Numer sprawy **6/2017 Załącznik Nr 1 do SIWZ**

**Szczegółowy opis przedmiotu zamówienia**

**Część I zamówienia – Zakup urządzeń wielofunkcyjnych – 2 szt.**

**A) Urządzenie wielofunkcyjne (duże) – 1 szt.**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/producent/nazwa | Urządzenie wielofunkcyjne |  |
|  | Prędkość kopiowania w czerni i kolorze | 25 str./min. A4, 15 str./min. A3 |  |
|  | Technologia powielania | kolorowa, cyfrowa, laser/led |  |
|  | Panel dotykowy | min. 22,8 cm (9") dotykowy LCD z możliwością personalizacji realizowanej przez urządzenie bez użycia aplikacji zewnętrznych. Personalizacja polegająca na zmianie tła pulpitu, ikon, kolorów, wyciąganiu skrótów funkcji na panel główny |  |
|  | Format oryginału i kopii | A5R-A3; 52-280 g/m² |  |
|  | Czas wykonania pierwszej kopii | max. 8 sekund |  |
|  | Zoom | 25% - 400% |  |
|  | Czas nagrzewania | max.12 sekund |  |
|  | Kody dostępu | min. 10000 |  |
|  | Pojemność pamięci | min. 4 GB RAM |  |
|  | Twardy dysk | min. 320 GB szyfrowanie na dysku kluczem AES256 bit |  |
|  | Procesor | min. 1300 MHz |  |
|  | Rozdzielczość | min. 3600x1200 dpi |  |
|  | Gramatura papieru | 52 - 280 g/m² |  |
|  | Taca odbiorcza | min. 400 arkuszy |  |
|  | Kasety | 2 x kaseta na papier x min. 550 arkuszy każda (80 g/m²), 1 Kaseta: A5R-A3, 60-256 g/m², 2 Kaseta: A5R-320 x 460 mm, 60-256 g/m², możliwość dokupienia podajnika dużej pojemości na 2000 arkuszy A4 |  |
|  | Podajnik ręczny | podajnik ręczny: 100x148 mm-320x460 mm, 52-280 g/m², baner (305x1200 mm, 90-163 g/m²) |  |
|  | Duplex | jednoprzebiegowy A5R-320 x 460 mm, 60-256 g/m² |  |
|  | Automat. podajnik dokumentów z rewersem | dwustronny jednoprzebiegowy; min. 300 arkuszy A5R-A3 (80g/m²), min. 240 obr./min., 35-209 g/m² |  |
|  | Drukarka sieciowa | język opisu strony PCL5e, PCL5c, PCL6 (PCL XL), XPS oraz emulacja PostScript 3 / Interfejsy sieciowe; 10 B ase-T/100 Base-TX/1000 B ase-T, High Speed USB 2.0, (WLAN-opcja) (IEEE802.11b/g/n), (Bluetooth-opcja), Wi-Fi Direct-opcja) / TopAccess - zdalne zarządzanie i konfiguracja urządzenia poprzez wbudowaną stronę www / rozdzielczość druku min. 3600x1200 dpi / drukowanie dwustronne / drukowanie z pamięci USB / wydruk; wstrzymany, tandemowy / oprogramowanie e-BRIDGE dla IT oraz Help Desk pozwalające na zdalną administrację, konfiguracje oraz zarządzanie urządzeniem / możliwość współpracy z systemem wydruku podążającego i rozliczania prac APSM / protokoły sieciowe TCP/IP (IPv4/IPv6), IPX/SPX, EtherTalk, NetBios po TCP/IP |  |
|  | Wsparcie systemowe | Windows 10/8/7/Vista/Server 2008 (32/64 bity), Windows Server 2012/Windows Server 2016/Server 2008 R2 (64 bity), Mac OS X 10.6.8-10.11, Linux/Unix, Citrix, Novell NetWare (NDPS), SAP, AS/400 |  |
|  | Druk mobilny | E-BRIDGE Print & Capture, AirPrint, mMopria Print Service |  |
|  | Skaner sieciowy | skanowanie w kolorze / szybkość skanowania min. 240 obr.min, 35-209 g/m², min. 300 arkuszy A5R-A3 (80g/m²), / skanowanie WS, do USB, e-mail, (SMB, FTP, FTPS, IPX/SPX, Lokalnie), do OCR, na skrzynkę (e-Filing), WIA, TWAIN / format plików JPEG, TIFF/XPS/PDF jedno/wielostronicowy, zabezpieczony PDF, Slim PDF, PDF/A, przeszukiwalny PDF, DOCX., XLSX, RTF, TXT |  |
|  | Urządzenie gotowe do pracy | zestaw pełno wartościowych tonerów, umożliwiający wydrukowanie min. 38000 wydruków czarno-białych A4, oraz 33000 wydruków kolorowych przy standardowym pokryciu 5%. |  |
|  | Stolik / szafka | tak |  |
|  | Wyposażenie dodatkowe: |  |  |
|  | Opcje | Podajnik na koperty; pojemność min. 50 kopert, 100 x 162 mm-240 x 380 mm, 60-85 g/m2 Papier: Pojemność min. 550 arkuszy (1 x kaseta), A5R-A4R, 60-256 g/m2 |  |
|  | Gwarancja | GWARANCJA min. 24 miesiące, maks. 60 miesięcy, w miejscu pracy urządzenia. Dostawca urządzenia winien złożyć na żądanie Zamawiającego dokument potwierdzający, że Wykonawca jest autoryzowanym dystrybutorem oferowanego urządzenia oraz posiada autoryzację producenta do świadczenia usług serwisowych, w tym do dostawy i instalacji oryginalnych części zamiennych na terenie Polski. |  |

**B) Urządzenie wielofunkcyjne (małe) – 1 szt.**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/producent/nazwa | Urządzenie wielofunkcyjne |  |
|  | prędkość kopiowania | min 25 str/min A-4 i min 14 stron/min A-3 |  |
|  | format oryginału i kopii | A5R-A3 |  |
|  | czas wykonania pierwszej kopii | max. 7 sekund |  |
|  | zoom | 25-400% w krokach co 1% |  |
|  | czas nagrzewania | max. 20 sekund |  |
|  | pojemność pamięci | RAM 512 MB |  |
|  | rozdzielczość | skanowanie min. 600 x 600 dpi,  drukowanie maks. 2400 x 600 dpi |  |
|  | kaseta | 64 - 80 g/m2 |  |
|  | podajnik boczny | podajnik ręczny; A5R-A3, 52-163 g/m2 |  |
|  | duplex | zespół kopiowania/drukowania dwustronnego A5R-A3, 64-80 g/m2 |  |
|  | automat. podajnik dokumentów | automatyczny podajnik dokumentów A5R-A3, 50-104 g/m2 |  |
|  | karta drukarki | język obsługi drukarki; PCL6, drukowanie min.2400 x 600 dpi, TopAccess – zdalne zarządzanie i konfiguracja urządzenia |  |
|  | karta sieciowa | interfejs; 10/100 BaseT, IPv6, USB 2.0 High-Speed |  |
|  | skaner sieciowy | skaner A3 kolorowy i sieciowy; skanowanie do e-mail, pliku SMB,FTP, do USB, TWAIN, skanowanie JPEG, TIFF / PDF |  |
|  | obsługiwane systemy operacyjne | Windows 10 / 8 / 7 / Vista / XP / Serwer 2008 / Serwer 2003 (32/64 bity) / Windows Serwer 2008 R2 (64 bity)/Serwer 2012/ Serwer 2016 |  |
|  | funkcje | kopiowanie dokumentów (ID copy), usuwanie krawędzi zewnętrznych, tryb kopiowanie 2w1/4w1, elektroniczne sortowanie |  |
|  | gwarancja | GWARANCJA min. 24 miesiące, maks. 60 miesięcy, w miejscu pracy urządzenia. Dostawca urządzenia winien złożyć na żądanie Zamawiającego dokument potwierdzający, że Wykonawca jest autoryzowanym dystrybutorem oferowanego urządzenia oraz posiada autoryzację producenta do świadczenia usług serwisowych, w tym do dostawy i instalacji oryginalnych części zamiennych na terenie Polski. |  |

............... ………...................................................................

Data Podpis upoważnionego przedstawiciela Wykonawcy

\*wypełnia Wykonawca

**Część II zamówienia – Zakup sprzętu telekomunikacyjnego**

**A) Centrala telefoniczna – 1 szt.**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/producent/nazwa | Centrala telefoniczna |  |
|  | budowa modułowa centrali | tak |  |
|  | obsługa ruchu w sieciach ISDN 2B+D | 4 |  |
|  | obsługa ruchu w sieciach GSM poprzez wbudowaną bramkę | 1 |  |
|  | obsługa połączeń VoIP poprzez wbudowany serwer | 2 kanały rozmówne |  |
|  | kierowanie ruchu wychodzącego – LCR – optymalizacja kosztów | 1 |  |
|  | Porty wewnętrzne AB (FXS) | min. 20 |  |
|  | sieciowanie i współpraca z centralami Slican zainstalowanymi w naszych Oddziałach | tak |  |
|  | rejestrowanie prowadzonych rozmów | min. 4 rozmowy jednocześnie |  |
|  | Możliwość rozbudowy o moduł zasilania zapasowego | tak |  |
|  | Pełna integracja z oprogramowaniem do rejestracji rozmów RecordMan serwer | tak |  |
|  | Obudowa Rack | max. 3U |  |
|  | Możliwość rozbudowy centrali (zwiększenie ilości portów miejskich i wewnętrznych bez konieczności wymiany centrali). | tak |  |
|  | Możliwość zdalnego nadzoru nad centralą prowadzoną przez serwis celem szybkiej diagnozy ewentualnych awarii i uszkodzeń oraz szybkiej możliwości wprowadzania zmian w oprogramowaniu na życzenie użytkownika | tak |  |
|  | Możliwość wykorzystania w cenie systemu: konferencji dla 3 uczestników - pakietu dodatkowych minut na zapowiedzi słowne -łącznie 20 minut | tak |  |
|  | Montaż centrali i konfiguracja według wskazań użytkownika oraz integracja z istniejącym systemem | tak |  |

**B) Telefony przewodowe – 13 szt.**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/producent/nazwa | Telefon przewodowy |  |
|  | przełącznik trybu wybierania Pulse / Tone | tak |  |
|  | ponowne wybieranie ostatniego numeru - REDIAL | tak |  |
|  | możliwość przekazania / transferu połączeń - FLASH | tak |  |
|  | wyłączenie mikrofonu, w trakcie rozmowy - MUTE | tak |  |
|  | wstawianie przerwy miedzy wybieranymi cyframi - PAUSE | tak |  |
|  | ustawienia dzwonka - przełącznik głośności dzwonka | tak |  |
|  | sygnalizacja IN-USE | tak |  |
|  | możliwość montażu telefonu na ścianie | tak |  |
|  | funkcja odsłuchu HF ONE WAY | tak |  |

**C) Telefony bezprzewodowe – 5 szt.**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/producent/nazwa | Telefon bezprzewodowy |  |
|  | System DECT min. 30 m zasięgu | tak |  |
|  | czas czuwania | min. 7 dni |  |
|  | Podświetlany wyświetlacz LCD | tak |  |
|  | pamięć REDIAL | min. 10 numerów |  |
|  | możliwość montażu telefonu na ścianie | tak |  |
|  | lokalizacja słuchawki | tak |  |
|  | czas rozmów | 15 godzin |  |
|  | książka telefoniczna | 50 wpisów |  |
|  | Dzwonki do wyboru | tak |  |

............... ………...................................................................

Data Podpis upoważnionego przedstawiciela Wykonawcy

\*wypełnia Wykonawca

**Część III zamówienia – Zakup i wdrożenie infrastruktury informatycznej**

**Zakup i wdrożenie infrastruktury informatycznej – sprzedaż, dostarczenie, instalacja oraz uruchomienie sprzętu komputerowego wraz   
z oprogramowaniem, zgodnie z wymaganiami określonymi przez Zamawiającego, w ilościach i asortymencie jak poniżej:**

1. **Komputer PC - 18 szt.**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/model/symbol/producent | Komputer stacjonarny |  |
|  | Procesor | Zaoferowany komputer musi osiągać w teście SYSmark® 2014SE wyniki nie gorsze niż:   * SYSmark 2014 SE Overall Rating – 1190 punktów, * Office Productivity– 1050 punktów, * Media Creation – 1320 punktów, * Data/Financial Analysis – 1200 punktów.   Zamawiający wymaga, aby powyższy wynik osiągnięty był na komputerze w oferowanej konfiguracji. Test musi być przeprowadzony dla minimum trzech iteracji przy rozdzielczości monitora 1920x1080/60Hz. Wymagane jest dołączenie do oferty wydruku z przeprowadzonego testu, potwierdzonego za zgodność z oryginałem przez Wykonawcę(później, nie do oferty). Wymagane testy wydajnościowe muszą zostać wykonane na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawienia BIOS jak również w samym środowisku systemu (np. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający w momencie dostawy sprzętu może wymagać na losowo wskazanym komputerze zainstalowania i uruchomienia przez Wykonawcę oprogramowania testującego w celu weryfikacji wyników testu. |  |
|  | Pamięć RAM | 8GB, możliwość rozbudowy do 64GB |  |
|  | Parametry pamięci masowej | 256GB SSD |  |
|  | Wyposażenie multimedialne | Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem DirectX 12, OpenGL 4.0, pamięć współdzielona z pamięcią RAM, dynamicznie przydzielana do min. 1,7 GB  Min 24-bitowa Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition |  |
|  | Obudowa | Typu small form factor z obsługą kart PCI Express wyłącznie o niskim profilu, fabrycznie przystosowana do pracy w pionie i w poziomie. Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego i dysku twardego bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych, śrub radełkowych) oraz posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) oraz kłódki (oczko w obudowie do założenia kłódki). Obudowa musi być wyposażona w zamek szybkiego dostępu i musi być usytuowany na tylnym panelu. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz wpisanym na stałe w BIOS. |  |
|  | Napęd optyczny | DVD RW |  |
|  | Oprogramowanie | Windows 10 PRO lub rozwiązanie równoważne zgodne w 100% z Microsoft Office 2016 oraz  systemem domenowym MS Windows Active Directory jak również w pełni kompatybilne z oprogramowaniem posiadanym przez zamawiającego, o którym mowa w niniejszym opisie przedmiotu zamówienia (PROGMED, AXON, MARCEL). Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę Zamawiający rozumie zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. |  |
|  | Zgodność z systemami operacyjnymi i standardami | Oferowane modele komputerów muszą posiadać certyfikat producenta oferowanego systemu operacyjnego, potwierdzający poprawną współpracę oferowanych modeli komputerów z oferowanym systemem operacyjnym (należy załączyć na pisemne żądanie Zamawiającego wydruk ze strony producenta oprogramowania) |  |
|  | Zdalne zarządzanie | Wbudowana w płytę główną technologia zarządzania  i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca:  monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej;  zdalną konfigurację ustawień BIOS,  zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego;  technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0 (http://www.dmtf.org/standards/mgmt/dash/). |  |
|  | BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera,  Pełna obsługa BIOS za pomocą klawiatury i myszy.  Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:   * wersji BIOS, * numerze seryjnym i dacie wyprodukowania komputera, * włączonej lub wyłączonej funkcji aktualizacji BIOS * ilości i prędkości zainstalowanej pamięci RAM, oraz sposobie obsadzeniu slotów pamięci * typie, prędkości oraz wielkości z pamięci cache L2 i L3 zainstalowanego procesora * pojemności zainstalowanego lub zainstalowanych dysków twardych * wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA oraz M SATA   Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS)  Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.  Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego,  Możliwość wyłączenia/włączenia karty sieciowej, z funkcją PXE,  Możliwość włączenia/wyłączenia kontrolera SATA  Możliwość włączenia/wyłączenia kontrolera audio,  Możliwość włączenia/wyłączenia układu TPM.  Możliwość włączenia/wyłączenia czujnika otwarcia obudowy i ustawienia go w tryb cichy  Możliwość włączenia/wyłączenia wzbudzania komputera za pośrednictwem portów USB,  Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. |  |
|  | Zasilanie | Zasilacz o mocy max 180W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%. |  |
|  | Karta sieciowa | Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE , umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem. |  |
|  | Wymagania dodatkowe | Wbudowane porty: min. 1 x RS232, 2 x PS/2, HDMI, 2x Display Port, min. 10 portów USB wyprowadzonych na zewnątrz komputera: 6x USB 3.0 (Min. 2 z przodu obudowy), 4x USB 2.0, port słuchawkowo-mikrofonowy na przednim panelu obudowy  Klawiatura USB w układzie programisty  Mysz optyczna USB z dwoma klawiszami oraz rolką (scroll) |  |
|  | Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy jałowej (IDLE) wynosząca maksymalnie 22 dB (załączyć oświadczenie producenta) |  |
|  | Certyfikaty i standardy | Dokumenty, które należy złożyć na pisemne wezwanie Zamawiającego:   * Certyfikat ISO9001 dla producenta sprzętu. * Deklaracja zgodności CE. * Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram |  |
|  | Gwarancja | 3-letnia gwarancja producenta świadczona na miejscu u klienta.  Czas reakcji serwisu - do końca następnego dnia roboczego.  Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera - dokumenty potwierdzające załączyć do oferty.  Długość gwarancji musi wynikać bezpośrednio z numeru seryjnego komputera i być weryfikowalna na stronie internetowej producenta sprzętu.  Oświadczenie producenta potwierdzające, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych Wykonawcy lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.  W przypadku awarii, dyski twarde zostają u Zamawiającego.  Wszystkie powyższe dokumenty należy złożyć na pisemne wezwanie Zamawiającego. |  |
|  | Wsparcie techniczne | Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.  Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony. |  |

1. **Monitor - 18 szt.**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/model/symbol/producent | Monitor |  |
|  | Typ ekranu | Ekran ciekłokrystaliczny z aktywną matrycą 21,5” (16:9), powłoka antyodblaskowa |  |
|  | Rozmiar plamki | Max 0.255mm |  |
|  | Jasność | min.250 cd/m2 |  |
|  | Kontrast | 1000:1 (typowy), 4mln:1 (dynamiczny) |  |
|  | Kąty widzenia (pion/poziom) | 178/178 stopni |  |
|  | Czas reakcji matrycy | Max 6 ms (gray to gray) |  |
|  | Rozdzielczość maksymalna | 1920 x 1080 at 60Hz |  |
|  | Gamy koloru | min. 82% (CIE 1976)  min. 72% (CIE 1931) |  |
|  | Obracanie w pionie | TAK |  |
|  | Pochylenie monitora | W zakresie min. 25 stopni |  |
|  | Wydłużenie w pionie | Tak, min 130 mm |  |
|  | Bezpieczeństwo | Monitor musi być wyposażony w tzw. Kensington Slot |  |
|  | Złącze | 1x DisplayPort, 1 x HDMI, 1 x VGA, 3X USB 3.0, |  |
|  | Gwarancja | Minimum 3 lata na miejscu u klienta.  Czas reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta– dokumenty potwierdzające należy złożyć na pisemne wezwanie Zamawiającego.  Oświadczenie producenta monitora, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem – należy złożyć na pisemne wezwanie Zamawiającego. |  |
|  |
|  |
|  |
|  | Inne | Zdejmowana podstawa oraz otwory montażowe w obudowie VESA 100mm  Głośniki wbudowane lub dedykowane głośniki producenta monitora podłączane do obudowy w formie listwy głośnikowej |  |
|  |

1. **Filtr prywatyzujący do monitora – 3 szt.**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/model/symbol/producent | Filtr prywatyzujący do monitora |  |
|  | Przekątna ekranu | 21,5” |  |
|  | Proporcje ekranu | 16:9 |  |
|  | Kolor | Czarny |  |
|  | Antyodblaskowy | TAK |  |
|  | Odporność na zarysowania | TAK |  |
|  | Gwarancja | Min. 1 rok |  |

1. **Drukarka – 14 szt.**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/model/symbol/producent | Drukarka laserowa |  |
|  | Format | A4 |  |
|  | Technologia druku | Druk Laserowy |  |
|  | Rozdzielczość druku | 600x600 dpi |  |
|  | Szybkość drukowania | Min. 22 str/min |  |
|  | Podajnik papieru | Podajnik na 150 arkuszy, podajnik z priorytetem poboru na 10 arkuszy |  |
|  | Odbiornik wydruków | Odbiornik papieru na min. 100 arkuszy |  |
|  | Nośniki | Papier (do druku laserowego, zwykły, fotograficzny), koperty, etykiety, pocztówki |  |
|  | Obsługiwane formaty nośników | A4,A5, A6, B5 (JIS) |  |
|  | Maksymalne dopuszczalne miesięczne obciążenie | Min. 10 000 stron |  |
|  | Pamięć wewnętrzna | Min. 128MB |  |
|  | Interfejsy | 1x USB 2.0, Wi-Fi 802.11b/g/n |  |
|  | Gwarancja | 1 rok |  |

1. **Listwa zasilająca – 19 szt.**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ | Listwa zasilająca |  |
|  | Typ gniazda wyjściowego | Euro |  |
|  | Liczba gniazd wyjściowych | Min. 5 szt. |  |
|  | Długość przewodu zasilającego | min. 3 metry |  |
|  | Prąd znamionowy | 10A |  |
|  | Gwarancja | 5 lat |  |

1. **Drukarka etykiet – 1 szt.**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/model/symbol/producent | Drukarka etykiet |  |
|  | Technologia druku | termiczny / termotransferowy |  |
|  | Rozdzielczość drukowania | 203dpi |  |
|  | Prędkość druku | min. 127mm/s |  |
|  | Obsługiwane kody kreskowe | Codabar, Code 11 (ZPL), Code 39, Code 93, Code 128, EAN- 13, EAN- 14 (ZPL), German Post Code (EPL), GS1 DataBar (RSS), Industrial 2- of - 5, ISBT-128 (ZPL), Japanese Postnet (EPL), Logmare (ZPL), MSI, Plessey, Postnet, Standard 2 -of -5 (ZPL), UCC/ EAN- 128 (EPL), UPC- A, UPC-A i UPC- E z rozszerzeniami 2 - lub 5- cyfrowymi EAN, UPC i rozszerzenia 2- lub 5- cyfrowe EAN (ZPL), CodaBlock (ZPL), Code 49 (ZPL), Data Matrix, (ZPL), MaxiCode, MicroOPDF417, PDF417, QR Code |  |
|  | Interfejs | szeregowyRS232/ DB- 9, USB, |  |
|  | Max. Szerokość/długość etykiet | 104 mm/990 mm |  |
|  | Dodatkowe funkcje | Zgodność z oprogramowaniem PROGMED, obsługa rolek z etykietami 32x20 nawiniętymi po 2500 szt. |  |
|  | Gwarancja | 1 rok |  |

1. **Niszczarka – 2 szt.**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/model/symbol/producent | Wolnostojąca wydajna niszczarka do niszczenia dokumentów, spinaczy, małych zszywek, kart plastikowych, płyt CD/DVD |  |
|  | Przeznaczenie | Niszczenie: papier, spinacze, małe zszywki, karty plastikowe, płyty CD/DVD |  |
|  | Szerokość szczeliny wejściowej | min. 235 mm |  |
|  | Wydajność | min. 20 kartek A4/70g |  |
|  | Stopień bezpieczeństwa | P-4, T-4, O-1 |  |
|  | Wielkość ścinka | max. 4x38mm |  |
|  | Pojemność kosza | min. 55L |  |
|  | Prędkość cięcia | min. 4,5m/min |  |
|  | Gwarancja | min. 2 lata na urządzenie/20 lat na noże tnące |  |
|  | Dodatkowe funkcje | * funkcja Start/Stop * funkcja cofania * informacja o przepełnionym koszu * informacja o zacięciach * informacja o otwartych drzwiach/wyjętym koszu/zdjętej głowicy |  |

1. **Serwer – 1 sztuka**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/producent/nazwa | Serwer sprzętowy |  |
|  | Obudowa | Obudowa typu Rack o wysokości maksymalnej 2U, z możliwością instalacji do 16 dysków 2.5” HotPlug wraz kompletem szyn wraz z organizatorem kabli do montażu w standardowej szafie Rack. |  |
|  | Płyta główna | Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |
|  | Procesor | Dwa procesory min. ośmiordzeniowe dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku  minimum 660 punktów w teście SPECint\_rate\_base2006 dostępnym na stronie internetowej www.spec.org dla konfiguracji dwuprocesorowej  Do oferty należy załączyć wynik testu dla oferowanego modelu serwera wraz z oferowanym modelem procesora. |  |
|  | Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |  |
|  | Pamięć RAM | 64 GB pamięci RAM typu RDIMM o częstotliwości pracy 2400MHz.  Płyta powinna obsługiwać do 1.5TB pamięci RAM i być wyposażona w minimum 24 sloty pamięci.  Możliwe zabezpieczenia pamięci: Memory Rank Sparing, Memory Mirror, SBEC, Lockstep |  |
|  | Sloty PCI Express | Minimum cztery sloty x16 generacji 3 o prędkości x8 niskoprofilowe.  Minimum dwa sloty x16 generacji 3 o prędkości x16 pełnej długości i wysokości. |  |
|  | Karta graficzna | Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024 |  |
|  | Wbudowane porty | Minimum 4 porty USB z czego min. 2 w technologii 3.0 , 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232.  Rozwiązanie nie może zostać uzyskane przy pomocy adapterów przejściówek oraz dodatkowych kart. |  |
|  | Interfejsy sieciowe | Minimum cztery interfejsy sieciowe 1Gb Ethernet RJ45, interfejsy sieciowe nie mogą zajmować żadnego z dostępnych slotów PCI Express oraz portów USB. Wsparcie dla protokołów IPv6. Możliwość instalacji wymiennie modułów udostępniających:   * minimum dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseT * cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ * minimum dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseT |  |
|  | Kontroler dysków | Zainstalowany sprzętowy kontroler dyskowy, obsługujący tryby RAID : 0, 1, 5, 6, 10, 50, 60 i posiadający minimum 1GB nieulotnej pamięci CACHE. |  |
|  | Wewnętrzna pamięć masowa | Możliwość instalacji dysków twardych SATA, SAS, NearLine SAS i SSD.  Zainstalowane minimum 2 dyski Hot-Plug 300GB SAS 12Gb/s 10k RPM oraz 7 dysków Hot-Plug 1.2 TB SAS 12Gb/s 10k RPM.  Możliwość instalacji wewnętrznego modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w 2 jednakowe nośniki typu flash z możliwoscią konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmiejszenia ilości wnęk na dyski twarde. |  |
|  | Zasilacze | Redundantne zasilacze Hot Plug o mocy maksymalnej 750W każdy wraz z kablami zasilającymi o długości min. 2m każdy. |  |
|  | Wentylatory | Minimum 6 redundantnych wentylatorów Hot-Plug |  |
|  | System Operacyjny | Brak systemu operacyjnego |  |
|  | Bezpieczeństwo | * Elektroniczny panel informacyjny umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze, adresach MAC kart sieciowych, numerze serwisowym serwera, aktualnym zużyciu energii, nazwie serwera, modelu serwera. * Zintegrowany z płytą główną moduł TPM. * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Fabryczne oznaczenie urządzenia, wykonane przez producenta serwera informujące Zamawiającego m.in. o numerze serwisowym serwera, pełnej nazwie podmiotu Zamawiającego, modelu serwera; gwarantujące Zamawiającemu dostawę nowego, nieużywanego i nie pochodzacego z innych projektów sprzętu. * Fizyczne zabezpieczenie dedykowane przez producenta serwera uniemożliwiające wyjęcie dysków twardych umieszczonych na froncie obudowy przez nieuprawnionych użytkowników. |  |
|  | Karta zarządzająca | Zainstalowana niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany 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 * 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 * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej * możliwość podłączenia lokalnego poprzez złącze RS-232 |  |
| Dodatkowe opogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:   * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych * Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta * Wsparcie dla protokołów– WMI, SNMP, IPMI, WSMan, Linux SSH * Możliwość oskryptowywania i uruchamiania w oparciu o harmonogram procesu wykrywania urządzeń * Szczegółowy opis wykrytych systemów oraz ich komponentów * Możliwość eksportu raportu do CSV, HTML, XLS * Grupowanie urządzeń w oparciu o kryteria użytkownika * Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń * Szybki podgląd stanu środowiska * Podsumowanie oraz szczegółowy status urządzenia/elementu/komponentu * Generowanie alertów przy zmianie stanu urządzenia * Filtry raportów umożliwiające podgląd najważniejszych zdarzeń * Integracja z service desk producenta dostarczonej platformy sprzętowej * Możliwość przejęcia zdalnego pulpitu i podmontowania wirtualnego napędu * Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu- Przesyłanie alertów „as-is” do innych konsol firm trzecich * Możliwość definiowania ról administratorów * Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów w oparciu o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) * Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta * Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów |  |
|  | Gwarancja | Minimum 3 lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do 4 godzin od przyjęcia zgłoszenia (uszkodzone dyski twarde pozostają u Zamawiającego), możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Urządzenie musi pochodzić z legalnego źródła, zakupione w autoryzowanym kanale sprzedaży producenta w Polsce. |  |
|  | Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001, musi też posiadać deklarację CE. |  |
| Serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016.  Dokumenty na potwierdzenie powyższych wymagań należy złożyć na pisemne wezwanie Zamawiającego. |  |
|  | Dokumentacja | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. |  |
| Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |

1. **Oprogramowanie systemowe – 1 zestaw**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
| 1. | Typ/producent/nazwa | Oprogramowanie systemowe |  |
| 2. | System operacyjny | Z uwagi na jednorodność środowiska informatycznego, opartego o usługi Microsoft Windows Active Directory, Zamawiający wymaga dostarczenia licencji na system Microsoft Windows Server 2016 w ilości pozwalającej na uruchomienie czterech maszyn wirtualnych na dostarczonym serwerze.  Musi istnieć możliwość przenoszenia dostarczonych licencji pomiędzy serwerami Zamawiającego (wyklucza się licencjonowanie typu OEM). Dopuszcza się także inne rozwiązanie równoważne zgodne w 100% z systemem domenowym MS Windows Active Directory jak również w pełni kompatybilne z oprogramowaniem posiadanym przez zamawiającego, o którym mowa w niniejszym opisie przedmiotu zamówienia (PROGMED, AXON, MARCEL). Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. Dodatkowo Zamawiający zastrzega sobie prawo do zweryfikowania funkcjonalności, wydajności  i kompatybilności zaoferowanego rozwiązania równoważnego poprzez analizę jego możliwości. W przypadku skorzystania przez Zamawiającego z ww. uprawnienia Sprzedający jest zobowiązany w terminie 3 dni od dnia otrzymania od Zamawiającego wezwania do dostarczenia testowej wersji zaproponowanego rozwiązania dostarczyć to rozwiązanie do siedziby Zamawiającego. |  |
| 3. | Licencje dostępowe | Zamawiający wymaga dostarczenia 20 szt. licencji dostępowych typu Device dla systemu Windows Server 2016 lub równoważnych zgodnych z dostarczanym w ramach zamówienia systemem operacyjnym. |  |

1. **Oprogramowanie do wykonywania kopii zapasowych maszyn wirtualnych Hyper-V – 1 zestaw**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/producent/nazwa | Oprogramowanie do wykonywania kopii zapasowych maszyn wirtualnych Hyper-V |  |
|  | Funkcjonalność oprogramowania | 1. Oprogramowanie do archiwizacji musi współpracować z infrastrukturą wirtualizacji opartą na Microsoft Hyper-V 2012, 2012 R2 i 2016, jak również z VMware vSphere w wersji 4.1, 5.0, 5.1, 5.5, 6.0 2. Rozwiązanie musi współpracować z hostami Hyper-V zarządzanymi przez System Center Virtual Machine Manager, zgrupowanymi w klastry jak i niezarządzanymi (standalone); 3. Rozwiązanie musi współpracować z hostami ESX i ESXi zarządzanymi przez VMware vCenter jak i hostami niezarządzanymi (standalone); 4. Rozwiązanie nie może instalować żadnych swoich komponentów (agent) w archiwizowanych maszynach wirtualnych; 5. Rozwiązanie musi wspierać backup wszystkich systemów operacyjnych w wirtualnych maszynach, które są wspierane przez VMware i Hyper-V; 6. Serwer kopii zapasowych musi mieć możliwość instalacji na następujących systemach operacyjnych:   a.       Microsoft Windows Server 2008 SP2 (x64),  b.      Microsoft Windows Server 2008 R2,  c.       Microsoft Windows 7 SP1,  d.      Windows Server 2012,  e.      Windows Server 2016,  f.      Windows 8;   1. Rozwiązanie musi oferować odzyskiwanie całych obrazów maszyn wirtualnych z obrazów, pojedynczych plików z systemu plików znajdujących się wewnątrz wirtualnej maszyny. Rozwiązanie musi umożliwiać odzyskanie plików i/lub całych maszyn wirtualnych na zasadzie „one-click restore”. Rozwiązanie musi umożliwiać odzyskiwanie plików z następujących systemów plików:   a.       Linux: ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS,  b.      BSD: UFS, UFS2,  c.       Solaris: ZFS,  d.      Mac: HFS, HFS+,  e.      Windows: NTFS, FAT, FAT32, ReFS;   1. Rozwiązanie musi umożliwiać natychmiastowe odzyskanie wirtualnej maszyny i jej uruchomienie bez kopiowania na storage podłączony do hostów ESX (wbudowana funkcjonalność NFS Server) i Hyper-V; 2. Rozwiązanie musi umożliwiać bezpośrednie odzyskiwanie obiektów z takich usług jak: Active Directory (użytkownicy i grupy), Microsoft Exchange (emaile i kontakty), Microsoft SharePoint (dokumenty) i Microsoft SQL (tabele i rekordy) z maszyn wirtualnych środowiska VMware i Hyper-V; 3. Rozwiązanie musi zapewniać szybkie odzyskiwanie danych ze skrzynek pocztowych Microsoft Exchange 2010/2013 bez potrzeby uruchamiania maszyny wirtualnej (odzyskiwanie bezpośrednio z bazy danych \*.EDB); 4. Rozwiązanie musi zapewniać szybkie odzyskiwanie danych z witryn Microsoft SharePoint 2010 bez potrzeby uruchamiania maszyny wirtualnej (odzyskiwanie bezpośrednio z bazy danych \*.MDF); 5. Rozwiązanie musi umożliwiać indeksowanie plików zawartych w archiwach maszyn wirtualnych z systemem operacyjnym Windows w celu szybkiego ich przeszukiwania; 6. Rozwiązanie musi umożliwiać równoczesne przetwarzanie wielu maszyn wirtualnych; 7. Rozwiązanie musi w pełni korzystać z mechanizmów zawartych w VMware vStorage API for Data Protection, w szczególności być zgodnym z mechanizmem Changed Block Tracking. 8. Rozwiązanie musi umożliwiać wykorzystanie technologii CBT dla platformy VMware również dla maszyn wirtualnych, które posiadają już migawkę; 9. Rozwiązanie musi mieć wbudowane mechanizmy podobne do technologii CBT, również dla platformy Hyper-V w celu przyśpieszenia procesu backupu; 10. Rozwiązanie musi korzystać z mechanizmów VSS (Windows Volume Shadowcopy) wbudowanych w najnowsze systemy operacyjne z rodziny Windows; 11. Rozwiązanie musi mieć wbudowane mechanizmy deduplikacji i kompresji archiwum w celu redukcji zajmowanej przez archiwa przestrzeni dyskowej; 12. Rozwiązanie musi mieć możliwość archiwizacji na napędach taśmowych; 13. Rozwiązanie musi mieć możliwość instalacji centralnej konsoli do zarządzania większą ilością serwerów archiwizujących oraz jednoczesnego zarządzania backupami środowiska VMware i Hyper-V; dostęp do tej konsoli musi być realizowany przez przeglądarkę WWW; 14. Rozwiązanie musi mieć wbudowany mechanizm informowania o pomyślnym lub niepomyślnym zakończeniu procesu archiwizacji poprzez email, zapis do Event Log’u Windows lub wysłanie komunikatu SNMP; 15. Rozwiązanie musi mieć możliwość rozbudowy procesu archiwizacji o dowolne skrypty tworzone przez administratora i dołączane do zadań archiwizacyjnych; 16. Rozwiązanie musi mieć wbudowaną możliwość replikacji wirtualnych maszyn pomiędzy hostami ESX i ESXi, w tym możliwość replikacji ciągłej; 17. Rozwiązanie musi mieć wbudowaną możliwość replikacji maszyn wirtualnych pomiędzy hostami Hyper-V, w tym możliwość replikacji ciągłej; 18. Rozwiązanie musi mieć możliwość tworzenia środowiska wirtualnego laboratorium w środowisku VMware lub Hyper-V; 19. Rozwiązanie musi mieć możliwość występowania i zatwierdzania wniosków o tworzenie środowisk w wirtualnym laboratorium w środowisku VMware lub Hyper-V; 20. Rozwiązanie musi zapewnić możliwość sprawdzenia poprawności wykonania archiwum poprzez odtworzenie wirtualnej maszyny w izolowanym środowisku i jej uruchomienie w środowisku VMware lub Hyper-V; 21. Rozwiązanie musi zapewnić możliwość sprawdzenia poprawności wykonania replikacji poprzez odtworzenie wirtualnej maszyny w izolowanym środowisku i jej uruchomienie w środowisku VMware; 22. Rozwiązanie musi mieć możliwość integracji z środowiskiem VMware vCloud Director a w szczególności możliwość archiwizacji metadanych vCD i atrybutów vApps oraz odzyskiwanie tych elementów bezpośrednio do vCD; 23. Rozwiązanie musi umożliwiać zapisanie konfiguracji całej instalacji w celu przywrócenia jej po reinstalacji całego systemu; 24. Rozwiązanie musi mieć możliwość dodatkowego skopiowania punktów przywracania do innej lokalizacji; 25. Rozwiązanie musi mieć możliwość wykonywania archiwizacji zgodnie z rotacyjnym schematem GFS (Grandfather-father-son). |  |
|  | Licencje | Wymagane jest dostarczenie licencji w ilości niezbędnej do poprawnej obsługi kopii zapasowych maszyn wirtualnych na dostarczonym serwerze zgodnie z opisem w pkt. 8 |  |
|  | Wsparcie | Trzy lata wsparcia świadczonego przez producenta rozwiązania, obejmującego dostęp do aktualizacji, nowych wersji oprogramowania i pomocy technicznej |  |

1. **Dyski twarde do serwera kopii zapasowych – 5 sztuk**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
| 1. | Typ dysku, wykonanie | Dysk talerzowy, 2.5” SFF Hot-Plug |  |
| 2. | Interfejs dysku | SAS 6G |  |
| 3. | Prędkość obrotowa | Minimum 7200 obr./min. |  |
| 4. | Pojemność dysku | Minimum 1 TB |  |
| 5. | Dodatkowe wymagania | Dysk musi współpracować z serwerem HP DL380 G7 posiadanym przez Zamawiającego i znajdować się na liście akcesoriów do rozbudowy serwera (według najnowszej dostępnej wersji dokumentu QuickSpecs dla serwera DL 380 G7) |  |

1. **Przełącznik sieciowy – 1 sztuka**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/producent/nazwa | Przełącznik sieciowy |  |
|  | Obudowa | Do montażu w szafie Rack 19", o wysokości nie wiecej niż 1U, wraz z kompletem odpowiednich szyn, wyposażona w zintegrowany zasilacz. |  |
|  | Porty | Minimum 48 portów Gigabit Ethernet BaseT/RJ45, minimum 4 porty 1/10 Gigabit Ethernet SFP+, minimum 1 port USB do konfiguracji przełącznika, 1 port RJ45 do portu konsoli wraz z odpowiednim kablem RJ45-RS232. |  |
|  | Pamięć | Pamięć flash min. 256MB  Bufor pamięci dla pakietów minimum 4MB  Pamięć procesora minimum 1GB |  |
|  | Wydajność przełącznika | Przepustowość magistrali minimum 176 Gbps  Prędkość przełączania minimum 112 Mpps  Minimum 8 kolejek na port dla ruchu o różnej klasie obsługi. |  |
|  | Funkcjonalność warstwy 2 | Obsługa minimum 4000 VLAN  Obsługa minimum 32000 adresów MAC  Obsługa protokołów: 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP, 802.1v Protocol-based VLANs, 802.1p Ethernet Priority (User Provisioning and Mapping), 802.1AB LLDP, 802.1D Spanning Tree, 802.1S 802.1W Rapid Spanning Tree (RSTP), RSTP-Per VLAN, Multiple Spanning Tree (MSTP), BPDU guard, BPDU filtering, 802.1X Network Access Control. |  |
|  | Funkcjonalność warstwy 3 | Trasy routingu statycznego: minimum 256  Trasy routingu dynamicznego: minimum 10000  Obsługa protokołów routingu: RIPv1, IRPv2, OSPF, OSPFv2, OSPFv3.  Obsługa protokołu VRRP |  |
|  | Multicast | Obsługa protokołów IGMPv1, IGMPv2, PIM-SM, PIM-DM, MLDv1, MLDv2 |  |
|  | Zarządzanie siecią i bezpieczeństwo | Połączenie szyfrowane: SSL/SSH,  Autentykacja dostępu do przełącznika w oparciu o Radius lub TACACS+  Listy dostępu (ACL) warstwy 2/3/4  Obsługa RMON,  Obsługa SNMP v2 i v3,  Obsługa sFlow,  Możliwość przechowywania dwóch wersji oprogramowania na przełączniku,  Obsługa 802.1x w tym:  - MAC-based authentication  - MAC authentication bypass  - Guest VLAN  Zarządzenie przez CLI i przez przeglądarkę internetową,  Radius  Radius Accounting  RADIUS Tunnel Authentication  Serwer i klient DHCP  Simple Network Time Protocol (SNTP)  TLS protocol, version 1.0  Wsparcie dla ramek typu Jumbo 9,000 bajtów  Broadcast storm control  Trivial File Transfer Protocol (TFTP) Rev. 2  Honorowanie wartości 802.1p oraz IP DSCP  Wsparcie kolejkowania Strict priority oraz algorytmu weighted round robin (WRR)  Port security  Private VLAN |  |
|  | Certyfikaty i standardy | Przełącznik musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001, musi też posiadać deklarację CE. |  |
|  | Gwarancja | Minimum 3 lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do 4 godzin od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do 5 lat. Urządzenie musi pochodzić z legalnego źródła, zakupione w autoryzowanym kanale sprzedaży producenta w Polsce. |  |

1. **Konsola rack z KVM - 1 szt.**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/producent/nazwa | Konsola rack z KVM |  |
|  | Monitor | Technologia: TFT-LCD  Przekątna: minimum 18,5”  Rozdzielczość: minimum 1280x1024  Jasność: minimum 250 cd/m²  Kontrast: minimum 1000:1 |  |
|  | Urządzenia wejściowe | Klawiatura z touchpadem |  |
|  | KVM | Minimum 8-portowy, zamontowany z tyłu konsoli rack.  Możliwość podłączenia dodatkowych zewnętrznych przełączników KVM w celu rozszerzenia liczby portów KVM.  Możliwość zabezpieczenia dostępu do KVM hasłem użytkownika (w trybie podglądu sesji) i administratora (w trybie podglądu sesji i konfiguracji KVM). |  |
|  | Porty KVM | Minimum 8 portów RJ45.  Minimum 8 kabli z portami USB i VGA do podłączenia serwerów o długości nie mniejszej niż 2 metry.  Możliwość wykorzystania okablowania strukturalnego LAN kategorii 5e/6 i dedykowanych adapterów KVM do przesłania sygnału na odległości minimum 40m (przy rozdzielczości 1280x1024 @ 50Hz). |  |
|  | Gwarancja | Minimum 3 lata gwarancji realizowanej w serwisie producenta (dotyczy wszystkich komponentów zestawu). |  |

1. **UPS - 1 szt.**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/producent/nazwa | UPS |  |
|  | Obudowa | Typu rack 19”, wysokość nie przekraczająca 2U wyposażona w wyświetlacz LCD informujący o stanie zasilacza, bateriach. |  |
|  | Typ zasilacza | Online, podwójna konwersja. |  |
|  | Napięcie wejściowe | AC 230V, 50Hz |  |
|  | Napięcie wyjściowe | AC 230V, 50Hz |  |
|  | Moc | 3000VA / 2700W |  |
|  | Czas podtrzymania | Minimum 12 min. przy 50% obciążenia i 4 min. przy 100% obciążenia. |  |
|  | Złącza | Minimum 6x IEC-320 C13, 2x IEC-320 C19, 1x RJ45, 1x USB. |  |
|  | Zarządzanie | Wbudowana karta do zarządzania zasilaczem przez sieć LAN, złącze RJ45. |  |
|  | Oprogramowanie | Oprogramowanie typu agent, pozwalające na automatyczne wyłączenie systemów operacyjnych z rodziny Microsoft Windows w przypadku awarii zasilania UPS. |  |
|  | Certyfikaty | Zasilacz musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001, musi też posiadać deklarację CE. |  |
|  | Gwarancja | Minimum 3 lata gwarancji na zasilacz i baterię, realizowanej  w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. |  |

1. **Listwa do dystrybucji zasilania - 1 szt.**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Typ/producent/nazwa | Listwa do dystrybucji zasilania |  |
|  | Obudowa | Typu rack 19”, wysokość 1U |  |
|  | Napięcie znamionowe | AC 230V, 50Hz |  |
|  | Kabel zasilający | Długość minimum 2.5m, 3x1.5mm² |  |
|  | Wtyk wejściowy | IEC320 C20 16A/250V |  |
|  | Gniazda wyjściowe | 9x NF C61-314 (standard PL) 16A/250V |  |
|  | Dopuszczalne obciążenie | 16A (3680W) |  |

1. **Oprogramowanie do obsługi poradni – 9 szt. licencji (w tym 1 szt. z obsługą rehabilitacji)**

| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- |
| Funkcjonalność oprogramowania | Prowadzenie dokumentacji elektronicznej w poradniach AOS wszystkich specjalizacji |  |
| Wymiana danych z NFZ w otwartym formacie XML (umowy, deklaracje, raporty statystyczne, rachunki refundacyjne, faktury, kolejki oczekujących, zestawienia zbiorcze) |  |
| Obsługa sesji terapeutycznych |  |
| Planowanie cykli rehabilitacyjnych w oparciu o zdefiniowaną bazę zabiegów, sprzętu i personelu |  |
| Import puli numerów recept, wypełnianie i drukowanie recept  w gabinetach lekarskich |  |
| Wbudowany gruper JGP |  |
| Komunikacja z systemem laboratorium (eksport zleceń, odbieranie wyników badań, dostęp do wyników badań laboratoryjnych dla wszystkich lekarzy) |  |
| Komunikacja z systemem PACS (eksport zleceń, dostęp do wyników badań dla wszystkich lekarzy) |  |
| Automatyczna weryfikacja umówionych pacjentów w systemie EWUŚ |  |
| Wymiana danych pomiędzy filiami |  |
| Definiowanie harmonogramów pracy lekarzy |  |
| Obsługa SMS i email (powiadamianie pacjentów o terminach wizyt, wysyłanie wiadomości do wybranej grupy pacjentów) |  |
| Obsługa kwalifikowanych podpisów cyfrowych |  |
| Definiowanie ankiet udostępnianych do wypełnienia lekarzom przy wizytach z wybranej poradni |  |
| Wbudowane słowniki ICD9, ICD10, słownik terytorialny GUS |  |
| Wbudowana baza leków |  |
| Możliwość eksportu danych z dowolnych raportów i zestawień do plików w formacie Excel, CSV |  |
| Serwis www dla pacjentów pozwalający na umawianie i przeglądanie wizyt |  |
| Połączenie z centralką telefoniczną |  |
| Obsługa drukarek fiskalnych |  |
| Obsługa umów prywatnych |  |
| Pełna integracja z systemem PROGMED |  |

1. **Oprogramowanie antywirusowe – 11 szt. licencji (w tym 2 szt. dla serwerów)**

| **L.p.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowane**\* |
| --- | --- | --- | --- |
|  | Ochrona antywirusowa i antyspyware | Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10 |  |
| Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim. |  |
| Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives. |  |
| Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. |  |
| Wbudowana technologia do ochrony przed rootkitami. |  |
| Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. |  |
| Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. |  |
| 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. |  |
| 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 |  |
| Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. |  |
| Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. |  |
| Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. |  |
| Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. |  |
| Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. |  |
| 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. |  |
| Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego). |  |
| 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). |  |
| Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. |  |
| Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. |  |
| Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. |  |
| 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. |  |
| Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. |  |
| Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. |  |
| Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. |  |
| Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. |  |
| Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. |  |
| Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. |  |
| Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. |  |
| 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. |  |
| 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. |  |
| Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. |  |
| Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła. |  |
| Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. |  |
| Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji. |  |
| 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. |  |
| System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. |  |
| 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 , urządzeń przenośnych oraz urządzeń dowolnego typu. |  |
| Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. |  |
| Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia. |  |
| Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. |  |
| W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. |  |
| Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika |  |
| Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). |  |
| Oprogramowanie musi posiadać zaawansowany skaner pamięci. |  |
| Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp. |  |
| 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. |  |
| 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. |  |
| 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. |  |
| Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. |  |
| Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur. |  |
| Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. |  |
| Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http |  |
| Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback). |  |
| Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). |  |
| Program ma być w pełni zgodny z technologią CISCO Network Access Control. |  |
| 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. |  |
| Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania. |  |
| Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. |  |
| Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline. |  |
| W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji. |  |
| Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. |  |
| Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych. |  |
|  | Ochrona serwera plików Windows | Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016, SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012. |  |
| Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. |  |
| Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. |  |
| Wbudowana technologia do ochrony przed rootkitami i exploitami. |  |
| Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. |  |
| Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. |  |
| Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. |  |
| System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. |  |
| Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego. |  |
| Możliwość skanowania dysków sieciowych i dysków przenośnych. |  |
| Skanowanie plików spakowanych i skompresowanych. |  |
| Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi. |  |
| Aplikacja powinna wspierać mechanizm klastrowania. |  |
| Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). |  |
| Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. |  |
| Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. |  |
| Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia. |  |
| 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. |  |
| Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. |  |
| System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. |  |
| Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. |  |
| Dodanie automatycznych wyłączeń nie wymaga restartu serwera. |  |
| Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. |  |
| Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. |  |
| W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione. |  |
| Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego. |  |
| System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). |  |
| 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. |  |
| 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. |  |
| 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. |  |
| Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. |  |
| W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e‑mail. |  |
| 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. |  |
| Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo. |  |
| System antywirusowy ma być w pełni zgodny z technologią CISCO NAC. |  |
| 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. |  |
| 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. |  |
| System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. |  |
| 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. |  |
| 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. |  |
| 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. |  |
| 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). |  |
| Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. |  |
| Aplikacja musi wspierać skanowanie magazynu Hyper-V |  |
| Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów |  |
| 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). |  |
| System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). |  |
| Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. |  |
| Administracja zdalna | Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012, 2016 oraz systemach Linux. |  |
| Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). |  |
| Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL. |  |
| Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta. |  |
| Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. |  |
| Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. |  |
| Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający. |  |
| Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. |  |
| Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. |  |
| Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. |  |
| Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny. |  |
| Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym. |  |
| Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. |  |
| Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu. |  |
| Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. |  |
| Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy. |  |
| Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. |  |
| Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. |  |
| Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania. |  |
| Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. |  |
| Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. |  |
| W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania z Internetu. |  |
| Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. |  |
| Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS. |  |
| Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi. |  |
| Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. |  |
| Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej |  |
| Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji. |  |
| Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. |  |
| Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. |  |
| Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany. |  |
| Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji. |  |
| Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym. |  |
| Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. |  |
| Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. |  |
| Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów. |  |
| Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp. |  |
| Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta. |  |
| Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej. |  |
| Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku. |  |
| Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania. |  |
| Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie. |  |
| Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. |  |
| Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS. |  |
| Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego. |  |
| Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. |  |
| Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. |  |
| Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu. |  |
| Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta. |  |
| Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji. |  |
| Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty. |  |
| Serwer administracyjny musi być wyposażona w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana. |  |
| Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań. |  |
| Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar |  |

1. **Usługa wdrożenia nowej infrastruktury teleinformatycznej**

| **L.p.** | **Usługi wymagane przez Zamawiającego** | **Wartości/funkcjonalności oferowane przez Wykonawcę\*** |
| --- | --- | --- |
|  | Wykonanie we współpracy z Zamawiającym audytu istniejącej konfiguracji środowiska IT pod kątem dobrych praktyk i poprawności pracy, ze szczególnym uwzględnieniem konfiguracji kontrolerów domeny Active Directory i usług pokrewnych, serwerów aplikacyjnych, konfiguracji kopii zapasowych, adresacji IP i reguł dostępowych i skryptów. Wprowadzenie poprawek na bazie obserwacji audytowych. |  |
|  | Opracowanie projektu technicznego i harmonogramu wdrożenia w konsultacji z Działem IT Zamawiającego, w tym opracowanie scenariuszy testów akceptacyjnych. |  |
|  | Instalacja najnowszych wersji oprogramowania układowego/systemowego na dostarczonych urządzeniach, jak i na obecnie posiadanym przez Zamawiającego sprzęcie, tzn. przełącznikach sieciowych, serwerach HP DL380 G7. |  |
|  | Instalacja fizyczna dostarczonego sprzętu według wskazań Zamawiającego. |  |
|  | Konfiguracja dostarczonego przełącznika sieciowego w zakresie VLAN, STP, 802.1x Network Login, DHCP Snooping, SNMP, routing IP, Port Security. |  |
|  | Uruchomienie nowego serwera, instalacja i konfiguracja dostarczonego systemu operacyjnego Microsoft Windows Server 2012 R2/2016, uruchomienie roli Hyper-V w konsultacji z Zamawiającym. |  |
|  | Przygotowanie maszyn wirtualnych na serwerze wirtualizacyjnym, instalacja systemów operacyjnych Microsoft Windows Server 2012R2/2016. |  |
|  | Konfiguracja dwóch kontrolerów domeny Active Directory Microsoft Windows 2016 wraz z usługami pokrewnymi (DNS, DHCP). Migracja kont użytkowników (ok. 200), grup, uprawnień z istniejącej domeny Active Directory. Podłączenie wszystkich stacji roboczych (ok. 80 szt.)i serwerów do nowej domeny. Skopiowanie danych wraz z uprawnieniami na nowe serwery. Konfiguracja zasad zabezpieczeń grupy (GPO) wg dobrych praktyk i wymagań Zamawiającego. Konfiguracja serwera zasad sieciowych 802.1x zgodnie z wymaganiami Zamawiającego. |  |
|  | Migracja aplikacji zainstalowanych na serwerach aplikacyjnych (medyczne PROGMED, finansowe AXON) do nowo utworzonych maszyn wirtualnych wraz z utrzymaniem bieżącej funkcjonalności i rekonfiguracją stacji roboczych użytkowników aplikacji. |  |
|  | Przygotowanie maszyny wirtualnej i zmigrowanie serwera systemu laboratoryjnego (Centrum firmy MARCEL) wraz z utrzymaniem bieżącej funkcjonalności i rekonfiguracją stacji roboczych użytkowników aplikacji. |  |
|  | Przygotowanie maszyny wirtualnej i zmigrowanie obecnego serwera www wraz z utrzymaniem obecnego systemu zabezpieczeń. |  |
|  | Przygotowanie maszyny wirtualnej, instalacja aktualnej wersji serwera ESET RA w zwirtualizowanej postaci. Migracja ustawień i podłączenie klientów z obecnie funkcjonującego systemu Zamawiającego. |  |
|  | Montaż dysków twardych w serwerze kopii zapasowych. |  |
|  | Instalacja systemu kopii zapasowych na wskazanym przez Zamawiającego serwerze. Opracowanie polityki wykonywania kopii zapasowych i ich odzyskiwania na wypadek awarii. Skonfigurowanie zadań kopii zapasowych wszystkich uruchomionych w ramach wdrożenia maszyn wirtualnych zgodnie z wymaganiami Zamawiającego. |  |
|  | Konfiguracja zasilacza awaryjnego i jego karty zarządzającej tak, aby w przypadku awarii zasilania było możliwe automatyczne wyłączenie serwerów według wymagań Zamawiającego, oraz ich automatyczne uruchomienie w uzgodnionym czasie po awarii, jak również wysłanie wiadomości e-mail informującej o występujących zdarzeniach na wskazany adres. |  |
|  | Instalacja, konfiguracja i montaż dostarczonych stacji roboczych wraz z monitorami w miejsce sprzętu obecnie użytkowanego; przeniesienie wszystkich zgromadzonych danych i aplikacji z obecnie użytkowanego sprzętu oraz pokaz sprawności technicznej dostarczonego sprzętu i przeszkolenie pracowników Zamawiającego w zakresie obsługi i bezpiecznej eksploatacji sprzętu. |  |
|  | Instalacja dostarczonego oprogramowania na stacjach roboczych zgodnie z wymaganiami Zamawiającego. |  |
|  | Odłączenie od systemu informatycznego wszystkich zmigrowanych serwerów. |  |
|  | Przeprowadzenie testów akceptacyjnych potwierdzających zgodność wykonanych prac wdrożeniowych z wymogami Zamawiającego. |  |
|  | Opracowanie dokumentacji powdrożeniowej z całości prac. |  |
|  | Realizacja dwudniowych warszatów w siedzibie Zamawiającego przedstawiających wdrożone rozwiązanie dla administratora Zamawiającego w zakresie: wdrożonej architektury AD, scenariuszy awarii poszczególnych elementów systemu, środowiska wirtualizacyjnego, systemu kopii zapasowych. |  |

............... ………...................................................................

Data Podpis upoważnionego przedstawiciela Wykonawcy

\*wypełnia Wykonawca