Załącznik nr 5 do SWZ
(szczegółowy opis przedmiotu zamówienia)

Zestawienie zakresu dostaw sprzętu oraz usług:

1. **Stacje robocze 7szt. o minimalnych parametrach**

| Parametr | Opis funkcjonalny |
|---|---|
| **Zastosowanie** | Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, dostępu do Internetu oraz poczty elektronicznej, |
| **Matryca** | Komputer przenośny typu notebook z ekranem min. 15,6" o rozdzielczości FHD (1920 x 1080) z podświetleniem LED matryca matowa, jasność min. 220nits, kontrast 400:1 |
| **Procesor** | Procesor min. 4 rdzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 9904 punktów |
| **Pamięć RAM** | min. 8 (1x8) GB DDR4 |
| **Pamięć masowa** | min. 256 GB SSD NVMe, |
| **Karta graficzna** | Zintegrowana z procesorem |
| **Multimedia** | Dwukanałowa karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki stereo o średniej mocy min. 2x 2W, cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy.<br><br>Kamera internetowa o rozdzielczości min. HD trwale zainstalowana w obudowie matrycy, dioda informująca użytkownika o aktywnej kamerze. |
| **Bateria i zasilanie** | Czas pracy na baterii minimum 380 minut potwierdzony przeprowadzonym testem MobileMark 25 Battery Life (do oferty załączyć wydruk przeprowadzonego testu)<br><br>Zasilacz o mocy min. 65W.<br><br>Konstrukcja komputera musi umożliwiać demontaż samej baterii lub wszystkich zainstalowanych baterii, samodzielnie bez udziału serwisu w okresie gwarancyjnym. Bateria nie może być trwale zespolona z płytą główną. |
| **Obudowa** | Obudowa notebooka wzmocniona, szkielet i zawiasy notebooka wykonany z wzmacnianego metalu. |
| **BIOS** | BIOS zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i myszy.<br><br>BIOS musi umożliwiać przeprowadzenia inwentaryzacji sprzętowej poprzez wyświetlenie informacji o: wersji BIOS, numerze seryjnym i dacie produkcji komputera, wielkości, prędkości i sposobie obsadzenia zainstalowanej pamięci RAM, typie zainstalowanego procesora, |

| | |
|---|---|
| | zainstalowanym dysku twardym (pojemność, model), MAC adresie wbudowanej w płytę główną karty sieciowej.<br><br>Funkcja blokowania/odblokowania portów USB<br><br>Możliwość, ustawienia hasła dla administratora oraz użytkownika dla BIOS'u, po podaniu hasła użytkownika możliwość jedynie odczytania informacji, brak możliwości wł/wy funkcji. Hasła silne opatrzone o litery, cyfry i znaki specjalne.<br><br>Możliwość przypisania w BIOS numeru nadawanego przez Administratora. |
| **Bezpieczeństwo** | System diagnostyczny z graficzny interfejsem dostępny z poziomu BIOS lub menu BOOT'owania umożliwiający użytkownikowi przeprowadzenie wstępnej diagnostyki awarii poprzez przetestowanie: procesora, pamięci RAM, dysku, płyty głównej i wyświetlacza. Pełna funkcjonalność systemu diagnostycznego musi być dostępna również w przypadku braku lub uszkodzenia oraz sformatowania dysku twardego, braku dostępu do sieci LAN i internetu oraz nie może być realizowana przez narzędzia zewnętrzne podłączane do komputera (np. pamięć USB flash ].<br><br>Dedykowany układ szyfrujący TPM 2.0<br><br>Złącze na linkę zabezpieczającą przed kradzieżą. |
| **Certyfikaty** | Certyfikat ISO 9001 dla producenta sprzętu (załączyć do oferty)<br><br>Certyfikat ISO 50001 dla producenta sprzętu (załączyć do oferty)<br><br>Deklaracja zgodności CE (załączyć do oferty)<br><br>Certyfikat Energy Star lub TCO dla oferowanego modelu. |
| **System operacyjny** | Zainstalowany oryginalny system operacyjny Windows 11 Professional lub z możliwością downgrade'u do Win 10 lub równoważny.<br><br>Parametry równoważności:<br><br>• Pełna integracja z domeną Active Directory MS Windows (posiadaną przez Zamawiającego) opartą na serwerach Windows Server 2012<br>• Zarządzanie komputerami poprzez Zasady Grup (GPO) Active Directory MS Windows (posiadaną przez Zamawiającego), WMI.<br>• Zainstalowany system operacyjny nie wymaga aktywacji za pomocą telefonu lub Internetu.<br>• Pełna integracja z systemami VideoTel, Płatnik.<br>• Pełna obsługa ActiveX<br><br>Wszystkie w/w funkcjonalności nie mogą być realizowane z zastosowaniem wszelkiego rodzaju emulacji i wirtualizacji Microsoft Windows 10 |

| | |
|---|---|
| **Wymagania dodatkowe** | Wbudowane porty i złącza: HDMI 1.4, RJ-45 (karta sieciowa wbudowana), min. 3xUSB w tym min. 2 port USB 3.2 gen1 typ-A, czytnik kart SD 3.0, współdzielone złącze słuchawkowe stereo i złącze mikrofonowe, złącze zasilania (zasilacz nie może zajmować portów USB)<br><br>Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN 802.11AC, moduł bluetooth 4.1<br><br>Klawiatura (układ US - QWERTY) z wydzieloną klawiaturą numeryczną, touchpad z strefą przewijania w pionie, poziomie wraz z obsługą gestów, opcjonalnie z wbudowanym podświetleniem |
| **Warunki gwarancji** | Min. 3-letnia gwarancja producenta świadczona na miejscu u klienta<br><br>Czas reakcji serwisu - do końca następnego dnia roboczego. Dedykowany portal producenta do zgłaszania awarii lub usterek, możliwość samodzielnego zamawiania zamiennych komponentów oraz sprawdzenie okresu gwarancji, fabrycznej konfiguracji.<br><br>Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. |

**2. Skaner dokumentów – 1 szt.**

| Parametr | Opis funkcjonalny |
|---|---|
| **Typ skanera (obudowa)** | Kompaktowy skaner A4 z automatycznym podajnikiem dokumentów (ADF) |
| **Sposoby skanowania** | Skanowanie jednostronne<br>Skanowanie dwustronne w jednym przebiegu<br>Prosta ścieżka podawania papieru zapewniająca prawidłowe układanie dokumentów po zeskanowaniu na tacy odbiornika |
| **Automatyczny podajnik dokumentów (ADF)** | O pojemności co najmniej 100 arkuszy A4 (80 g/m$^2$) z możliwością regulacji bocznych prowadnic podajnika |
| **Obsługiwane formaty (nie złożone na pół)** | Minimum w zakresie A4, A5, A6, B5, B6<br>Minimalny rozmiar: 50 x 50 mm<br>Maksymalny rozmiar: 216 x 355 mm |
| **Obsługa długich dokumentów** | do 6 m |
| **Gramatura obsługiwanych dokumentów w trybie podawania automatycznego bez korzystania z dodatkowych akcesoriów** | 20 – 460 g/m$^2$ |
| **Obsługa niestandardowych nośników** | Karty plastikowe oraz ID do grubości 1.4mm (w tym tłoczone), paszporty oraz broszury do grubości 5 mm (np. paszport) |
| **Detekcja podwójnych pobrań** | Co najmniej jeden czujnik ultradźwiękowy z funkcją automatycznego zachowania obrazu dla umyślnie nałożonych obiektów (takich jak przyklejone notatki lub przymocowane taśmą paragony) zgodnie z ustawionym wzorcem |
| **Ochrona skanowanych dokumentów** | Ochrona dokumentów w oparciu o detekcję przekosu obrazu. |
| **Szybkość skanowania (dla dokumentów A4 przy 200 oraz 300 dpi w trybach mono i kolor)** | Minimum 45 arkuszy/min., 100 obrazów/min |
| **Typowe dzienne obciążenie skanera** | minimum do 7 500 arkuszy (kartek) |
| **Układ optyczny (przetwornik obrazu)** | Wykonany w technologii CCD (Charge Coupled Device) lub CIS (Contact Image Sensor) – minimum przetwornik w skanerze ADF - 1 z przodu, 1 z tyłu |
| **Optyczna rozdzielczość skanowania** | optyczna 600 dpi, sterownik 1200 dpi |
| **Wyjściowa rozdzielczość skanowania** | 60-600 dpi z możliwością skokowej regulacji co 1 dpi |
| **Tryby koloru skanowania** | Monochromatyczny, odcienie szarości, kolor |
| **Obsługiwane systemy operacyjne** | Windows 11, Windows 10, Windows Server 2022, Windows Server 2019, Windows Server 2016 |

| | |
|---|---|
| **Interfejsy komunikacyjne** | Minimum USB 3.2 Gen 1 oraz Ethernet 10BASE-T/100BASE-TX/1000BASE-T (wszystkie interfejsy fabrycznie zintegrowane w urządzeniu) |
| **Obsługiwane sterowniki** | Zgodne ze standardem TWAIN oraz ISIS |
| **Funkcje poprawy jakości skanów** | Obsługa poniższych funkcjonalności dla zarówno dla standardu TWAIN oraz ISIS:<br>1) automatyczna poprawa jakości skanowanych dokumentów<br>2) automatyczne prostowanie i orientacja obrazu<br>3) automatyczne przycinanie do oryginalnego rozmiaru dokumentu<br>4) automatyczne usuwanie niezadrukowanych stron<br>5) automatyczna detekcja koloru<br>6) automatyczna naprawa uszkodzonych lub zagiętych krawędzi dokumentu<br>7) interaktywna regulacja koloru, jasności i kontrastu bez konieczności ponownego skanowania<br>8) skanowanie wielostrumieniowe w jednym przebiegu z możliwością wyboru dowolnej kombinacji trybów koloru<br>9) łączenie i dzielenie obrazów<br>10) redukcja pionowych smug powstających na wskutek zabrudzenia<br>11) wypełnianie otworów w obrazie |
| **Funkcje dołączonego oprogramowania obsługującego standardy TWAIN oraz ISIS** | Detekcja i separacja na podstawie kodów kreskowych typu 3z9, ITF, EAN128, NW7, separacja dokumentów za pomocą niezadrukowanej kartki, odczytaną wartością ze strefy OCR, tzw. "patch code" (typ 1, 2, 3, 4, T) oraz na podstawie układu formularza.<br>Automatyczne nazewnictwo plików za pomocą kodów kreskowych i wartości odczytanej ze strefy OCR z tworzeniem wielopoziomowej struktury katalogów.<br>Podświetlanie pustych stron i sygnalizacja obrazów o niepewnej jakości w interfejsie użytkownika.<br>Obsługiwane formaty plików wyjściowych PDF, PDF/A, PDF przeszukiwalny, JPEG, JPEG2000, XLSX, DOCX, PPTX, TIFF, MTIFF, PNG, BMP.<br>Zapis plików wyjściowych dla poszczególnych strumieni obrazu do oddzielnych folderów na dysku z możliwością wyboru różnych rozszerzeń (formatów) plików, automatyczny odczyt informacji ze stref MRZ dla paszportów oraz dowodów osobistych i zapis do metadanych w formatach XML lub CSV.<br>Skanowanie bez konieczności podłączania skanera do lokalnej stacji roboczej i instalacji sterowników |
| **Funkcje dołączonego oprogramowania do zarządzania i monitoringu** | Działające w strukturze klient-serwer (dwukierunkowa komunikacja wyłącznie w obrębie lokalnej sieci LAN) umożliwiające scentralizowane zarządzanie i monitoring oferowanych skanerów w tym: zdalna aktualizacja sterowników, oprogramowania sprzętowego (firmware) i zdalna konfiguracja ustawień skanerów (na wielu stacjach jednocześnie), generowanie alertów o stanie skanera (błędy) i potrzebie wymiany elementów eksploatacyjnych. |

| | |
|---|---|
| **Ergonomia pracy** | Skaner ważący nie więcej niż 3.6 kg o powierzchni podstawy urządzenia mniejszej niż 0,052m$^2$<br>Możliwość obsługi procesu skanowania z przycisków znajdujących się na skanerze.<br>Maksymalny pobór mocy w trybie pracy mniejszy niż 22 W.<br>Możliwość integracji skanera z modułem drukującym realizującym automatyczny nadruk daty skanowania dokumentu po zeskanowaniu |
| **Materiały eksploatacyjne** | Materiały eksploatacyjne zainstalowane w skanerze pozwalające na zeskanowanie do 200 000 arkuszy |
| **Normy i regulacje** | Urządzenie posiada oznakowanie CE potwierdzające zgodność z wymaganiami UE nałożonymi na producenta, spełniające kryteria Energy Star oraz RoHS |

### 3. Usługi informatyczne w zakresie wdrożenia Portalu eUrzad

Wykonawca musi dostarczyć portal eUrząd zintegrowany z posiadanym przez Zamawiającego oprogramowaniem dziedzinowym firmy INFO-SYSTEM, o funkcyjnościach:

a) portal musi udostępniać komplet informacji o podatkach i opłatach lokalnych, a także dzierżaw, użytkowania wieczystego i zużycia wody.
b) Portal musi prezentować informację sposobie naliczenia podatku lub opłaty, o wysokości poszczególnych rat i terminie ich płatności, a także o istniejących zaległościach i należnych odsetkach.
c) Dane muszą być pobierane bezpośrednio z bazy danych urzędu, i być identyczne z tymi, którymi dysponują urzędnicy.
d) Portal musi być zintegrowany z usługami szybkich płatności online Blue Media oraz PayByNet, które pozwalają na uregulowanie wybranych należności.
e) Portal musi być zintegrowany z Krajowym Węzłem Identyfikacji Elektronicznej (KWIE / login.gov.pl) pozwalającym podatnikowi na zalogowanie do portalu.

Wykonawca dostarczy i wdroży rozszerzenie do posiadanego przez Wykonawcę systemu dziedzinowego firmy INFO-SYSTEM o nazwie „Uniwersalny Program Księgujący” który umożliwi:
a) rozliczenie wpłat dokonanych drogą elektroniczną
b) importowanie elektronicznych wyciągów bankowych
c) rejestracja wpłat wraz z należnymi odsetkami i kosztami na kontach podatników i płatników
d) wydruki kontrolne i sprawozdawcze

Dodatkowo należy skonfigurować i wdrożyć indywidualne konta bankowe dla wszystkich podatników w Gminie Kąkolewnica.

**4. Zakup serwera 1 szt.**

| Parametr | Opis funkcjonalny |
|---|---|
| **Obudowa** | serwerowa do montażu w szafie RACK 19" wraz z wysuwanymi szynami dedykowanymi do tego urządzenia przez producenta serwera.<br>Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.<br>Obudowa powinna posiadać możliwość instalacji interfejsu NFC do połączenia z aplikacją zarządzającą serwerem na telefonie. Aplikacja zarządzająca powinna być dostępna na Android i iOS obudowa powinna posiadać dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera.<br>Wentylatory powinny mieć możliwość wymiany podczas pracy systemu |
| **Zasilacze** | zestaw redundantnych zasilaczy o mocy co najmniej 600W każdy |
| **Płyta główna** | Płyta główna obsługująca co najmniej dwa procesory i co najmniej 16 slotów na pamięć<br>taktowaną przynajmniej z częstotliwością 3200MT/s przy użyciu odpowiednich procesorów.<br>Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Zintegrowany z płytą główną moduł TPM w wersji co najmniej 2.0 |
| **Procesor** | Procesory typu skalowalnego posiadające co najmniej 16 rdzeni działający co najmniej z częstotliwością 2.4GHz i dające w teście Passmark dostępnym na stronie https://www.cpubenchmark.net/ wynik nie mniejszy niż 29300 |
| **Pamięć RAM** | 128 GB pamięci RAM w modułach 32GB RDIMM przygotowanych na działanie z częstotliwością co najmniej 3200MT/s |
| **Dyski** | Miejsce na co najmniej 8 dysków w rozmiarze 2.5" wymienialne bez wyłączania systemu. Serwer ma mieć przewidzianą przez producenta możliwość dodania modułu pozwalającego na startowanie systemu z kart SD lub dysków M.2 skonfigurowanych w RAID1 nie zajmujących slotów na dyski.<br>Serwer powinien posiadać kontroler RAID umożliwiający konfigurację RAID 0,1,5,10,50,6<br>posiadający co najmniej 8GB pamięci cache zabezpieczonej przed awarią prądu.<br>W serwerze powinny być zainstalowane co najmniej cztery dyski co najmniej 1.92 SSD vSAS |
| **Karta sieciowa** | Zintegrowana na płycie głównej dwuportowa karta sieciowa 1GB |
| **Karta zarządzająca** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet<br>umożliwiająca:<br>- zdalny dostęp do graficznego interfejsu Web karty zarządzającej<br>- szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika<br>- możliwość podmontowania zdalnych wirtualnych napędów<br>- wirtualną konsolę z dostępem do myszy, klawiatury<br>- wsparcie dla IPv6 - wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH |

| | |
|---|---|
| | - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.<br>- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer<br>- integracja z Active Directory<br>- możliwość obsługi przez ośmiu administratorów jednocześnie<br>- Wsparcie dla automatycznej rejestracji DNS - wsparcie dla LLDP<br>- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej<br>- możliwość podłączenia lokalnego poprzez złącze RS-232.<br>- możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy.<br>- Monitorowanie zużycia dysków SSD<br>- możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,<br>- Automatyczne zgłaszanie alertów do centrum serwisowego producenta<br>- Automatyczne update firmware dla wszystkich komponentów serwera<br>- Możliwość przywrócenia poprzednich wersji firmware<br>- Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON<br>- Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych<br>- Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.<br>Serwer musi posiadać deklarację CE. |
| **Oprogramowanie** | Licencja Windows Server 2022 Standard zapewniająca pokrycie na wszystkie rdzenie procesora.<br><br>Licencje dostępowe 35 sztuk Windows Server 2022 User CALs (Standard or Datacenter) |
| **Warunki gwarancji** | 3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia - zgłoszenia przyjmowane 7 dni w tygodniu w trybie 24/7. Gwarancja musi obejmować całość rozwiązania nie powinno być tak aby jakaś część tego rozwiązania nie podlegała gwarancji. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. Producent musi dawać możliwość rozszerzenia gwarancji do 7-miu lat<br>W przypadku naprawy dysku - uszkodzony dysk zostaje u klienta.<br>Podczas trwania gwarancji producent powinien zapewnić narzędzia i procesy do proaktywnej oceny stanu technicznego oraz automatycznego zgłaszania usterek bez ingerencji człowieka.<br>Powinna być możliwość skorzystania z pomocy wsparcia producenta za pomocą komunikatora np. messenger, teams, WhatsApp.<br>Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. |

| | |
|---|---|
| | Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera<br>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

**5. Drukarkę kodów kreskowych 1 szt.**

| Parametr | Opis funkcjonalny |
|---|---|
| **metoda druku** | termiczna/termotransferowa |
| **rozdzielczość** | 203 dpi |
| **szerokość druku** | do 104mm |
| **prędkość druku** | do 127mm/s |
| **pamięć zainstalowana** | 4MB flash; 8MB SDRAM |
| **porty komunikacji** | USB, RS232, Parallel - LPT |
| **język oprogramowania** | EPL i ZPL |
| **temperatura pracy** | 4,4°C do 41°C |
| **gwarancja** | 12 miesięcy |

**6. Czytnik kodów kreskowych - Zgodnie z wymaganiami systemu EZD PUW dotyczącymi punktów kancelaryjnych 2 szt.**

| Parametr | Opis funkcjonalny |
|---|---|
| **Obsługiwane kody kreskowe** | 1D |
| **Technologia odczytu** | Linear Imager |
| **Maks. odległość odczytu [cm]** | 78.7 |
| **Wymagany kontrast kodu [%]** | 15 |
| **Rozdzielczość skanera** | 3 |
| **Dostępne interfejsy** | USB, KBW (PS/2), RS232 |
| **Dopuszczalna wilgotność otoczenia [%]** | od 5% do 85% |
| **Norma odporności** | IP53 |
| **Bezpieczny upadek na twardą pow. [m]** | 1,5 |
| **Szybkość skanowania** | 547 operacji skanowania na sekundę |
| **Źródło światła** | LED klasy 1 – 617 nm |
| **Min. kontrast druku** | 15% MRD |
| **Liczba odczytów za jednym ładowaniem** | Do 57 000 |
| **Gwarancja producenta** | 36 miesiecy |

## 7. Usługi doradcze w zakresie integracji

Celem prac jest przygotowanie środowiska teleinformatycznego, na potrzeby realizacji e-usług publicznych, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie.

Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa i wymagań Zamawiającego.

Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia. Wraz z oprogramowaniem należy dostarczyć Serwerowy System operacyjny na którym to należy zainstalować w/w oprogramowanie. Dodatkowo należy zainstalować agentów oprogramowania audytywnego na 40 stacjach roboczych.

Zamówienie dotyczy usługi polegającej na kompletnej migracji domeny Active Directory na nowy serwer dostarczany w zamówieniu.

Zamawiana usługa obejmuje:

1. Instalacja na nowym serwerze systemu operacyjnego Windows Server wraz ze wszystkimi aktualizacjami
2. Utworzenie nowej maszyny wirtualnej na posiadanym przez zamawiającego serwerze oraz instalacja na nim systemu operacyjnego Windows Server wraz ze wszystkimi aktualizacjami
3. Instalacja domeny Active Directory wraz z pełną jej konfiguracją według wymagań zamawiającego na serwerze wirtualnym Windows Server
4. Instalacja oraz konfiguracja serwisów niezbędnych oraz uzupełniających funkcjonalność Active Directory: DNS, DHCP, Print Server, File Server, WSUS
5. Utworzenie „jednostek organizacyjnych” w strukturze AD - odzwierciedlających typy obiektów administracyjnych wg wymogów zamawiającego
6. Przygotowanie „zasad grupy” (polityk GPO) dla każdej z jednostek organizacyjnych. Polityki GPO prócz ustawienia podstawowych funkcjonalności muszą uwzględniać:
    a. Wymagania złożoności haseł użytkowników, w tym ich długość, ważność, użyte znaki
    b. Blokadę konta przy określonej przez zamawiającego liczbie prób nieprawidłowego logowania
    c. Udostępnianie plików i drukarek w sieci
    d. Automatyczne aktualizacje systemów klienckich pobierane z wewnętrznego serwera WSUS
    e. Dostęp do systemów klienckich i serwerów poprzez zdalny pulpit według wymagań zamawiającego
    f. Przekierowanie folderów określonych przez zamawiającego ze stacji roboczych na zasób dyskowy kontrolera domeny
    g. Profile mobilne dla użytkowników określonych przez zamawiającego
7. Podłączenie określonych przez zamawiającego stacji roboczych do nowo utworzonej domeny. Podłączenie powinno uwzględnić zarówno konfigurację stacji roboczej do pracy w domenie jak również przeniesienie danych użytkowników do odpowiednich profili domenowych

8. Weryfikacja przeprowadzonej migracji stacji roboczych poprzez wielokrotne próby logowania się do domeny różnych użytkowników z różnych stacji roboczych
9. Instalacja i konfiguracja domeny Active Directory na nowo dostarczonym serwerze fizycznym w taki sposób, aby stanowił on zapasowy kontroler domeny. W przypadku awarii pierwszego kontrolera domeny – automatycznie przejmie on jego funkcje do czasu przywrócenia pełnej funkcjonalności pierwszego. Częstotliwość synchronizacji obydwu serwerów nie powinna być dłuższa niż 15 minut
10. Sprawdzenie poprawności działania zapasowego kontrolera domeny poprzez symulację awarii pierwszego. Symulacja odbywać się będzie na zasadzie odłączenia serwera od sieci LAN.
11. Przeszkolenie informatyka urzędu z obsługi domeny Active Directory (szkolenie trwające nie mniej niż 8 godzin)
12. Przygotowanie kompletnej dokumentacji powdrożeniowej.
13. Wdrożenie oraz szkolenie przeprowadzone muszą być przez inżyniera certyfikowanego MCTS (Microsoft Certified Technology Specjalist) o specjalności: Windows Server Active Directory Configuration.
14. Po instalacji Wykonawca zapewni wsparcie techniczne do wykonanej usługi na 12 miesięcy.

Usługa wdrożenia nowego środowiska wirtualnego oraz przeniesienie do niego obecnych serwerów fizycznych i wirtualnych wraz z zachowaniem całej funkcjonalności i struktury sieciowej.

Wymagania dotyczące wdrożenia:

Zaznacza się, iż wykonywane prace nie mogą wpływać na pracę Urzędu oraz nie mogą powodować przestojów w pracy. Przełączenie serwerów musi być przeprowadzone dnia poprzedzającego dzień wolny od pracy (piątek, sobota).

Zakres prac:

1. Instalacja dostarczonego serwera w szafie RACK oraz przygotowanie do pracy (aktualizacja i konfiguracja BIOS itp.)
2. Instalacja platformy wirtualizacyjnej na nowym serwerze
3. Instalacja i konfiguracja na wybranym przez Zamawiającego komputerze platformy zarządzającej środowiskiem wirtualnym.
4. Konfiguracja środowiska wirtualnego – w tym dokładne odzwierciedlenie fizycznej sieci serwerowej LAN w nowym środowisku wirtualnym
5. Migracja posiadanych serwerów fizycznych i wirtualnych do środowiska wirtualnego. Wymaga się, aby przed migracją wykonać pełną kopię zapasową serwera na bezpieczne urządzenie dostarczone przez Wykonawcę (przynajmniej RAID 1). Po migracji i powodzeniu testów w nowym środowisku – kopia zapasowa musi być usunięta dedykowanym do tego oprogramowaniem – tak aby nie możliwe było późniejsze odtworzenie danych.
6. Utworzenie nowej maszyny wirtualnej z systemem Windows Server 2021 Standard wraz z oprogramowaniem Microsoft SQL. Konfiguracja serwera pod pracę z bazą danych oprogramowania „Płatnik”
7. Migracja bazy danych oprogramowania „Płatnik” z obecnego serwera do jego nowej instancji wirtualnej. Przygotowanie i konfiguracja całego środowiska SQL – tak aby migracja dla pracowników Urzędu nie powodowała konieczności zmiany konfiguracji aplikacji na ich stacjach roboczych
8. Testy wszystkich serwerów. Każda funkcjonalność powinna być przetestowana przynajmniej z kilku stacji roboczych.

9. Szkolenie pracownika Zamawiającego z instalacji i konfiguracji środowiska wirtualizacyjnego trwające nie mniej niż 2 x 8 godzin.
10. Wdrożenie oraz szkolenie muszą być przeprowadzone przez inżyniera certyfikowanego przez producenta oferowanego oprogramowania wirtualizacyjnego.
11. Po instalacji Wykonawca zapewni wsparcie techniczne na min. 12 miesięcy, maksymalnie 4-8 godzinny czas reakcji od zgłoszenia usterki, awarii. Naprawa musi odbyć się w ciągu maksymalnie 48 godzin od zgłoszenia awarii

Opis czynności do wykonania podczas wdrożenia urządzenia brzegowego:

1) Analiza dotychczasowego środowiska sieciowego bezpośrednio związana z posiadanym przez Urząd urządzeniem brzegowym obejmująca sprawdzenie i usunięcie ewentualnych nieprawidłowości
2) Przeprowadzenie pomiaru przepustowości węzłów sieci doprowadzonych bezpośrednio do urządzenia i ewentualne usunięcie nie w pełni sprawnych połączeń
3) Aktualizacja oprogramowania urządzenia do najnowszej wersji dostępnej w dniu przeprowadzania usługi
4) Omówienie dotychczas stosowanych polityk bezpieczeństwa i skonfrontowanie ich z nowymi potrzebami
5) Przygotowanie nowych lub aktualizacja dotychczas stosowanych polityk bezpieczeństwa
6) Konfiguracja i zastosowanie modułów UTM
7) Wykonanie kopii zapasowej ustawień urządzenia
8) Testy przeciążeniowe urządzenia zarówno na samym firewall’u jak i na poszczególnych modułach UTM
9) Inżynier posiadający certyfikat NFS 4 będzie dostępny do pomocy i konsultacji przez cały okres trwania umowy.

W ramach usługi, następnego dnia po wykonaniu czynności konfiguracyjnych zostanie przeprowadzone ośmiogodzinne szkolenie informatyka z obsługi nowego oprogramowania na urządzeniu - kładące główny nacisk na nowe podejście do tematu ochrony sieci – NGFW (Next Generation FireWall) jak i na nowe funkcjonalności które zostały zaimplementowane w nowym oprogramowaniu.

## 8. Szkolenie on-line dla pracowników urzędu w zakresie obsługi zakupionego sprzętu i oprogramowania

Wykonawca w okresie wdrożenia przeprowadzi szkolenia dla Administratora systemu, łącznie w wymiarze 16 godzin szkolenia. Szkoleniem zostaną objęte osoby wskazane przez Zamawiającego z zakresie dostarczonego rozwiązania teleinformatycznego - dostarczonego sprzętu i oprogramowania oraz wykonanej konfiguracji systemu.

Celem szkolenia administratora będzie zapoznanie się z systemem informatycznym, poznanie poszczególnych funkcji i modułów oraz nauka jego obsługi w praktyce.

Wykonawca zobowiązany jest do przeprowadzenia szkoleń w formie instruktażu stanowiskowego dla personelu w podziale na role w Systemie. Taki sposób przeprowadzenia szkoleń jest najbardziej efektywny i umożliwi personelowi rozpoczęcie pracy zaraz po zakończeniu szkolenia.

**9. Rozbudowę zabezpieczeń logicznych (firewall, systemy IDS, IPS) – Router 1 szt.**

| Parametr | Opis funkcjonalny |
|---|---|
| **Wymagania ogólne** | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.<br><br>System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. |
| **Wsparcie dla IPv4 oraz IPv6 w zakresie:** | ● Firewall.<br>● Ochrony w warstwie aplikacji.<br>● Protokołów routingu dynamicznego. |
| **Redundancja** | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. |
| **Monitoring** | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.<br><br>Monitoring stanu realizowanych połączeń VPN. |
| **Interfejsy** | ● 10 portów Gigabit Ethernet RJ-45.<br>● 2 gniazdami SFP 1 Gbps.<br>● w ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. |
| **Wydajność** | 1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.<br>2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.<br>3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.<br>4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.<br>5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. |

| | |
|---|---|
| | 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.<br>7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps. |
| **Funkcje bezpieczeństwa** | 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.<br>2. Kontrola Aplikacji.<br>3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.<br>4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.<br>5. Ochrona przed atakami - Intrusion Prevention System.<br>6. Kontrola stron WWW.<br>7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.<br>8. Zarządzanie pasmem (QoS, Traffic shaping).<br>9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).<br>10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.<br>11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.<br>12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. |
| **Polityki, Firewall** | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.<br>2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:<br>3. Translację jeden do jeden oraz jeden do wielu.<br>4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.<br>5. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.<br>6. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. |
| **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:<br>● Wsparcie dla IKE v1 oraz v2. |

| | |
|---|---|
| | ● Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).<br>● Obsługa protokołu Diffie-Hellman grup 19 i 20.<br>● Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.<br>● Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.<br>● Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.<br>● Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.<br>● Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.<br>● Mechanizm „Split tunneling” dla połączeń Client-to-Site.<br>2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:<br>● Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.<br>● Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.<br>● Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |
| **Routing i obsługa łączy WAN** | 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:<br>● Routingu statycznego.<br>● Policy Based Routingu.<br>● Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |
| **Zarządzanie pasmem** | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.<br>2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.<br>3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |
| **Ochrona przed malware** | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).<br>2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.<br>3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).<br>4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu |

| | |
|---|---|
| | Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.<br>5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.<br>6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. |
| **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.<br>2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.<br>3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.<br>5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.<br>6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.<br>7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |
| **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.<br>2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.<br>4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.<br>5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |
| **Kontrola WWW** | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.<br>2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. |

| | |
|---|---|
| | 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.<br>4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.<br>5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.<br>6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.<br>7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |
| **Zarządzanie** | 1. wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.<br>2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.<br>3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.<br>4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.<br>5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.<br>6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.<br>7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |
| **Logowanie** | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.<br>2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona |

| | |
|---|---|
| | możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.<br>3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.<br>4. Musi istnieć możliwość logowania do serwera SYSLOG. |
| **Certyfikaty** | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:<br>● ICSA lub EAL4 dla funkcji Firewall. |
| **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:<br>a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy. |
| **Gwarancja oraz wsparcie** | 1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.<br>2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań |

## 10. Zakup specjalistycznego oprogramowania do zbierania logów i analizy sieci

Wykonawca dostarczy oprogramowanie wraz z licencją na nieograniczoną ilość urządzeń monitorowanych umożliwiające:

a) wykrywanie anomalii w działaniu urządzeń
b) monitorowanie wskaźników wilgotności i temperatury
c) obsługa szyfrowania AES, DES i 3DES dla protokołu SNMPv3
d) skanowanie sieci, wykrywanie urządzeń i serwisów TCP/IP interaktywne mapy sieci, mapy użytkownika, oddziałów, mapy inteligentne
e) jednoczesna praca wielu administratorów, zarządzanie uprawnieniami, dzienniki dostępu
f) serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.)
g) liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp.
h) możliwość nakładania na urządzenie liczników wydajności wg szablonu (wzorca) monitorowanie i zarządzanie maszynami wirtualnymi Vmware
i) działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń
j) liczniki SNMP v1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne)
k) kompilator plików MIB
l) obsługa pułapek SNMP
m) routery i switche: mapowanie portów
n) obsługa komunikatów syslog
o) alarmy zdarzenie - akcja
p) powiadomienia (pulpitowe, e-mail, SMS) oraz akcje korekcyjne (uruchomienie programu, restart komputera itp.)
q) raporty (dla urządzenia, oddziału, lub całej sieci)

## 11. Rozbudowa sieci LAN

Przedmiotem opracowania jest rozbudowa sieci okablowania logicznego, w budynku Urzędu Gminy w Kąkolewnicy.

Zakres szczegółowy prac obejmuje:

- budowę instalacji komputerowej kat.6, od punktu dystrybucyjnego do punktów abonenckich PL – 4x (2xRJ45)
- montaż punktów logiczne 2xRJ45 - 4 szt.
- montaż paneli rozdzielczych 24xRJ 45 – 1 kpl.
- montaż paneli porządkujących – 1 kpl.
- montaż listew instalacyjnych KIO 85x50 – 12m
- układanie kabla F/UTP LSOH kat. 6 - 280m

Wszystkie kable okablowania poziomego oznaczyć w sposób umożliwiający ich łatwą identyfikację. Oznaczenia nanieść na zewnętrznej otulinie PCV kabli, na obu ich końcach oraz na panelu krosowym i gniazdach odbiorczych. Sieć logiczna ma zostać zrealizowana w standardzie Ethernet, umożliwiające transmisję sygnałów w oparciu o określone protokoły i aplikacje (np.: 100 Base-TX, ATM 155Mb/s, 1000 Base-T). Przy budowie sieci należy stosować gniazda typu RJ 45 wyposażone w złącza szczelinowe. Poszczególne linie okablowania poziomego należy zaszyć w gniazdach odbiorczych. Przewody zacisnąć w złączach szczelinowych listewek przy pomocy narzędzia zaciskowego lub bez narzędziowo, o ile technologia tego nie wymaga. Pojedyncze kable zaszyć w złączach szczelinowych według znaczników na gniazdach (kolory przewodów muszą pokrywać się ze znacznikami w gniazdach).

**12. Zakup zarządzanych urządzeń sieciowych typu switch – 3 szt.**

| Parametr | Opis funkcjonalny |
|---|---|
| **Standardy** | IEEE 802.3 10BASE-T<br>IEEE 802.3u 100BASE-TX<br>IEEE 802.3ab 1000BASE-T<br>802.3ae 10 GbE<br>IEEE 802.3x Flow Control dla trybu pełnego dupleksu<br>Automatyczna negocjacja prędkości połączeń |
| **Ilość portów** | 24x gigabitowe porty Ethernet<br>4x SFP+ (10 Gb/s)<br>Tryby dostępne do 10/100 Mb/s i 1000 Mb/s |
| **Przepustowość przełączania** | 128 Gb/s |
| **Tablica adresów MAC** | 16000 wejść na urządzenie |
| **Prędkość przekazywania 64 bajtowych pakietów** | 95,24 Mpps |
| **Diody LED** | Power/Stacking ID/Fan Error (na urządzenie),<br>Link/Activity/Speed (na każdy port 10G SFP+) |
| **Certyfikaty** | CE, FCC, C-Tick, VCCI, BSMI, CCC |
| **Obsługa VLAN** | 802.Q Tagged VLAN 4K grup VLAN Konfigurowalne VID: 0 - 4094 GVRP Asymetryczny VLAN Auto Voice VLAN Auto Surveillance VLAN 2.0 VLAN w oparciu o MAC VLAN w oparciu o protokół |
| **Zarzadzanie Layer 2** | Tablica adresów MAC: do 16384 Flow Control 802.3x Flow Control HOL Blocking Prevention. Jumbo Frame - do 9216 bajtów IGMP Snooping IGMP v1/v2 Snooping; IGMP v3 awareness; do 512 grup IGMP; 128 statycznych adresów multicast; IGMP per VLAN; IGMP Snooping Querier; host-based IGMP Snooping Fast Leave. MLD Snooping MLD v1/v2 awareness; 512 grup; 128 statycznych adresów multicast; MLD Snooping per VLAN; host-based MLD Fast Leave; MLD Snooping Querier. Wykrywanie pętli (loopback detection) v4.07 802.3ad Agregacja połączeń (do 32 grup na urządzenie / 8 portów na grupę) Port Mirroring do 4 grup; one-to-one, many-to-one. Filtrowanie multicast ERPS (Ethernet Ring Protection Switching) |
| **Kontrola dostępu** | Kontrola w oparciu o: priorytet 802.1p; VLAN; adres MAC; rodzaj Ethernet; adres IP; DSCP; rodzaj protokołu; nr portu TCP/UDP; IPv6 DSCP; IPv6 flow label. ACL akcje Maks. 256 list kontroli dostępu 768 reguł Pojedyncze porty lub wiele portów na regułę ACL w oparciu o czas Statystyki ACL |
| **Zabezpieczenia** | Zabezpieczenie portu (port security) do 128 adresów MAC na port Broadcast / multicast / unicast storm control Dynamic ARP inspection D-Link Safeguard Engine DHCP Server Screening ARP Spoofing Prevention Maks. 64 wejścia SSH wsparcie v2; wsparcie IPv4 / IPv6. Ochrona przed atakami BPDU Ochrona przed atakami DoS SSL Wspiera wersje v1/v2/v3; wspiera IPv4 / IPv6. Segmentacja ruchu IP-MAC-Port Binding DHCP Snooping; IP Source Guard; Dynamic ARP Inspection; IPv6 DHCP Guard; IPv6 RA Guard; IPv6 Snooping; IPv6 Source Guard; IPv6 ND Inspection. |

| | |
|---|---|
| **Zarządzanie** | CLI (Command Line Interface) Serwer Telnet Klient TFTP IPv6 Nieghbor Discovery SNMP (v1, v2c, v3) SNMP Trap System Log (do 10000 wpisów) Komenda Debug Dual images Klient DHCP Wsparcie D-Link Network Assistant SNTP ICMPv6 IPv4 / IPv6 dual stack Automatyczna konfiguracja DHCP RMON v1 LLDP, LLDP-MED DHCP Relay Interfejs graficzny Web (GUI) Klient TFTP NTP Klient Telnet (wspiera tylko CLI) |
| **Gwarancja** | Okres gwarancji m.in. 24 miesiecy |

## 13. Zakup specjalistycznego oprogramowania – antywirusowego

Należy dostarczyć 40 licencji na oprogramowanie o minimalnych wymaganiach:

1. Rozwiązanie musi wspierać systemy operacyjne Windows 10,11 oraz Windows Server 2019
2. Rozwiązanie musi posiadać wsparcie dla dystrybucji 64-bitowych.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
6. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
7. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
8. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
9. Rozwiązanie musi posiadać dwa wbudowane 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.
14. Rozwiązanie musi posiadać możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
15. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Administrator musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
16. Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
17. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
18. Aktualizacje silnika detekcji muszą być dostępne z Internetu, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
19. Rozwiązanie musi posiadać możliwość pobierania aktualizacji za pośrednictwem serwera proxy.
20. Rozwiązanie musi być wyposażone tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi umożliwiać importowanie oraz eksportowanie ustawień lokalnie oraz zdalnie za pomocą dedykowanego narzędzia.
22. Wsparcie techniczne dla rozwiązania musi być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Do zarządzania oprogramowaniem konieczna jest konsola administracyjna o minimalnych wymaganiach:

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019 oraz systemach Linux.

2. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.
3. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
4. Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.
5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
6. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
7. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
8. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy.
9. Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.
10. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.
11. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.
12. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
13. Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym.
14. Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
15. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
16. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
17. Serwer administracyjny musi posiadać wsparcie dla „VDI” oraz „Golden Master Image”.
18. Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów.
19. Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy.
20. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
23. Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
24. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.
25. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
26. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
27. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
28. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio,

drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows z możliwością jego odinstalowania.

29. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
30. Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.
31. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
32. Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.
33. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
34. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
35. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
36. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.
37. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.
38. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
39. 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.
40. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.
41. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
42. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
43. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
44. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
45. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
46. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.

47. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
48. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.
49. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.
50. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
51. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.
52. Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta.
53. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
54. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
55. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
56. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.
57. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
58. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.
59. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF lub CSV.
60. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
61. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.
62. Powiadomienia mailowe mają być wysyłane w formacie HTML.
63. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.
64. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
65. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
66. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
67. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.
68. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.
69. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
70. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.

71. Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.
72. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
73. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.
74. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.
75. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.
76. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.
77. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.
78. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.
79. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.
80. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych.
81. Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault).
82. Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk.
83. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal).
84. Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.

**14. Zakup specjalistycznego oprogramowania do inwentaryzacji i zarządzania stacjami roboczymi**

Należy dostarczyć 40 licencji na oprogramowanie o minimalnych wymaganiach:

1. Zdalne wykrywanie komputerów w sieci
2. Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o aktualizacji
3. Wykorzystanie Active Directory do tworzenia drzewa sieci
4. Możliwość pogrupowania wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów)
5. Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc.)
6. Możliwość tworzenie własnych typów elementów wyposażenia
7. Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe)
8. Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.)
9. Możliwość wiązania elementów wyposażenia w zestawy
10. Możliwość użycia makrodefinicji w celu spersonalizowania nazw elementów w drzewku wyposażenia.
11. Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach
12. Możliwość podpinania dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików
13. Możliwość przypisania sprzętu do konkretnych osób
14. Możliwość przypisania sprzętu do dowolnej lokalizacji
15. Możliwość definiowania własnych, dowolnych atrybutów sprzętu
16. Możliwość przypisania stałego atrybut COA, który będzie uwzględniany na raportach wyposażenia i audytu
17. Możliwość definiowania szczegółowych informacji finansowych
18. Definiowanie bazy dostawców sprzętu i oprogramowania
19. Ewidencja zdarzeń serwisowych
20. Informacja na temat pojemności dysków twardych oraz wolnego miejsca
21. Generowanie protokołów przekazania\zwrotu\utylizacji sprzętu.
22. Możliwość generowania Karty informacyjnej dla elementu wyposażenia
23. Generowanie etykiet z kodami kreskowymi do inwentaryzacji wyposażenia
24. Drukowanie lub zapisywanie do pliku raportów ze szczegółami sprzętu
25. Możliwość określenia loga firmy oraz użycia go na wydrukach.
26. Możliwość cyklicznego wykonywania skanowania sprzętu z różnymi ustawieniami
27. Skanowanie WMI w skanerze "dyskietkowym" (Pen Drive)
28. Automatyczne monitorowanie i raportowanie zmian w podzespołach sprzętu
29. Możliwość importu informacji o wyposażeniu z pliku CSV
30. Mechanizm automatycznej ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu)
31. Mechanizm automatycznego tworzenia rekordów producenta sprzętu (na podstawie wyników skanowania sprzętu).
32. Obsługa kodów QR.
33. Możliwość powiązania wyposażenia z działem.
34. Automatyczna aktualizacji adresów IP komputerów bez zainstalowanego agenta.
35. Agent odczytuje identyfikator SID komputera

**Zarządzanie oprogramowaniem**

1. Inwentaryzacja licencji

2. Kompletna informacja na temat posiadanych licencji (typ, producent, czas ważności, informacje finansowe)
3. Możliwość przypisania licencji do komputera
4. Podpinanie załączników w dowolnym formacie
5. Definiowanie wymaganych atrybutów legalności (faktura, nośnik, COA, etc.)
6. Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecania skanów
7. Zdalny skan komputerów (bieżący lub okresowy)
8. Szablony ustawień skanowania
9. Identyfikacja zainstalowanych aplikacji
10. Możliwość rozliczania pakietów aplikacji
11. Możliwość rozliczania systemów operacyjnych
12. Rozliczanie liencji typu „Downgrade”
13. Możliwość cyklicznego wykonywania skanowania plików z różnymi ustawieniami
14. Prawidłowe rozpoznawanie aplikacji nawet mimo zmiany jej nazwy
15. Możliwość określania masek plików dla publikacji elektronicznych (e-book).
16. Skanowanie plików skompresowanych
17. Możliwość skanowania oraz identyfikacji zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lzh, lzma, msi, nrg, rar, tar, taz
18. Możliwość predefiniowanie profili skanowania (np. profil wzorcowy)
19. Skanowanie komputerów niepodłączonych do sieci
20. Możliwość wysyłania wyników skanowania offline na serwer FTP (Audyt)
21. Śledzenie zmian w stanie zainstalowanego oprogramowania
22. Możliwość porównania wyników skanowania oprogramowania
23. Audyt oprogramowania rozliczany automatycznie - informacja o stanie posiadanych licencji i faktycznie zainstalowanych programach
24. Historia audytów (Wyniki audytów są przechowywane w bazie danych - można do nich wracać w dowolnej chwili, porównywać je i generować stosowne raporty)
25. Wykrywanie plików multimedialnych
26. Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika)
27. Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji\pakietów\systemów operacyjnych
28. Możliwością definiowania własnych wzorców oprogramowania
29. Wsparcie procesu Audytu przez zaimportowanie materiału zdjęciowego i jego obróbkę
30. Wykrywanie kluczy/identyfikatorów programów
31. Definiowanie licencji przeznaczonych do przyszłego zakupu
32. Definiowanie kluczy seryjnych i przypisywanie do licencji
33. Gotowe metryki audytowanego komputera - załącznik do protokołu przekazania stanowiska komputerowego (sprzęt + oprogramowanie)
34. Drukowanie lub zapisywanie do pliku raportów ze szczegółami oprogramowania
35. Zbiorcze raporty wyników skanowania oprogramowania - Pakiety, pliki, systemy operacyjne, kluczy zainstalowanych aplikacji
36. "Wielkie raporty" (Możliwość utworzenia zbiorczych raportów obejmujących np. wszystkie przeskanowane pliki)
37. Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (*.msi)

**Kontrola wykorzystania sprzętu i oprogramowania**

1. Dane gromadzone dla konkretnych użytkowników (na bazie loginów) - jeden użytkownik może mieć przypisanych wiele loginów i pracować na różnych komputerach
2. Możliwość pogrupowania pracowników z podziałem na jednostki organizacyjne w firmie (np. względem działów)
3. Możliwość prezentacji 'stanu pracownika' (obecny, nieobecny, nowy).

4. Analiza aktywności użytkowników
5. Analiza zdarzeń sesji użytkownika (Logowanie, Wylogowanie, Zablokowanie, Odblokowanie, Nawiązanie połączenia RDP, Zakończenie połączenia RDP)
6. Analiza przerw w pracy
7. Analiza jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków)
8. Analiza wykorzystania poszczególnych aplikacji w czasie
9. Analiza czasu działania aplikacji na pierwszym planie i sumarycznie
10. Statystyki najczęściej wykorzystywanych aplikacji
11. Statystyki wykorzystania komputerów przez poszczególnych użytkowników
12. Statystyki aktywności pracownika i grup pracowników
13. Możliwość utworzenia działów firmy oraz określenia stawek godzinowych dla pracowników.
14. Kontrola wydruków - historia zadań drukowania zainicjowanych przez poszczególnych użytkowników
15. Kontrola wydruków - Monitoring wydruków obejmuje szczegółowe parametry (np. format papieru, orientacje, skalowanie, itd.)
16. Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz-b/kolor, dpi)
17. Monitorowanie wydruków na drukarkach sieciowych.
18. Monitorowanie użytkowników stacji terminalowych
19. Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.)
20. Blokowania niepożądanych aplikacji. Programy mogą być blokowane dla całej firmy lub tylko dla wybranych użytkowników.
21. Możliwość autoryzacji nośników zewnętrznych
22. Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych
23. Możliwość określenia praw dostępu w zależności od typu urządzenia, np. Pendrive, CD/ROM.
24. Możliwość blokowania dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.)
25. Definiowanie bazy informacji o napędach zewnętrznych.
26. Komunikacja z użytkownikami (Skype, mail) bezpośrednio z zakładki Pracownicy
27. Odczytywanie informacji o użytkownikach z Active Directory
28. Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień
29. Możliwość podglądu zdjęcia przypisanego do pracownika.
30. Ewidencja zdarzeń przypisanych do użytkowników
31. Powiadomienia przesyłane w czasie rzeczywistym o zdarzeniach, które miały miejsce w obrębie infrastruktury, systemu lub użytkowników
32. Informacje o awariach, poczynaniach użytkowników: zakończonej aktualizacji, akcji podpięcia przenośnych dysków, włożenia płyt do napędów CD/DVD, śledzenie uruchomienia aplikacji przez użytkownika, monitorowanie o małej ilości miejsca
33. Informacje o ostatnio zalogowanych osobach na stacjach klienckich.
34. Możliwość centralnego zarządzania wynikami skanowania sprzętu i oprogramowania
35. Funkcja automatycznego tworzenia działów na podstawie informacji odczytanych z Active Directory.

**Kontrola wykorzystania Internetu**

1. Raporty dotyczące aktywności użytkowników w Internecie oparte na loginach - jeden użytkownik może mieć przypisanych wiele loginów i pracować na różnych komputerach
2. Dokładna analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o wersji przeglądarki)
3. Analiza liczby wejść na poszczególne strony lub domeny
4. Analiza transferów komunikatorów internetowych (bez informacji o treści rozmów)
5. Analiza ruchu FTP (informacje o transferach, operacje na plikach, typy plików)
6. Blokowanie stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokowanie WWW po zawartości (ContentType)

7. Analiza odwiedzanych domen i stron
8. Kategoryzowanie stron internetowych

**Zdalny helpdesk**

1. Możliwość rejestracji i obsługi incydentów.
2. Możliwość dodawania załączników do incydentów
3. Możliwość określania uprawnień do incydentów (Publiczne, Prywatne, dla określonych działów)
4. Możliwość zarządzania filtrami zdefiniowanymi dla listy incydentów
5. Obsługa nazwy DNS oraz adresów IP (IPv4, IPv6) dla incydentów
6. Możliwość wydruku historii incydentu
7. Funkcjonalność kalendarza (Planowanie rozwiązania incydentów)
8. Możliwość powiązania incydentu z elementem zasobów
9. Zdalne operacje na plikach i katalogach
10. Zdalne zarządzanie procesami i rejestrem
11. Monitorowanie na odległość pracy wykonywanej na komputerze
12. Zdalny podgląd pulpitów wielu stacji (Funkcja Company Online)
13. Możliwość wywołania Windows Remote Desktop na danej stacji z poziomu aplikacji
14. Możliwość wysyłania wiadomości do użytkowników
15. Możliwość uruchamiana na stacjach programów z wiersza poleceń Command Line
16. Możliwość zdalnego uruchamiania komputera za pomocą funkcji Wake-On-Lan
17. Możliwość zdalnego przejęcia kontroli nad stacją roboczą
18. Możliwość zablokowania klawiatury i myszki na stacji klienckiej w trakcie przejęcia kontroli pulpitu zdalnego.
19. Możliwość przesłania kombinacji klawiszy Ctrl + Alt + Delete w zdalnym pulpicie.
20. Możliwość wysłania pytania o zgodę na zdalny dostęp lub wysłania komunikatu z informacją o rozpoczęciu podglądu pulpitu.
21. Obsługa wielu monitorów dla podglądu pulpitu.