Szafa powinna umożliwiać montaż urządzeń zgodnie ze standardem CEA-310E. Pionowe belki nośne szafy powinny pozwalać na przesuwanie ich w ramach obudowy.
- Listwa zasilająca PDU posiadająca minimum 8 gniazd 10A – 2 szt.
- Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.
- Szafa musi być wyprodukowana zgodnie z normą ISO 9001.

**Szafa GPD – 1 szt.**

- Wysokość minimum 199 cm, głębokość minimum 107cm, szerokość minimum 60 cm. Drzwi przednie i tylne perforowane, zdejmowane, zamykane na klucz. Boczne ściany dzielone, zdejmowane. Szafa powinna mieć możliwość łączenia z innymi szafami tego samego modelu. Szafa powinna być wyposażona w elementy stabilizujące.
- Szafa musi być kompatybilna ze wszystkimi zaoferowanymi urządzeniami
- Szafa powinna umożliwiać montaż urządzeń zgodnie ze standardem CEA-310E. Pionowe belki nośne szafy powinny pozwalać na przesuwanie ich w ramach obudowy.
- Listwa zasilająca PDU posiadająca minimum 8 gniazd 10A – 2 szt.
- Panel krosowy kategorii 6 UTP 24 porty 1U – 8 szt.
- Uchwyt kablowy z wieszakami 1U – 8szt
- Panel wentylacyjny z termostatem
- Półka na elementy aktywne o podwyższonej obciążalności
- Kaseta światłowodowa pusta, umożliwiająca montaż minimum 24 włókna światłowodowe
- Przynajmniej trzy lata gwarancji od momentu podpisania umowy z czasem reakcji do końca następnego dnia roboczego od zgłoszenia awarii, naprawa w miejscu instalacji szafy.
- Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.
- Zamawiający wymaga dokumentacji w języku polskim
- Szafa musi być wyprodukowana zgodnie z normą ISO 9001.
- W zakres zamówienia wchodzi również montaż istniejącego okablowania do dostarczonych przez wykonawcę paneli krosowych oraz dokonanie pomiarów skrosowanych kabli.

W obiekcie Zamawiającego zainstalowano okablowanie strukturalne kat. 6 oparte na kablach miedzianych kat. 6 UTP LSOH firmy Shrack. Zamawiający wymaga aby dostarczone patchpanele umożliwiały uzyskanie u producenta okablowania certyfikatu gwarancyjnego na

okres 20 lat. W tym celu wykonawca wykaże dysponowanie minimum 2 autoryzowanymi instalatorami systemu okablowania strukturalnego – osoby należy umieścić w wykazie określonym w punkcie VI. 1. 3 SIWZ.

Po montażu patchpaneli Wykonawca wykona pomiary dynamiczne sieci strukturalnej miernikiem min. klasy 3, wykonawca ma dysponować co najmniej jedną osobą posiadającą certyfikat CCTT lub jego równoważnik, wydany przez producenta (lub jego autoryzowanego przedstawiciela) przyrządu przewidzianego do pomiarów instalacji logicznej.

Przyrząd użyty do pomiarów musi posiadać aktualny certyfikat kalibracji przyrządu przewidzianego do pomiaru instalacji logicznej i elektrycznej.

**Switch – 10 szt.**

- Architektura sieci LAN - GigabitEthernet
- Liczba portów 1000BaseT (RJ45) - minimum 24 szt.
- Liczba gniazd GBIC – minimum 4 szt.
- Porty komunikacji - USB
- Zarządzanie, monitorowanie i konfiguracja:
    - CLI - Command Line Interface
    - DHCP Client - Dynamic Host Configuration Protocol (RFC 2131)
    - DHCP Server - Dynamic Host Configuration Protocol (RFC 2131)
    - FTP - protokół transmisji plików
    - HTTP - Hypertext Transfer Protocol
    - ICMP - Internet Control Message Protocol (RFC792)
    - IP Multicast / IGMP v1, v2, v3/ IGMP Proxy
    - IPv4 - Internet Protocol v4 (RFC 791) Upgradeable to v6 (RFC 1883)
    - RMON - Remote Monitoring
    - RMON II - Remote Monitoring ver. 2
    - SNMP - Simple Network Management Protocol
    - SNMPv2 - Simple Network Management Protocol ver. 2
    - SSH - Secure Shell
    - Telnet
    - TFTP - Trivial File Transfer Protocol
- Protokoły uwierzytelniania i kontroli dostępu

  - ACL bazujący na adresach IP i typie protokołu
  - ACL bazujący na adresach MAC
  - IEEE 802.1x - Network Login
  - IEEE 802.1x - Network Login (MAC-based Access Control)
  - IEEE 802.1x - Network Login (Port-based Access Control)
  - RADIUS - zdalne uwierzytelnianie użytkowników
  - TACACS+ - Terminal Access Controller Access Control System
- Obsługiwane protokoły i standardy
  - IGMP - Internet Group Management Protocol
  - IP multicast
  - IP QoS
  - IPv4
  - IPv6
  - Jumbo framesupport
  - IGMP - Internet Group Management Protocol
  - LoadBalancing
  - RADIUS - zdalne uwierzytelnianie użytkowników
  - SNMPv3 - Simple Network Management Protocol ver. 3
  - DHCP - Dynamic Host ConfigurationProtocol
- Rozmiar tablicy adresów MAC - 8000
- Algorytm przełączania - Store-and-Forward
- Prędkość magistrali wew. - 88 Gb/s
- Przepustowość - 41,7 mpps
- Bufor pamięci - 128 MB
- Warstwa przełączania - 2
- Możliwość łączenia w stos - Tak
- Maksymalna liczba urządzeń w stosie - 4
- Typ obudowy - rack 19"

- Maksymalny pobór mocy - 40 Wat
- Enhanced Limited Lifetime Warranty

**Router (GPD) – 1 szt.**

- Porty WAN - 2x 10/100/1000BaseT (RJ45)
- Porty LAN - 4x 10/100/1000BaseT (RJ45)
- Zarządzanie, monitorowanie i konfiguracja:
    - zarządzanie przez przeglądarkę WWW
    - SNMPv2 - Simple Network Management Protocol ver. 2
    - Syslog - Security Issues in Network Event Logging
- Obsługiwane protokoły routingu:
    - routing statyczny
    - routing dynamiczny
    - RIP v1 - Routing Information Protocol ver. 1
    - RIP v2 - Routing Information Protocol ver. 2
- Obsługiwane protokoły i standardy
    - IEEE 802.3 - 10BaseT
    - IEEE 802.3u - 100BaseTX
    - TCP/IP - Transmission Control Protocol/Internet Protocol
    - NAT - Network AddressTranslation
    - IEEE 802.3ab - 1000BaseT
    - DNS - DomainName System
    - DHCP Client - Dynamic Host Configuration Protocol Client
    - DHCP Server - Dynamic Host Configuration Protocol Server
    - UPnP - Universal plug-and-play
    - DynDNS - DynamicDomainName System
    - DMZ - Demilitarized Zone
    - IEEE 802.1p - Priority
- Obsługiwane protokoły VPN

  - IPSec pass-trough
  - PPTP pass-trough
  - L2TP pass-trough
- Dodatkowe funkcje
  - NAT Firewall
  - 4-portowy Switch
  - Filtrowanie IP
  - filtrowanie MAC
  - Filtrowanie URL
  - port forwarding (Virtual Server) - przekierowanie usług TCP/IP komputery w sieci
  - dzieli dostęp do internetu dostarczanego poprzez modem TV kablowej
  - dzieli dostęp do internetu dostarczanego poprzez modem DSLowy z wyjściem RJ45
  - DMZ
  - SPI Firewall - StatefulPacketInspection
  - port triggering - przyporządkowywanie zakresów portów wychodzących do przycho.
  - port binding - przypisywanie usług do konkretnego portu WAN
  - NSD - Network Service Detection

**Macierz dyskowa (GPD) - 1szt.**

- System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19"
- System musi zostać dostarczony w konfiguracji zawierającej minimum:
  - 12 dysków 300Gb SAS 15k
  - 12 dysków 1TB SATA
  - posiadać możliwość rozbudowy o kolejne dyski
- System musi wspierać dyski:
  - SAS 300GB, 450G, 600GB, 900GB i 1200GB
  - SATA 1TB, 2TB, 3TB, 4TB
  - SSD 100GB, 200GB, 800G

- Budowa systemu musi umożliwiać rozbudowę do modeli wyższych bez potrzeby migracji danych
- System musi mieć możliwość rozbudowy do 144 dysków
- Dwa kontrolery wyposażone w przynajmniej 6GB cache każdy
- W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny
- Oferowana macierz musi mieć minimum
    - 4 porty FC 8GB
    - 8 portów 1Gbeth,
    - 4 porty SAS,
- System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii minimum dwóch dysków w grupie RAID
- Macierz musi być wyposażona w system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy. System kopii migawkowych nie może powodować spadku wydajności macierzy +/-5%
- Macierz musi obsługiwać jednocześnie protokoły FC, iSCSi, CIFS i NFS - jeśli wymagane są licencje Zamawiający wymaga dostarczenia ich wraz z macierzą.
- Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych którą można stosować na macierzy/danych produkcyjnej dla wszystkich rodzajów danych. Macierz powinna mieć możliwość czynności odwrotnej tzn. cofnięcia procesu deduplikacji na zdeduplikowanym wolumenie
- Macierz musi posiadać funkcjonalność integracji wykonywania (snapshotu, odtworzenia, replikacji, klonu) z Vmware na 3 hosty fizyczne. Wszystkie operacje powinny być wykonywane z widoku konsoli Vcenter.
- Macierz musi posiadać funkcjonalność tworzenia wirtualnych klonów, które nie wymagają kopiowania danych na dyskach macierzy
- Macierz musi posiadać funkcjonalność kompresji danych
- Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Win 2003/2008, Linux, Vmware, Unix
- Macierz musi posiadać funkcjonalność błyskawicznego odtwarzania danych z snapshotu nie wymagająca kopiowania danych.
- Macierz musi posiadać funkcjonalność pozwalającą na wirtualizację macierzy (z fizycznej macierzy tworzenie wirtualnych partycji)

- Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenow logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie
- Macierz musi pozwalać na wykorzystywanie dysków SSD w celu zwiększania szybkości zapisu i odczytu z dysków SAS lub SATA
- Macierz musi posiadać funkcjonalność priorytetyzacji zadań
- Macierz musi posiadać możliwość automatycznego informowania przez macierz i przesyłania przez pocztę elektroniczną raportów o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne macierzy.
- Producent musi dostarczyć usługę w postaci portalu WWW umożliwiającą następujące funkcjonalności:
    - Narzędzie do tworzenia procedury aktualizacji oprogramowania macierzowego.
        - procedura musi opierać się na aktualnych danych pochodzących z macierzy oraz najlepszych praktykach producenta.
        - procedura musi uwzględniać systemy zależne np, macierze replikujące
        - procedura musi umożliwiać generowanie planu cofnięcia aktualizacji.
    - Wyświetlanie statystyk dotyczących wydajności, utylizacji, oszczędności uzyskanych dzięki funkcjonalnością macierzy.
    - Wyświetlanie konfiguracji macierzy oraz porównywanie jej z najlepszymi praktykami producenta w celu usunięcia błędów konfiguracji.
- Gwarancja i serwis: 3 lata gwarancji producenta z czasem dostawy elementu na następny dzień roboczy od diagnozy problemu oraz 3 lata subscrybcji do oprogramowania

**Laptopy – 12 szt.**

- Procesor typu X86, 64-bitowy. Procesor powinien osiągać w teście wydajności PassMarkPerformanceTest co najmniej wynik 3500 punktów Passmark CPU Mark.
- Wyświetlacz kolorowy 15-15,6” TFT – matryca matowa,
- Dysk twardy 500GB, 7200 rpm
- Pamięć RAM – min 4GB, możliwość rozbudowy do min 16GB
- Karta graficzna – min. 1GB własnej pamięci
- Zintegrowana karta dźwiękowa, wbudowane 2 głośniki
- Karta sieciowa 1x10/100/1000BaseT Gigabitehthernet (RJ45)
- Napęd DVD ±RW/DVD±R, obsługa Dual Layer

- Złącza i porty zewnętrzne: złącze typu Keningston Lock, USB min. 2.0 – min. 3 porty, wyjście VGA, wyjście cyfrowego sygnału video, slot ExpressCard, wyjście słuchawkowe – 3,5mm, wejście mikrofonowe – 3,5mm, oraz inne – jeżeli są niezbędne do prawidłowego podłączenia pozostałych elementów zestawu
- Klawiatura sprzętowa QWERTY, zintegrowana z obudową
- Waga max. 3,5kg
- Akumulator zapewniający czas pracy na baterii minimum 5 godz.
- Zasilacz sieciowy 230V
- Instrukcja techniczno-instalacyjna w języku polskim
- Touchpad oraz dodatkowo mysz optyczna o rozdzielczości min. 800 dpi – przewodowa USB
- W obudowie notebooka zintegrowany mechaniczny zamek zapobiegający samoczynnemu otwarciu notebooka,
- System operacyjny Windows 7 wersja Pro wraz z najnowszą wersją ServicePack (licencja + nośniki)
- Dodatkowo nośnik z wersją instalacyjną ww. oprogramowania
- Nośnik ze wszystkimi niezbędnymi sterownikami
- Gwarancja: 3 lata z serwisem następnego dnia w siedzibie klienta

**Stacje robocze – 2kpl (komputer, monitor).**

- Typ obudowy komputera: Mini Tower
- Typ zainstalowanego procesora : Intel Core i5
- Pojemność pamięci cache [L3] 6 MB
- Ilość zainstalowanych dysków: 2 szt.
- Pojemność zainstalowanego dysku:
  - 1 TB SATA III
  - 32 GB SSD
- Pojemność zainstalowanej pamięci RAM: 8192 MB
- Maksymalna pojemność pamięci RAM: 32768 MB
- Rodzaj zainstalowanej pamięci: DDR3
- Częstotliwość szyny pamięci 1600 MHz
- Ilość banków pamięci 4 szt.

- Ilość wolnych banków pamięci 2 szt.
- Producent chipsetu zainstalowanej płyty głównej: Intel
- Typ zainstalowanej karty graficznej: ATI Radeon HD 7770
- Zainstalowana pamięć wideo: 2048 MB
- Zintegrowana karta dźwiękowa
- Zintegrowana karta sieciowa
- Typ zintegrowanej karty sieciowej: 10/100/1000 Mbit/s
- Bezprzewodowa karta sieciowa
- Typ bezprzewodowej karty sieciowej: IEEE 802.11b/g/n
- Bluetooth: Tak
- Ilość slotów PCI-E 1x: 3 szt.
- Ilość wolnych slotów PCI-E 1x: 3 szt.
- Ilość slotów PCI-E 16x 1 szt.
- Ilość wolnych slotów PCI-E 16x 0 szt.
- Interfejsy
    - 1 x 15-stykowe D-Sub (wejście na monitor)
    - 1 x HDMI
    - 6 x USB 2.0
    - 4 x USB 3.0
    - 1 x RJ-45 (LAN)
    - 1 x wyjście słuchawkowe (na froncie obudowy)
    - 1 x wejście na mikrofon (na froncie obudowy)
    - 1 x wejście na mikrofon
    - 1 x wejście liniowe
    - 1 x wyjście liniowe (przód)
    - 1 x wyjście liniowe (tył)
    - 1 x wyjście liniowe (boki)
    - 1 x wyjście liniowe (środek/sub)

  - 1 x SPDIF
  - 4 x USB 2.0 (tylny panel)
  - 2 x USB 2.0 (przedni panel)
  - 2 x USB 3.0 (tylny panel)
  - 2 x USB 3.0 (przedni panel)
- Napędy wbudowane: Blu-ray (BD-R/RE/ROM) | DVD±RW DL
- Moc zasilacza: 350 Wat
- System operacyjny: Microsoft Windows 7 Professional 64-bit
- Dołączone wyposażenie
  - Czytnik kart pamięci 19-in-1
  - Klawiatura bezprzewodowa
  - mysz bezprzewodowa
- Monitor
  - Format ekranu monitora: panoramiczny
  - Przekątna ekranu minimum 19 cali
  - Technologia podświetlenia: LED
  - Rozdzielczość obrazu minimum 1600 x 900 pikseli Czas reakcji matrycy: 5 ms Jasność minimum 250 cd/m2 Kontrast minimum 1000:1 Kąt widzenia poziomy minimum 170 stopni Kąt widzenia pionowy minimum 160 stopni Liczba wyświetlanych kolorów minimum 16,7 mln Wbudowany zasilacz
- Gwarancja: 3 lata z serwisem następnego dnia w siedzibie klienta
- Monitor i Stacja robocza od jednego producenta

**UPS 2700W – 1szt.**

- Typ obudowy: Rack
- Wysokość obudowy max 3U
- Posiadający graficzny wyświetlacz LCD
- Możliwość podłączenia dodatkowego modułu bateryjnego.
- Czas podtrzymania wraz z modułem przy obciążeniu 50% / 100% : 12 minut / 5 minut
- Złącza: 1x RS232, 1x USB, 8x C13, 1x C19
- Wewnętrzna karta umożliwiająca zarządzenie zasilaczem poprzez siec LAN

- Moc znamionowa minimum 2700 W
- Line Interactive
- Zarządzanie poprzez sieć Ethernet
- Zamawiający wymaga dokumentacji w języku polskim

**UPS 1000W – 1szt.**

- Typ obudowy: Rack
- Moc znamionowa: 1000 W
- Czas pracy przy 100% obciążeniu: ok. 5 minut
- Czas pracy przy 50% obciążeniu: ok. 14 minut
- Zarządzanie poprzez sieć Ethernet
- Line Interactive
- Zamawiający wymaga dokumentacji w języku polskim

**Konsola KVM – 1 szt.**

- 8 portowy przełącznik KVM
- Przyłącze KVM, USB
- Obudowa 1U
- Monitor LCD 18’5” do instalacji w szafie rack wraz z zintegrowaną klawiatura i urządzeniem wskazującym, min. 1 złącze USB 3.0
- Klawiatura US (QWERTY) oraz touchpad
- Przełącznik KVM 8-portowy dedykowany przez producenta oferowanego monitora rack, zajmujący wraz z monitorem wysokość maksymalnie 1U w szafie Rack, w komplecie 8 sztuk kabli umożliwiający podłączenie serwerów interfejsem USB.
- Przynajmniej trzy lata gwarancji od momentu podpisania umowy z czasem reakcji do końca następnego dnia roboczego od zgłoszenia awarii, naprawa w miejscu instalacji szafy.
- Zamawiający wymaga dokumentacji w języku polskim

**Serwery główne – 3 szt.**

- Obudowa Rack o wysokości maks. 1U z możliwością instalacji min. 8 dysków 2.5" Hot Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem kabli

- Posiadająca dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera.
- Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
- Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
- Dwa procesory sześciordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku
- min. 441 punktów w teście SPECint_rate_base2006 dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej
- Do oferty należy załączyć wynik testu dla oferowanego modelu serwera.
- 64 GB pamięci RAM typu LV RDIMM o częstotliwości pracy 1333MHz
- Płyta powinna obsługiwać do 768GB, na płycie głównej powinno znajdować się minimum 24 sloty przeznaczonych dla pamięci
- Możliwe zabezpieczenia pamięci: Memory Rank Sparing, Memory Mirror, SBEC, Lockstep
- Min. 2 sloty PCI Express x16 generacji 3 połowy wysokości, minimum 1 slot PCI Express x8 połowy wysokości
- Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024
- min. 5 portów USB 2.0 , 4 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232
- Minimum 4 porty typu Gigabit Ethernet Base-T z wsparciem dla protokołu IPv6 oraz możliwością iSCSIboot. Interfejsy sieciowe nie mogą zajmować żadnego z dostępnych slotów PCI-Express. Możliwość instalacji wymiennie modułów udostępniających:
    - 2 porty Gigabit Ethernet Base-T oraz 2 porty 10Gb Ethernet SFP+
    - 2 porty Gigabit Ethernet Base-T oraz 2 porty 10Gb Ethernet BaseT
    - 4 portów 10Gb Ethernet SFP+
- Możliwość zainstalowania wewnętrznego modułu z redundantnymi kartami SD oraz klucza USB. Możliwość skonfigurowania mirroru pomiędzy redundantnymi kartami SD.
- Sprzętowy kontroler dyskowy, posiadający min. 512MB nieulotnej pamięci cache , możliwe konfiguracje poziomów RAID : 0, 1, 5, 6, 10, 50, 60
- Możliwość instalacji dysków twardych SATA, SAS, NearLine SAS, SSD, oraz samoszyfrujacych dostępnych w ofercie producenta serwera.
- Zainstalowane 2 dyski twarde o pojemności min. 146GB SAS 15k RPM każdy, skonfigurowane fabrycznie w RAID 1.

- Możliwość instalacji wewnętrznego modułu dedykowanego dla hypervisorawirtualizacyjnego, wyposażonego w 2 jednakowe nośniki typu flash z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
- Wbudowany napęd DVD-ROM
- Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
- Redundantne zasilacze o mocy maks. 750W każdy
- Minimum 6 redundantnych wentylatorów Hot-Plug
- Zintegrowany z płytą główną moduł TPM. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
- VMwareESXi w wersji min. 5.1 Essensial Plus – licencja obejmująca 3 serwery 2 procesorowe - wraz z 3 letnim wsparciem technicznym oraz dokumentacją.
- Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:
    - zdalny dostęp do graficznego interfejsu Web karty zarządzającej
    - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera, )
    - szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika
    - możliwość podmontowania zdalnych wirtualnych napędów
    - wirtualną konsolę z dostępem do myszy, klawiatury
    - wsparcie dla IPv6
    - wsparcie dla WSMAN (Web Service for Managament); SNMP; IPMI2.0, VLAN tagging, Telnet, SSH
    - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer
    - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
    - integracja z Active Directory
    - możliwość obsługi przez dwóch administratorów jednocześnie
    - wsparcie dla dynamic DNS
    - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej

- możliwość podłączenia lokalnego poprzez złącze RS-232
- w przypadku awarii karty sieciowej, kontrolera RAID dla dysków wewnętrznych lub płyty głównej, w przypadku wymiany serwisowej zostaną wczytane automatycznie te same ustawienia i wersje firmware, BIOS, specyficzne dla danych komponentów zapisane na wbudowanej w kartę zarządzającą pamięci flash. Jeśli funkcjonalność ta wymaga płatnych komponentów lub usługi dodatkowej to powinny zostać uwzględnione w wycenie.

- Trzy lata gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365.
- W przypadku awarii, dyski twarde pozostają własnością Zamawiającego.
- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty.
- Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem – dokumenty potwierdzające załączyć do oferty.
- Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001.
- Serwer musi posiadać deklaracja CE.
- Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2008 R2 x64, x86, Microsoft Windows Server 2012.
- Zamawiający wymaga dokumentacji w języku polskim
- Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

**Serwer do backupu – 1 szt.**

- Obudowa typu tower z możliwością instalacji min. 8 dysków 3.5" Hot Plug oraz konwersji do wersji rack
- Obudowa posiadająca dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera.
- Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
- Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
- Dwa procesory czterordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku

- min. 198 punktów w teście SPECint_rate_base2006 dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej.
- Do oferty należy załączyć wynik testu dla oferowanego modelu serwera
- 64 GB pamięci RAM typu LV RDIMM o częstotliwości pracy 1333MHz.
- Płyta powinna obsługiwać do 384GB pamięci RAM, na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych dla pamięci
- Możliwe zabezpieczenia pamięci: Memory Rank Sparing, Memory Mirror, SBEC, Lockstep
- Minimum 6 złącz PCI Express, w tym:
    - minimum 1 złącze generacji 2, x8 o prędkości x4
    - minimum 1 złącze generacji 2, x8 o prędkości x1
    - minimum 2 złącza generacji 3, x16
    - minimum 2 złącza generacji 3, x8 o prędkości x4
- W każdym przypadku opis slotu dotyczy jego przepustowości a nie tylko długości. Wszystkie sloty powinny umożliwiać instalację kart pełnej długości i wysokości.
- Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024
- min. 9 portów USB 2.0, 2 porty RJ45, 1 port VGA, min. 1 port RS232
- Wbudowana dwuportowa karta Gigabit Ethernet
- Sprzętowy kontroler dyskowy, posiadający min. 512MB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID : 0, 1, 5, 6, 10, 50, 60
- Możliwość instalacji dysków twardych SATA, SAS, NearLine SAS, SSD oraz samoszyfrujących dostępnych w ofercie producenta serwera.
- Zainstalowane 2 dyski twarde o pojemności min. 300GB SAS 15k RPM każdy, skonfigurowane fabrycznie w RAID 1.
- Możliwość instalacji wewnętrznego modułu dedykowanego dla hypervisorawirtualizacyjnego, wyposażonego w 2 jednakowe nośniki typu flash z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
- Wbudowany napęd DVD-ROM
- Możliwość instalacji wewnętrznego napędu taśmowego lub na wymienne dyski twarde
- Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
- Redundantne zasilacze o mocy maks. 750W każdy

- Minimum 2 redundantne wentylatory wewnątrz obudowy
- Zintegrowany z płytą główną moduł TPM. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
- Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:
    - zdalny dostęp do graficznego interfejsu Web karty zarządzającej
    - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera, )
    - szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika
    - możliwość podmontowania zdalnych wirtualnych napędów
    - wirtualną konsolę z dostępem do myszy, klawiatury
    - wsparcie dla IPv6
    - wsparcie dla WSMAN (Web Service for Managament); SNMP; IPMI2.0, VLAN tagging, Telnet, SSH
    - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer
    - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
    - integracja z Active Directory
    - możliwość obsługi przez dwóch administratorów jednocześnie
    - wsparcie dla dynamic DNS
    - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
    - możliwość podłączenia lokalnego poprzez złącze RS-232
    - w przypadku awarii karty sieciowej, kontrolera RAID dla dysków wewnętrznych lub płyty głównej, w przypadku wymiany serwisowej zostaną wczytane automatycznie te same ustawienia i wersje firmware, BIOS, specyficzne dla danych komponentów zapisane na wbudowanej w kartę zarządzającą pamięci flash. Jeśli funkcjonalność ta wymaga płatnych komponentów lub usługi dodatkowej to powinny zostać uwzględnione w wycenie.
- Trzy lata gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365.
- W przypadku awarii, dyski twarde pozostają własnością Zamawiającego.

- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty.
- Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem – dokumenty potwierdzające załączyć do oferty.
- Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001.
- Serwer musi posiadać deklaracja CE.
- Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Windows Server 2008 R2 x64,, x86, Microsoft Windows Server 2012.
- Zamawiający wymaga dokumentacji w języku polskim
- Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

**Drukarka sieciowa kolorowa – 1 szt.**

- Prędkość A4/ A3 25/ 13 str. w kolorze i czerni
- Podajnik boczny na 100 arkuszy (do 256 gramatura)
- Podajnik dolny 2 x 500 arkuszy (do 256 gramatura)
- RADF (automatyczny podajnik dokumentów na 100 ark)
- Automatyczny dupleks
- Pamięć 2 GB RAM / 160 GB HDD
- Drukarka sieciowa
- Skaner sieciowy kolorowy
- Karta sieciowa gigabit ethernet
- Technologia HyPas (przeglądarka internetowa)
- Dwa zestawy serwisowe na 200 000 kopii/ wydruków

**Drukarka sieciowa czarno-biała – 1 szt.**

- Prędkość wydruku: 45 stron /min
- Podajnik na 500 kartek
- Standardowy interfejs: USB 2.0 (Hi-Speed), 2 USB Host Interfaces, Gigabit Ethernet
- Rozdzielczość: 1,200 dpi

- Moduł dwustronny: Duplex jako standard A4
- Napięcie zasilania: AC 220 ~ 240 V, 50/60 Hz

**Serwer Proxy – outsourcing 3 lata**

Wykonawca udostępni Zamawiającemu serwer dedykowany na okres 3 lat z zainstalowanym serwerem Proxy o parametrach nie mniejszych niż:

- Technologia: Sandy Bridge
- Procesor minimum Intel Core i5-2400
- Intel Smart Cache minimum 6MB
- Rdzenie minimum 4
- Wątki minimum 4
- Zegar minimum 3.1GHz
- Turbo Boost minimum 3.4GHz
- Wirtualizacja: tak
- Pamięć RAM minimum 16 GB DDR3
- Dysk twardy 2x minimum 2TB SATA3
- RAID SOFT - 0/1
- Karta sieciowa GigaEthernet
- Połączenie sieciowe 100 Mbps
- Przepustowość wejściowa (z Internetu do providera) 100 Mbps
- Przepustowość wychodząca (od providera do Internetu) 100 Mbps
- Adres IP IPv4 1 szt.
- Zdalny reboot serwera 24/7
- Obsługa systemów operacyjnych Linux, BSD, Microsoft Windows
- Secondary DNS

**Kamera kopułkowa – 6 szt.**

Wykonawca dostarczy oraz podłączy do istniejącego systemu monitoringu 6 kamer – po dwie na każdej kondygnacji budynku. Kamery mają posiadać parametry nie słabsze niż:

- Mechaniczny filtr podczerwieni

- Możliwość pracy w podczerwieni
- Rozdzielczość pozioma: 700 TVL
- Czułość: od 0.00003 lx/F=1.2 (DSS)
- Szeroki zakres dynamiki (WDR) - funkcja poprawiająca jakość obrazu dla różnych poziomów oświetlenia sceny
- Wydłużony czas ekspozycji (DSS)
- DIS - cyfrowa stabilizacja obrazu
- DNR - cyfrowa redukcja szumu
- HLC - funkcja redukująca efekt oślepiania kamery
- Typ obiektywu: z automatyczną przysłoną typu D, f =2.5 ~ 12 mm
- Możliwość 3-osiowej regulacji położenia modułu kamerowego
- Zoom: 16 x cyfrowy
- 12 stref prywatności
- Dodatkowe funkcje: odbicie lustrzane i obrót obrazu o 180°, detekcja ruchu
- Menu ekranowe w języku polskim, programowane za pomocą przycisków wewnątrz obudowy kamery
- Obudowa w kolorze białym
- Zasilanie: 12 VDC

Wykonawca zobowiązuje się do dostarczenia niżej wymienionego oprogramowania:

1. EndNote
2. Origin Lab Pro
3. Statistica plus Zestaw Medyczny
4. Vector NTI Express lub równoważny
5. Pakiet biurowy Microsoft Office 2010 lub nowszy
6. Oprogramowanie antywirusowe
7. Oprogramowanie do backupu
8. Oprogramowanie do systemu zarządzania pracą biobanku

Wszystkie licencje na oprogramowanie mają umożliwiać przenoszenie oprogramowania pomiędzy komputerami w zależności od potrzeb zamawiającego.

**Specyfikacja oprogramowania:**

**Ad. 1) EndNote – 1 licencja**

**Program do zarządzania bazą danych bibliograficznych**

1. Tworzenie bazy informacji bibliograficznej i modyfikację jej zawartości.
2. Praca programu możliwa jako samodzielna aplikacja w środowisku systemu operacyjnego, ale mająca dodatkową możliwość pracy jako aplikacja "web-based".
3. Przeglądanie on-line baz dostępnych via Internet ze zdefiniowanymi plikami połączeń do katalogów bibliotek wiodących uczelni na świecie.
4. Import z baz danych off-line i możliwość definiowania własnych filtrów importu.
5. Dostęp do baz danych za pomocą protokołu Z39.50
6. Łatwa zmiana stylu wykazu bibliografii i dostępny szeroki zestaw stylów bibliograficznych.
7. Możliwość cytowania na poziomie pracy z edytorem tekstu i współpraca z edytorami MS Word, Mac Word, WordPerfect i Open.Office Writer.
8. Opcja poszukiwania pełnego tekstu publikacji dla odszukanej referencji.
9. Możliwość definiowania załączników do rekordów referencyjnych w formie plików w lokalnej sieci lub dostępnych via Internet.
10. Przeszukiwanie bazy, z możliwością szukania w plikach pdf załączonych do referencji i tworzenie referencji z plików pdf.
11. Możliwość dodawania do bazy i cytowania referencji typu "Online Database", "Online Multimedia", "Figure", "Equation", "ElectronicBook", "Blog" oraz możliwość definiowania rodzaju referencji przez użytkownika.
12. Zdefiniowane strategie wyszukiwania mogą być zapamiętane i wykorzystane w przyszłości.

**Ad. 2) Origin Lab Pro – 1 licencja**

**Program do analizy i wizualizacji danych o następujących możliwościach:**

1. Obszerny zestaw rodzajów tworzonych wykresów dla prezentacji 2D i 3D z możliwością tworzenia map izolinii w układzie kartezjańskim i biegunowym, wykresów z wielokrotnymi

osiami Y, mechanizmem przerywania osi X oraz procedurą zarządzania biblioteką szablonów wykresów.

2. Analiza statystyczna danych obejmująca między innymi wyznaczanie statystyk opisowych, testowanie hipotez, ANOVA (również w wersji "repeatedmeasures"), test nieparametryczne, analiza przeżywalności i krzywe ROC.

3. Analiza danych obejmująca: interpolacje i ekstrapolacje 2D i 3D, różniczkowanie, całkowanie.

4. Liniowe i nieliniowe dopasowanie krzywych z szerokim zestawem wbudowanych modeli, możliwością definiowania własnych funkcji dopasowania oraz modułem zarządzania zestawem wzorców funkcji dopasowania

5. Procedury dopasowania pików w opcji "single peakfit" i "multiplepeakfit".

6. Procedury z grupy "signalprocessing" (między innymi wygładzanie danych, filtracja FFT, transformacja FFT, przekształcenie falkowe - wavelets, transformacja Hilberta, korelacja) i "image processing" (między innymi regulowanie parametrów obrazu, transformacje aytmetyczne włącznie z filtrami morfologicznymi, konwersje obrazu, transformacje geomertyczne, filtry uśredniające i wyostrzające, detekcja krawędzi).

7. Bezpośredni import danych z przyrządów laboratoryjnych poprzez pliki ASCII z możliwością definiowania filtrów importu.

8. Definiowanie szablonów wykresów, arkuszy danych, procedur importu danych, procedur analizy danych.

9. Definiowanie wariantów wizualizacji jako środek do szybkiej zmiany formatu rysunku np. zmiana z prezentacji kolorowej na prezentację w odcieniach szarości, podmiana kroju pisma we wszystkich tekstach na rysunku, itp.

10. Dopisywanie procedur w języku skryptowym i w języku C z obszerną biblioteka procedur numerycznych z zakresu algebry liniowej i funkcji specjalnych.

11. Możliwość czytania plików i współpracy z LabView, MATLAB i Mathematica.

12. Dodatkowe procedury

13. Krótkoczasowa transformata Fourier'a STFT (Short Time Fourier Transform)

14. Transformacja Hilberta

15. Transformacja 2D oraz filtry bazujące na tej transformacji, korelacja 2D oraz przekszatałcenie falkowe(Wavelets).

16. Analiza i przetwarzanie obrazów(Image Analysis and Processing)

**Ad. 3) Statistica plus Zestaw Medyczny – 1 licencja**

Cechy użytkowe oprogramowania:

- Polskojęzyczne środowisko pracy w programie;
- Wersja jednostanowiskowa, działająca lokalnie na jednym komputerze (bez pracy zdalnej)
- Egzemplarz oprogramowania z licencją producenta, bez ograniczenia w czasie
- Pomoc techniczna do aktualnych wersji oprogramowania musi być świadczona przez polskie biuro producenta oprogramowania w języku polskim (za pośrednictwem poczty elektronicznej i telefonicznie w godzinach pracy biura producenta)
- Do instalowanego oprogramowania musi być dołączona pomoc elektroniczna zawierająca opisy poszczególnych modułów i opcji oprogramowania

Środowisko pracy z programem i korzystanie z zewnętrznych danych

- Dane powinny być składowane w arkuszu danych umożliwiającym interakcyjne wprowadzanie i przekształcanie danych (sortowanie, transformacje zmiennych, ułóż w stertę/rozrzuć po zmiennych) oraz import i eksport danych (m.in. z plików Excel i plików tekstowych).
- Oprogramowanie musi mieć możliwość łączenia z bazami danych przez OLE DB lub ODBC.
- Wczytywanie i zapis danych w formacie Excel (.xls i .xlsx), tekstowym, html.
- Wczytywanie i zapis plików danych w formatach: STATISTICA, SPSS, SAS, JMP, Minitab
- Oprogramowanie musi zawierać wbudowany, zgodny ze standardami język programowania Visual Basic, który umożliwia dostęp programowy do funkcji programu, programowanie własnych procedur analitycznych oraz automatyzację prac.
- Dostęp do aplikacji poprzez interfejs COM.
- Oprogramowanie musi działać na stanowisku komputerowym pod kontrolą systemu operacyjnego Windows XP/Vista/7/8 lub ich odpowiednikach serwerowych.
- Możliwość instalacji wersji dedykowanej pod 32- lub 64- bitowy system Windows.

Zarządzanie wynikami

- Oprogramowanie musi zapewniać możliwość tworzenia raportów z analizy, z możliwością zapisania w formacie PDF.
- Przesyłanie wyników (tabel, wykresów) do dokumentów edytora tekstowego (np. MsWord).
- Raport otrzymywany przy pomocy oprogramowania powinien przypominać dokument edytora tekstu, a poszczególne obiekty (np. wykresy, arkusze, arkusz czy wykres MS Excel) umieszczane są w nim kolejno, jeden za drugim.
- Oprogramowanie powinno pozwalać na zapis dokumentów (arkuszy danych i wyników, raporty) w postaci plików HTML, gotowych do opublikowania w Internecie lub Intranecie.
- Możliwość aktualizacji utworzonych wykresów po zmianie danych źródłowych (automatycznie lub „ręcznie" przez użytkownika)
- Możliwość edycji wykresów po ich wstawieniu do dokumentu edytora tekstowego (tzn. wykresy mogą być wstawiane jako obiekty OLE)

Wymagana funkcjonalność oprogramowania:

Oprogramowanie powinno udostępniać w jednym środowisku użytkownika następujące funkcje analityczne:

- Statystyki podstawowe i tabele
- Dopasowanie rozkładów
- Regresja wieloraka
- Analiza wariancji (ANOVA)
- Statystyki nieparametryczne
- Ogólne modele liniowe
- Uogólnione modele liniowe i nieliniowe
- Ogólne modele regresji
- Modele cząstkowych najmniejszych kwadratów
- Komponenty wariancyjne
- Analiza przeżycia

- Estymacja nieliniowa
- Linearyzowana regresja nieliniowa
- Analiza log-liniowa tabel liczności
- Szeregi czasowe i prognozowanie
- Modelowanie równań strukturalnych
- Analiza skupień
- Analiza czynnikowa
- Składowe główne i klasyfikacja
- Algorytm NIPALS dla analizy składowych głównych i metody cząstkowych najmniejszych kwadratów
- Analiza kanoniczna
- Analiza rzetelności i pozycji
- Drzewa klasyfikacyjne
- Analiza korespondencji
- Skalowanie wielowymiarowe
- Analiza dyskryminacyjna
- Ogólne modele analizy dyskryminacyjnej
- Analiza mocy testów
- Kreator regresji logistycznej
- Metaanaliza i metaregresja
- Test post hoc ANOVA Friedmana
- Krzywe ROC
- Miary powiązania/efektów dla tabel 2x2
- Definiowanie reguł poprawności danych
- Analiza brakujących danych
- Przekodowanie na zmienne sztuczne

- Wykres Blanda-Altmana

**Ad 4)** Program do analizy, adnotacji i ilustracji cząsteczek DNA, RNA, białek- **VectorNTI Express** lub równoważny– **1 licencja**

**Ad 5) Pakiet biurowy Microsoft Office 2010 Professional lub nowszy – 14 licencja**

**Ad 6) Oprogramowanie antywirusowe – 20 licencji typu desktop, 1 licencja serwerowa, 1 licencja dla aplikacji zarządzającej**

1. Pełne wsparcie dla systemu Windows 2000/XP/Vista/Windows 7/Windows 8.
2. Wsparcie dla Windows Security Center (Windows XP SP2).
3. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
4. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.
5. Pomoc w programie (help) i dokumentacja do programu w języku polskim.
6. Skuteczność programu potwierdzona nagrodami VB100 i co najmniej dwie inne niezależne organizacje takie jak ICSA labs lub Check Mark.

**Ochrona antywirusowa i antyspyware**

7. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
8. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
9. Wbudowana technologia do ochrony przed rootkitami.
10. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
11. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
12. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
13. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
14. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.

15. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
16. Możliwość skanowania dysków sieciowych i dysków przenośnych.
17. Skanowanie plików spakowanych i skompresowanych.
18. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).
19. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
20. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
21. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
22. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
23. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
24. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
25. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
26. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird do wersji 5.x i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).
27. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird do wersji 5.x i Windows Live Mail.
28. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
29. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
30. Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.

31. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.

32. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.

33. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.

34. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.

35. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.

36. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.

37. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

38. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.

39. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.

40. Aplikacja musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.

41. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.

42. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.

43. W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.

44. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.

45. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.

46. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.

47. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.

48. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

49. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

50. Interfejs programu ma oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.

51. Interfejs programu ma mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb wysokiego kontrastu.

52. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.

53. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.

54. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji musi być takie samo.

55. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.

56. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.

57. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.

58. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.

59. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.

60. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych

61. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.

62. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.

63. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.

64. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.

65. Użytkownik ma posiadać możliwość takiej konfiguracji aplikacji aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika

66. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).

67. Moduł HIPS musi posiadać możliwość pracy w jednym z czterech trybów:

    - tryb automatyczny z regułami gdzie aplikacja automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to aplikacja pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym aplikacja uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu aplikacja musi samoczynnie przełączyć się w tryb pracy oparty na regułach.

68. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.

69. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.

70. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.

71. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.

72. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.

73. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.

74. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.

75. Aplikacja musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.

76. Aplikacja musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http

77. Aplikacja musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).

78. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).

79. Aplikacja musi być w pełni zgodna z technologią Network Access Protection (NAP).

80. Program ma być w pełni zgodny z technologią CISCO Network Access Control (NAC).

81. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.

82. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.

83. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie aplikacja włączała powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.

84. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.

85. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

**Stacje Robocze Apple Mac OS X**

1. Procesor 32-bit (x86) / 64-bit (x64), Intel®.
2. Pełnewsparciedlasystemów Mac OS X 10.5.x (Leopard), Mac OS X 10.6.x (Snow Leopard) oraz Mac OS X 10.7.x (Lion) Mac OS X 10.8 (Mountain Lion )
3. Wersja programu dostępna zarówno w języku polskim jak i angielskim.
4. Pomoc w programie (help) w języku polskim.
5. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
6. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
7. Wbudowana technologia do ochrony przed rootkitami.
8. Skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
9. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
10. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności).
11. Możliwość skanowania dysków sieciowych i dysków przenośnych.
12. Skanowanie plików spakowanych i skompresowanych.
13. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
14. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.

15. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.

16. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.

17. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.

18. Możliwość wykonania skanowania z poziomu menu kontekstowego.

19. Aktualizacje modułów analizy heurystycznej.

20. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie mają być wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.

21. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.

22. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

23. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

24. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD oraz portów USB.

25. Funkcja blokowania nośników wymiennych ma umożliwiać wyłączenie dostępu do nośników : Napęd CD-Rom, Dyskietka, Firewire, USB, HotPlug, Inne.

26. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.

27. Aktualizacja systemu antywirusowego ma być dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).

28. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.

29. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po wystąpieniu zdarzenia).
30. Program umożliwia automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego.
31. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
32. Praca programu musi być niezauważalna dla użytkownika.
33. Program ma umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień.
34. Program ma posiadać dwie wersje interfejsu (standardowy – z ukrytą częścią ustawień oraz zaawansowany – z widocznymi wszystkimi opcjami).
35. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania oraz dokonanym skanowaniem komputera.
36. Program ma umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy" na modyfikację konfiguracji programu.
37. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
38. Możliwość zdalnego zarządzania programem z poziomu Administracji zdalnej. Program ma umożliwiać zdefiniowanie głównego i pomocniczego serwera administracji zdalnej.

**Stacje robocze Linux**

1. Wymagania systemowe: procesor 32-bit (x86) / 64-bit (x64), AMD®, Intel®.
2. Minimum 150MB wolnej pamięci RAM.
3. Minimum 120MB miejsca na dysku.
4. Pełne wsparcie dla dystrybucji opartych na systemach Debian i RedHat (Ubuntu, OpenSuse, Fedora, Mandriva, RedHat). Dodatkowe wymagania systemowe :
    a. Kernel 2.6.x
    b. Biblioteki GNU C w wersji 2.3 lub nowszej
    c. GTK+ 2.6 w wersji nowszej
    d. Zalecana kompatybilność z LSB 3.1

5. Wsparcie dla dystrybucji 32- i 64-bitowych.
6. Wersja programu dostępna zarówno w języku polskim jak i angielskim.
7. Pomoc w programie (help) w języku polskim.
8. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
9. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
10. Wbudowana technologia do ochrony przed rootkitami.
11. Skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
12. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
13. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności).
14. Możliwość skanowania dysków sieciowych i dysków przenośnych.
15. Skanowanie plików spakowanych i skompresowanych.
16. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
17. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
18. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
19. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
20. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
21. Możliwość wykonania skanowania z poziomu menu kontekstowego.
22. Aktualizacje modułów analizy heurystycznej.

23. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.

24. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.

25. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

26. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

27. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD oraz portów USB.

28. Funkcja blokowania nośników wymiennych ma umożliwiać wyłączenie dostępu do nośników : Napęd CD-Rom, Dyskietka, Firewire, USB, HotPlug, Inne.

29. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.

30. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.

31. Aktualizacja systemu antywirusowego ma być dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).

32. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.

33. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po wystąpieniu zdarzenia).

34. Program umożliwia automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego.

35. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

36. Praca programu musi być niezauważalna dla użytkownika.

37. Program ma umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień.

38. Program ma posiadać dwie wersje interfejsu (standardowy – z ukrytą częścią ustawień oraz zaawansowany – z widocznymi wszystkimi opcjami).

39. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania oraz dokonanym skanowaniem komputera.

40. Program ma umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy" na modyfikację konfiguracji programu.

41. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

42. Możliwość zdalnego zarządzania programem z poziomu Administracji zdalnej. Program ma umożliwiać zdefiniowanie głównego i pomocniczego serwera administracji zdalnej.

**Ochrona serwera plików Linux**

1. Skaner antywirusowy, antyspyware

2. Możliwość skanowania wszystkimi modułami programu (heurystyka, sygnatury, adware/spyware, aplikacje niepożądane, aplikacje niebezpieczne )

3. Skanowanie plików, plików spakowanych, archiwów samorozpakowujących, plików wiadomości e-mail

4. Konfiguracja wszystkich modułów oprogramowania ma być możliwa poprzez edycję jednego pliku konfiguracyjnego

5. Możliwość ustawień limitów dla modułu skanującego względem maksymalnego rozmiaru pliku, maksymalnej liczby warstw kompresji, maksymalnego rozmiaru archiwum, maksymalnego czasu skanowania, maksymalnego rozmiaru archiwum samorozpakowującego, rozszerzenia skanowanego pliku

6. Możliwość skanowania podkatalogów oraz podążania za łączami symbolicznymi (symlinkami) w systemie

7. Możliwość definicji maksymalnego poziomu głębokości skanowanych podkatalogów

8. Możliwość tworzenia kwarantanny dla plików zainfekowanych w dowolnej lokalizacji w systemie plików

9. Możliwość zdefiniowania częstotliwości aktualizacji programu z dokładnością do jednej minuty.

10. Brak potrzeby instalacji dodatkowych zależności do systemu oprócz biblioteki LIBC, oprogramowanie po instalacji jest od razu gotowe do pracy
11. Wbudowany bezpośrednio w program system obsługi plików spakowanych niewymagający zewnętrznych komponentów zainstalowanych w systemie
12. Brak potrzeby instalacji źródeł jądra systemu oraz kompilacji jakichkolwiek modułów jądra do skanowania plików na żądanie
13. Możliwość tworzenia przynajmniej pięciu poziomów dokładności czyszczenia zainfekowanych plików
14. Możliwość skanowania alternatywnych strumieni danych ( ADS ) obecnych w systemie plików NTFS
15. Wsparcie dla integracji oprogramowania z modułem Dazuko Access Controll ( DAC ) który odpowiada za skanowania plików w trybie on-access podczas zdarzeń typu otwarcie, zamknięcie oraz wykonanie pliku
16. Wsparcie dla skanowania za pośrednictwem biblioteki współdzielonej LIBC, która umożliwia skanowanie plików które są otwierane, zamykane lub wykonywane przez serwery plików (ftp, Samba ) które wykorzystują zapytania do biblioteki LIBC
17. Możliwość zdefiniowania liczby wątków oraz liczby procesów dla każdego z modułów skanujących
18. Możliwość tworzenia różnych akcji (przynajmniej 5-ciu różnych) w zależności od typu zdarzenia (w przypadku pliku nie przeskanowanego, pliku przeskanowanego, pliku zainfekowanego ).
19. Logowanie wykonanych akcji na plikach oraz zdarzeń dla poszczególnych modułów oprogramowania
20. Wsparcie dla zewnętrznego serwera logującgosyslog, możliwość definiowania dowolnego pliku logu ( np. daemon, mail, user itp. )
21. Możliwość zdefiniowania przynajmniej sześciu poziomów logowania programu
22. Możliwość zdalnego zarządzania z wykorzystaniem serwera zdalnego zarządzania instalowanego na systemach Windows 8, 7, Vista, XP, 2000; Windows Server 2012, 2008 R2, 2008, 2003, 2000
23. Możliwość łatwej konfiguracji produktu za pomocą prostej w użyciu konsoli administracyjnej spod systemów Windows 8, 7, Vista, XP, 2000; Windows Server 2012, 2008 R2, 2008, 2003, 2000

24. Możliwość zdefiniowania hasła zabezpieczającego służącego zabezpieczeniu podłączenia do serwera zdalnego zarządzania
25. Możliwość uruchomienia interfejsu programu dostępnego przez przeglądarkę Web
26. Interfejs ma umożliwiać modyfikację ustawień programu oraz jego aktualizację i przeskanowanie dowolnego obszaru systemu plików a także przegląd statystyk dotychczas przeskanowanych plików
27. Interfejs programu dostępny przez przeglądarkę Web wykorzystuje wbudowany w program serwer http
28. Możliwość uruchomienia interfejsu Web na dowolnym porcie TCP
29. Możliwość uruchomienia interfejsu Web na dowolnym interfejsie sieciowym
30. Możliwość zabezpieczenia dostępu do interfejsu Web poprzez zdefiniowanie nazwy użytkownika i hasła
31. Interfejs Web ma przedstawić administratorowi dokładny wynik skanowania poszczególnych plików w systemie wraz z możliwością pobrania tych wyników w postaci pliku tekstowego celem późniejszej analizy
32. Możliwość podglądu informacji o licencji bezpośrednio z poziomu interfejsu Web która zawiera przynajmniej informacje o liczbie dni do wygaśnięcia licencji, nazwę użytkownika licencji oraz pełną nazwę produktu którego dotyczy licencja
33. Program ma być wyposażony w graficzny menadżer kwarantanny dostępny z poziomu interfejsu Web. Menadżer ma oferować administratorowi możliwość przeglądu, pobrania, dodania i usunięcia plików w kwarantannie
34. Menadżer kwarantanny ma posiadać możliwość wyszukiwania plików znajdujących się w kwarantannie przynajmniej po nazwie pliku, dacie dodania pliku (możliwość definiowania przedziałów czasowych), rozmiarze (możliwość definiowania minimalnej i maksymalnej wielkości) oraz ilości plików (możliwość definiowania minimalnej i maksymalnej ilości)
35. Interfejs Web do zarządzania produktem ma opierać się o wbudowane w program biblioteki PHP w wersji nie niższej niż 5.2.8
36. Interfejs dostępny poprzez przeglądarkę Web ma umożliwiać zarządzanie programem również wtedy, gdy przeglądarka nie obsługuje kodu JavaScript
37. Możliwość stworzenia lokalnego repozytorium aktualizacji dla przynajmniej dwóch różnych produktów antywirusowych instalowanych na stacjach Windows
38. Możliwość tworzenia osobnych ustawień skanowania dla poszczególnych użytkowników w systemie

39. Możliwość definicji użytkownika systemowego z prawami którego zostanie uruchomiony demon skanujący

40. Współpraca z mechanizmem automatycznej wysyłki podejrzanych plików do laboratorium producenta

41. Wysyłka podejrzanych plików ma być możliwa bezpośrednio do producenta lub za pośrednictwem serwera zdalnego zarządzania

42. Możliwość uaktywnienia dodatkowych funkcjonalności programu (moduł skanujący pocztę e-mail oraz moduł skanujący dla bramek sieciowych) które nie wymagają od użytkownika instalacji dodatkowych zależności ani modułów a jedynie zaczytanie dodatkowych plików licencji

43. Możliwość instalacji na dowolnym systemie Linux 2.2.x, 2.4.x, 2.6.x

44. Producent ma dostarczyć pakiety instalacyjne w formacie RPM (dla dystrybucji Red HatMandriva, Suse oraz innych z nimi zgodnych), DEB (dla dystrybucji Debian, Ubuntu oraz innych z nimi zgodnych) oraz archiwum TGZ dla wszystkich pozostałych

45. Możliwość instalacji na systemie FreeBSD 5.x, 6.x i 7.x

46. Możliwość instalacji na systemach NetBSD oraz Solaris

47. Wsparcie dla platform 32 oraz 64 bitowych

48. Architektura programu umożliwia jego uruchomienie i optymalizację zarówno dla systemów jedno jak i wieloprocesorowych

49. System ma mieć możliwość powiadomienia administratora o wykryciu infekcji oraz powiadomienia o zbliżającym się terminie wygaśnięcia licencji za pośrednictwem poczty e-mail.

50. Możliwość szybkiej konfiguracji oprogramowania poprzez skrypt powłoki. Skrypt umożliwia prostą konfigurację oprogramowania stosownie do wykrytego systemu operacyjnego w jakim oprogramowanie zostało zainstalowane.

51. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

**Ochrona serwera plików Windows**

1. Wsparciedlasystemów: Microsoft Windows Server 2000, 2003 (32 oraz 64 bit), 2008 (32 oraz 64 bit), 2008 R2, 2012, Microsoft Windows Small Business Server 2003, 2003 R2, 2008, 2011.

2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
4. Wbudowana technologia do ochrony przed rootkitami.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
10. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
11. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
12. Możliwość skanowania dysków sieciowych i dysków przenośnych.
13. Skanowanie plików spakowanych i skompresowanych.
14. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (z uwzględnieniem plików bez rozszerzeń).
15. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
16. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
17. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
18. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
19. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
20. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.

21. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
22. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
23. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (commandline).
24. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
25. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
26. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
27. Aktualizacje modułów analizy heurystycznej.
28. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie mają być wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
29. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
30. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
31. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
32. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
33. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.

34. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e mail.

35. Interfejs programu ma oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.

36. Interfejs programu ma mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb wysokiego kontrastu.

37. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.

38. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.

39. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.

40. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.

41. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.

42. System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie, ma także istnieć opcja dezaktywacji tego mechanizmu.

43. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.

44. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.

45. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.

46. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD oraz portów USB.

47. Funkcja blokowania portów USB ma umożliwiać administratorowi zdefiniowanie listy portów USB w komputerze, które nie będą blokowane (wyjątki).

48. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.

49. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.

50. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.

51. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.

52. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).

53. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.

54. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).

55. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu.

56. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

57. Praca programu musi być niezauważalna dla użytkownika.

58. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.

59. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

**Ad 7) Oprogramowanie do backupu**

Rozwiązanie powinno składać się z modułów służących do tworzenia kopii zapasowych, replikacji i monitorowania raportowania środowisk wirtualnych.

**Moduł do tworzenia kopii zapasowych i replikacji**

- Oprogramowanie do archiwizacji powinno współpracować z infrastrukturą wirtualizacji opartą na VMware ESX oraz ESXi w wersjach 3.5, 4.0, 4.1, 5 oraz 5, jak również Hyper-V 2008 R2 i Hyper-V 2012 (w tym obsługa formatu dysków wirtualnych *.vhdx)
- Rozwiązanie powinno współpracować z hostami ESX i ESXi zarządzanymi przez VMwarevCenter jak i hostami nie zarządzanymi (standalone)
- Rozwiązanie powinno współpracować z hostami Hyper-V zarządzanymi przez System Center Virtual Machine Manager, zgrupowanymi w klastry jak i nie zarządzanymi (standalone)
- Rozwiązanie nie może instalować żadnych swoich komponentów (agent) w archiwizowanych maszynach wirtualnych.
- Rozwiązanie musi wspierać backup wszystkich systemów operacyjnych w wirtualnych maszynach, które są wspierane przez VMware i Hyper-V
- Rozwiązanie powinno mieć możliwość instalacji na następujących systemach operacyjnych zarówno w wersji 32 jak i 64 bitowej:
    - Microsoft Windows XP SP3
    - Microsoft Windows Server 2003 SP2
    - Microsoft Windows Vista SP2
    - Microsoft Windows Server 2008 SP2
    - Microsoft Windows Server 2008 R2
    - Microsoft Windows 7 SP1
    - Windows Server 2012
    - Windows 8
- Rozwiązanie powinno dawać możliwość odzyskiwania całych obrazów maszyn wirtualnych z obrazów, pojedynczych plików z systemu plików znajdujących się wewnątrz wirtualnej maszyny. Rozwiązanie musi umożliwiać odzyskanie plików na zasadzie „one-clickrestore”. Rozwiązanie musi umożliwiać odzyskiwanie plików z następujących systemów plików:
    - Linux - ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS
    - Unix - JFS, XFS, UFS
    - BSD - UFS, UFS2

- Solaris - UFS, ZFS
- Mac - HFS, HFS+
- Windows - NTFS, FAT, FAT32

- Rozwiązanie powinno umożliwiać natychmiastowe odzyskanie wirtualnej maszyny i jej uruchomienie bez kopiowania na storage podłączony do hostów. Taka sama funkcjonalność powinna być zapewniona dla środowiska Hyper-V
- Rozwiązanie powinno umożliwiać odzyskiwanie bezpośrednie odzyskiwanie obiektów z takich usług jak Active Directory (użytkownicy i grupy), Microsoft SQL (tabele i rekordy) z maszyn wirtualnych środowiska VMware
- Rozwiązanie musi zapewniać szybkie odzyskiwanie danych ze skrzynek pocztowych Microsoft Exchange 2010 bez potrzeby uruchamiania maszyny wirtualnej (odzyskiwanie bezpośrednio z bazy danych *.EDB) dla środowisk VMware i Hyper-V
- Rozwiązanie powinno umożliwiać indeksowanie plików zawartych w archiwach maszyn wirtualnych z systemem operacyjnym Windows w celu szybkiego ich przeszukiwania
- Rozwiązanie powinno w pełni korzystać z mechanizmów zawartych w VMwarevStorage API for Data Protection a w szczególności być zgodnym z mechanizmem Changed Block Tracking
- Rozwiązanie powinno mieć wbudowane mechanizmy podobne do technologii CBT również dla platformy Hyper-V w celu przyśpieszenia procesu backupu.
- Rozwiązanie powinno korzystać z mechanizmów VSS (Windows Volume Shadowcopy) wbudowanych w najnowsze systemy operacyjne z rodziny Windows.
- Rozwiązanie powinno mieć wbudowane mechanizmy deduplikacji i kompresji archiwum w celu redukcji zajmowanej przez archiwa przestrzeni dyskowej
- Rozwiązanie powinno mieć możliwość instalacji centralnej konsoli do zarządzania większą ilością serwerów archiwizujących oraz jednoczesnego zarządzania backupami środowiska VMware i Hyper-V
- Dostęp do tej konsoli powinien być realizowany przez przeglądarkę WWW
- Rozwiązanie powinno mieć wbudowany mechanizm informowania o pomyślnym lub niepomyślnym zakończeniu procesu archiwizacji poprzez email, zapis do EventLog'u Windows lub wysłanie komunikatu SNMP.
- Rozwiązanie powinno mieć możliwość rozbudowy procesu archiwizacji o dowolne skrypty tworzone przez administratora i dołączane do zadań archiwizacyjnych

- Rozwiązanie powinno mieć wbudowaną możliwość replikacji wirtualnych maszyn pomiędzy hostami ESX i ESXi oraz w tym możliwość replikacji ciągłej
- Rozwiązanie powinno mieć wbudowaną możliwość replikacji maszyn wirtualnych pomiędzy hostami Hyper-V
- Rozwiązanie powinno mieć możliwość tworzenia środowiska wirtualnego laboratorium w środowisku VMware
- Rozwiązanie powinno mieć możliwość występowania i zatwierdzania wniosków o tworzenie środowisk w wirtualnym laboratorium w środowisku VMware
- Rozwiązanie powinno zapewnić możliwość sprawdzenia poprawności wykonania archiwum poprzez odtworzenie wirtualnej maszyny w izolowanym środowisku i jej uruchomienie w środowisku VMware.
- Rozwiązanie powinno być zgodne z konfiguracją rozproszonego przełącznika VMware (Distributed Virtual Switch)
- Rozwiązanie powinno mieć możliwość automatycznej zmiany numeracji IP maszyn przywracanych w środowiskach centrum zapasowego w przypadku awarii centrum podstawowego
- Rozwiązanie powinno mieć możliwość integracji z macierzami HP Lefthand i oprogramowanie HP StoreVirtual. Rozwiązanie musi umożliwiać odzyskiwanie wirtualnych maszyn, plików z tych maszyn i uruchamianie maszyn bezpośrednio z migawki wykonanej przez rozwiązanie HP (tzw. SAN Snapshot)
- Rozwiązanie musi umożliwiać zapisanie konfiguracji całej instalacji w celu przywrócenia jej po reinstalacji całego systemu.

**Moduł do monitorowania i raportowania**

- System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMwarevSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnegoVMware w wersji 5.x, 4.x oraz 3.x – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2.0 oraz 3.0 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Server

- System musi mieć możliwość instalacji na systemach operacyjnych w wersjach 32 i 64 bitowych:
    - Microsoft Windows XP SP3
    - Microsoft Windows 2003 SP2
    - Microsoft Windows Vista SP2
    - Microsoft Windows 2008 SP2
    - Microsoft Windows 2008 R2 SP1
    - Microsoft Windows 7 SP1
    - Microsoft Windows 8
    - Microsoft Windows 2012
- System musi obsługiwać następujące bazy danych w wersjach 32 i 64 bitowych:
    - Microsoft SQL Server 2005
    - Microsoft SQL Server 2008
    - Microsoft SQL Server 2008 R2
    - Microsoft SQL Server 2012
- System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
- System musi umożliwiać integrację tak utworzonej hierarchii z zewnętrznymi bazami CMDB
- System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
- System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
- System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
- Silnik raportowania powinien być oparty o SQL Server Reporting Services w celu zapewnienia bezpiecznego dostępu do raportów dla wielu użytkowników z uwzględnieniem ról, jakie pełnią w organizacji

- System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
- System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
- System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
- System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
- System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
- System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
- System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
- System do prezentacji raportów powinien używać SQL Server Reporting Services w celu jednoczesnego dostępu do raportów wielu użytkowników z określonymi przez administrator systemu uprawnieniami.
- System powinien być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
- System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
- System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
- System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
- Minimalny interwał czasowy dla zadań kolekcjonowania i raportowania musi wynosić min 1 godzinę
- System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów

- System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
- System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
- System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
- System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
- System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn wirtualnych, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
- System musi mieć możliwość generowania raportu planowania pojemności (capacityplanning) bazującego na scenariuszach 'what-if".

**Ad 8) Oprogramowanie do systemu zarządzania pracą biobanku**

System zarządzania biobankiem ma za zadanie zbierać, przechowywać w bazie danych oraz przetwarzać wszelkie informacje konieczne do pracy biobanku. Oprogramowanie serwerowe i klienckie ma pracować na systemach operacyjnych Microsoft Windows w oparciu o otwartą bazę danych (Open Source). Wymaga się desktopowej aplikacji klienckiej – samodzielnej aplikacji nie wymagającej przeglądarki internetowej. Dostarczone oprogramowanie ma być z licencją serwerową, na nielimitowaną liczbę stanowisk klienckich. Ponadto Zamawiający żąda przekazania kodu źródłowego wraz z dokumentacją techniczną pozwalającą na dokonywanie zmian w systemie. Wykonawca zobowiąże się do świadczenia wsparcia technicznego w zakresie wprowadzania stosownych zmian w oprogramowaniu na życzenie zamawiającego przez okres 12 miesięcy.

Wykonawca wraz z dostawą przekaże autorskie prawa majątkowe do dostarczonego oprogramowania umożliwiające instalację oprogramowania również w innych instytucjach. System zarządzania biobankiem ma być skalowalny, intuicyjny dla użytkownika oraz zawierać następujące moduły:

- Moduł ewidencjonowania pacjentów
- Moduł wprowadzania wyników badań
- Moduł wyszukiwania próbek
- Moduł zamawiania próbek natychmiast
- Moduł zamawiania próbek wg harmonogramu
- Moduł monitorowania warunków środowiskowych

- Moduł monitorowania lodówek i zamrażarek
- Moduł integracji czytników kodów, skanerów płaskich oraz drukarek
- Zarządzanie zasobami ludzkimi
- Zarządzanie zasobami sprzętowymi
- Zarządzanie magazynem odczynników
- Moduł raportowania
- Moduł komunikacji z robotami
- Moduł integracji z aparaturą badawczą
    - Stacje pipetujące
    - Decappery
    - Real time PCR
    - Czytnik płytek
    - DHPLC
    - Systemy dokumentacji żeli
    - Analizator immunochemiczny
    - Analizator biochemiczny
    - System analiz autoimmunologicznych
- Moduł udostępniania danych statystycznych

System ma zwierać następujące funkcjonalności:

- Obsługa skanerów kodów 1D oraz 2D
- Zapewnić swobodę modyfikacji i usuwania danych, jednak dane dotychczasowe muszą pozostać w bazie jako ukryte.
- Możliwość usunięcia danych pacjenta oraz jego próbek
- Zapewnić pełną rozliczalność i zapisywać wszystkie informacje o pracy użytkowników w systemie.
- Sporządzanie i dołączanie protokołów pobrania próbki
- Rejestrowanie próbek w oparciu o zarejestrowane zlecenia
- Pełna identyfikowalność próbek
- Gromadzenie danych o biobankowanych próbkach

- Raportowanie pracy urządzeń
- Raportowanie badań
- Raportowanie biobankowanych próbek
- Stała kontrola dostępnych zasobów wraz z terminami ważności
- Ostrzeżenia o wyczerpywaniu się zapasów oraz generowanie druków zapotrzebowania
- Pełna historia zasobów magazynowych
- Generowanie i drukowanie etykiet dla poszczególnych materiałów
- Zarządzanie lokalizacją próbek – przenoszenie próbki między lokalizacjami
- Możliwość skanowania dokumentów on-line i przechowywania ich w bazie danych
- Przypisywanie dokumentów do pacjentów, badań, zasobów, materiałów i sprzętu
- Samodzielne dodawanie do systemu nowych odczynników i innych materiałów
- Kartoteka przyjęć i wydań z magazynu
- Wyszukiwanie próbek wg definiowanych przez użytkownika filtrów
- Możliwość zamawiania wyszukanych próbek zarówno natychmiast jak i na daną godzinę
- Możliwość zapisania wyników wyszukiwania
- Możliwość zmiany miejsca dostarczenia próbek
- Graficzny sposób wskazywania miejsca dostarczania próbek (moduł mapy)

**Moduł udostępniania danych statystycznych**

Moduł udostępniania danych służy do przekazywania zanonimizowanych danych statystycznych podmiotom trzecim. Na podstawie wybranych przez klienta filtrów system wyszukuje rekordy w bazie danych oraz zwraca ilość wyszukanych rekordów. Wartość ta jest przekazywana do klienta, może on w tym momencie dokonać zakupu wybranej ilości rekordów. Po zaakceptowaniu i opłaceniu zamówienia klient otrzymuje zanonimizowane dane statystyczne w oparciu o własny filtr. Wyszukiwanie danych będzie możliwe po uprzednim zalogowaniu się klienta do panelu www i wybraniu odpowiednich filtrów. W systemie należy uwzględnić system bilingowy, w którym klient będzie mógł przeglądać historię swoich transakcji. Aplikacja ma zawierać moduł raportowania, służący do generowania wyników sprzedaży, najczęściej wybieranych filtrów itp. Cały system ma opierać się o dwie aplikacje – część dostępną dla klienta za pomocą panelu www, oraz część dostępną wyłącznie dla inwestora, pozostającą w odrębnej sieci intranet, odizolowanej od internetu za pomocą serwera proxy. Aplikacja zewnętrzna może jedynie wysyłać zapytania o rekordy do

aplikacji wewnętrzej. Aplikacja wewnętrzna pobiera rekordy z bazy danych na podstawie wybranych filtrów, anonimizuje je i przesyła do bazy danych aplikacji zewnętrznej. Droga taka zapobiega wyciekowi newralgicznych danych. Do pracy w systemie wymagane jest zdefiniowanie użytkowników, haseł i poziomów dostępu. Użytkownicy podzieleni są na 3 grupy: Super Administrator, Administratorzy i Użytkownicy. Stosownie do poziomu użytkownika ładowane jest inne menu Systemu. Uprawnienia mają być każdorazowo sprawdzane również w trakcie otwierania każdej części systemu. Super Administrator ma uprawnienia do wszystkich części Sytemu, w tym do sekcji Administratora. W tej części Systemu można: zarządzać użytkownikami, zarządzać tabelami, mieć wgląd w aktualnie zalogowanych użytkowników i przeglądać logi Systemu. W zarządzaniu użytkownikami należy przewidzieć możliwość dodawania, edycji i usuwania wszystkich użytkowników w Systemie. W zarządzaniu tabelami danych należy przewidzieć możliwość dodawania dodatkowych pól danych w tabelach. Każde dodane dodatkowo pole ma być edytowalne (nazwa, opis, typ pola, widoczność). Należy również przewidzieć możliwość jego usunięcia. Log systemu ma pokazywać w chronologicznym porządku zapis wszystkich działań poszczególnych użytkowników Systemu.