Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Szczegółowy Opis Przedmiotu Zamówienia

na dostawę sprzętu i oprogramowania związaną z realizacją projektu w ramach grantu „Cyfrowy Powiat”

Spis treści

1. Zestawienie ilościowe.

Część nr 1 – Dostawa maszyny serwerowej dla potrzeb systemów i aplikacji.

Lp.	Nazwa	Ilość
1.	Dostawa serwera	1 szt.

Część nr 2 – Zakup specjalistycznego oprogramowania do zarządzania infrastrukturą IT.

Lp.	Nazwa	Ilość
1.	Dostawa oprogramowania do zarządzania infrastrukturą IT	1 szt.

Część nr 3 – Zakup i wdrożenie zabezpieczeń sieciowych klasy UTM.

Lp.	Nazwa	Ilość
1.	Dostawa urządzenia wraz z oprogramowaniem	1 szt.

Część nr 4 – Zakup i wdrożenie systemu elektronicznej komunikacji.

Lp.	Nazwa	Ilość
1.	Zakup i wdrożenie systemu elektronicznej komunikacji, wspierający realizację zadań ustawowych.	1 szt.

2. Przedmiot zamówienia dla części nr 1.

2.1. Wymagania ogólne w zakresie dostawy sprzętu.

1. Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt musi być fabrycznie nowy (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale" oraz „end-of-support" producenta.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do wskazanej lokalizacji przez Zamawiającego.
7. Wykonawca jest odpowiedzialny za dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
8. Dla dostaw sprzętu informatycznego z systemem operacyjnym Zamawiający wymaga fabrycznie nowego systemu operacyjnego (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego systemu operacyjnego nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku systemu operacyjnego naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

2.2. Zasada równoważności rozwiązań.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.

2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań, materiałów i urządzeń służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności.
5. Brak określenia „minimum" oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania testującego wraz z testowanym urządzeniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić na komputerze o oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
9. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza

oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów/produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

2.3. Dostawa serwera (1 szt.).

Minimalne parametry techniczne i funkcjonalne:

1. Dostarczony serwer ma utworzyć klaster wysokiej wydajności (HA) pracy awaryjnej „failover cluster” z istniejącym serwerem Fujitsu PRIMERGY RX2540 M4 o parametrach podstawowych: Intel® Xeon® Silver 4110, 128 GB, 3.3 TB HDD z systemem operacyjnym Windows Server 2019 w wersji Standard, na którym zainstalowane są cztery maszyny wirtualne. Wykonawca jest zobligowany do dostarczenia wszelkich niezbędnych elementów w celu uruchomienia klastra pracy awaryjnej „failover cluster”.
2. **Obudowa:** typu RACK, wysokość nie więcej niż 2U Szyny umożliwiające wysunięcie serwera z szafy stelażowej.
3. **Płyta główna:** dwuprocesorowa; wyprodukowana i zaprojektowana przez producenta serwera; 6 złącz PCI Express generacji 3 w tym: 3 złącza o prędkości x16; 3 złącza o prędkości x8; 12 gniazd pamięci RAM; Obsługa minimum 768 GB pamięci RAM; Zainstalowany moduł TPM; wsparcie dla technologii: Memory Scrubbing, SDDC,Advanced ECC.
4. **Procesory:** jeden procesor 10-rdzeniowy, architektura x86_64, taktowanie bazowe 2,4GHz, zapewniający wydajność min. 15000 pkt. (dla pojedynczego procesora) w teście Passmark CPU Mark, znajdujący się na liście https://www.cpubenchmark.net/cpu_list.php (wynik na dzień 02.02.2023).

5. **Pamięć RAM:** 128 GB pamięci RAM, DDR4 Registered, 2933Mhz.
6. **Dyski twarde:** minimum 8 wnęk dla dysków twardych Hotplug 3,5", bez zainstalowanych dysków.
7. **Kontrolery LAN:** trwale zintegrowana karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 1Gbit Base-T ze wsparciem iSCSI i iSCSI boot.
8. **Kontrolery I/O:** kontroler RAID dla wewnętrznych dysków twardych posiadający obsługujący poziomy RAID: 0,1,10,5,50,6,60 posiadający 2GB pamięci cache.
9. **Porty:** zintegrowana karta graficzna ze złączem VGA, 2 porty USB 3.0 na panelu przednim, 1 port USB 3.0 wewnętrzny, 4 porty USB 3.0 dostępne z tyłu serwera, 1 port serial/RS232 – możliwość rozbudowy, ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.
10. **Zasilanie/chłodzenie:** dwa zasilacze hotplug o sprawności 94% (tzw klasa Platinum) o mocy 450W, redundancja zasilania, redundantne wentylatory.
11. **Zarządzanie:** wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera, zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:

niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera,

dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym,

dostęp poprzez przeglądarkę Web, SSH,

zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii,

zarządzanie alarmami (zdarzenia poprzez SNMP),

możliwość przejęcia konsoli tekstowej,

możliwość zarządzania przez min 3 administratorów jednocześnie,

opcjonalne przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM),

obsługa serwerów proxy (autentykacja),

obsługa VLAN,

możliwość konfiguracji parametru Max. Transmission Unit (MTU),

wsparcie dla protokołu SSDP,

obsługa protokołów TLS 1.2, SSL v3,

obsługa protokołu LDAP,

integracja z HP SIM,

synchronizacja czasu poprzez protokół NTP,

możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej.

a) oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna).
b) wbudowana w kartę zarządzającą (lub zainstalowana) pamięc flash o pojemności minimum 16 GB; Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN – opcja rozbudowy.
c) serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej – opcja rozbudowy.

12. **Wspierane OS:** Microsoft Windows Server 2022, 2019, 2016, VMWare vSphere 6.7, Suse Linux Enterprise Server 12, Red Hat Enterprise Linux 7.
13. **Dokumentacja/inne:** elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy; serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy; ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; w czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
14. **Gwarancja:** 5 lat gwarancji producenta serwera w trybie onsite z gwarantowanym przyjazdem do miejsca użytkowania sprzętu certyfikowanego przez producenta pracownika serwisu do końca następnego dnia roboczego, uszkodzone dyski nie podlegają zwrotowi organizacji serwisowej; zgłaszanie usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu (bez udziału administratora); firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
15. **System operacyjny:** Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne

używanie na oferowanym serwerze. Licencja w najnowszej wersji dostępnej produkcyjnie z prawem do obniżenia wersji o co najmniej dwie generacje.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

- Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
- Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
- Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
- Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
- Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
- Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
- Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
- Wbudowane wsparcie instalacji i pracy na wolumenach, które:
  b) pozwalają na zmianę rozmiaru w czasie pracy systemu,
  c) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
  d) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
  e) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
- Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
- Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
- Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
- Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- Dostępne dwa rodzaje graficznego interfejsu użytkownika:
  a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
  b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
- Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.

- Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
- Mechanizmy logowania w oparciu o:
  a) Klasyczny, Login i hasło,
  b) Karty z certyfikatami (smartcard),
  c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
- Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
- Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
- Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
- Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
- Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
- Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
  a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
  b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
     i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
     ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
     iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
     iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
  c) Zdalna dystrybucja oprogramowania na stacje robocze.
  d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
  e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
     i. Dystrybucję certyfikatów poprzez http
     ii. Konsolidację CA dla wielu lasów domeny,

iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f) Szyfrowanie plików i folderów.
g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
i) Serwis udostępniania stron WWW.
j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
k) Wsparcie dla algorytmów Suite B (RFC 4869),
l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
iii. Obsługi 4-KB sektorów dysków
iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

- Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
- Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
- Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
- Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
- Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
- Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

- Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
- Dokumenty potwierdzające jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, ze oferowany serwer spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzenie serwerem oraz stworzenie klastra w oparciu o system klasy Microsoft Windows Serwer Standard 2019 z możliwością użytkowania systemu przez 100 użytkowników lub równoważne zgodnie z poniżej określonymi warunkami równoważności. Warunki równoważności dla dostawy oprogramowania Microsoft Windows Serwer Standard 2019 wraz z 100 licencjami dostępowymi Microsoft Windows Server 2019 CAL Device.

3. Przedmiot zamówienia dla części nr 2.

3.1. Wymagania ogólne w zakresie dostawy oprogramowania do zarządzania infrastrukturą IT.

1. Dostarczone oprogramowanie musi monitorować 100 sztuk stacji roboczych, na których będzie zainstalowany agent.
2. Dostarczone oprogramowanie musi być wolne od wad prawnych.
3. Niedopuszczalne jest oprogramowanie prototypowe.
4. Wymagania licencyjne dla dostarczonego oprogramowania:
   - Licencjobiorcą licencji będzie Starostwo Powiatowe w Ostrołęce.
   - Licencje muszą zostać wystawione na czas nieoznaczony (bezterminowy).
   - Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.

- Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet). Użytkownik może pracować w dowolny dostępny technologicznie sposób.
- Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
- Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
- Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym komputerze klienckim (licencja nie może być przypisana do komputera/urządzenia), a liczba komputerów (stacji roboczych) nie może przekraczać liczby dozwolonej wg zakupionej licencji.
- Wykonawca zapewni minimum 12 miesięczną gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.
- dostępność oprogramowania w dowolnej konfiguracji modułowej (funkcjonalnej) według rzeczywistych indywidualnych potrzeb użytkownika.
- możliwość dokupienia modułów (rozszerzenia funkcjonalności) oraz zwiększenia liczby zarządzanych stacji roboczych w ramach jednej licencji w dowolnym czasie.

3.2. Zasada równoważności rozwiązań.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań, służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.

5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

3.3. Dostawa, funkcjonalność oprogramowania do zarządzania infrastrukturą IT.

SPECYFIKACJA TECNICZNA OPROGRAMOWANIA

Oprogramowanie powinno mieć budowę modułową, która ma składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana musi być przy użyciu szyfrowanego protokołu TLS 1.2. Program musi umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą.

Moduły muszą umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program powinien wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open source bez limitu ilości danych, baza danych nie może wymagać dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających powinna wykorzystywać 64-bitowy system operacyjny Windows. Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., muszą być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Powinny być one również grupowane w osobnym, dedykowanym oknie, co pozwoli na zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.

Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych Administratorów – (nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników).

Główny Administrator musi mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną (np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów). Działania administratorów muszą mieć odzwierciedlenie w dzienniku z listą czynności wykonanych przez administratorów, (modyfikacja obiektów znajdujących się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta). Działania administratorów powinny być automatycznie eksportowane do zewnętrznego kolektora Syslog.

WYMAGANIA W ZAKRESIE MONITOROWANIA INFRASTRUKTURY (BEZAGENTOWO)

Monitorowanie musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

- wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
- wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)
- wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
- wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
- wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze
- wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
- wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny
- zablokowania mapy urządzeń przed przypadkową edycją
- serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów
- serwerów pocztowych:
  - program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty
  - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem)
  - program ma możliwość wykonywania operacji testowych
  - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa
- monitorowania serwerów WWW i adresów URL

- cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
- obsługi szyfrowania SSL/TLS w powiadomieniach e-mail
- obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID
- obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
- monitoringu routerów i przełączników wg:
  - zmian stanu interfejsów sieciowych
  - ruchu sieciowego
  - podłączonych stacji roboczych – graficzna prezentacja panelu switcha
  - ruchu generowanego przez podłączone do portów stacje robocze
- serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
- wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
- wydajności systemów Windows:
  - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

W celu lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Wydziały) program powinien tworzyć dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program powinien posiadać również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.

Program powinien umożliwiać również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Administrator powinien mieć możliwość samodzielnego budowania Alarmów Zdarzeń z wykorzystaniem ciągu przyczynowo skutkowego – np. poprzez wskazanie dowolnego zdarzenia z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie.

Program powinien umożliwiać automatyczną konfigurację wykonywania akcji alarmów po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut, oraz umożliwiać dla wykonania akcji nałożenie ograniczenia czasowego np. nie wykonuj między 8:00-16:00. i pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia.

Oprogramowanie powinno umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0. Program powinien mieć możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

WYMAGANIA W ZAKRESIE INWENTARYZACJI

Program musi automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

- prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
- obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
- informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
- zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
- posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
- umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
- umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
- umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
- umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
- umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.

Moduł inwentaryzacji zasobów musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:

- przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
- tworzenia powiązań między zasobami a urządzeniami,
- tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
- wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
- definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości (dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz),
- określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,

- określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
- definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
- importu danych z zewnętrznego źródła (.CSV),
- przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
- tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
- oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
- ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
- generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
- przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
- konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
- konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
- archiwizacji i porównywania audytów zasobów,
- tworzenia kodów kreskowych dla zasobów,
- drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów , które posiadają numer inwentarzowy,
- inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
- możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
- inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
- definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

- skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
- informacje o aplikacjach używanych w organizacji.
- tworzenie własnych wzorców aplikacji.
- tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
- informacje o komputerach, na których aplikacja została wykryta.
- zarządzanie posiadanymi licencjami.
- wskazywanie osób odpowiedzialnych za licencję.
- wskazanie użytkowników licencji.

- tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
- rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
- audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
- zarządzanie posiadanymi licencjami: raport zgodności licencji.
- możliwość przypisania do programów numerów seryjnych, wartości itp.
- okna audytowe powinny posiadać możliwość filtrowania elementów per oddział.

WYMAGANIA W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW

Program musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

- faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
- procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
- rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
- informacji o edytowanych przez użytkownika dokumentach,
- historii pracy (cykliczne zrzuty ekranowe),
- listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),
- transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
- wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
- nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Program ponadto powinien posiadać możliwość:

- blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych subdomen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.
- blokowania ruchu na wskazanych portach TCP/IP,
- blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,

- wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia,
- przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
- definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.
- generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.
- blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. (np. reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami).

WYMAGANIA W ZAKRESIE REALIZACJI ZDALNEJ POMOCY UŻYTKOWNIKOM

W ramach kontroli stacji użytkownika program musi udostępnić podgląd pulpitu użytkownika i mieć możliwość przejęcia nad nim kontroli oraz zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla).

Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W niniejszym programie/module powinna znajdować się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które będą przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie powinno pozwalać na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth2.0. Program/moduł powinien umożliwiać również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach") oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę.

Użytkownicy powinni mieć możliwość monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron.

Program/moduł ten powinien zawierać komunikator (czat), który umożliwi prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto pozwolić na:

- zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej
- rozmowy również między „zwykłymi" użytkownikami
- przesyłanie plików między rozmówcami w trybie online
- tworzenie pokojów tematycznych, rozmów grupowych
- oznaczanie kontaktów jako „ulubionych" na liście kontaktów

- uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku
- wyświetlanie w trybie jasnym lub ciemnym

Program/moduł powinien zawierać bazę wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic), umożliwiać informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy.
Dostęp do systemu zgłoszeń oraz bazy wiedzy powinien być realizowany przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym. Funkcjonalność programu/modułu powinna umożliwiać również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika. Ponadto powinien umożliwiać również:

- pobieranie listy użytkowników z Active Directory,
- zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
- zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
- tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,
- automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,
- definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,
- przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,
- procesowanie zgłoszeń użytkowników z wiadomości e-mail,
- integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,
- tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
- wykonywanie operacji na wielu zgłoszeniach równocześnie,
- dołączanie załączników do zgłoszeń,
- rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
- szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
- wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
- zrzuty ekranowe (podgląd pulpitu),
- zdalną modyfikację rejestrów,
- dystrybucję oprogramowania przez Agenty,
- definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,
- przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,

- dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
- zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
- możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
- planowanie nieobecności pracowników helpdesk,
- obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,
- generowanie raportów obsługi helpdesk,
- zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),
- zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
- wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików.

Oprogramowanie powinno posiadać funkcjonalny portal informacyjny w formie platformy WWW, który pozwali na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami, z możliwością rozmieszczenia ustalonym przez administratora. Zawartość każdego z paneli informacyjnych będzie automatycznie odświeżana oraz może być:

- udostępniana w trybie „tylko do odczytu" z zabezpieczeniem tokenem.
- wyświetlana w trybie jasnym lub ciemnym (nocnym).

Oprogramowanie powinno umożliwiać zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego. Widgety powinny prezentować dane ze wszystkich modułów funkcjonalnych oprogramowania:

- liczniki wydajności, alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, ostatnie urządzenia w sieci,
- zmiany w konfiguracji sprzętowej urządzeń z Agentami, zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, alarmy dla Zasobów,
- statystyki z obszaru wydruków, statystki użycia aplikacji, użycie łącza, aktywność WWW,
- statystyki z obsługi zgłoszeń, lista najnowszych nierozwiązanych zgłoszeń, lista najstarszych nierozwiązanych zgłoszeń, zgłoszenia z naruszonym SLA, zgłoszenia, których SLA wkrótce wygaśnie,
- ostatnio podłączone nośniki zewnętrzne, ostatnie operacje na plikach (wraz z filtrowaniem),

Program musi być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje. Program powinien mieć globalną wyszukiwarkę, zwracającą wyniki obiektów różnego typu na podstawie wyszukiwanych słów kluczowych, np.: urządzenia, użytkownicy, zasoby, elementy interfejsu konsoli zarządzającej, elementy opcji.

Program musi być dostępny w języku polskim wraz z Podręcznikiem Użytkownika w formie strony internetowej.

4. Przedmiot zamówienia dla części nr 3.

4.1. Wymagania ogólne w zakresie dostawy sprzętu.

1. Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt musi być fabrycznie nowy (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale" oraz „end-of-support" producenta.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do wskazanej lokalizacji przez Zamawiającego.
7. Wykonawca jest odpowiedzialny za dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
8. Dla dostaw sprzętu informatycznego z systemem operacyjnym Zamawiający wymaga fabrycznie nowego systemu operacyjnego (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego systemu operacyjnego nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku systemu operacyjnego naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

4.2. Zasada równoważności rozwiązań.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.

2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań, materiałów i urządzeń służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności.
5. Brak określenia „minimum" oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia poprawności przeprowadzonych testów może wezwać Wykonawcę do przedstawienia wskazanego przez Zamawiającego oprogramowania testującego wraz z testowanym urządzeniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić na komputerze o oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
9. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania

testującego wraz z testowanym urządzeniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić na komputerze o oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.

10. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów/produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

4.3. Dostawa urządzenia wraz z oprogramowaniem (1 szt.).

Minimalne parametry techniczne i funkcjonalne:

1. **Elementy systemu bezpieczeństwa:**
   - Urządzenie musi mieć możliwość jednoczesnej pracy w trybie Layer 3 (routing), transparentnym (most) i Layer 2 (port mirroring) bez konieczności wirtualizacji sprzętu
   - Możliwość stworzenia minimum 128 wirtualnych interfejsów zdefiniowanych jako VLAN w oparciu o standard 802.1Q.

- W zakresie Firewall, obsługa nie mniej niż 1 500 000 jednoczesnych połączeń i 130 000 nowych połączeń na sekundę.
- System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o minimalnej pojemności 8 GB do celów logowania i raportowania.
- Możliwość rozszerzenia pamięci do 2 TB poprzez dodatkowy dysk SSD bez otwierania obudowy urządzenia
- Musi posiadać 2x USB 3.0 z przodu urządzenia
- System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu.
- System musi mieć możliwość włączenia min 1 systemu wirtualnego bez dodatkowej licencji i możliwości rozszerzenia do minimum 5 poprzez dodatkową licencję w przyszłości
- Systemy wirtualne muszą obsługiwać QOS
- System pełniący funkcję zapory musi posiadać nie mniej niż: 2x SFP+, 8x SFP, 8x GE interfejsów
- Urządzenie musi posiadać podwójne zasilanie.

2. **Funkcjonalności:**
   - Kontrola dostępu — zapora sieciowa Stateful Inspection
   - Ochrona przed wirusami - komercyjny antywirus [AV]
   - Poufność danych - IPSec VPN i SSL VPN
   - Kontrola witryn sieci Web — filtr URL
   - Kontrola zawartości poczty - antyspam (dla protokołów SMTP, POP3)
   - Kontrola przepustowości i ruchu [QoS i kształtowanie ruchu] z alokacją Tunnel w oparciu o strefę bezpieczeństwa, interfejs, adres, użytkownika/grupę użytkowników, serwera/ grupę serwerów, aplikację/grupę aplikacji, TOS, VLAN
   - Kontrola aplikacji i rozpoznawanie ruchu P2P (wideo, gry itp.) oraz ograniczanie nowych połączeń i jednoczesnych sesji
   - Reputacja IP
   - Cloud Sandbox
3. **Wydajność:**
   - Analiza ruchu szyfrowanego protokołem SSL
   - Wydajność Firewall co najmniej 10 Gb/s
   - Wydajność skanowania strumienia danych z włączonymi funkcjami: NGFW z włączonym IPS i kontrolą aplikacji 3 Gb/s
   - Wydajność ochrony przed atakami (IPS) minimum 5Gb/s
   - Wydajność AV nie mniej niż 4Gb/s
   - Inspekcja SSL Proxy nie mniejsza niż 750Mbps
   - Wydajność skanowania z włączoną kontrolą aplikacji, AV, IPS, filtrem URL nie mniejsza niż: 1.8Gbps.
4. **Funkcjonalności VPN:**
   - Wydajność IPSec VPN, nie mniej niż 5 Gb/s
   - Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja
   - Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem.
   - Monitorowanie stanu tuneli VPN i utrzymywanie ich aktywności
   - Praca w toplogiach Hub and Spoke i Mesh
   - Wspierane mechanizamy : IPSec NAT Traversal, DPD, Replay Detection, Xauth, DHCP over IPsec,

- Wsparcie grup DH dla IKEv1: 1,2,5,19,20,21,24
- Wsparcie grup DH dla IKEv2: 1,2,5,14,15,16,19,20,21,24
- Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance)
- Obsługa PnPVPN (Plug and Play VPN)

5. **Routing:**
   - Rozwiązanie musi zapewniać: obsługę Policy Routing, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP, IS-IS
   - Obsługa Policy Based Routing
   - Funkcjonalność Virtual Wire
6. **Translacja adresów NAT:**
   - Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego.
   - Obsługa NAT46, NAT64, DNS64
   - Wsparcie dla STUN
7. **Polityka bezpieczeństwa systemu:**
   - Polityka bezpieczeństwa systemu bezpieczeństwa musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje bezpieczeństwa, rejestrowanie zdarzeń i zarządzanie pasmem sieci (w tym gwarantowaną i maksymalną przepustowość, priorytety).
   - Możliwość budowania min. 8000 polityk
   - Musi posiadać funkcjonalność asystenta polityk, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego
   - Musi być w stanie skonfigurować agregowane polityki
   - Musi być w stanie ograniczyć sesje na podstawie źródłowego adresu IP, docelowego adresu IP, harmonogramu, protokołu aplikacji (mysql, ms-sql, sqlnet, pobieranie P2P)
8. **Wydzielenie stref bezpieczeństwa:**
   - Możliwość tworzenia osobnych stref bezpieczeństwa Firewall, np. DMZ, LAN, VPN
   - Musi mieć możliwość konfiguracji oddzielnych wirtualnych routerów
   - Musi mieć możliwość konfigurowania oddzielnych wirtualnych przełączników
9. **Ochrona antywirusowa:**
   - Silnik antywirusowy musi by ć oparty na przepływie tzw. flow-based
   - Musi umożliwiać skanowanie protokołów HTTP, SMTP, POP3, IMAP, FTP / SFTP, SMB
   - Możliwość ręcznego dodawania lub usuwania sygnatury MD5 do bazy danych AV
   - Musi obsługiwać wykrywanie wirusów w plikach skompresowanych, takich jak RAR, ZIP, GZIP, BZIP2, TAR, a także wykrywać wielowarstwowe pliki skompresowane dla nie mniej niż 5 warstw dekompresji
10. **Równoważenie obciążenia:**
    - Obsługa redundantnego równoważenia obciążenia ISP i ISP z wykrywaniem łącza dla określonej nazwy domeny oraz monitorowanie stanu łącza poprzez aktywną metodę wykrywania
    - Obsługa równoważenia obciążenia serwerów w oparciu o weighted hashing, weighted least-connection i weighted round-robin
    - Kontrola stanu serwera, monitorowanie sesji i ochrona sesji
11. **Ochrona IPS:**
    - Ochrona IPS musi opierać się przynajmniej na analizie protokołu i sygnatury.

- Baza danych wykrytych ataków musi zawierać co najmniej 12000 sygnatur. Dodatkowo musi być w stanie wykrywać anomalie protokołów i ruchu, które stanowią podstawową ochronę przed atakami DoS i Ddos.
- Funkcjonalność zapobiegania atakom SQL injection, XSS injection
- Możliwość budowania własnych niestandardowych reguł IPS

12. **Obrona przed atakiem:**
    - Ochrona przed nieprawidłowym działaniem protokołu
    - Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment itp.
    - Wsparcie IPv4 jak i IPv6 dla ochrony przed DNS query flood i DNS reply flood
    - Biała lista docelowych adresów IP
13. **Kontrola aplikacji:**
    - Kontrola aplikacji musi być w stanie kontrolować ruch w oparciu o głęboką analizę pakietów, a nie tylko w oparciu o wartości portów TCP/UDP
    - Baza danych aplikacji zawierająca ponad 4700 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka
14. **Filtr adresów URL:**
    - Baza filtrów URL pogrupowana w co najmniej 64 kategorie tematyczne. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków.
    - Możliwość zdefiniowania własnej bazy kategorii www.
    - Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL.
    - Kategoria takie jak hazard, malware, spam, botnety
    - Obsługa Safe Search
    - Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne
    - Dostosowanie strony ostrzeżenia
15. **Ochrona danych:**
    - Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy
    - Identyfikacja protokołu pliku, w tym HTTP、FTP、SMTP, POP3、IMAP
    - Obsługa deszyfracji SSL do filtrowania plików przesyłanych przez HTTPS, SMTPS, POP3S, IMAPS
    - Filtrowanie plików przesyłanych przez SMB
16. **Reputacja IP:**
    - Identyfikacja i filtrowanie ruchu z ryzykownych adresów IP, takich jak hosty botnet, spamerzy, węzły Tor, podejrzane hosty i adresy IP atakujące metodą brute force
    - Logowanie, odrzucanie pakietów lub blokowanie dla różnych rodzajów ryzykownego ruchu IP
17. **Zapobieganie botnetom:**
    - Wykrywanie intranetowych hostów botnetu, monitorując połączenia C&C i blokowanie dalszych zaawansowanych zagrożeń takich jak botnet i oprogramowanie ransomware
    - Wsparcie DNS sinkhole
    - Wsparcie wykrywania tunelowania DNS
    - Wyrywanie i blokowanie DGA
18. **Cloud Sandbox:**
    - Złośliwe oprogramowanie emulowane w wirtualnym środowisku oparte na architekturze chmury w celu wykrywania nieznanych zagrożeń

- Obsługa protokołów, takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB
- Obsługa typów plików : PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i skryptów
- Obsługa blokowania wyników wykrywania w celu szybkiego blokowania nieznanych zagrożeń

19. Uwierzytelnianie użytkownika:

- System bezpieczeństwa musi być w stanie przeprowadzić uwierzytelnianie tożsamości użytkownika z nie mniej niż:
  - Statyczne hasła i definicje użytkowników przechowywane w lokalnej bazie danych systemu
  - Statyczne hasła i definicje użytkowników przechowywane w bazach danych zgodnych z LDAP
  - Hasła dynamiczne (RADIUS) oparte o zewnętrzne bazach danych
  - Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA
- Musi umożliwiać budowę architektury uwierzytelniania pojedynczego logowania w środowisku Active Directory
- Wsparcie usług terminalowych
- Uwierzytelnianie użytkownika przez Web przed dostępem do internetu
- Obsługa dwuskładnikowego uwierzytelniania, SMSy, certyfikaty i tokeny

20. Raportowanie i przeglądanie logów:

- Wbudowany w system bezpieczeństwa system raportowania i przeglądania logów nie może wymagać dodatkowej licencji na jego działanie
- W zakresie zaimplementowanych funkcjonalności systemu raportowania i przeglądania logów nie mniej niż:
  - Posiadanie predefiniowanych raportów dla ruchu internetowego, modułu IPS, skanera antywirusowego i antyspamowego
  - Generowanie co najmniej 10 rodzajów raportów

21. System logowania:

- Wraz z systemem musi być zapewniony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy chmurowej, do której dostęp jest cały czas z dowolnego urządzenia oraz dedykowanej aplikacji mobilnej.

22. Certyfikaty - Rozwiązanie musi:

- posiadać certyfikat Common Criteria EAL4+ lub posiadać certyfikat ICSA Labs dla funkcji Firewall
- być pozycjonowanym w raporcie Gartnera przez ostatnie 8 lat

23. Zarządzanie:

- Elementy systemu muszą mieć możliwość zarządzania lokalnie (HTTPS, SSH) oraz współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja między systemami bezpieczeństwa a platformami zarządzania musi odbywać się za pomocą protokołów szyfrowanych.
- Zarządzanie urządzeniem i konfiguracja musi odbywać się za pośrednictwem WebUI bez instalowania oddzielnego oprogramowania, takiego jak dedykowana konsola

24. Gwarancja – Dostawa musi zawierać również:

- 12-miesięczną gwarancję producenta na dostarczone elementy systemu
- Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 12 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C)
- Wsparcie techniczne dystrybutora rozwiązań w języku polskim
- Wdrożenie rozwiązania przez dystrybutora oferowanego produktu.

- Szkolenie oferowanego rozwiązania prowadzone przez certyfikowanego inżyniera dystrybutora (stacjonarnie u dystrybutora)
- 12-miesięczną gwarancję NBD
- Oferta musi być złożona przez autoryzowanego partnera

5. Przedmiot zamówienia dla części nr 4.

5.1. Wymagania ogólne w zakresie dostawy systemu.

Proponowany system powinien spełniać wymagania elektronicznego obiegu dokumentów, wspierający realizację zadań ustawowych wraz z funkcjonalnością elektronicznej komunikacji z podległymi jednostkami organizacyjnymi w zakresie elektronicznych dokumentów sprawozdań, elektronicznych dokumentów wniosków o zmianę w planie, sporządzania elektronicznego dokumentu zbiorczej deklaracji VAT. System musi mieć możliwość współpracy z systemami funkcjonującymi u Zamawiającego:

- **Budżet** pakietu Ratusz® autorstwa firmy Rekord SI – system ewidencji planu i analizy wykonania budżetu,
- **Finanse** pakietu Ratusz® autorstwa firmy Rekord SI – system finansowo-księgowy,

w zakresie integracji z planem budżetowym jednostek organizacyjnych Starostwa Powiatowego w Ostrołęce.

Lista jednostek organizacyjnych Starostwa:

- Zespół Szkół Powiatowych w Baranowie
- Zespół Szkół Powiatowych w Czerwinie
- Zespół Szkół Powiatowych w Goworowie
- Zespół Szkół Powiatowych w Kadzidle
- Zespół Szkół Powiatowych w Łysych
- Zespół Szkół Powiatowych w Myszyńcu
- Zespół Szkół Powiatowych w Troszynie
- Powiatowe Centrum Pomocy Rodzinie
- Placówka Opiekuńczo Wychowawcza w Czarnowcu
- Poradnia Psychologiczno Pedagogiczna w Czerwinie
- Poradnia Psychologiczno Pedagogiczna w Myszyńcu
- Powiatowy Urząd Pracy w Ostrołęce
- Środowiskowy Dom Samopomocy
- Zarząd Dróg Powiatowych

5.2. Zasada równoważności rozwiązań.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań, materiałów i urządzeń służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.
4. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.

5.3. Dostawa, funkcjonalność systemu elektronicznej komunikacji.

Dostarczony system musi być wolny od wad prawnych i fizycznych.

Wymagania licencyjne dla dostarczonego oprogramowania:

1. Licencjobiorcą licencji będzie Starostwo Powiatowe w Ostrołęce.
2. Licencje muszą zostać wystawione na czas nieoznaczony (bezterminowy).
3. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
4. Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet). Użytkownik może pracować w dowolny dostępny technologicznie sposób.
5. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
6. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
7. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym komputerze klienckim (licencja nie może być przypisana do komputera/urządzenia).

8. Wykonawca zapewni minimum 12 miesięczną gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.

Wymagana funkcjonalność systemu w zakresie portalu komunikacji elektronicznej jednostek organizacyjnych oraz urzędu:

Portal ma służyć jednostkom jako platforma komunikacyjna na linii urząd – jednostka organizacyjna. Dostęp do danych powinien odbywać się w trybie on-line za pomocą przeglądarki internetowej.

Wymagania:

- wspólna baza danych budżetowych dostępna z dowolnego miejsca (zarówno w Urzędzie, jak i w jednostkach),
- praca na tych samych dokumentach (dokumenty zmieniają statusy, w zależności od podejmowanych czynności),
- możliwe składanie dokumentów on-line bezpośrednio do zainteresowanego wydziału (z pominięciem kancelarii),
- wymiana danych z systemami finansowo-księgowymi oraz systemem Besti@.

Plan – zbiór dokumentów planu dochodów i wydatków, z wybraną dokładnością (rodzaj finansowania, dysponent/jednostka, dział, rozdział, grupa paragrafów, paragraf, pozycja, zadanie budżetowe). Możliwość dokonywania zmian w planie przez użytkowników według określonych uprawnień (w ramach grupy paragrafów) lub składania wniosków o zmianę w planie.

- edycja oraz analiza dokumentów planu,
- składanie wniosków o zmianę planu,
- tworzenie załączników/projektów uchwał na podstawie wniosków,
- import/eksport dokumentów planu do modułu finansowo-księgowego Starostwa Powiatowego,
- eksport danych do systemu Besti@.

Sprawozdania – zbiór cząstkowych sprawozdań budżetowych i finansowych, wprowadzanych bezpośrednio do systemu lub importowanych z modułu finansowo - księgowego.

- udostępnienie formularzy sprawozdań budżetowych i finansowych dostępnych w module budżetowym,
- możliwość importu sprawozdań z systemu finansowo-księgowego,
- eksport danych do systemu Besti@.

Analiza budżetu – analiza planu, wykonania, środków do dyspozycji z wybraną dokładnością, wg uprawnień Użytkownika do jednostek.

Administracja – tworzenie/import słowników, przypisywanie ról i uprawnień.

Wymagana funkcjonalność systemu w zakresie centralnej ewidencji i rozliczania podatku VAT:

- prowadzenie przez jednostki organizacyjne gminy rejestrów VAT
- generowanie i zatwierdzanie (z wykorzystaniem podpisu elektronicznego) na ich podstawie jednostkowych dokumentów sumarycznych
- łączenie na poziomie budżetu gminy w deklarację zbiorczą VAT-7
- przeglądarkowy interfejs użytkownika oraz technologia trójwarstwowa

Wymagany jest podział na dwa typy rejestrów cząstkowych VAT:

- sprzedaży,
- zakupów/nabyć.

Zgodnie z tym podziałem system ma umożliwiać sporządzanie wydruków rejestrów cząstkowych dla sprzedaży i nabyć. Rejestr sprzedaży ma umożliwiać wprowadzanie następujących informacji tyczących podatku należnego:

- symbol rejestru VAT – wybór z listy dostępnych zdefiniowanych w słowniku,
- kod VAT – określający sposób naliczenia wartości podatku należnego,
- datę faktury, datę wykonania usługi/dostawy, datę obowiązku podatkowego,
- dane kontrahenta: NIP, nazwę, adres, kraj,
- numer faktury,
- typ i numer dokumentu księgowego – oznaczenia zgodne z zapisem w księgach rachunkowych jednostki,
- opis z faktury,
- przedmiot dostawy/rodzaj usługi – służący do weryfikacji dokonanej transakcji pod kątem prawidłowego jej zakwalifikowania do rejestru VAT,
- kwoty netto, kwoty VAT, kwoty brutto w rozbiciu na poszczególne stawki (zgodne ze zdefiniowanymi w słowniku) z faktury,
- sumaryczne wartości netto, VAT i brutto z faktury – wyliczane na podstawie wcześniejszych zapisów,
- kwotę podatku VAT należnego.

Rejestr nabyć/zakupów ma umożliwiać wprowadzanie następujących informacji tyczących podatku naliczonego:

- symbol rejestru VAT – wybór z listy dostępnych zdefiniowanych w słowniku,
- kod VAT – umożliwiający alokację nabycia w związku z rodzajem sprzedaży: dla działalności całkowicie podlegającej odliczeniu, dla działalności mieszanej (opodatkowanej i zwolnionej; opodatkowanej i niepodlegającej; opodatkowanej, zwolnionej i niepodlegającej); dla działalności w całości niepodlegającej VAT,
- czy zakup dotyczy paliwa, części samochodowych – art. 86a ustawy o VAT – tzw. 50% odliczenie,
- datę faktury, datę dostawy/dokonania usługi (u dostawcy), datę wpływu faktury, datę odliczenia – prawo do odliczenia,
- dane kontrahenta: NIP, nazwę, adres, kraj,

- numer faktury,
- typ i numer dokumentu księgowego – oznaczenia zgodne z zapisem w księgach rachunkowych jednostki,
- opis z faktury,
- przedmiot dostawy/rodzaj usługi – służący do weryfikacji dokonanej transakcji pod kątem prawidłowego jej zakwalifikowania do rejestru VAT i prawidłowego przypisania (alokacji) kodu VAT,
- kwoty netto, kwoty VAT, kwoty brutto w rozbiciu na poszczególne stawki z faktury,
- sumaryczne wartości netto, VAT i brutto z faktury – wyliczane na podstawie wcześniejszych zapisów,
- kwotę podatku VAT do odliczenia po zastosowaniu art. 86a i 86c-h ustawy o VAT,
- kwotę podatku VAT do odliczenia po zastosowaniu par. 90 ustawy o VAT,
- końcową kwotę podatku do odliczenia.

W zakresie rejestrów cząstkowych VAT system ma mieć możliwość nadawania uprawnień, gdzie:

- pracownik jednostki ma mieć dostęp tylko do rejestrów cząstkowych VAT tworzonych w danej jednostce,
- osoba z zarządu powiatu nie może ingerować w zawartość jednostkowych cząstkowych rejestrów VAT.

Wymagany jest podział na dwa typy dokumentów:

- dotyczących sprzedaży,
- dotyczących zakupów/nabyć.

Dokumenty mają prezentować zawartość rejestrów cząstkowych w formie kwot zagregowanych, czyli ich podsumowania i być sporządzane oraz zatwierdzane na szczeblu jednostki. System ma pozwalać na automatyczne generowanie dokumentów sumarycznych na podstawie zatwierdzonych wcześniej rejestrów cząstkowych w celu zapewnienia spójności pomiędzy kwotami syntetycznymi (dokument sumaryczny), a kwotami analitycznymi (rejestry cząstkowe). Struktura zapisanych w nich danych ma zapewnić możliwość automatycznego wygenerowania deklaracji VAT-7 na poziomie gminy. System ma mieć możliwość bezpośredniego wprowadzania (lub korygowania) rejestrów cząstkowych do portalu.
W zakresie sumarycznych dokumentów sprawozdawczych system ma mieć możliwość nadawania uprawnień, gdzie:

- pracownik jednostki ma mieć dostęp tylko do dokumentów sumarycznych tworzonych w danej jednostce,
- osoba z zarządu powiatu nie może ingerować w zawartość jednostkowych dokumentów sumarycznych.

Wymagana jest możliwość automatycznego sporządzania zbiorczej deklaracji VAT-7 (VAT-7/korekta) na szczeblu gminy na podstawie jednostkowych dokumentów sumarycznych składanych przez poszczególne jednostki za dany miesiąc (okres) podatkowy. Operator ma mieć możliwość decydowania o sposobie rozliczenia nadwyżki podatku naliczonego do zwrotu. Deklaracja VAT-7 ma uwzględniać tylko dokumenty zatwierdzone i podpisane przez uprawnioną osobę. W zakresie deklaracji VAT-7 system ma mieć możliwość nadawania uprawnień osoba z zarządu gminy to sporządzenia deklaracji.

Wymagane jest aby system posiadał następujące elementy umożliwiające jego parametryzację:

- wartość wskaźnika(ów) struktury sprzedaży (WSS) z możliwością podania wartości współczynnika: prognozowanej - uwzględnianej w bieżących rozliczeniach i rzeczywistej uwzględnianej podczas dokonywania korekty podatku do odliczenia po zakończeniu roku,
- słownik jednostek organizacyjnych wraz z określeniem użytkowników mających uprawnienia o obsługi rejestrów cząstkowych i dokumentów sumarycznych w ramach tych jednostek,
- słownik prewspółczynników obowiązujących w konkretnych jednostkach z możliwością podania wartości prewspółczynnika: prognozowanej - uwzględnianej w bieżących rozliczeniach i rzeczywistej uwzględnianej podczas dokonywania korekty podatku do odliczenia po zakończeniu roku,
- słownik aktualnie obowiązujących stawek podatku VAT,
- słownik rejestrów VAT – sprzedaż (podatek należny)
- słownik rejestrów VAT – nabycia (podatek naliczony)
- słownik kodów podatku VAT określający schematy wyliczania kwoty podatku do odliczenia, z uwzględnieniem nabyć dla działalności w całości opodatkowanej, działalności mieszanej, działalności zwolnionej lub niepodlegającej podatkowi VAT.

Dodatkowo wymagane jest aby była możliwość:

Wyliczania rocznej kwoty korekty podatku naliczonego po zakończeniu roku podatkowego, w tym:

- wyliczenia rzeczywistych wartości wskaźnika WSS dla poszczególnych jednostek,
- wyliczenia kwoty podatku do odliczenia za miniony rok podatkowy wg skorygowanych (rzeczywistych) wartości WSS i prewspółczynników,
- rozliczenia różnicy pomiędzy kwotą podatku rzeczywiście odliczonego, a kwotą przysługującego odliczenia wg wskaźników rzeczywistych na deklaracji za pierwszy okres rozliczeniowy roku następnego.
- sporządzania rejestrów korekt rocznych dla wskazanych rodzajów nabyć, związanych z zakupem środków trwałych (WNiP) o wartości powyżej 15 tys. PLN netto, zakupem nieruchomości oraz zakupami dla potrzeb prowadzonych inwestycji.

Pozostałe wymagania:

1. Dostarczane oprogramowanie musi w całości posiadać polskojęzyczny interfejs i instrukcję obsługi w języku polskim. W języku polskim muszą być również wyświetlane wszystkie komunikaty przekazywane przez System.
2. Dostarczane oprogramowanie musi działać w modelu przetwarzania transakcyjnego, gwarantującego bezpieczeństwo danych.
3. Dostarczane oprogramowanie musi przechowywać wszystkie dane w postaci bazy danych.
4. Dostarczane oprogramowanie musi umożliwiać pracę na bazie typu Open Source bądź na komercyjnym systemie bazodanowym. Dopuszcza się przechowywanie poza bazą danych plików w postaci repozytorium dyskowego. Ich integralność z systemem musi być zapewniona przez metadane opisujące poszczególne pliki.

5. Dostarczane oprogramowanie musi cechować się przyjaznym interfejsem użytkownika wykorzystującym: menu, moduły, listy, formularze, przyciski, referencje (linki) itp.
6. Dostarczone oprogramowanie musi cechować się skalowalnością zarówno pod względem ilości przetwarzanych danych, jak i liczby użytkowników.
7. Wszystkie interfejsy zewnętrzne dostarczanego oprogramowania muszą być oparte na standardowych rozwiązaniach - w obszarach stosowalności standardów wymienionych w Rozporządzeniu w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012r., poz. 526), a w pozostałych obszarach będą stosowane powszechnie stosowane standardy (w szczególności standardy otwarte).
8. Wdrożone oprogramowanie musi zapewniać możliwość tworzenia kopii zapasowych danych.
9. Dokumentacja użytkownika dla każdego elementu oprogramowania musi zawierać opis funkcji programu, wyjaśniać zasady pracy z programem oraz zawierać opisy przykładowych scenariuszy pracy.
10. Zamawiający wymaga od Wykonawcy przeprowadzenia instruktaży teoretycznych i praktycznych dla użytkowników wewnętrznych wskazanych przez urząd w zakresie niezbędnym do właściwego i pełnego wykorzystania przez nich możliwości jakie oferują.
11. Wykonawca przeprowadzi we współpracy ze wskazanymi przez urząd pracownikami analizę stanowiskową zadań realizowanych w systemie charakterystycznych dla konkretnych merytorycznych stanowisk pracowniczych.
12. Wykonawca przeprowadzi instruktaż dla administratorów w zakresie zarządzania użytkownikami i uprawnieniami oraz zabezpieczania i odtwarzania danych systemu.
13. Materiały merytoryczne niezbędne dla przeprowadzenia instruktaży użytkowników oprogramowania muszą być opracowane przez Wykonawcę oraz przekazane Zamawiającemu wraz z prawem do ich dalszego powielania i wykorzystywania w trakcie późniejszych instruktaży organizowanych i prowadzonych przez Zamawiającego lub osoby trzecie dla użytkowników Systemów.
14. Wykonawca musi opracować i dostarczyć materiały merytoryczne dla uczestników poszczególnych instruktaży, najpóźniej w dniu rozpoczęcia instruktażu, w formie papierowej lub elektronicznej (w formacie .docx i .pdf).
15. Wykonawca musi dostarczyć instrukcje obsługi dla administratorów i użytkowników i przekazać je Zamawiającemu wraz z prawem do ich dalszego powielania i wykorzystywania w trakcie późniejszych instruktaży organizowanych i prowadzonych przez Zamawiającego lub osoby trzecie dla użytkowników systemów.
16. Wykonawca jest zobowiązany do uaktualniania i dostarczania nowych wersji instrukcji obsługi dla administratorów i użytkowników w przypadku każdej zmiany wpływającej na sposób funkcjonowania oprogramowania, która nastąpi w okresie objętym gwarancją.
17. W okresie udzielonej gwarancji Wykonawca zobowiąże się do dostarczania wolnych od wad i zgodnych z aktualnie obowiązującym prawem kolejnych wersji oprogramowania składającego się na przedmiot zamówienia.
18. Wykonawca zobowiąże się do aktualizacji dokumentacji użytkownika i/lub administratora.

19. Wykonawca zapewni w dni robocze w godzinach od 8:00 do 16:00 obecność specjalistów mających niezbędną wiedzę i doświadczenie z zakresu eksploatacji przedmiotu zamówienia, którzy będą odpowiedzialni za przyjmowanie zgłoszeń i realizację działań naprawczych wynikających z analizy ujawnionych problemów, wykrytych błędów i wad systemów, niewłaściwego działania systemu, spadku wydajności.
20. W ramach gwarancji określonej w zawartej umowie Wykonawca będzie zobowiązany do nieodpłatnego:
    a. usuwania błędu, awarii, wady z przyczyn zawinionych przez Wykonawcę będących konsekwencją wystąpienia: błędu w systemie, błędu lub wady fizycznej pakietu aktualizacyjnego lub instalacyjnego, błędu w wykonaniu usług przez Wykonawcę;
    b. usuwania błędu, awarii, wady związanych z realizacją usługi wdrożenia oprogramowania;
    c. usuwania błędów lub awarii spowodowanych aktualizacjami oprogramowania.
21. Wykonawca będzie musiał informować Zamawiającego o dostępnych aktualizacjach i poprawkach oprogramowania najpóźniej w ciągu 7 dni od dnia publicznego udostępnienia aktualizacji bądź poprawki.
22. Zgłaszający, w przypadku wystąpienia błędu, awarii, wady przesyłać będzie do Wykonawcy przy pomocy środków komunikacji formularz zgłoszenia wystąpienia błędu/awarii/wady.