

Załącznik nr 1 do SIWZ

## **OPIS PRZEDMIOTU ZAMÓWIENIA**

**Zakup infrastruktury informatycznej**

w ramach projektu

**Rozwój e-usług publicznych w Gminie Zembrzyce**

Projekt finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego (EFRR) w ramach Regionalnego Programu Operacyjnego Województwa Małopolskiego na lata 2014 – 2020, II Osi Priorytetowej „CYFROWA MAŁOPOLSKA”, Działanie 2.1 „E-administracja i otwarte zasoby”.

## I. WSTĘP

Dla potrzeb realizacji projektu pn.: „Rozwój e-usług publicznych w Gminie Zembrzyce”, dofinansowanego z EFRR w ramach Regionalnego Programu Operacyjnego Województwa Małopolskiego na lata 2014-2020, II oś priorytetowa CYFROWA MAŁOPOLSKA, Działanie 2.1 „E-administracja i otwarte zasoby”, niniejsze zamówienie obejmuje swoim zakresem zakup niezbędnej infrastruktury teleinformatycznej, służącej do realizacji celów w/w projektu.

## II. ZAKRES DOSTAW I USŁUG

Niniejsze zamówienie dotyczy dostaw i usług zgodnie z poniższym zestawieniem. Oferowane rozwiązania i usługi muszą być zgodne z minimalnymi wymaganiami zawartymi w niniejszej specyfikacji.

LP.	NAZWA URZĄDZENIA / USŁUGI	IŁOŚĆ	JEDN.
1.	Serwer baz danych	1	szt.
2.	Serwer aplikacji i e-usług	1	szt.
3.	Macierz dyskowa	1	szt.
4.	System backup	1	szt.
5.	Urządzenie ochrony sieci UTM	1	szt.
6.	Zasilacz awaryjny UPS	1	szt.
7.	Zestaw komputerowy z systemem operacyjnym i pakietem biurowym	2	kpl.
8.	System operacyjny	7	szt.
9.	Skaner dokumentów A4	1	szt.
10.	Stanowisko Potwierdzenia Profilu Zaufanego	1	kpl.
11.	Instalacja i konfiguracja infrastruktury sprzętowej	1	kpl.

## III. RÓWNOWAŻNOŚĆ ROZWIĄZAŃ

W celu zachowania reguły konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych w treści niniejszego OPZ, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności przez to rozwiązanie oferowanych, nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym 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.

Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt 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 pod względem:

- gabarytów i konstrukcji (wielkość, rodzaj, właściwości fizyczne, liczba elementów składowych),
- charakteru użytkowego (tożsamość funkcji),
- charakterystyki materiałowej (rodzaj i jakość materiałów),

- d) parametrów technicznych (wytrzymałość, trwałość, dane techniczne, dane hydrauliczne, charakterystyki linowe, konstrukcja),
- e) parametrów bezpieczeństwa użytkowania,
- f) standardów emisyjnych.

W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób. Za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całość systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, identycznych dla obu rozwiązań, dla których to warunków rozwiązania te są dedykowane.

Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, iż spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

#### **IV. WYMAGANIA OGÓLNE**

Zamawiający wymaga od wykonawcy dostarczenia przedmiotu zamówienia do lokalizacji, którą jest siedziba Zamawiającego, na własny koszt.

Zamawiający wymaga instalacji urządzeń we wskazanym przez Zamawiającego miejscu, wykonania niezbędnych połączeń urządzeń przy wykorzystaniu okablowania dostarczonego przez Wykonawcę wraz z urządzeniami oraz konfiguracji dostarczonego sprzętu oraz oprogramowania.

Zamawiający wymaga konfiguracji dostarczonego sprzętu i oprogramowania zgodnie z opracowanym w terminie do 7 dni po podpisaniu umowy przez Wykonawcę i zaakceptowanym przez Zamawiającego planem wdrożenia wraz z procedurami bezpieczeństwa.

Po instalacji i konfiguracji sprzętu, Wykonawca wykona testy połączeń i wydajności urządzeń celem weryfikacji poprawności wykonanej konfiguracji. Pozytywny wynik testów będzie podstawą podpisania protokołu odbioru.

Całość dostarczonego w ramach zamówienia oprogramowania wraz z licencjami musi pochodzić z legalnego źródła. Licencje nie mogą pochodzić z recyklingu. Oprogramowanie wraz z licencjami musi być zainstalowane na dostarczonym sprzęcie oraz zarejestrowane zgodnie z wymaganiami/wytycznymi producenta dostarczonego oprogramowania.

#### **V. GWARANCJA I RĘKOJMIA**

Zamawiający wymaga minimum 60 miesięcy gwarancji na przedmiot zamówienia (dotyczy wszystkich części). Gwarancja musi uwzględniać automatyczne aktualizacje systemu oraz całodobowe wsparcie techniczne świadczone w języku polskim.

Okres gwarancji/rękojmi liczony będzie od daty sporządzenia protokołu odbiorczego przedmiotu zamówienia.

Wszystkie urządzenia oraz oprogramowanie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy. Zamawiający nie dopuszcza rozwiązań pochodzących z rynku wtórnego.

Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.

Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.

## **VI. OZNACZENIE CE**

Wszystkie dostarczone urządzenia muszą być oznakowane znakiem CE zgodnie z wymogami deklaracji zgodności WE wystawionej przez producenta lub jego upoważnionego przedstawiciela, w celu potwierdzenia zgodności z dyrektywami Nowego Podejścia lub równoważnym.

W przypadku braku w/w certyfikatu na internetowych stronach producenta, Wykonawca będzie musiał dołożyć dokument potwierdzający spełnienie przez produkt wymagań jakościowych.

## VII. MINIMALNE WYMAGANIA

### 1. Serwer baz danych

NAZWA KOMPONENTU	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
<b>OBUDOWA</b>	Obudowa typu RACK o wysokości maksymalnej 2U, z możliwością instalacji min. 8 dysków Hot-Plug w ramach jednej obudowy wraz kompletem szyn umożliwiających montaż w standardowej szafie RACK oraz wysuwanie serwera do celów serwisowych.
<b>PŁYTA GŁÓWNA</b>	Płyta główna z możliwością zainstalowania do dwóch procesorów oraz wyposażona w minimum 24 sloty pamięci z możliwością obsługi minimum 3072 GB RAM.
<b>PROCESOR</b>	Dwa procesory wielordzeniowe osiągające w teście PassMark CPU Mark wynik min. 18.000 punktów dla konfiguracji dwuprocesorowej według wyników ze strony <a href="https://www.cpubenchmark.net/cpu_list.php">https://www.cpubenchmark.net/cpu_list.php</a>
<b>PAMIĘĆ RAM</b>	Minimum 64 GB pamięci RAM typu RDIMM 2666 MT/s. z możliwością rozbudowy do 768GB. Możliwe zabezpieczenia pamięci: ECC, SDDC, Rank Sparing
<b>SLOTY PCI EXPRESS</b>	minimum sześć slotów generacji 3.0, w tym minimum 2 sloty o prędkości x16
<b>KARTA GRAFICZNA</b>	Zintegrowana karta graficzna umożliwiająca rozdzielczość minimum 1920x1200
<b>WBUDOWANE PORTY</b>	Minimum 5 portów USB w tym co najmniej trzy w wersji 3.0 lub nowszej. Minimum 2 porty graficzne VGA lub nowsze. Porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
<b>INTERFEJSY SIECIOWE</b>	Minimum dwa interfejsy sieciowe 10 Gb Ethernet w standardzie Base-T. Minimum dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ . Jeden interfejs 1Gb w standardzie Base-T do zarządzania serwerem. Minimum dwa interfejsy zapewniające połączenie z urządzeniami zewnętrznymi z prędkością minimum 8Gb/s. Jeżeli interfejsy wymagają dostarczenie dodatkowych modułów takich jak np. wkładki światłowodowe, to Wykonawca musi je zapewnić w ramach dostawy. Zamawiający wymaga dostarczenia kabli minimum 2m dla każdego wbudowanego interfejsu sieciowego.
<b>KONTROLER DYSKÓW</b>	Zainstalowany sprzętowy kontroler dyskowy RAID : 0, 1, 5, 6, 10, 50, 60, nieulotna pamięć cache o pojemności min. 1GB.
<b>PAMIĘĆ MASOWA</b>	Zainstalowane 2 dyski twarde minimum 600GB SAS 10k RPM Hot Plug. Możliwość instalacji dysków twardych SATA, SAS, NearLine SAS i SSD. Możliwość instalacji modułu dedykowanego dla hypervisora wirtualizacyjnego.
<b>ZASILANIE</b>	Dwa redundantne zasilacze Hot Plug, każdy o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujące w sieci 230V 50/60Hz prądu zmiennego wraz z kablami zasilającymi o dł.min. 1,5m każdy.
<b>WENTYLATORY</b>	Minimum 4 redundantne wentylatory typu Hot-Plug.
<b>BEZPIECZEŃSTWO</b>	Panel diagnostyczny lub sygnalizacja LED umieszczona na froncie obudowy. Zintegrowany z płytą główną moduł TPM2.0.

	Fizyczne zabezpieczenie dedykowane przez producenta serwera chroniące przed nieuprawnionym dostępem do dysków twardej, montowane z przodu obudowy.
<b>ZARZĄDZANIE</b>	<p>Oprogramowanie do zdalnego zarządzania serwerem: monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.), monitorowanie w czasie rzeczywistym poboru prądu przez serwer, zbieranie logów błędów hardware, przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury, montowanie wirtualnych napędów, zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego, wysyłanie zawiadomień drogą mailową lub poprzez SNMP.</p> <p>Nie dopuszcza się rozwiązań serwerowych wymagających dokupowania dodatkowych licencji umożliwiających zarządzanie serwerem i dostarczających wyżej wymienione funkcjonalności.</p>
<b>DOKUMENTACJA</b>	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>
<b>SYSTEM OPERACYJNY</b>	<p>Zainstalowane na serwerze oprogramowanie wraz z licencją uprawniającą do uruchamiania co najmniej dwóch serwerowych systemów operacyjnych w środowisku wirtualnym.</p> <p>Licencja na oprogramowanie musi uwzględniać wszystkie rdzenie procesorów zainstalowanych w serwerze.</p> <p>Wsparcie (na umożliwiającym to sprzęcie) dodawania pamięci RAM bez przerywania pracy.</p> <p>Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości.</p> <p>Wbudowane wsparcie instalacji i pracy na wolumenach które:</p> <ul style="list-style-type: none"> <li>- pozwalają na zmianę rozmiaru w czasie pracy systemu,</li> <li>- umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,</li> <li>- umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów,</li> <li>- umożliwiają zdefiniowanie list kontroli dostępu (ACL).</li> </ul> <p>Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</p> <p>Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.</p> <p>Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię <a href="#">ASP.NET</a>.</p> <p>Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów .</p> <p>Wbudowana zaporę internetową (firewall) z obsługi definiowanych reguł dla ochrony połączeń internetowych i intranetowych</p> <p>Graficzny interfejs użytkownika.</p> <p>Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.</p> <p>Możliwość zmiany języka interfejsu po zainstalowaniu systemu dla co najmniej języka polskiego i angielskiego.</p> <p>Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</p>

	<p>Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.</p> <p>Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).</p> <p>Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:</p> <ul style="list-style-type: none"> <li>- Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,</li> <li>- 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: <ul style="list-style-type: none"> <li>• podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,</li> <li>• ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,</li> <li>• odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.</li> </ul> </li> </ul> <p>Zdalna dystrybucja oprogramowania na stacje robocze.</p> <p>Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej</p> <p>PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:</p> <ul style="list-style-type: none"> <li>- dystrybucję certyfikatów poprzez http,</li> <li>- konsolidację CA dla wielu lasów domeny,</li> <li>- automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.</li> </ul> <p>Szyfrowanie plików i folderów.</p> <p>Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).</p> <p>Serwis udostępniania stron <a href="http://www">WWW</a>.</p> <p>Wsparcie dla protokołu IP w wersji 6 (Ipv6).</p> <p>Wbudowane usługi VPN pozwalające na zestawienie minimum 500 równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.</p> <p>Oferowany serwer musi znajdować się na liście kompatybilności producenta systemu operacyjnego dostarczonego wraz z serwerem. W przypadku braku możliwości weryfikacji przez Zamawiającego na stronach internetowych producentów, Zamawiający na etapie weryfikacji oferty będzie wymagał przedstawienia dokumentów potwierdzających spełnienie przez produkt w/w wymagania.</p>
<p><b>INNE</b></p>	<p>Zamawiający wymaga montażu serwera we wskazanej szafie RACK. Wszystkie elementy niezbędne do instalacji (śruby montażowe, kable, przewody, listwy zasilające, itp.) muszą być zapewnione przez Wykonawcę.</p> <p>Na dostarczonym serwerze Wykonawca skonfiguruje system operacyjny zgodnie z wytycznymi Zamawiającego dostarczonymi na etapie realizacji.</p>

## 2. Serwer aplikacji i e-usług

NAZWA KOMPONENTU	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
<b>OBUDOWA</b>	Obudowa typu RACK o wysokości maksymalnej 2U, z możliwością instalacji min. 8 dysków Hot-Plug w ramach jednej obudowy wraz kompletem szyn umożliwiających montaż w standardowej szafie RACK oraz wysuwanie serwera do celów serwisowych.
<b>PŁYTA GŁÓWNA</b>	Płyta główna z możliwością zainstalowania do dwóch procesorów oraz wyposażona w minimum 24 sloty pamięci z możliwością obsługi minimum 3072 GB RAM.
<b>PROCESOR</b>	Dwa procesory wielordzeniowe osiągające w teście PassMark CPU Mark wynik min. 18.000 punktów dla konfiguracji dwuprocesorowej według wyników ze strony <a href="https://www.cpubenchmark.net/cpu_list.php">https://www.cpubenchmark.net/cpu_list.php</a>
<b>PAMIĘĆ RAM</b>	Minimum 64 GB pamięci RAM typu RDIMM 2666 MT/s z możliwością rozbudowy do 768GB. Możliwe zabezpieczenia pamięci: ECC, SDDC, Rank Sparring
<b>SLOTY PCI EXPRESS</b>	minimum sześć slotów generacji 3.0, w tym minimum 2 sloty o prędkości x16
<b>KARTA GRAFICZNA</b>	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
<b>WBUDOWANE PORTY</b>	Minimum 5 portów USB w tym co najmniej trzy w wersji 3.0 lub nowszej. Minimum 2 porty graficzne VGA lub nowsze. Porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
<b>INTERFEJSY SIECIOWE</b>	Minimum dwa interfejsy sieciowe 10 Gb Ethernet w standardzie Base-T. Minimum dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ . Jeden interfejs 1Gb w standardzie Base-T do zarządzania serwerem. Minimum dwa interfejsy zapewniające połączenie z urządzeniami zewnętrznymi z prędkością minimum 8Gb/s. Jeżeli interfejsy wymagają dostarczenie dodatkowych modułów takich jak np. wkładki światłowodowe, to Wykonawca musi je zapewnić w ramach dostawy. Zamawiający wymaga dostarczenia kabli minimum 2m dla każdego wbudowanego interfejsu sieciowego.
<b>KONTROLER DYSKÓW</b>	Zainstalowany sprzętowy kontroler dyskowy RAID : 0, 1, 5, 6, 10, 50, 60, nieulotna pamięć cache o pojemności min. 1GB.
<b>PAMIĘĆ MASOWA</b>	2 dyski twarde 600GB SAS 10k RPM Hot Plug. Możliwość instalacji dysków twardych SATA, SAS, NearLine SAS i SSD. Możliwość instalacji modułu dedykowanego dla hypervisora wirtualizacyjnego.
<b>ZASILANIE</b>	Dwa redundantne zasilacze Hot Plug, każdy o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujące w sieci 230V 50/60Hz prądu zmiennego wraz z kablami zasilającymi o dł.min. 1,5m każdy.
<b>WENTYLATORY</b>	Minimum 4 redundantne wentylatory typu Hot-Plug.
<b>BEZPIECZEŃSTWO</b>	Panel diagnostyczny lub sygnalizacja LED umieszczona na froncie obudowy. Zintegrowany z płytą główną moduł TPM2.0. Fizyczne zabezpieczenie dedykowane przez producenta serwera chroniące przed nieuprawnionym dostępem do dysków twardych, montowane z przodu obudowy.
<b>ZARZĄDZANIE</b>	Oprogramowanie do zdalnego zarządzania serwerem: monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa



	<p>wentylatorów, itp.), monitorowanie w czasie rzeczywistym poboru prądu przez serwer, zbieranie logów błędów hardware, przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury, montowanie wirtualnych napędów, zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego, wysyłanie zawiadomień drogą mailową lub poprzez SNMP.</p> <p>Nie dopuszcza się rozwiązań serwerowych wymagających dokupowania dodatkowych licencji umożliwiających zarządzanie serwerem i dostarczających wyżej wymienione funkcjonalności.</p>
<b>DOKUMENTACJA</b>	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>
<b>SYSTEM OPERACYJNY</b>	<p>Zainstalowane na serwerze oprogramowanie wraz z licencją uprawniającą do uruchamiania co najmniej dwóch serwerowych systemów operacyjnych w środowisku wirtualnym.</p> <p>Licencja na oprogramowanie musi uwzględniać wszystkie rdzenie procesorów zainstalowanych w serwerze.</p> <p>Wsparcie (na umożliwiającym to sprzęcie) dodawania pamięci RAM bez przerywania pracy.</p> <p>Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości.</p> <p>Wbudowane wsparcie instalacji i pracy na wolumenach które:</p> <ul style="list-style-type: none"> <li>- pozwalają na zmianę rozmiaru w czasie pracy systemu,</li> <li>- umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,</li> <li>- umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,</li> <li>- umożliwiają zdefiniowanie list kontroli dostępu (ACL).</li> </ul> <p>Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</p> <p>Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.</p> <p>Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię <a href="#">ASP.NET</a>.</p> <p>Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów .</p> <p>Wbudowana zaporę internetową (firewall) z obsługi definiowanych reguł dla ochrony połączeń internetowych i intranetowych</p> <p>Graficzny interfejs użytkownika.</p> <p>Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.</p> <p>Możliwość zmiany języka interfejsu po zainstalowaniu systemu dla co najmniej języka polskiego i angielskiego.</p> <p>Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</p> <p>Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.</p> <p>Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).</p>

	<p>Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:</p> <ul style="list-style-type: none"> <li>- Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,</li> <li>- 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:             <ul style="list-style-type: none"> <li>• podłączenie do domeny w trybie offline - bez dostępnego połączenia sieciowego z domeną,</li> <li>• ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika - na przykład typu certyfikatu użytego do logowania,</li> <li>• odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.</li> </ul> </li> </ul> <p>Zdalna dystrybucja oprogramowania na stacje robocze.</p> <p>Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej</p> <p>PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:</p> <ul style="list-style-type: none"> <li>- dystrybucję certyfikatów poprzez http,</li> <li>- konsolidację CA dla wielu lasów domeny,</li> <li>- automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.</li> </ul> <p>Szyfrowanie plików i folderów.</p> <p>Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).</p> <p>Serwis udostępniania stron <a href="http://www">WWW</a>.</p> <p>Wsparcie dla protokołu IP w wersji 6 (IPv6).</p> <p>Wbudowane usługi VPN pozwalające na zestawienie minimum 500 równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.</p> <p>System operacyjny musi być dostarczony wraz z 35 licencjami dostępowymi dające użytkownikom prawo korzystania z usług udostępnianych przez serwer oraz umożliwiające korzystanie z jego zasobów.</p> <p>Oferowany serwer musi znajdować się na liście kompatybilności producenta systemu operacyjnego dostarczonego wraz z serwerem. W przypadku braku możliwości weryfikacji przez Zamawiającego na stronach internetowych producentów, Zamawiający na etapie weryfikacji oferty będzie wymagał przedstawienia dokumentów potwierdzających spełnienie przez produkt w/w wymagania.</p>
<p><b>INNE</b></p>	<p>Zamawiający wymaga montażu serwera we wskazanej szafie RACK. Wszystkie elementy niezbędne do instalacji (śruby montażowe, kable, przewody, listwy zasilające, itp.) muszą być zapewnione przez Wykonawcę.</p> <p>Na dostarczonym serwerze Wykonawca skonfiguruje system operacyjny zgodnie z wytycznymi Zamawiającego dostarczonymi na etapie realizacji.</p> <p>Instalacja, uruchomienie i konfiguracja serwera usług katalogowych wraz z założeniem kont użytkowników wraz z przypisaniem ról lub funkcji. Konfiguracja musi umożliwiać uwierzytelnianie użytkowników i urządzeń w sieci komputerowej oraz ich autoryzację dostępu.</p>

	<p>Uruchomienie i konfiguracja serwera DHCP i DNS zgodnie z wytycznymi Zamawiającego przedstawionymi na etapie instalacji i konfiguracji.</p> <p>Instalacja i uruchomienie oprogramowania zarządzającego dostarczonego z serwerem.</p>
--	--

### 3. Macierz dyskowa

NAZWA KOMPONENTU	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
<b>OBUDOWA</b>	<p>Obudowa typu RACK do instalacji w standardowej szafie 19"o wysokości maksymalnej 2U wraz kompletem szyn umożliwiającym montaż w standardowej szafie RACK.</p> <p>Możliwość instalacji do 12 dysków 3.5" Hot Plug w jednostce kontrolerowej macierzy.</p> <p>Możliwość rozbudowy macierzy do co najmniej 250 napędów dyskowych poprzez dodatkowe moduły dyskowe, bez wymiany kontrolerów.</p> <p>Możliwość mieszania półek dyskowych 3,5" i 2,5".</p>
<b>KONTROLERY</b>	<p>Minimum 2 kontrolery pracujące w trybie active/active, z funkcjonalnością SAN.</p> <p>Zabezpieczenia RAID realizowane za pomocą sprzętowego, dedykowanego układu.</p> <p>Wymagane poziomy RAID 1, 5,6,10,50.</p>
<b>CACHE</b>	<p>Minimum 16GB pamięci cache z możliwością rozszerzenia z wykorzystaniem karty flash lub dysków SSD.</p> <p>Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na dyski lub posiadać podtrzymywanie bateryjne.</p>
<b>PRZESTRZEŃ DYSKOWA</b>	<p>Minimum 6 TB dostępnej przestrzeni netto zbudowanej w oparciu o grupę RAID5.</p> <p>Możliwość obsługi dysków SSD, SAS, NL-SAS.</p> <p>Możliwość rozbudowy macierzy za pomocą nowych dysków o większych pojemnościach oraz dysków typu SSD/Flash – zoptymalizowanych pod kątem zapisu bądź odczytu.</p> <p>Możliwość mieszania różnych rodzajów dysków w ramach jednej półki dyskowej.</p>
<b>INTERFEJSY</b>	<p>Minimum 4 interfejsy o prędkości minimum 8Gb/s umożliwiającymi podłączenie z dostarczonymi serwerami. Jeżeli wymagane, interfejsy muszą być wyposażone w odpowiednie wkładki.</p> <p>Macierz musi być dostarczona z odpowiednimi kablami o długości 2 m każdy umożliwiającymi podłączenie z zaferowanymi serwerami.</p>
<b>ZASILACZE</b>	<p>Minimum dwa redundantne, typu Hot-Plug, o mocy dopasowanej do samodzielnego zapewnienia zasilania dla całego urządzenia przy pełnym obciążeniu dyskami jednostki kontrolera.</p>
<b>WYDAJNOŚĆ</b>	<p>Obsługa minimum 512 logicznych wolumenów o rozmiarze do 256TB</p> <p>Obsługa minimum 128 grup RAID</p> <p>Możliwość obsługi minimum 256 hostów.</p> <p>Brak ograniczenia ilości dysków hot-spare.</p>
<b>REPLIKACJA DANYCH</b>	<p>Wymagana funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation).</p> <p>Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych lub testów</p>

	<p>systemów komputerowych. Wymagane dostarczenie w/w funkcjonalności umożliwiającej wykonanie minimum 128 kopii migawkowych LUN.</p> <p>W przypadku odtworzenia danych z dowolnej kopii migawkowej, urządzenie musi pozwalać na poprawne zachowanie także wcześniejszych jak i późniejszych snapshotów, z zachowaniem możliwości kolejnego odtworzenia danych zarówno ze wszystkich istniejących (starszych i nowszych) kopii dostępnych dla danego zasobu.</p> <p>Tworzenie na żądanie pełnej fizycznej kopii danych (klon) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Wymagane dostarczenie w/w funkcjonalności umożliwiającej wykonanie minimum 64 kopii danych LUN typu klon.</p> <p>Funkcjonalność kopiowania na żądanie danych ze źródłowego zasobu LUN na docelowy zasób LUN (ang. Lun Copy). Wymagane dostarczenie w/w funkcjonalności umożliwiającej wykonanie minimum 32 kopii LUN.</p>
<b>ZARZĄDZANIE</b>	<p>Zdalne zarządzanie oraz automatyczne informowanie centrum serwisowego o awarii.</p> <p>Stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów.</p> <p>Macierz powinna być zarządzalna zarówno z poziomu linii komend (CLI), jak również poprzez min. jeden interfejs graficzny (GUI).</p> <p>GUI powinno umożliwiać ustawienie nazwy systemu, konfigurację serwera NTP, dodawanie kolejnych zasobów dyskowych, zmianę hasła administratora, tworzenie raid group oraz wolumenów danych, migrację danych z innego systemu storage poprzez porty SAS lub FC, listowanie wolumenów podpiętych do danego hosta.</p> <p>Możliwość autentykacji poprzez LDAP.</p>
<b>BEZPIECZEŃSTWO</b>	<p>Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania.</p> <p>Wymagana jest redundancja wszystkich elementów urządzeń tj. kontrolerów, zasilaczy, wentylatorów i ścieżek do dysków. Wymiana tych elementów musi się odbywać bez konieczności wyłączenia urządzeń.</p>
<b>WSPARCIE DLA SYSTEMÓW OPERACYJNYCH</b>	<p>Microsoft® Windows®, VMware®, Hyper-V®, SLES, RHES</p>
<b>DOKUMENTACJA</b>	<p>Dokumentacji w języku polskim lub angielskim</p>
<b>INNE</b>	<p>Zamawiający wymaga montażu macierzy w szafie RACK, podłączenia z dostarczonymi serwerami, uruchomienia oraz konfiguracji zgodnie z wytycznymi Zamawiającego dostarczonymi na etapie realizacji z uwzględnieniem zaakceptowanego planu wdrożenia.</p> <p>Konfiguracja musi uwzględniać utworzenie minimum jednej grupy RAID w oparciu o dostarczone dyski.</p>

#### 4. System Backup

NAZWA KOMPONENTU	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
<b>INFORMACJE OGÓLNE</b>	<p>System backup-u danych musi realizować wszystkie poniższe funkcjonalności.</p> <p>Rozwiązanie musi umożliwiać tworzenie kopii zapasowych na dyskach twardych zapewniających wysoką dostępność poprzez przechowywanie danych na macierzy RAID, minimum 0, 1, 5, 6, 10, 50, 60.</p>
<b>OBUDOWA</b>	<p>Obudowa typu RACK 19" o wysokości maksymalnie 2U.</p>
<b>PROCESOR</b>	<p>Jeden procesor wielordzeniowy osiągający w teście PassMark CPU Mark wynik min. 9.000 punktów według wyników ze strony <a href="https://www.cpubenchmark.net/cpu_list.php">https://www.cpubenchmark.net/cpu_list.php</a></p>

<b>PAMIĘĆ RAM</b>	<p>Minimum 32 GB pamięci RAM typu RDIMM 2666 MT/s z możliwością rozbudowy do 768GB.</p> <p>Możliwe zabezpieczenia pamięci: ECC, SDDC, Rank Sparring</p>
<b>PRZESTRZEŃ DYSKOWA</b>	<p>Dostępna przestrzeń dyskowa do przechowywania kopii zapasowych zbudowana w oparciu o grupę RAID1 nie może być mniejsza jak 4TB.</p>
<b>INTERFEJSY SIECIOWE</b>	<p>Minimum dwa interfejsy sieciowe 10Gb Ethernet w standardzie Base-T.</p> <p>Minimum dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ .</p> <p>Jeden interfejs 1Gb w standardzie Base-T do zarządzania serwerem.</p> <p>Zamawiający wymaga dostarczenia kabli minimum 2m dla każdego wbudowanego interfejsu sieciowego.</p>
<b>WBUDOWANE PORTY</b>	<p>Minimum 1 x VGA lub nowszy;</p> <p>Minimum 2 porty USB 3.0.</p> <p>Porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.</p>
<b>ZASILANIE</b>	<p>Dwa redundantne zasilacze Hot Plug, każdy o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujące w sieci 230V 50/60Hz prądu zmiennego wraz z kablami zasilającymi o dł.min. 1,5m każdy.</p>
<b>BEZPIECZEŃSTWO</b>	<p>Panel diagnostyczny lub sygnalizacja LED umieszczona na froncie obudowy.</p> <p>Zintegrowany z płytą główną moduł TPM2.0.</p> <p>Fizyczne zabezpieczenie dedykowane przez producenta serwera chroniące przed nieuprawnionym dostępem do dysków twardej, montowane z przodu obudowy.</p>
<b>ZARZĄDZANIE</b>	<p>Oprogramowanie do zdalnego zarządzania serwerem: monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.), monitorowanie w czasie rzeczywistym poboru prądu przez serwer, zbieranie logów błędów hardware, przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury, montowanie wirtualnych napędów, zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego, wysyłanie zawiadomień drogą mailową lub poprzez SNMP.</p> <p>Nie dopuszcza się rozwiązań serwerowych wymagających dokupowania dodatkowych licencji umożliwiających zarządzanie serwerem i dostarczających wyżej wymienione funkcjonalności.</p>
<b>TWORZENIE KOPII</b>	<p>Rozwiązanie musi zapewnić funkcjonalność scentralizowanego systemu wykonywania kopii zapasowych w heterogenicznym środowisku (różne systemy operacyjne) z wykorzystaniem protokołów typu klient-serwer używający jako warstwę transportu TCP/IP: SMB, CIFS, SSHFS.</p> <p>Rozwiązanie musi posiadać wsparcie producenta oprogramowania dla instalacji systemu zarządzania na platformie wirtualnej.</p> <p>Rozwiązanie musi umożliwiać archiwizację otwartych plików baz danych.</p> <p>Musi umożliwiać archiwizację maszyn wirtualnych pracujących pod kontrolą minimum Microsoft Hyper-V, VMWare.</p> <p>Musi umożliwiać archiwizowanie danych z Microsoft Active Directory oraz rejestru systemowego i plików przechowywanych na dyskach systemu Microsoft Windows. Agent backupu musi współpracować z systemami operacyjnymi posiadającymi aktualnie wspieranych przez firmę Microsoft.</p> <p>Agent ma wspierać mechanizm deduplikacji danych.</p> <p>Agent nie wymaga dodatkowej licencji i może być zainstalowany na dowolnej liczbie komputerów.</p> <p>Rozwiązanie ma wspierać archiwizację otwartych i edytowanych plików.</p>

	<p>Rozwiązanie ma posiadać funkcję automatycznego backupu otwartego i edytowanego pliku.</p> <p>Rozwiązanie ma umożliwiać wykonywanie backupu w oparciu o harmonogram utworzony przez administratora.</p> <p>Rozwiązanie musi umożliwiać definiowanie różnych strategii wykonywania backupu dla poszczególnych obiektów podlegających backupowi.</p> <p>Wykonywanie backupu na lokalnie dostarczonym urządzeniu.</p> <p>Wykonywanie kopii na dyski oparte o technologię przyrostowej kopii migawkowej na poziomie bloków danych – tylko pierwszy backup jest pełny, pozostałe tylko przyrostowe (bez konieczności wykonywania kolejnych kopii pełnych), dla serwerów fizycznych i wirtualnych.</p> <p>Zarządzanie wieloma urządzeniami tego samego typu przy użyciu jednego interfejsu graficznego.</p> <p>Rozwiązanie musi umożliwiać utworzenie repozytorium danych zapisanych na urządzeniu na dyski lokalne oraz replikację na zewnętrzne nośniki typu taśmy, VTL, NAS</p>
<b>ODTWARZANIE DANYCH</b>	<p>Odtwarzanie danych musi odbywać się przy użyciu mechanizmów - dedykowanego klienta odtwarzania dla systemów Windows, interfejsu WWW.</p> <p>Dane muszą być odtwarzane przez administratorów urządzenia lub użytkowników końcowych w zależności od uprawnień.</p>
<b>RAPORTOWANIE</b>	<p>Rozwiązanie backupowe powinno udostępniać raporty pozwalające na analizę kluczowych elementów, takich jak minimum archiwizowania i odtwarzania danych oraz wykorzystania dostępnych zasobów dyskowych i systemowych.</p>
<b>ADMINISTRACJA SYSTEMEM KOPII ZAPASOWYCH I</b>	<p>Rozwiązanie ma być konfigurowane za pomocą graficznego interfejsu.</p> <p>Informowanie w formie wiadomości e-mail o statusie wykonania zadań backupowych.</p> <p>Pełne centralne zarządzanie przez www modułem wykonywania kopii zapasowych na serwerach w zakresie:</p> <ul style="list-style-type: none"> <li>• konfiguracji parametrów wykonywania kopii zapasowych,</li> <li>• przydzielania zadań wykonywania kopii zapasowych,</li> <li>• monitorowania stanu wykonania kopii zapasowych,</li> <li>• powiadamiania o stanie zadań backupu drogą mailową,</li> <li>• przeglądania i odtwarzania wybranych elementów wykonanych kopii zapasowych,</li> <li>• monitorowania w trybie graficznym aktualnego stanu systemu z uwzględnieniem:             <ul style="list-style-type: none"> <li>– statusu wykonanych zadań backupu (udane/nieudane),</li> <li>– aktualnej wielkości danych backupowych,</li> <li>– aktualnej zajętości repozytorium backupu.</li> </ul> </li> </ul>
<b>DOKUMENTACJA</b>	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>
<b>INNE</b>	<p>System musi być skonfigurowany zgodnie z wytycznymi administratora Zamawiającego, w sposób umożliwiający na automatyczne tworzenie kopii bezpieczeństwa z systemów zainstalowanych na dostarczonych serwerach.</p> <p>Pomiędzy urządzeniami składającymi się na system backup-u muszą być wszystkie połączenia kablowe zapewniające poprawny przebieg procesu tworzenia kopii zapasowych.</p>

	<p>Konfiguracja musi zapewniać tworzenie kopii dziennych, tygodniowych, miesięcznych z możliwością zapisywania na zewnętrznym napędzie oraz odtwarzanie danych z wykonanych kopii zapasowych.</p> <p>Wykonawca przeprowadzi instruktarz dla administratora Zamawiającego w zakresie uruchomionych rozwiązań, w stopniu umożliwiającym administratorowi samodzielną konfigurację i administrację urządzeniami.</p>
--	---

## 5. Urządzenie ochrony sieci - UTM

NAZWA KOMPONENTU	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
<b>INFORMACJE OGÓLNE</b>	<p>Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe.</p> <p>System musi być dostarczony z licencjami dla wszystkich funkcji bezpieczeństwa ze wsparciem na okres minimum 60-ciu miesięcy liczoną od dnia zakończenia wdrożenia całego systemu.</p> <p>Dopuszcza się, aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia.</p> <p>W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>Rozwiązanie musi być wyposażone w pamięć minimum 250GB do przechowywania logów.</p> <p>System musi zapewnić monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączności sieciowych.</p> <p>Dostarczone rozwiązanie musi umożliwić łączenie w klastr Active-Active lub Active-Passive każdego z elementów systemu.</p> <p>Rozwiązanie musi pozwalać na, wyłączenie / włączenie każdego z modułów rozwiązania, bez restartowania rozwiązania.</p> <p>Wymagane jest automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.</p>
<b>PORTY</b>	Minimum 8 interfejsów RJ45 Ethernet 10/100/1000.
<b>FUNKCJE BEZPIECZEŃSTWA</b>	<p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:</p> <ul style="list-style-type: none"> <li>- Kontrola dostępu – zapora ogniowa klasy Stateful Inspection</li> <li>- Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). System AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.</li> <li>- Poufność danych - IPSec VPN oraz SSL VPN</li> <li>- Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]</li> <li>- Kontrola stron Internetowych – Web Filter [WF]</li> <li>- Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3)</li> <li>- Kontrola pasma oraz ruchu [QoS i Traffic shaping]</li> <li>- Kontrola aplikacji oraz rozpoznawanie ruchu P2P</li> <li>- Analiza ruchu szyfrowanego protokołem SSL</li> </ul>
<b>WYDAJNOŚĆ</b>	<p>Wydajność systemu Firewall min 3 Gbps.</p> <p>Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus min. 400 Mbps.</p>

	<p>Wydajność ochrony przed atakami (IPS) min 2 Gbps.</p> <p>Wydajność VPN IPSec, nie mniej niż 600 Mbps.</p> <p>Musi zapewnić obsługę nie mniej niż 250 tys. jednoczesnych połączeń oraz 15 tys. nowych połączeń na sekundę.</p>
<b>FIREWALL</b>	<p>Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.</p> <p>Musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. W przypadku kiedy system nie posiada dysku lub nie pozwala na podłączenie zewnętrznych nośników, musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.</p> <p>Tworzenie obiektów dynamicznych.</p> <p>Podzielenie reguł firewalla na logiczne grupy.</p> <p>Tworzenie reguł firewalla uruchamianych dla SSL VPN.</p> <p>Definiowanie reguł na firewallu, automatycznie wyłączających się w ustalonym czasie.</p> <p>Obsługa translacji NAT adresu źródłowego i NAT adresu docelowego.</p> <p>Tworzenie wydzielonych stref bezpieczeństwa Firewall np. DMZ.</p> <p>Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.</p> <p>Przechwytywanie i rozszyfrowywanie ruchu SSL.</p> <p>Blokowanie pojedynczych funkcji konkretnych aplikacji.</p>
<b>VPN</b>	<p>Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site.</p> <p>Rozwiązanie musi posiadać możliwość tworzenia specjalnych tuneli VPN, służących do zarządzania urządzeniami, niezależnie od głównego tunelu VPN.</p> <p>Rozwiązanie musi obsługiwać tryb mieszany VPN.</p> <p>Rozwiązanie musi zapewnić możliwość wyznaczania transportów zapasowych.</p> <p>Rozwiązanie musi zapewniać budowanie tuneli VPN w oparciu o protokół IPSec.</p> <p>Rozwiązanie musi zezwalać na nawiązywanie połączeń SSL VPN w trybie portalowym.</p> <p>Rozwiązanie musi posiadać w standardzie, darmowego klienta SSL VPN dla systemów MS Windows.</p> <p>Rozwiązanie musi umożliwiać tworzenie kanałów VPN (client-2-site) wykorzystując wbudowany w Windows mechanizm tworzenia połączeń PPTP (bez aplikacji firm trzecich).</p> <p>Rozwiązanie musi zapewniać centrum autoryzacji na lokalnym serwerze VPN.</p> <p>Rozwiązanie musi umożliwiać uwierzytelnianie użytkowników VPN za pomocą certyfikatów cyfrowych i/lub logowania.</p> <p>Oferowany klient VPN musi być stworzony przez tą samą firmę co dostarczone rozwiązanie.</p> <p>Oferowany klient VPN ma być dedykowany na platformy Windows.</p> <p>Oferowany klient VPN musi posiadać graficzny interfejs użytkownika.</p> <p>Rozwiązanie musi umożliwiać przydzielanie ustawień tunelu VPN client-to-site na podstawie przynależności użytkownika do grupy zabezpieczeń w usłudze katalogowej Active Directory lub LDAP.</p> <p>Rozwiązanie musi posiadać możliwość uwierzytelniania certyfikatem X.509 przy integracji z zewnętrzną infrastrukturą PKI i przydzielanie ustawień tunelu VPN client-to-site w zależności od atrybutów certyfikatu.</p>



	<p>Rozwiązanie musi zapewniać obsługę uwierzytelniania stron przy tworzeniu tuneli VPN typu site-to-site oraz client-to-site za pomocą certyfikatów X.509 ze struktury PKI zarządzanej przez dowolny serwer PKI z obsługą list CRL.</p> <p>Rozwiązanie musi umożliwiać zarządzania pasmem w ramach tunelu VPN.</p> <p>Rozwiązanie musi automatycznie zmieniać trasowanie ruchu VPN w przypadku awarii tunelu VPN.</p> <p>Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</p> <p>Praca w topologii Hub and Spoke oraz Mesh.</p> <p>Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.</p> <p>Obsługa ssl vpn w trybach portal oraz tunel.</p>
<b>IPS</b>	<p>Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów.</p> <p>Możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.</p>
<b>ANTYWIRUS</b>	<p>Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). System AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.</p>
<b>WEB FILTER</b>	<p>Baza filtra WWW pogrupowana w min 50 kategorii tematycznych.</p> <p>W ramach filtra www muszą być dostępne m.in. kategorie spyware, malware, spam, proxy avoidance, sieci społecznościowe, zakupy.</p> <p>Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.</p>
<b>KONTROLA APLIKACJI</b>	<p>Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p>
<b>INTERFEJSY WIRTUALNE</b>	<p>Możliwość tworzenia min 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.</p>
<b>OBSŁUGA ROUTINGU</b>	<p>Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.</p>
<b>UWIERZYTELNIANIE</b>	<p>Uwierzytelnianie tożsamości użytkowników za pomocą minimum:</p> <ul style="list-style-type: none"> <li>- haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu;</li> <li>- haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP;</li> <li>- haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych ;</li> </ul> <p>Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.</p>
<b>RAPORTOWANIE</b>	<p>System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.</p> <p>W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jest nie mniej niż:</p> <ul style="list-style-type: none"> <li>- Posiadanie predefiniowanych raportów dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego</li> <li>- Generowanie co najmniej 25 różnych typów raportów</li> </ul> <p>System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania.</p> <p>Rozwiązanie musi umożliwiać generowanie statystyk w czasie rzeczywistym.</p>

<b>POLITYKA BEZPIECZEŃSTWA</b>	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
<b>AKTUALIZACJA</b>	Wymagane jest automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
<b>ZARZĄDZANIE</b>	<p>Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>Rozwiązanie ma umożliwiać zdalne zarządzania firewallem, VPN oraz pozostałymi serwisami z jednej graficznej konsoli administracyjnej dostępnej przez przeglądarkę Internetową.</p> <p>Rozwiązanie musi posiadać możliwość przeglądania zmian nanoszonych przez automatyczne aktualizacje systemu, z graficznej konsoli administracyjnej.</p> <p>Rozwiązanie musi posiadać funkcję, która pozwala na zapisywanie zmian konfiguracji urządzenia.</p> <p>Rozwiązanie musi zapewnić obsługę uwierzytelniania administratorów przy pomocy hasła (lokalnego lub synchronizowanego z usługą katalogową).</p> <p>Rozwiązanie musi wspierać administrację urządzeniem opartą na rolach i współdzieleniu pracy kilku administratorów jednocześnie. System musi zapobiegać konfliktom między administratorami oraz logować wszystkie zmiany wprowadzane przez wszystkich administratorów.</p> <p>Rozwiązanie musi zapewniać możliwość integracji z Centralnym Zarządzaniem wszystkimi urządzeniami, pracującymi w strukturze geograficznie rozproszonej w wielu lokalizacjach jednocześnie.</p> <p>Rozwiązanie musi zapewniać możliwość uruchamiania własnych skryptów z poziomu CLI.</p> <p>Urządzenie musi posiadać bazę predefiniowanych skryptów, do dyspozycji administratora, dostępnych z poziomu CLI.</p> <p>Rozwiązanie musi mieć możliwość zarządzania systemem przez większą liczbę administratorów o określonych uprawnieniach.</p>
<b>CERTYFIKATY</b>	Certyfikat Common Criteria EAL4+ lub równoważny.
<b>INNE</b>	<p>Urządzenie musi być skonfigurowane zgodnie z wytycznymi administratora Zamawiającego, z uwzględnieniem minimalnych prac:</p> <ul style="list-style-type: none"> <li>– Weryfikacja założeń wdrożenia</li> <li>– Konfiguracja sieci (interfejsy i routing)</li> <li>– Konfiguracja firewalla</li> <li>– Konfiguracja NAT</li> <li>– Konfiguracja IPS – zgodnie z wymaganiami klienta</li> <li>– Konfiguracja dodatkowych usług sieciowych tj. DHCP, DNS Proxy</li> <li>– Integracja z AD lub założenie wewnętrznej bazy użytkowników (bez dodawania użytkowników).</li> <li>– Konfiguracja transparentnej autoryzacji w AD – konfiguracja po stronie urządzenia, inżynier nie instaluje agenta SSO a jedynie instruuje klienta jak powinna przebiegać instalacja.</li> <li>– Konfiguracja VPN: <ul style="list-style-type: none"> <li>• IPSec Site-to-Site– zgodnie z otrzymanymi od klienta parametrami tuneli.</li> <li>• IPSec Client-to-Site – konfiguracja urządzenia i jednej wzorcowej stacji klienckiej na kliencie dedykowanym lub ShrewVPN.</li> </ul> </li> <li>– Konfiguracja SSL VPN lub PPTP VPN.</li> </ul>

	<p>Urządzenie musi zostać podłączone do istniejącej infrastruktury Zamawiającego i uruchomione w celu weryfikacji poprawności konfiguracji.</p> <p>Wykonawca przeprowadzi instruktarz dla administratora Zamawiającego w zakresie w/w zagadnień, w stopniu umożliwiającym administratorowi samodzielną konfigurację i administrację urządzenia.</p> <p>W okresie minimum 36 miesięcy od podpisania protokołu odbioru, wykonawca zapewni wsparcie techniczne.</p>
--	--

## 6. Zasilacz awaryjny UPS

NAZWA KOMPONENTU	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
<b>MOC WYJŚCIOWA CZYNNA</b>	Moc wyjściowa czynna musi być dobrana w sposób umożliwiający podtrzymanie bateryjne zasilania przez minimum 15 minut przy 100% obciążenia w przypadku zaniku zasilania głównego, wszystkich urządzeń dostarczonych w ramach projektu i zainstalowanych w szafie serwerowej RACK z uwzględnieniem 10% zapasu mocy dla przyszłych rozszerzeń systemu, przy czym nie może być mniejsza niż 2500 W
<b>RODZAJ URZĄDZENIA</b>	Zasilacz typu line-interactive.
<b>WEJŚCIE</b>	Zakres napięcia wejściowego: 170 - 280 V Zakres częstotliwości napięcia wejściowego: 50/60 Hz ±3%
<b>PRÓG PRZEŁĄCZENIA</b>	190 – 250 ±5%
<b>WYJŚCIE</b>	Sinusoidalny kształt napięcia wyjściowego Zniekształcenie napięcia wyjściowego < 5% Zakres napięcia wyjściowego 220V/230V/240V
<b>WYDAJNOŚĆ</b>	Minimum 93%
<b>ZABEZPIECZENIE</b>	wejście - przeciwzwarcowe i przeciwprzepięciowe wyjście - przeciwzwarcowe i przeciążeniowe
<b>GNIAZDA PRZYŁĄCZA WYJŚCIOWEGO</b>	Minimum 4 x IEC C13 (10A)
<b>PORTY</b>	Min.1x USB, 1x RJ45 (SNMP)
<b>INNE</b>	Zimny start. Przewód zasilający zakończony wtyczką z uziemieniem. Oprogramowanie zarządzające – monitorujące. Dźwiękowa sygnalizacja rozładowania baterii. Wyświetlacz LCD. Możliwość instalacji dodatkowych modułów bateryjnych gwarantujących dłuższe czasy podtrzymania zasilania. Obsługa SNMP UPS zostanie wstawione do pomieszczenia wskazanego przez Zamawiającego, zainstalowany, podłączony do istniejącej infrastruktury elektrycznej i teletechnicznej oraz uruchomiony.
<b>CERTYFIKATY</b>	Zgodność z dyrektywą RoHS UE lub równoważną.

## 7. Zestaw komputerowy z systemem operacyjnym i pakietem biurowym

NAZWA KOMPONENTU	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
<b>STACJA KOMPUTEROWA</b>	
<b>OBUDOWA</b>	Małogabarytowa z obsługą kart PCI Express, wyposażona w min. 1 kieszeń wewnętrzną dedykowaną dla dysku twardego, Obudowa powinna fabrycznie umożliwiać montaż min 1 szt. dysku 2,5" lub dysku 3,5"
<b>PROCESOR</b>	Wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 7000 punktów.
<b>PAMIĘĆ OPERACYJNA RAM</b>	Minimum 8GB DDR4 2666 MHz, możliwość rozbudowy do min 32GB.
<b>PAMIĘĆ MASOWA</b>	Minimum 1 x 256 GB SSD
<b>GRAFIKA</b>	Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem DirectX 12 lub nowszym, OpenGL 4.6 lub nowszym, OpenCL 1.2 lub nowszym; Pamięć współdzielona z pamięcią RAM, obsługująca rozdzielczości minimum 1920x1200 @ 60Hz.
<b>KARTA SIECIOWA</b>	Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika)
<b>WYPOSAŻENIE MULTIMEDIALNE</b>	Min 24-bitowa karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik 2W w obudowie komputera.
<b>PORTY</b>	Minimum 1 port HDMI; Minimum 2 porty DisplayPort; Minimum min. 8 portów USB wyprowadzonych na zewnątrz komputera w tym min 4 porty USB 3.1; min. 2 porty USB 3.0 z przodu obudowy. Minimum 1 port audio tzw. combo ( słuchawka/mikrofon) i min. 1 port Line-out Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
<b>ZASILANIE</b>	Zasilacz o mocy max. 250W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności nie mniejszej niż 80% przy pełnym obciążeniu.
<b>ZGODNOŚĆ Z SYSTEMAMI OPERACYJNYMI I STANDARDAMI</b>	Potwierdzenie kompatybilności komputera na daną platformę systemową (w przypadku braku możliwości weryfikacji przez Zamawiającego na stronie www producenta platformy systemowej Wykonawca na żądanie Zamawiającego dostarczy na etapie weryfikacji oferty potwierdzonej za zgodność z oryginałem wydruk potwierdzający kompatybilności komputera na daną platformę systemową).
<b>BEZPIECZEŃSTWO</b>	Urządzenie musi być wyposażone w dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego.
<b>Bios</b>	BIOS zgodny ze specyfikacją UEFI. Pełna obsługa BIOS za pomocą klawiatury i myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: <ul style="list-style-type: none"> <li>– wersji BIOS,</li> <li>– zainstalowanej pamięci RAM,</li> <li>– rodzaj napędów optycznych,</li> </ul>

	<ul style="list-style-type: none"> <li>– pojemności zainstalowanego dysku twardego,</li> <li>– MAC adresie zintegrowanej karty sieciowej,</li> <li>– kontrolerze audio,</li> </ul> <p>Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS).</p>
<b>WYMAGANIA DODATKOWE</b>	<p>Klawiatura USB w układzie polski programisty. Mysz USB.</p>
<b>SYSTEM OPERACYJNY</b>	<p>Zainstalowany system operacyjny klasy PC, spełniający wszystkie poniższe wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji.</p> <p>Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) - wymagane podanie nazwy strony serwera WWW;</p> <p>Internetowa aktualizacja zapewniona w języku polskim;</p> <p>Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;</p> <p>Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play, Wi-Fi);</p> <p>Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta;</p> <p>Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;</p> <p>Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie, praca systemu w trybie ochrony kont użytkowników;</p> <p>Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;</p> <p>Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie. Aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych;</p> <p>Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi;</p> <p>Wbudowany system pomocy w języku polskim;</p> <p>Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);</p> <p>Możliwość zarządzania stacją roboczą poprzez polityki - przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;</p> <p>Wdrażanie IPSEC oparte na politykach - wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;</p> <p>Wsparcie dla logowania przy pomocy smartcard;</p> <p>Rozbudowane polityki bezpieczeństwa - polityki dla systemu operacyjnego i dla wskazanych aplikacji;</p> <p>Narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;</p>

	<p>Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 - możliwość uruchomienia aplikacji działających we wskazanych środowiskach;</p> <p>Wsparcie dla JScript i VBScript - możliwość uruchamiania interpretera poleceń,</p> <p>Zdalna pomoc i współdzielenie aplikacji - możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem;</p> <p>Graficzne środowisko instalacji i konfiguracji;</p> <p>Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;</p> <p>Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe;</p> <p>Możliwość przywracania plików systemowych;</p> <p>Funkcjonalność pozwalająca na identyfikację sieci komputerowych, do których jest system podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików ftp.);</p> <p>Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);</p> <p>Możliwość, w ramach posiadanej licencji, do używania co najmniej dwóch wcześniejszych wersji oprogramowania systemowego.</p>
<b>CERTYFIKATY</b>	<p>Deklaracja zgodności z dyrektywą RoHS lub równoważną.</p> <p>Certyfikat zgodności z dyrektywą WEEE Parlamentu Europejskiego sprawie zużytego sprzętu elektrotechnicznego i elektronicznego.</p> <p>Certyfikat zgodności ze standardem EPEAT na poziomie minimum Silver.</p> <p>Oferowany komputer musi spełniać wymogi specyfikacji technicznej Energy Star i posiadać oznaczenie znakiem usługowym ENERGY STAR lub spełniać kryteria efektywności energetycznej co najmniej równoważne z koniecznymi do uzyskania takiego oznaczenia.</p> <p>W przypadku braku w/w certyfikatów na internetowych stronach producenta, Zamawiający na etapie weryfikacji oferty będzie wymagał przedstawienia dokumentów potwierdzających spełnienie przez produkt w/w wymagań jakościowych.</p>
<b>MONITOR</b>	
<b>TYP EKRANU</b>	Ekran ciekłokrystaliczny z aktywną matrycą IPS typu LED min. 23,8" (16:9) z utwardzoną powłoką antyodblaskową,
<b>PARAMETRY MATRYCY</b>	<p>Jasność: 250 cd/m<sup>2</sup></p> <p>Kontrast: Typowy 1000:1</p> <p>Rozdzielczość 1920 x 1200 przy 60Hz</p> <p>Czas reakcji: max 8ms</p>
<b>ZŁĄCZA</b>	1x Display Port, 4 x USB, w tym minimum 2 porty w wersji 3.0 , 1 x HDMI
<b>CERTYFIKATY</b>	EPEAT Gold, Energy Star, WEEE lub certyfikaty równoważne do wymienionych, bądź urządzenie musi spełniać kryteria jakościowe co najmniej równoważne z koniecznymi do uzyskania takiego oznaczenia. W przypadku braku w/w certyfikatów na internetowych stronach producenta, Zamawiający na etapie weryfikacji oferty będzie wymagał przedstawienia dokumentów potwierdzających spełnienie przez produkt w/w wymagań jakościowych.
<b>PAKIET BIUROWY</b>	
<b>INTERFEJS UŻYTKOWNIKA</b>	Pełna polska wersja językowa interfejsu użytkownika.

	<p>Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) - użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.</p>
<p><b>TWORZENIE I EDYCJA DOKUMENTÓW ELEKTRONICZNYCH</b></p>	<p>Kompletny i publicznie dostępny opis formatu, Zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766), umożliwia wykorzystanie schematów XML, Musi wspierać w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A. 1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766),</p>
<p><b>EDYTOR TEKSTÓW</b></p>	<p>Edycja i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, Wstawianie oraz formatowanie tabel, Wstawianie oraz formatowanie obiektów graficznych, Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, Automatyczne tworzenie spisów treści, Formatowanie nagłówków i stopek stron, Sprawdzanie pisowni w języku polskim, Śledzenie zmian wprowadzonych przez użytkowników, Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, Określenie układu strony (pionowa/pozioma), Wydruk dokumentów, Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną Pracę na dokumentach utworzonych przy pomocy minimum Microsoft Word 2010, 2013, 2016, 2019 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu, Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem, Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa, Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.</p>
<p><b>ARKUSZ KALKULACYJNY</b></p>	<p>Tworzenie raportów tabelarycznych, Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych</p>

	<p>Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.</p> <p>Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)</p> <p>Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową analizę wariantową i rozwiązywanie problemów optymalizacyjnych</p> <p>Tworzenie raportów tabeli przestawnych umożliwiającą dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych</p> <p>Wyszukiwanie i zamiana danych</p> <p>Wykonywanie analiz danych przy użyciu formatowania warunkowego</p> <p>Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie</p> <p>Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności</p> <p>Formatowanie czasu, daty i wartości finansowych z polskim formatem I. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.</p> <p>Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania minimum Microsoft Excel 2010, 2013, 2016, 2019 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleczeń.</p> <p>Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.</p>
<p><b>NARZĘDZIE DO PRZYGOTOWYWANIA I PROWADZENIA PREZENTACJI</b></p>	<p>Prezentowanie przy użyciu projektora multimedialnego,</p> <p>Drukowanie w formacie umożliwiającym robienie notatek,</p> <p>Zapisanie jako prezentacja tylko do odczytu,</p> <p>Nagrywanie narracji i dołączanie jej do prezentacji,</p> <p>Opatrywanie slajdów notatkami dla prezentera,</p> <p>Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,</p> <p>Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,</p> <p>Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,</p> <p>Możliwość tworzenia animacji obiektów i całych slajdów,</p> <p>Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym, monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera,</p> <p>Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania minimum Microsoft PowerPoint 2010, 2013, 2016, 2019.</p>
<p><b>NARZĘDZIE DO ZARZĄDZANIA INFORMACJĄ PRYWATNĄ (POCZTĄ ELEKTRONICZNĄ KALENDARZEM, KONTAKTAMI I ZADANIAMI)</b></p>	<p>Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,</p> <p>Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,</p> <p>Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,</p> <p>Automatyczne grupowanie poczty o tym samym tytule,</p> <p>Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,</p> <p>Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia,</p> <p>Udostępnianie Kalendarza innym użytkownikom,</p> <p>Przeglądanie kalendarza innych użytkowników,</p>



	<p>Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,</p> <p>Zarządzanie listą zadań,</p> <p>Zlecanie zadań innym użytkownikom,</p> <p>Zarządzanie listą kontaktów,</p> <p>Udostępnianie listy kontaktów innym użytkownikom, przeglądanie listy kontaktów innych użytkowników,</p> <p>Możliwość przesyłania kontaktów innym użytkownikom.</p>
<b>INNE</b>	<p>Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców;</p> <p>Do aplikacji musi być dostępna pełna dokumentacja w języku polskim,</p>

## 8. System operacyjny

NAZWA KOMPONENTU	WYMAGANE MINIMALNE PARAMETRY FUNKCJONALNE
<b>FUNKCJONALNOŚĆ</b>	<p>System operacyjny klasy PC, spełniający wszystkie poniższe wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji.</p> <p>Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) - wymagane podanie nazwy strony serwera WWW;</p> <p>Internetowa aktualizacja zapewniona w języku polskim;</p> <p>Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;</p> <p>Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play, Wi-Fi);</p> <p>Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta;</p> <p>Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;</p> <p>Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie, praca systemu w trybie ochrony kont użytkowników;</p> <p>Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;</p> <p>Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie. Aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych;</p> <p>Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi;</p> <p>Wbudowany system pomocy w języku polskim;</p> <p>Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);</p>

	<p>Możliwość zarządzania stacją roboczą poprzez polityki - przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;</p> <p>Wdrażanie IPSEC oparte na politykach - wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;</p> <p>Wsparcie dla logowania przy pomocy smartcard;</p> <p>Rozbudowane polityki bezpieczeństwa - polityki dla systemu operacyjnego i dla wskazanych aplikacji;</p> <p>Narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;</p> <p>Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 - możliwość uruchomienia aplikacji działających we wskazanych środowiskach;</p> <p>Wsparcie dla JScript i VBScript - możliwość uruchamiania interpretera poleceń,</p> <p>Zdalna pomoc i współdzielenie aplikacji - możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem;</p> <p>Graficzne środowisko instalacji i konfiguracji;</p> <p>Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;</p> <p>Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe;</p> <p>Możliwość przywracania plików systemowych;</p> <p>Funkcjonalność pozwalająca na identyfikację sieci komputerowych, do których jest system podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików ftp.);</p> <p>Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);</p> <p>Możliwość, w ramach posiadanej licencji, do używania co najmniej dwóch wcześniejszych wersji oprogramowania systemowego.</p>
--	---

## 9. Skaner dokumentów A4

NAZWA KOMPONENTU	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
RODZAJ SKANERA	A4 dwustronny z automatycznym podajnikiem (ADF) z możliwością podpięcia modułu Flatbed
ROZDZIELCZOŚĆ	Optyczna 600 dpi
PRĘDKOŚĆ SKANOWANIA	50 kartek na minutę w trybie SIMPLEX, 120 obrazów na minutę
DZIENNE OBCIĄŻENIE	4000 stron
SKANOWANE FORMATY	A8-A4 w trybie automatycznym, A3 w trybie ręcznym
PANEL KONTROLNY	LCD z możliwością predefiniowania minimum 7 profili skanowania i uruchomienia ich z poziomu skanera.
PODAJNIK PAPIERU	80 arkuszy A4 o gramaturze 80g/m <sup>2</sup>
GRAMATURA PAPIERU	35-410 g/m <sup>2</sup>
INTERFEJSY	USB 2.0

<b>FORMATY SKANOWANYCH PLIKÓW</b>	JPEG, PDF, TIFF, BMP, RTF
<b>WSPARCIE DLA STEROWNIKÓW</b>	TWAIN, ISIS
<b>JAKOŚĆ SKANOWANIA</b>	<p>Czujnik podwójnych pobrań dokumentów;          Likwidacja przekosu;          Automatyczne rozpoznawanie wielkości i rozmiaru dokumentu;          Usuwanie kolorów;          Skanowanie dwustrumieniowe kolor i czarno-biały za jednym przebiegiem;          Interaktywna regulacja koloru, regulacja jasności i kontrastu;          Automatyczna rotacja dokumentu, automatyczne wykrywanie koloru,          Inteligentne wygładzanie koloru tła;          Inteligentne wypełnienie krawędzi obrazu;          Scalanie obrazów;          Wykrywanie pustych stron na podstawie procentowej zawartości oraz rozmiarze pliku;          Filtrowanie smug;          Filtr ostrości.</p>

## 10. Stanowisko Potwierdzenia Profilu Zaufanego

NAZWA KOMPONENTU	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
<b>INFORMACJE OGÓLNE</b>	Stanowisko Potwierdzenia Profilu Zaufanego będzie zorganizowane na zestawie komputerowym wskazanym przez Zamawiającego. Dla potrzeb stanowiska wymagane będzie dostarczenie drukarki A4.
<b>DRUKARKA</b>	<p>Laserowa kolorowa A4 pozwalająca na automatyczny druk dwustronny, z funkcją kopiowania i skanowania          Technologia druku: laserowa          Rozdzielczość druku 600 x600          Prędkość druku 25 str./min          Wydajność: 40.000 stron A4/miesiąc          Podajnik papieru: 250 arkuszy z możliwością rozbudowy do 500 arkuszy          Automatyczny podajnik papieru: 50 arkuszy          Języki drukowania: PCL6, PCL5c, emulacja Postscript Level3, PDF, natywna obsługa pakietu biurowego          Wyświetlacz LCD kolorowy, dotykowy          Wbudowana karta Ethernet 10/100/1000 Base-TX          Port USB 2.0          Wbudowana pamięć 256 MB DRAM          Wbudowany skaner płaski z automatycznym podajnikiem dokumentów          Skanowanie dwustronne automatyczne          Prędkość skanowania 25 str./min</p>
<b>DOKUMENTACJA STANOWISKA PPZ</b>	<p>Opisane w dokumentacji świadczenie usługi na stanowisku musi być zgodnie z Rozporządzeniem Ministra Cyfryzacji z dnia 29 czerwca 2020 r. w sprawie profilu zaufanego i podpisu zaufanego (Dz.U. 2020 poz.1194):</p> <ol style="list-style-type: none"> <li>procedurze nadawania uprawnień do obsługi punktu potwierdzania profili zaufanych ePUAP</li> <li>procedurze utworzenia punktu potwierdzającego profil zaufany ePUAP</li> </ol>

i zgodnie z Rozporządzeniem Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (Dz.U. 2019 poz.1969).

Dokumentacja będzie obejmowała:

- a) procedurę zarządzania profilami zaufanymi ePUAP;
- b) procedurę utworzenia punktu potwierdzającego profil zaufany ePUAP;
- c) procedura nadawania uprawnień do potwierdzania, przedłużania ważności i unieważniania profili zaufanych ePUAP;
- d) wypełniony wniosek o utworzeniu Punktu Autoryzacji Profilu Zaufanego zgodnie z obowiązującym wzorem.