Załącznik nr 1 do SIWZ

Opis Przedmiotu Zamówienia (OPZ)

dotyczący postępowania o udzielenie zamówienia na:

dostawę sprzętu i oprogramowania

w ramach projektu pn.: „Projekt zintegrowanej informacji geodezyjno-kartograficznej Powiatu Gołdapskiego”

prowadzonego w trybie przetargu nieograniczonego o wartości równej lub wyższej niż kwoty określonej w przepisach wydanych na podstawie art. 11 ust. 8 Ustawy Prawo Zamówień Publicznych

Sporządzony zgodnie z art. 36 ust. 1 i 2 ustawy prawo zamówień publicznych.

Znak postępowania: GN.272.8.2018

Spis treści

1. Ogólne informacje

Niniejszy przedmiot zamówienia jest częścią projektu pn. „Projekt zintegrowanej informacji geodezyjno-kartograficznej Powiatu Gołdapskiego”, którego celem jest cyfryzacja zasobu geodezyjnego i kartograficznego oraz udostępnienie go poprzez e-usługi o wysokim stopniu dojrzałości.
Przedmiot zamówienia został podzielony na dwie części:

Część 1, której przedmiotem jest:
- Utworzenie e-usług publicznych wraz z uruchomieniem funkcjonalności płatności on-line oraz uruchomienie geoportalu zgodnego ze standardem WCAG 2.0
- Modernizacja systemów dziedzinowych
- Platforma GIS - budowa geoportalu
- Szyna usług integrująca usługi ePUAP, EZD i systemy dziedzinowe
- Szkolenie dla pracowników z zakresu obsługi wdrożonych e-usług.

Część 2, której przedmiotem jest:
- Dostawa następującego sprzętu serwerowego i urządzeń:
  - Serwer – 1 szt.
  - Centralny UPS – 1 szt.
  - UTM – 1 szt.
  - Serwer NAS – 1 szt.

Opisane poniżej wymagania stanowią zakres minimalnych oczekiwań Zamawiającego dla przedmiotu dostawy. Zamawiający dopuszcza równoważność rozwiązań:

1. Wszędzie tam, gdzie przedmiot zamówienia jest opisany poprzez wskazanie znaków towarowych, patentów lub pochodzenia, Zamawiający dopuszcza zastosowanie przez Wykonawcę rozwiązań równoważnych w stosunku do opisanych w SIWZ, pod warunkiem, że będą one posiadały, co najmniej takie same lub lepsze parametry techniczne, funkcjonalne i nie obniżą określonych w SIWZ standardów.
2. W przypadku, gdy Wykonawca zaproponuje urządzenia, instalacje, materiały i inne elementy równoważne, zobowiązany jest wykonać i załączyć do oferty zestawienie wszystkich zaproponowanych urządzeń, instalacji, materiałów oraz innych elementów równoważnych i wykazać ich równoważność w stosunku do urządzeń, instalacji, materiałów i innych elementów opisanych w SIWZ, stanowiącej opis przedmiotu zamówienia ze wskazaniem nazwy, strony i pozycji, których dotyczy.
3. Wszystkie zaproponowane przez Wykonawcę równoważne urządzenia, instalacje, materiały lub inne elementy muszą:
   a. posiadać parametry techniczne i funkcjonalne nie gorsze od określonych w SIWZ,
   b. zapewniać pełną kompatybilność sprzętową i programową z rozwiązaniami określonymi w SIWZ,
   c. posiadać stosowne certyfikaty, świadectwa dopuszczenia oraz atesty.

1.1. Miejsce realizacji usług

Usługi będą realizowane w siedzibie Zamawiającego pod adresem:

Powiat Gołdapski

Starostwo Powiatowe w Gołdapi
ul. Krótka 1
19-500 Gołdap

1.2. Termin i Harmonogram Wykonania Zamówienia

Przedmiot umowy musi być zrealizowany zgodnie z Harmonogramem w nie przekraczalnym terminie określonym w tabelach poniżej.

Część 1

Nazwa zadania	**Termin realizacji**
Utworzenie e-usług publicznych wraz z uruchomieniem funkcjonalności płatności on-line oraz dostosowaniem strony geoportalu do standardu WCAG 2.0	**do dnia 31.05.2019**
Modernizacja systemów dziedzinowych	**do dnia 31.04.2019**
Platforma GIS (budowa geoportalu)	**do dnia 31.04.2019**
Szyna usług integrująca usługi ePUAP, EZD i systemy dziedzinowe	**do dnia 31.04.2019**
Szkolenie dla pracowników z zakresu obsługi wdrożonych e-usług oraz z zakresu szyny usług	**do dnia 30.06.2019**

Część 2

Nazwa zadania	**Termin realizacji**
Dostawa sprzętu serwerowego i urządzeń	**30 dni roboczych od podpisania umowy**
W tym montaż i uruchomienie sprzętu serwerowego i urządzeń nie dłużej niż 14 dni – (praca po godzinach pracy urzędu w dni wolne lub na stanowiskach na których pracują osoby nieobecne w pracy).	

2. Część 1

2.1. Utworzenie e-usług publicznych wraz z uruchomieniem funkcjonalności płatności on-line oraz uruchomieniem geoportalu zgodnego ze standardem WCAG 2.0

W ramach niniejszego zadania zostanie uruchomionych 15 e-usług o wysokim poziomie dojrzałości (3, 4 i 5 poziom dojrzałości). E-usługi będą dostępne z poziomu strony geoportalu, który również zostanie uruchomiony w ramach projektu.

W ramach zadania zostaną uruchomione następujące e-usługi:

a. Usługa przeglądania mapy
b. Usługa zgłaszania prac geodezyjnych i uzgadniania listy materiałów zasobu
c. Usługa obsługi zgłoszeń uzupełniających
d. Generowanie dokumentu opłaty wraz z płatnością elektroniczną
e. Usługa przeglądania zgłoszonych zakończonych/nieza-kończonych prac geodezyjnych
f. Pobranie materiałów zasobu z obszaru zgłoszonej pracy wraz z Licencją
g. Pobieranie danych z bazy EGiB, GESUT, BDOT 500, BDSOG
h. Przekazywanie wyników pracy
i. Zamówienie zbioru danych RCiWN
j. Usługa generowania licencji i wydania zbioru danych RCiWN
k. Usługa potwierdza-jąca występowanie określonej osoby lub instytucji w bazie EGiB
l. Usługa pozyskiwania atrybutów obiektów bazy danych EGiB, geokodowania podmiotu ewidencyjnego, udostępniania informacji dla gminy wg wskazanych instytucji, udostępniania informacji dla gminy wg wskazanych osób fizycznych udostępniania informacji dla gminy wg wskazanych działek.
m. Zamówienie mapy ewidencji gruntów i budynków lub mapy zasadniczej wraz z generowaniem licencji i wydaniem produktu. E-usługa wykorzystuje EWMAPA
n. Zamówienie Wypisu/Wypisu i Wyrysu/Wyrysu z bazy EGiB wraz z generowaniem licencji i wydaniem produktu. E-usługa wykorzystuje EWOPIS
o. Zamówienie rejestrów, kartotek, skorowidzów, wykazów, zestawień tworzonych w bazie danych EGiB wraz z generowaniem licencji i wydawaniem produktu

Zadanie to obejmuje uruchomienie funkcjonalności e-płatności. System ten umożliwi dokonywanie płatności przez Internet w ramach świadczonych e-usług. Zintegrowany system płatności będzie sprzęgnięty z systemami dziedzinowymi w Starostwie, elektronicznym obiegiem dokumentów oraz wdrażanymi e-usługami. Dane dotyczące płatności będą przesyłane do właściwego systemu dziedzinowego, dzięki czemu będzie możliwa aktualizacja danych w czasie rzeczywistym. System pozwoli na dokonywanie płatności przy pomocy kart debetowych, kredytowych oraz poprzez przelewy elektroniczne z dowolnego z większych banków oferujących e-przelewy na terenie Polski.

Dzięki integracji systemu płatności z systemami dziedzinowymi oraz nowo wdrożonymi e-usługami, możliwe będzie zaczytywanie części danych z profilu użytkownika.

Funkcjonalności systemu płatności elektronicznych:

a. Umożliwi dokonywanie wpłat z tytułu opłat generowanych z poziomu systemów dziedzinowych pozwalając na uregulowanie drogą elektroniczną, opłat za czynności urzędowe oraz innych opłat w zakresie realizowanych e-usług.
b. Będzie prezentować zalogowanemu klientowi listę opłat, jaką powinien wnieść w związku z założoną w jednostce sprawą/złożonym wnioskiem. Lista opłat będzie pozwalała na wyszukiwanie oraz filtrowanie.
c. Będzie pobierać dane z platformy e-usług oraz systemów dziedzinowych i dla zalogowanych użytkowników będzie wyświetlać następujące informacje: dane wymiarowe i wymagane płatności.
d. System będzie prezentować historie płatności. Historia płatności będzie w prosty sposób (lista) prezentowała wszystkie opłaty wniesione przez użytkownika.

W Powiecie Gołdapskim w wyniku realizacji niniejszego zamówienia zostaną wdrożone (uruchomione) poniższe e-usługi o poniżej określonym stopniu ich dojrzałości.

Nr	Nazwa usługi	Opis (proces biznesowy)	Stopień dojrzałości	Relacja	Tryb
1	2	3	4	5	6
1	Usługa przeglądania mapy	Na żądanie użytkownika generowanie obrazu mapy zawierającej elementy mapy ewidencyjnej i mapy zasadniczej w oparciu o usługę WMS. Użytkownik wybiera poprzez stronę internetową obszar oraz zakres tematyczny, usługa zwraca obraz mapy. Zakres tematyczny zawiera warstwy- > kontury działek wraz z atrybutami powierzchnia, nr działki>warstwa BDOT i GESUT	3	A2A A2B A2C	publiczny
2	Usługa zgłaszania prac geodezyjnych i uzgadniania listy materiałów zasobu	Zalogowanemu użytkownikowi zostaje udostępniony częściowo wypełniony (personalizacja) formularz zgłoszenia, użytkownik wskazuje na obrazie mapy w geoportalu zakres przestrzenny wykonywanej pracy, a usługa przetwarza ten zakres na ciąg współrzędnych, powoduje zapisanie zgłoszenia w systemie dziedzinowym oraz pobranie i przekazanie on-line zalogowanemu użytkownikowi numeru ewidencyjny z rejestru zgłoszeń. (personalizacja - każdemu zgłoszeniu przyporządkowany jest określony zakres terytorialny wykonywanej pracy) Użytkownikowi zostaje udostępniony specjalistyczny komunikator pomiędzy nim	5	A2B	publiczny (chroniony hasłem)

		a ośrodkiem umożliwiający wykonanie uzgodnienia listy materiałów on-line w ramach zgłoszonego zakresu pracy wraz z możliwością wstępnej kalkulacji opłaty.(personalizacja: obszar zgłoszonej pracy umożliwia wybór odpowiednich dokumentów z zasobu)			
3	Usługa obsługi zgłoszeń uzupełniających	Zalogowanemu użytkownikowi zostaje udostępniony częściowo wypełniony (personalizacja) formularz zgłoszenia danej pracy geodezyjnej wraz z nadanym numerem z rejestru zgłoszeń w celu modyfikacji (uzupełnienia) zapotrzebowania na materiały zasobu, np. w związku ze zmianą zakresu pracy.	5	A2B	publiczny (chroniony hasłem)
4	Generowanie dokumentu opłaty wraz z płatnością elektroniczną	Ośrodek generuje Dokument Obliczenia Opłaty (DOO) i automatycznie powiadamia Wykonawcę o konieczności wniesienia opłaty wraz z możliwością dokonania jej drogą elektroniczną.	4	A2B	publiczny (chroniony hasłem)
5	Usługa przeglądania zgłoszonych zakończonych/niezakończonych prac geodezyjnych	Uprawniony użytkownik może zażądać wyświetlenia z Rejestru zgłoszeń prac, prac zakończonych/niezakończonych, a usługa zidentyfikuje zalogowanego użytkownika i wyświetli informacje o jego wykonanych i zakończonych/ niezakończonych pracach.	3	A2B	publiczny (chroniony hasłem)
6	Pobranie materiałów zasobu z obszaru zgłoszonej pracy wraz z Licencją	Po stwierdzeniu dokonania wpłaty Ośrodek generuje Licencję i przesyła ją wykonawcy, który poprzez usługę zawężoną do obszaru zgłoszonej pracy i uzgodnionej listy materiałów (personalizacja) umożliwia Wykonawcy automatyczne pobranie materiałów zasobu.	4	A2B	publiczny (chroniony hasłem)
7	Pobieranie danych z bazy EGiB, GESUT, BDOT 500, BDSOG	Po dokonaniu opłaty Ośrodek udostępnia specjalną usługę pobrania danych przez zalogowanego użytkownika z bazy EGiB, GESUT, BDOT 500, BDSOG z zakresu zgłoszonej pracy.	3	A2B	publiczny (chroniony hasłem)
8	Przekazywanie wyników pracy	Wykonawca przekazuje on-line wyniki pracy. Wykonawcy automatycznie przekazywane są informacje o wyniku kontroli.	4	A2B	publiczny (chroniony hasłem)
9	Zamówienie zbioru danych RCiWN	Na udostępnionym do wglądu wykazie obiektów niezawierających cen/ wartości nieruchomości rzeczoznawca zaznacza pozycje, które go interesują i je zamawia. Automatycznie generowany jest i wysyłany DOO.	4 (5)	A2B A2C	publiczny (chroniony hasłem)
10	Usługa generowania Licencji i wydania zbioru danych RCiWN	Rzeczoznawca dokonuje wpłaty (on-line lub przesyła dokument wpłaty). Automatycznie generowana jest Licencja, a dla zaznaczonych pozycji ukazują się ceny transakcji lub wartości nieruchomości, które może pobrać	4 (5)	A2B A2C	publiczny (chroniony hasłem)

		rzeczoznawca.			
11	Usługa potwierdzająca występowanie określonej osoby lub instytucji w bazie EGiB	Uprawniony użytkownik (komornik) podaje w wywołanym oknie dane dotyczące osoby fizycznej (np. nazwisko i imię, PESEL) lub instytucji (np.nazwa, NIP), a usługa sprawdza zawartość danych w bazie EGiB i zwrotnie informuje, czy osoba lub instytucja o wskazanych danych występuje lub nie występuje w bazie EGiB.	4	A2B	publiczny (chroniony hasłem)
12	Usługa pozyskiwania atrybutów obiektów bazy danych EGiB, geokodowania podmiotu ewidencyjnego, udostępniania informacji dla gminy wg wskazanych instytucji, udostępniania informacji dla gminy wg wskazanych osób fizycznych udostępniania informacji dla gminy wg wskazanych działek.	Publiczny dostęp do danych geodezyjnych, możliwych do udostępnienia publicznego, zawierający dane dot.: -powierzchni -klasyfikacji działki -nr działki	3	A2C	publiczny
13	Zamówienie mapy ewidencji gruntów i budynków lub mapy zasadniczej wraz z generowaniem licencji i wydaniem produktu. E-usługa wykorzystuje EWMAPA	Użytkownik uzupełnia on-line wniosek formularz P+P3 wraz ze wskazaniem przestrzennej lokalizacji obszaru, którego dotyczy zamówienie i podpisuje go z wykorzystaniem profilu zaufanego e-PUAP lub systemu PZGiK. Generowanie i wysłanie DOO. Użytkownik dokonuje wpłaty (on-line lub przesyła dokument wpłaty). Generowanie i wysłanie licencji do użytkownika oraz generowanie określonego produktu: - w postaci elektronicznej (wysyłka on-line), - w postaci nieelektronicznej (papierowej lub nośnika zewnętrznego) i przesyła go pocztą tradycyjną.	4	A2A A2B A2C	publiczny

14	Zamówienie Wypisu/Wypisu i Wyrysu/Wyrysu z bazy EGiB wraz z generowaniem licencji i wydaniem produktu. E-usługa wykorzystuje EWOPIS	Użytkownik uzupełnia on-line wniosek formularz EGiB wraz ze wskazaniem przestrzennej lokalizacji obszaru, którego dotyczy zamówienie, i przesyła go z wykorzystaniem profilu zaufanego e-PUAP lub systemu PZGiK. Generowanie i wysłanie DOO. Użytkownik dokonuje wpłaty (on-line lub przesyła dokument wpłaty). Generowanie i wysłanie licencji do użytkownika oraz generowanie określonego produktu+C12: w postaci elektronicznej (wysyłka on-line), w postaci nieelektronicznej (papierowej lub nośnika zewnętrznego) i przesyła go pocztą tradycyjną. E-usługa umożliwia dokonywanie opłat	4	A2A A2B A2C	publiczny
15	Zamówienie rejestrów, kartotek, skorowidzów, wykazów, zestawień tworzonych w bazie danych EGiB wraz z generowaniem licencji i wydawaniem produktu	Użytkownik uzupełnia on-line formularz wniosku P+P2 wraz ze wskazaniem przestrzennej lokalizacji obszaru, którego dotyczy zamówienie i podpisuje go z wykorzystaniem profilu zaufanego e-PUAP lub systemu PZGiK. Generowanie i wysłanie DOO . Użutkownik dokonuje wpłaty (on-line lub przesyła dokument wpłaty). Generowanie i wysłanie licencji do użytkownika oraz generowanie zamówionego produktu w postaci elektronicznej (wysyłka on-line) lub w postaci nieelektronicznej (papierowej lub nośnika zewnętrznego) i przesyła go pocztą tradycyjną	4	A2A A2B A2C	publiczny

2.2 Szyna usług integrująca usługi ePUAP, EZD i systemy dziedzinowe

Aby zrealizować możliwość świadczenia elektronicznych usług publicznych konieczne jest połączenie wdrażanych w Starostwie systemów i rozwiązań informatycznych. Wdrożona zostanie szyna usług integrująca usługi e-PUAP, EZD i systemy dziedzinowe. Dzięki temu będzie możliwe zautomatyzowanie przepływu dokumentów elektronicznych z platformy e-PUAP i EZD do systemów dziedziniowych. Zadanie to zakłada wbudowanie mechanizmu integrującego EZD z instrukcją integratora oraz zdefiniowanie szablonów przepływów oraz integracji z systemami dziedzinowymi. Dzięki temu deklaracje i formularze składane przez e-PUAP będą przesyłane automatycznie do EZD, a następnie do systemów dziedzinowych, gdzie będą umieszczane w odpowiednich polach systemu. Dzięki temu możliwe będzie korzystanie z wdrażanych e-usług poprzez platformę e-PUAP.

2.3 Modernizacja systemów dziedzinowych

Systemy dziedzinowe zostaną dostosowane do współpracy z wdrożonymi e-usługami.

W chwili obecnej Starostwo wykorzystuje następujące oprogramowanie dziedzinowe:

Posiadane oprogramowanie		
Lp.	**Rodzaj oprogramowania (dziedzina)**	**Nazwa producenta i oprogramowania, wersja oprogramowania (jeśli występuje)**
1.	System finansowo-księgowy	Sputnik Software Sp. z o.o. Foka PRO 1.07.014.11
2.	System rejestracji wpłat i wypłat	Foka PRO 1.07.014.11
3.	System elektronicznego obiegu dokumentów	Sputnik Software Sp. z o.o. Proton
4.	Prowadzenie danych stanowiących infrastrukturę informacji przestrzennej	GEOBID spółka z o.o. EWMAPA 12 FB
5.	Prowadzenia ewidencji gruntów, budynków i lokali	GEOBID spółka z o.o. EWOPIS 6
6.	Ewidencjonowanie i zarządzanie dokumentami państwowego zasobu geodezyjnego i kartograficznego	GEOBID spółka z o.o. OŚRODEK 8
7.	Zakładanie oraz prowadzenie rejestru punktu osnowy geodezyjnej	GEOBID spółka z o.o. BANK OSNÓW 3
8.	Obsługa użytkowania wieczystego i trwałego zarządu	GEOBID spółka z o.o. UW 4 – UŻYTKOWANIE WIECZYSTE I TRWAŁY ZARZĄD
9.	Ewidencja mienia skarbu państwa	GEOBID spółka z o.o. MIENIE 2

Modernizacja pozwoli na zaciąganie danych z systemów dziedzinowych, a także aktualizacje dziedzinowych baz danych powstałe na skutek świadczenia e-usług. Pozwoli to na pełne wykorzystanie potencjału e-usług o wysokim poziomie dojrzałości. Modernizacja systemów dziedzinowych ma na celu znaczne ułatwienie przepływu informacji w Starostwie poprzez automatyzację tego procesu. Dzięki przeprowadzeniu integracji systemów dziedzinowych możliwe będzie nie tylko automatyczne przesyłanie danych pomiędzy nimi, a platformą e-usług, ale też przesyłanie danych pomiędzy zmodernizowanymi systemami. Dzięki modernizacji systemów dziedzinowych ich obsługa stanie się prostsza i bardziej intuicyjna. Pozwoli to na szybszą i bardziej wydają pracę pracowników Starostwa Powiatowego oraz dodatkowo, dzięki automatyzacji przyczyni się do zmniejszenia się częstotliwości występowania błędów ludzkich. Dzięki wdrożeniu zasad i procedur związanych z bezpieczeństwem obiegu informacji i przechowywania danych osobowych wzrośnie poziom bezpieczeństwa danych.

2.4 Platforma GIS - budowa geoportalu

Celem platformy GIS jest udostępnienie zdigitalizowanych treści oraz e-usług dla użytkowników. Treści udostępniane poprzez geoportal będą należeć do Starostwa Powiatowego w Gołdapi i będą obejmować obszar Powiatu Gołdapskiego. Dostęp do treści będzie zależny od uregulowań prawnych dotyczących udostępniania danych geodezyjnych i kartograficznych przez Starostwo Powiatowe. Samo korzystanie z platformy GIS oraz e-usług nie będzie płatne, ale Wnioskodawca będzie pobierać opłaty zgodnie z zapisami prawa geodezyjnego i kartograficznego.

Podstawowe cechy geoportalu internetowego:

- publikacja danych na geoportalu krajowym poprzez wystawienie odpowiedniej usługi WMS i WFS,
- obsługa warstw i import danych z obcych usług WMS i WFS,
- prezentowanie skali mapy, współrzędnych x,y, informacji o układzie współrzędnych,
- prezentacja zdefiniowanej przez użytkownika lub administratora mapy,
- prezentacja legendy w układzie drzewa zgodnie z wybraną lub wygenerowaną przez użytkownika lub administratora mapą (kategorie i warstwy),
- możliwość wyszukiwania obiektów na mapie (np. wg. działek, adresów, współrzędnych x, y),
- możliwość przesuwania mapy,
- możliwość zbliżania/oddalania prezentowanej mapy,
- możliwość operowania suwakiem skali,
- możliwość pomiaru odległości,
- wyświetlanie informacji o wskazanym obiekcie,
- przeglądanie wybranego elementu mapy,
- możliwość zgłaszania uwag, pytań i sugestii przez użytkowników geoportalu,
- przeglądarka internetowa stanowi interfejs klienta systemu.
    - Geoportal internetowy prawidłowo działa w następujących przeglądarkach internetowych: Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome.
- geoportal internetowy posiada interfejs dla poszczególnych modułów, którego spójność wyrażać się będzie poprzez:
    - jednolitą szatę graficzną interfejsu opisowego
    - jednolitą szatę graficzną interfejsu graficznego
    - logiczną spójność interfejsów
    - standaryzację typowych funkcji.
- Strona portalu musi być zabezpieczona certyfikatem SSL:
    - zgodność ze standardem X.509 v.3 (RFC5280)
    - zabezpieczony funkcją skrótu SHA2
    - obsługa siły szyfrowania połączeń do 256 bitów
    - wsparcie dla SGC (Server Gated Cryptography)
    - obsługa kluczy o długości 4096 bitów i więcej
    - minimalna długość kluczy kryptograficznych: RSA lub DSA 2048 bit, EC 571 bit: NIST K-571 oraz NIST B-571
    - możliwa jest weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP
    - weryfikacja jakości certyfikatu za pomocą narzędzia: https://www.ssllabs.com/ssltest/. Wymagana ocena w teście „A”
- Wymagany jest audyt podatności dostarczonego systemu np. narzędzie OpenVAS.
- Wykonawca dostarczy wszelkie wymagane komponenty programistyczne oraz sprzętowe wymagane do uruchomienia e-usług np.: EWMAPA serwer WMS w ramach złożonej oferty

2.5 Zakres usług szkoleniowych

Usługi szkoleniowe zostaną dokonane w celu zapoznania pracowników Zamawiającego (6 osób) z zasad działania i funkcjonowania dostarczonych systemów teleinformatycznych oraz sprzętu. Pracownicy odbędą m.in. szkolenia z systemu informacji przestrzennej GIS oraz zintegrowanych systemów dziedzinowych. Szkolenie ma na celu przygotowanie pracowników do prawidłowej i sprawnej obsługi interesantów na podstawie wdrożonego systemu i zbudowanej infrastruktury.

3. Część 2

3.1. Parametry techniczne oraz wymagania dla sprzętu

W ramach niniejszego zadania do Powiatu Gołdapskiego mają zostać dostarczone, zainstalowane i uruchomione poniżej przedstawiony elementy infrastruktury sprzętowej:

1. Serwer,
2. Centralny UPS,
3. UTM,
4. Serwer NAS.

3.1.1. Serwer

Serwer - 1 szt.	
Parametr	**Wartości minimalne**
Obudowa	Maksymalnie 2U RACK 19 cali wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie rack wraz z panelem frontowym zabezpieczającym dyski przed ich nieautoryzowanym wyciągnięciem.
Płyta główna	Płyta główna z możliwością instalacji minimum dwóch fizycznych procesorów 22, 20, 18, 16, 14, 12, 10, 8, 6, 4 rdzeniowych.
Procesor	Minimum dwa procesory min.4-rdzeniowe, min.3,5GHz osiągające (z zaoferowanym serwerem) w testach SPECint_rate2006 wynik nie gorszy niż 495 punktów lub SPECint_rate_base2006 wynik nie gorszy niż 576 pkt. Wynik testu musi być publikowany na stronie www.spec.org (załączyć wydruk ze strony do oferty). **Dokumenty potwierdzające spełnienie powyższych wymagań załączyć na wezwanie Zamawiającego zgodnie z art. 26 ust. 2 ustawy prawo zamówień publicznych**
Pamięć operacyjna	Minimum 64 GB w modułach dwubankowych (8x 16GB) w technologii RDIMM DDR4 i częstotliwości max wspieranej przez zaoferowany procesor. Serwer umożliwia możliwość rozbudowy do minimum 3TB Minimum 24 sloty na pamięć. Zabezpieczenia pamięci: min. Advanced ECC
Sloty rozszerzeń	Minimum 2 sloty PCI-Express Generacji 3 w tym minimum jeden slot x8 (prędkość slotu – bus width) pełnej wysokości oraz minimum jeden slot x8 (prędkość slotu – bus width). Możliwość rozbudowy o dodatkowy, trzeci slot PCI-Express Generacji 3 x16 (prędkość slotu – bus width).
Dysk twardy	Możliwość zainstalowania do 8 dysków typu Hot Swap, SAS/SATA/SSD, 2,5”. Zainstalowane: 6 dysków o pojemności min. 2TB 7,2k rpm NL-SAS 12G Możliwość rozbudowy/rekonfiguracji serwera do obsługi 10 wewnętrznych dysków 2,5’’

Kontroler	Kontroler macierzowy SAS 12Gb z min. 2GB cache, z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę do min. 8 napędów dyskowych SAS oraz obsługujący poziomy: min. RAID 0/1/1+0/5/5+0/6/6+0 Możliwość rozbudowy pamięci cache do min. 4GB poprzez rozbudowę kontrolera lub wymianę kontrolera.
Interfejsy sieciowe LAN	Minimum 4 porty Ethernet 1GbE z funkcją Wake-On-LAN, RJ45, niezmniejszający ilości dostępnych slotów PCI-E Minimum 2 porty 10Gb SFP+ ze wsparciem RoCE, Jumbo Frames, iTunnel Offload dla VXLAN i NVGRE, niezmniejszający ilości dostępnych slotów PCI-E wyposażone w kompatybilne moduły SFP oraz patchcordy
Karta graficzna	Zintegrowana karta graficzna
Porty	5 x USB 3.0 (w tym min. 2szt wewnętrzne). 1x VGA Wewnętrzny slot na kartę microSD. Zamawiający dopuszcza rozwiązanie umożliwiające uzyskanie slotu microSD poprzez przejściówkę USB na microSD pod warunkiem, że zaproponowane rozwiązanie (przejściówka) musi znajdować się w ogólnodostępnej karcie katalogowej producenta serwera i jest przez niego wspierane oraz certyfikowane. Oferent ma podać link do strony producenta. Serwer musi posiadać możliwość rozbudowy w razie potrzeby o dodatkowe porty: - VGA dostępny z przodu serwera (opcjonalnie), - port szeregowy z tyłu serwera, Ilości portów nie mogą być osiągnięte przez użycie przejściówek.
Dodatkowe napędy	Wbudowany napęd DVD-RW
Zasilacz	2 zasilacze redundantne o mocy max. 500W, typ Hot-plug, typu min. Platinum.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug Serwer musi być przygotowany do pracy w temperaturze otoczenia do 45st.C.
Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS) . Możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD/DVD/ISO i FDD. Karta zdalnego zarządzania musi posiadać wbudowaną pamięć flash, minimum 4GB, w tym minimum 1GB dostępny dla użytkownika serwera. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną, posiadające dedykowany port RJ45.
Wsparcie dla Systemów Operacyjnych i Systemów Wirtualizacyjnych	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) Vmware Citrix XenServer Oracle Linux
Szyny montażowe	Szyny montażowe przeznaczone do montażu serwera w szafie RACK umożliwiające wysunięcie całego serwera.
Oprogramowanie systemowe	Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym lub dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. 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. 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 techologię ASP.NET. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. Graficzny interfejs użytkownika. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. 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 konsumpcji informacji w dokumentach (Digital Rights Management). 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. c)Zdalna dystrybucja oprogramowania na stacje robocze. d)Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej. e)PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: •Dystrybucję certyfikatów poprzez http, •Konsolidację CA dla wielu lasów domeny, •Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. 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)Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. Wsparcie dostępu do zasobu dyskowego SSO 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; Wymagana najnowsza dostępna wersja na dzień publikacji ogłoszenia o zamówieniu. **System musi posiadać licencje dostępowe dla minimum pięćdziesięciu użytkowników.**
Certyfikaty	**Serwer musi posiadać deklaracje CE lub równoważną – załączyć do oferty**. Przez dokument równoważny zamawiający rozumie taki, który potwierdza zgodność oferowanych urządzeń co najmniej z: - R & TTE 1999/5/EC1, - rozporządzeniem Komisji (WE) nr 1275/2008, - przepisami dyrektywy ErP 2009/125/WE. **Serwer musi być wyprodukowany zgodnie z normą ISO-9001 lub równoważną - załączyć do oferty dokument poświadczający**. Przez normę równoważną zamawiający rozumie taką, która co najmniej: - określa politykę jakości organizacji; - określa wymagania dotyczące wyrobu oraz umożliwia ich przegląd; - określa cele w zakresie jakości wyrobów; - reguluje kwestie odpowiedzialności kierownictwa; - definiuje uprawnienia pracowników; - definiuje politykę środowiskowa organizacji; - określa jej cele, zadania i programy środowiskowe; - definiuje i wskazuje niezbędne zasoby, role, odpowiedzialność i uprawnienia; - opisuje sterowanie operacyjne oraz gotowość i czasy reakcji na awarie; - wskazuje metody monitorowania i pomiaru wyrobów i procesów. Wymagane jest aby serwer znajdował się na liście certyfikowanych serwerów producenta systemu operacyjnego jaki jest zainstalowany na serwerze – załączyć do oferty dokument potwierdzający. **Dokumenty potwierdzające spełnienie powyższych wymagań załączyć na wezwanie Zamawiającego zgodnie z art. 26 ust. 2 ustawy prawo zamówień publicznych**.
Gwarancja i wsparcie techniczne	Min. 60-miesięcy gwarancji producenta serwera w trybie NBD On-Site, , naprawa w miejscu instalacji serwera. Gwarancja z usługą „Uszkodzone dyski pozostają własnością Zamawiającego”. Pakiet serwisowy winien być składnikiem serwera oraz ma być przypisany do sprzętu na etapie jego produkcji bez konieczności późniejszego aktywowania, rejestrowania lub innych działań ze strony Zamawiającego. Serwis serwera musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta posiadającego certyfikat ISO 9001 lub równoważny na świadczenie usług serwisowych - **dokumenty potwierdzające załączyć do oferty**. Przez normę równoważną zamawiający rozumie taką, która co najmniej: - określa politykę jakości organizacji; - określa wymagania dotyczące wyrobu oraz umożliwia ich przegląd; - określa cele w zakresie jakości wyrobów; - reguluje kwestie odpowiedzialności kierownictwa; - definiuje uprawnienia pracowników; - definiuje politykę środowiskowa organizacji; - określa jej cele, zadania i programy środowiskowe; - definiuje i wskazuje niezbędne zasoby, role, odpowiedzialność i uprawnienia; - opisuje sterowanie operacyjne oraz gotowość i czasy reakcji na awarie;. **Dokumenty potwierdzające spełnienie powyższych wymagań załączyć na wezwanie Zamawiającego zgodnie z art. 26 ust. 2 ustawy prawo zamówień publicznych**.
Wymagania ogólne	Wykonawca ma obowiązek instalacji i konfiguracji systemu operacyjnego. Przygotowania w porozumieniu z przedstawicielem Zamawiającego maszyn wirtualnych koniecznych do wdrożenia geoportalu i eusług.

3.1.2. Centralny UPS

Centralny UPS - 1 szt.	
Parametr	**Wartości minimalne**
Moc pozorna	40000VA
Moc skuteczna	36000Watts
Obudowa	Tower
Typologia	Pure Sine Wave
Konfiguracja fazowe WE/WY	Thee Phase input – Three Phase output: - 3 fazowe wejście - 3 fazowe wyjście
Złącza	RS-232, RS-485, EPO, SNMP Card, Dry contacts,
Napięcie wejściowe	380V/400V/415V(line to line) 220V/230V/240V(line to neutral)
Częstotliwość wejściowa	50/60Hz
Napięcie wyjściowe	380V/400V/415V, three phase - 3 fazowe 220V/230V/240V, one phase - 1 fazowe
Zabezpieczenie przeciążeniowe	<105%,long time operation 105%<load [ładowanie]<110%, transfer to bypass po 60 minutach 110%<load [ładowanie]<125%, transfer to bypass po 10 minutach 125%<load [ładowanie]<150%, transfer to bypass po 1 minucie >150%, transfer to bypass po 200ms
Wydajność systemowa	Tryb Normal: 95% Tryb ECO: 98%
Wydajność w trybie baterii	95%
Wyświetlacz	LCD
Głośność	nie więcej niż 55(dB)
Maksymalna ilość jednostek w trybie równoległym	4 szt.
Gwarancja i certyfikaty	Min. 60-miesięcy gwarancji producenta UPS musi posiadać deklaracje CE lub równoważną
Czas podtrzymania	Minimalny czas podtrzymania przy obciążeniu 100% powinien wynosić przynajmniej 15 min, a przy obciążeniu 50% przynajmniej 36 min
Inne	Wykonawca ma obowiązek zainstalować UPS w miejscu wskazanym przez Zamawiającego (piwnica budynku) oraz podłączyć go do dedykowanej dla sieci komputerowej sieci elektrycznej z użyciem własnych materiałów oraz personelu technicznego.

3.1.3. UTM

UTM - 1 szt.	
Parametr	**Wartości minimalne**
Wymagania Ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci

	osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego
Redundancja, monitoring i wykrywanie awarii	1.W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2.Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3.Monitoring stanu realizowanych połączeń VPN.
Interfejsy	1.System realizujący funkcję Firewall musi dysponować minimum 20 portami Gigabit Ethernet RJ-45, 2 gniazdami SFP 1 Gbps wraz z kompatybilnymi modułami SFP 2.System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie dostarczonego wraz z urządzeniem kompatybilnego modemu 3G/4G oraz instalacji oprogramowania z klucza USB
Parametry wydajnościowe	1.W zakresie Firewall'a obsługa nie mniej niż 2 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę. 2.Przepustowość Stateful Firewall: nie mniej niż 7,4 Gbps dla pakietów 512 B. 3.Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps. 4.Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA1: nie mniej niż 4 Gbps. 5.Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 1,9 Gbps. 6.Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem AES256-SHA1 lub AES256-SHA256) dla ruchu http – minimum 130 Mbp.
Funkcje Systemu Bezpieczeństwa:	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1.Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2.Kontrola Aplikacji. 3.Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4.Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5.Ochrona przed atakami - Intrusion Prevention System. 6.Kontrola stron WWW. 7.Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8.Zarządzanie pasmem (QoS, Traffic shaping). 9.Analiza ruchu szyfrowanego protokołem SSL. 10.Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
Polityki, Firewall	1.Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2.System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: •Translację jeden do jeden oraz jeden do wielu •Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

	3.W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
Połączenia VPN	1.System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: •Wsparcie dla IKE v1 oraz v2. •Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM) •Obsługa protokołu Diffiego-Hellman grup 19 i 20 •Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. •Tworzenie połączeń typu Site-to-site oraz Client-to-Site. •Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. •Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. •Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth •Mechanizm „Split tunneling" dla połączeń Client-to-Site 2.System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: •Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. •Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. 3.Dla modułów: IPSec VPN oraz SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. Klient VPN musi umożliwiać weryfikację stanu bezpieczeństwa stacji zdalnej. 4.Rozwiązanie powinno zapewniać funkcjonalność VTEP (VXLAN Tunnel End Point)
Routing i obsługa łączy WAN	1.W zakresie routingu rozwiązanie powinno zapewniać obsługę: •Routingu statycznego •Policy Based Routingu •Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2.System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
Zarządzanie pasmem	1.System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2.Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3.System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Kontrola Antywirusowa	1.Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2.System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3.Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
Ochrona przed atakami	1.Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2.Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3.Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4.System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 5.Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies
Kontrola aplikacji	1.Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

	2.Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3.Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4.Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P, Botnet. 5.Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur
Kontrola WWW	1.Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2.W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware, phishing, spam, Dynamic DNS, proxy avoidance. 3.Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4.Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5.System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 6.Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
Uwierzytelnianie użytkowników w ramach sesji	1.System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: •Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. •Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. •Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2.Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3.Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
Zarządzanie	1.Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2.Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3.Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4.System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5.System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6.System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
Logowanie	1.System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2.W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3.Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4.Musi istnieć możliwość logowania do serwera SYSLOG. 5. System musi umożliwiać retencję danych przez okres min. 24 miesięcy.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:

	•ICSA lub EAL4 dla funkcji Firewall •ICSA lub NSS Labs dla funkcji IPS •ICSA dla funkcji: SSL VPN, IPSec VPN
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering, Logowaniena okres min. 60 miesięcy.
Gwarancja oraz wsparcie	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5 Wykonawca powinien zapewnić wsparcie Zamawiającemu w zakresie: • uruchomienia nowego urządzenia • wstępnej konfiguracji urządzenia w zakresie: konfiguracji łącza internetowego, konfiguracji stref bezpieczeństwa, konfiguracji VPN • rozwiązywania bieżących problemów zgłaszanych przez Zamawiającego • wsparcie będzie świadczone telefonicznie, pocztą elektroniczną lub za pomocą narzędzi do zdalnej pomocy
Opisy do wymagań ogólnych.	Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

3.1.4. Serwer NAS

Serwer NAS- 1 szt.	
Parametr	**Wartości minimalne**
Obudowa	Maksymalnie 2U RACK 19cali umożliwiająca montaż min. 18 dysków wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie rack.
Procesor	Zainstalowany min.1 procesor 4-rdzeniowy osiągający w teście wydajności CPU wynik min. 6980 punktów. Wymagana publikacja procesora i wyniku na stronie CPU Benchmark http://www.cpubenchmark.net/cpu_list.php
Pamięć RAM	Zainstalowane min. 32GB z technologią ECC, Możliwością rozbudowy do min.128GB, Min. 3 sloty pamięci pozostają wolne.
Pamięć FLASH	4 GB DOM
Dyski	14 dyski o minimalnych parametrach: - pojemność: 4 TB, - interfejs: SATA 6 Gb/s, - obroty na minutę: 7200, - pamięć podręczna: 128 MB, - format: 3,5” - przeznaczenie: do NAS-ów lub serwerów,

	- MTBF (godziny): 2 000 000 - certyfikaty i standardy: RoHS - szybkość przesyłania danych między hostem a dyskiem: min. 200MB/s. Oferowane dyski muszą być widnieć jako kompatybilne na stronie producenta serwera NAS.
Rozbudowa	Możliwość rozbudowy do min. 146 dysków
Zasilanie	2 Redundantne, moc zasilaczy max. 450W
Pule dyskowe	Tak
Thin provisioning dla woluminu i LUN	Tak
Migawki	Min. 65 536 na urządzenie
Backup	Oprogramowanie do backupu autorstwa producenta macierzy z nieograniczoną liczbą licencji na końcówki, które umożliwia synchronizowanie wybranych katalogów w czasie rzeczywistym na serwer lub przesyłanie ich zgodnie z ustalonym harmonogramem.
Cache	Uruchomiony i skonfigurowany SSD Cache
Wirtualizacja	Możliwość podłączenia do Vmware, Citrix lub Hyper-V, możliwość uruchomienia maszyn wirtualnych bezpośrednio na macierzy bez konieczność posiadania zewnętrznych wirtualizatorów
Złącza sieciowe	Zintegrowane min. 4 x 1 GbE RJ45 i min. 2 x 10GbE SFP+ wyposażone w kompatybilne moduły SFP oraz patchcordy Możliwość rozbudowy o dodatkowe porty LAN.
Złącza PCIe	Min. 3sztuki PCIe 3.0 Obsługujące adaptery sieciowe 10GbE / 40GbE oraz PCIe NVMe SSD
Auto tiering	Tak
Szyfrowanie	Szyfrowanie ze wsparciem sprzętowym całych woluminów lub tylko wybranych udziałów sieciowych
iSCSI	Wbudowany inicjator i target iSCSI
Replikacja	Replikacja między urządzeniami w czasie rzeczywistym
Wymagania ogólne	Możliwość podłączenia do kontrolera domeny Microsoft lub uruchomienie kontrolera domeny na bazie SAMBA 4 ; Zaawansowane uprawnienia do folderów z obsługą ACL na poziomie podfolderów w protokołach i usługach CIFS/SMB, AFP, FTP oraz Menadżerze plików; Windows ACL;
Gwarancja	Min. 5 lat NBD

4. Warunki świadczenia serwisu gwarancyjnego, wsparcia użytkowników Help Desk, asysty technicznej oraz asysty wdrożeniowej

4.1. Warunki ogólne

1. Wykonawca zobowiązany jest do udzielenia Zamawiającemu gwarancji na przedmiot Umowy i zobowiązuje się świadczyć serwis gwarancyjny w okresie nie krótszym niż określony w **SIWZ, Załączniku nr 1 do SIWZ oraz złożonej ofercie**.
2. Okres świadczenia gwarancji rozpoczyna się z dniem podpisania przez Strony Protokołu Odbioru końcowego Produktu.
3. W okresie trwania gwarancji Wykonawca jest zobowiązany do wykonywania świadczeń gwarancyjnych polegających na:
   a) skutecznym Rozwiązaniu Zgłoszeń, w tym Incydentów i Problemów zgłaszanych przez Zamawiającego;
   b) świadczeniu merytorycznych konsultacji Zamawiającemu, w szczególności odpowiadania na Zapytania Zamawiającego, w zakresie funkcjonowania i obsługi Systemu i jego poszczególnych elementów;
   c) dostarczaniu, instalacji i wdrażaniu niezbędnych lub celowych poprawek (w tym tzw. łat programowych - ang. „patch") Systemu wraz z przekazaniem kompletnej Dokumentacji poprawek, instrukcji instalacji, instrukcji użytkowania;
   d) innych koniecznych działaniach zapewniających prawidłowe - tzn. nieograniczone czasowo i funkcjonalnie działanie Systemu.
4. Wszelkie świadczenia dostarczone przez Wykonawcę w ramach gwarancji będą wykonywane przez wykwalifikowany i posiadający wystarczającą wiedzę na temat Systemu personel.
5. Wykonawca jest zobowiązany zrealizować wszelkie świadczenia w ramach gwarancji w taki sposób aby zapewnić pełną funkcjonalność Systemu w trakcie i po zrealizowaniu świadczenia.
6. Wszelkie działania związane z świadczeniem gwarancji muszą być wykonywane za wiedzą i akceptacją Zamawiającego.
7. W okresie trwania Serwisu gwarancyjnego Wykonawca zobowiązany jest do:
   a) nieodpłatnego dostarczania nowych wersji lub uaktualnienia Oprogramowania w przypadku gdy nastąpią zmiany w obowiązującym prawodawstwie, wymagające nowszej wersji lub uaktualnienia Oprogramowania,
   b) instalacji nowych wersji lub uaktualnień Oprogramowania w terminach uzgodnionych z Zamawiającym,
   c) prowadzenia konsultacji i udzielania porad w zakresie zainstalowanej nowej wersji lub uaktualnień Oprogramowania: telefonicznie, faksem, pocztą elektroniczną poprzez zapewnienie uprawnionym pracownikom Zamawiającego dostępu do Help Desku Wykonawcy w zakresie niezbędnym do użytkowania Systemu,
   d) usprawniania obsługi Systemu poprzez wprowadzanie autorskich udoskonaleń w technologii i funkcjonalności Oprogramowania,
   e) informowania Zamawiającego o dostępnych aktualizacjach / poprawkach Oprogramowania.

8. Wykonawca ma obowiązek wskazać zamawiającemu nr telefonu oraz email pod jaki mogą dzwonić lub wysyłać zgłoszenia i zapytania użytkownicy systemu.
9. Telefoniczne wsparcie użytkowników oraz telefoniczne zgłaszanie awarii muszą być dostępne w godzinach pracy zamawiającego.

4.2. Wsparcie użytkowników Help Desk

1. Wykonawca zobowiązany jest świadczyć usługę Help Desk dla przedmiotu oferty.
2. Wykonawca w okresie świadczenia serwisu gwarancyjnego ponosi odpowiedzialność z tytułu gwarancji za Błędy Oprogramowania / Awarie oraz ich usunięcie.
3. Błąd musi być opisany przez zgłaszającego w sposób umożliwiający odtworzenie błędu w środowisku wzorcowym Wykonawcy. Jeżeli odtworzenie błędu nie będzie możliwe w środowisku wzorcowym, Wykonawca zdiagnozuje błąd w środowisku Zamawiającego,
4. Wykonawca w ramach świadczeń Gwarancji zobowiązany jest do skutecznego Rozwiązania Zgłoszenia w terminach określonych w umowie z Zamawiającym.
5. Czas Rozwiązania Zgłoszenia odnosi się do Oprogramowania dostarczonego przez Wykonawcę w ramach niniejszego postępowania. Wykonawca odpowiedzialny jest za usuwanie Błędów Oprogramowania wynikających z nieprawidłowego (niezgodnego z instrukcją) działania Oprogramowania.
6. Jeżeli w wyniku zastosowania przez Wykonawcę wszelkich działań, Wykonawca stwierdzi, że Zgłoszenie było bezzasadne, wówczas Zgłaszający po wcześniejszym ustaleniu kosztów może odpłatnie zlecić wykonanie naprawy lub zlecić jej realizację w ramach puli godzin przysługującej mu Asysty Technicznej.
7. W uzasadnionych przypadkach Czas Rozwiązania Zgłoszenia, o których mowa w pkt 5 mogą zostać przedłużone za porozumieniem Przedstawicieli Stron. O zmianie terminów Rozwiązania Zgłoszenia Wykonawca poinformuje Zamawiającego e-mailem.

4.3. Asysta techniczna

1. Wykonawca zobowiązany jest świadczyć usługę Asysty Technicznej dla przedmiotu oferty.
2. Celem świadczenia usług Asysty technicznej jest bezpłatne wsparcie techniczne w używaniu Oprogramowania, do którego Zamawiający uzyskał licencję na podstawie niniejszego postępowania. Zamawiający przekaże Wykonawcy imienną listę osób uprawnionych ze strony Zamawiającego do korzystania z Asysty technicznej.
3. Wykonawca zobowiązany jest świadczyć bezpłatną Asystę techniczną przez okres zgodnie z Ofertą. Okres i zakres Asysty technicznej rozpoczyna się z dniem podpisania przez Strony Protokołu Odbioru Końcowego.
4. Wykonawca zapewni świadczenie Asysty technicznej w języku polskim.
5. Wykonawca zagwarantuje świadczenie usługi Asysty technicznej wyłącznie przez wykwalifikowany personel, przez co rozumie się osobę/osoby z doświadczeniem, posiadające odpowiednie kwalifikacje merytoryczne i wiedzę na temat Systemu, po odpowiednim przeszkoleniu, cechujące się odpowiednimi predyspozycjami do kontaktu z Użytkownikiem Końcowym tj. komunikatywnością, dobrą dykcją, odpornością na stres, cierpliwością, pozytywnym

nastawieniem do Użytkownika Końcowego. Personel Wykonawcy świadczący usługę Asysty technicznej musi posiadać umiejętności pracy z „trudnym użytkownikiem" np. zdenerwowanym, niecierpliwym, zadającym niejasne pytania lub udzielający niejasnych odpowiedzi – nieobeznanym w temacie

6. Przedmiotem usługi Asysty technicznej świadczonej przez Wykonawcę na rzecz Zamawiającego jest:
   a) gotowość do świadczenia konsultacji telefonicznych,
   b) gotowość do świadczenia zdalnej pomocy użytkownikom Systemów poprzez szyfrowane połączenia do komputera użytkownika za zgodą i pod nadzorem Zamawiającego,
   c) gotowość do ewentualnego uruchomienia niezbędnej i koniecznej obsługi danych poprzez szyfrowane kanały dostępowe pomiędzy Wykonawcą a Zamawiającym.

Każdorazowa usługa realizacji Asysty technicznej prowadzona jest na podstawie zlecenia usługi oraz zakończona Protokołem Odbioru opisującym czas trwania usługi i jej zakres.

W ramach okresu Asysty technicznej Zamawiający będzie miał do wykorzystania pulę 40 godzin w każdym roku obowiązywania gwarancji i asysty technicznej, przeznaczonych na:

- świadczenie konsultacji telefonicznych oraz zdalnej pomocy Użytkownikom Końcowym,
- realizację zleconych przez niego dowolnych modyfikacji lub rozszerzeń Oprogramowania.

Zarejestrowany czas pracy poświęcony na Asystę Techniczną będzie sukcesywnie pomniejszać wielkość puli, aż do jej wyczerpania.

Zamawiający wymaga, by Wykonawca, w terminie do 5 dni roboczych od początku każdego miesiąca realizacji Asysty Technicznej, dostarczył Zamawiającemu w formie elektronicznej w tym w plikach .xls lub równoważnych Raport z Asysty dotyczący w szczególności działania usługi Help Desk. Raport powinien zawierać: wykaz wszystkich Zgłoszeń wraz z identyfikatorem zgłoszenia, tematem zgłoszenia, wskazaniem modułu w Systemie którego dotyczy Zgłoszenie, kategorią zgłoszenia, priorytetem zgłoszenia, danymi Użytkownika zgłaszającego, sposobem rozwiązania zgłoszenia, treścią odpowiedzi w przypadku Zapytania, opisem modyfikacji w przypadku Modyfikacji, datą rejestracji, datę i godzinę zamknięcia Zgłoszenia.

5. Słownik

Nazwa	Opis
API	Application Programming Interface, interfejs programowania aplikacji – jest to sposób rozumiany, jako ściśle określony zestaw reguł i ich opisów, w jaki programy komunikują się między sobą. API definiuje się na poziomie kodu źródłowego dla takich składników oprogramowania jak np. aplikacje, biblioteki czy system operacyjny. Zadaniem API jest dostarczenie odpowiednich specyfikacji podprogramów, struktur danych, klas obiektów i wymaganych protokołów komunikacyjnych. Elementem API jest dokumentacja techniczna umożliwiająca jego wykorzystanie przez zewnętrzne systemy.
Administrator	Użytkownik konfigurujący i zarządzający System i Infrastrukturą

Architektura systemu teleinformatycznego	opis składników systemu teleinformatycznego, powiązań i relacji pomiędzy tymi składnikami
Awaria	oznacza sytuację, w której nie jest możliwe prawidłowe użytkowanie Systemu z powodu uszkodzenia lub utraty spójności danych, struktur danych, błędnego funkcjonowania platformy systemowo-sprzętowej lub innej przyczyny powodującej, że system nie działa zgodnie z wymaganiem zamówienia. Jednocześnie nie jest znane obejście umożliwiające realizację celu zadania
Baza danych	zbiór danych lub innych materiałów i elementów zgromadzonych według określonej systematyki lub metody, dostępnych środkami elektronicznymi
Błąd	niezgodne z dokumentacją użytkową lub wymaganiami Zamawiającego określonymi w SIWZ, instrukcjami lub innych dokumentach wytworzonych w czasie wdrożenia, działanie Oprogramowania aplikacyjnego, systemowego, sprzętu lub działania innego oprogramowania (np. standardowego), w skutek, którego niezgodnie zadziałało Oprogramowanie aplikacyjne. Jednocześnie znane jest obejście umożliwiające realizację celu zadania.
Czas dostarczenia rozwiązania	Okres czasu od wysłania Zgłoszenia do usunięcia przyczyny problemu lub zastosowania Rozwiązania Zastępczego
Dokumentacja	wszelka dokumentacja sporządzona przez Wykonawcę dostarczona i modyfikowana w wyniku realizacji umowy
Dzień roboczy	dzień przypadający od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy
ESB, szyna usług, szyna ESB (ang. Enterprise Service Bus)	- oparte na otwartych standardach oprogramowanie typu, „middleware", które dostarcza możliwość bezpiecznego współdziałania (interoperacyjność) aplikacji poprzez interfejsy usług sieciowych (web services). Szyna usługowa zapewnia wymianę informacji pomiędzy aplikacjami opartymi na różnych technologiach, działających na różnych platformach poprzez usługi integracyjne takie jak transformacje i inteligentny routing informacji. Dzięki zastosowaniu takiego rozwiązania usługi mogą być dowolnie konfigurowane, rozszerzane, przemieszczane lub podmieniane bez przerywania pracy systemów biznesowych lub modyfikowania aplikacji.
ESP	Elektroniczna Skrzynka Podawcza
EZD	Elektroniczne Zarządzania Dokumentacją. Oprogramowanie dedykowane do wykonywania ewidencji czynności kancelaryjnych w JST w rozumieniu przepisów Instrukcji Kancelaryjnych. Oprogramowanie to realizuje funkcji rejestracji, przechowywanie dokumentów w wersji elektronicznej w repozytoriach oraz ewidencjonowania obiegu korespondencji i spraw w obrębie JST.
ePUAP	Elektroniczna Platforma Usług Administracji Publicznej https://epuap.gov.pl
Formularz Elektroniczny	graficzny interfejs użytkownika wystawiany przez oprogramowanie służący do przygotowania wygenerowania dokumentu elektronicznego zgodnego z odpowiadającym mu wzorem dokumentu elektronicznego w rozumieniu przepisów rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 roku w sprawie sporządzania pism w postaci dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz.U. z 2011, Nr206, poz.1216).
Integralność	właściwość polegająca na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony
KPA	Kodeks Postepowania Administracyjnego
Okno Serwisowe	Okienko od 8:00 do 16:00 w dni robocze Zamawiającego.
PKI	Infrastruktura Klucza Publicznego
PZ ePUAP	Profil Zaufany ePUAP
System	System obejmujący łącznie Platformę systemowo-sprzętową, Oprogramowania aplikacyjne
System PZGiK	Uporządkowany i całościowy układ zintegrowany z systemami teleinformatycznymi wykorzystywanymi do przetwarzania danych w odpowiadających im bazach danych, o których mowa w art. 4 ust. 1a pkt 1–5 i pkt 7–11 oraz ust. 1b, art. 7a pkt 16a, art. 24b ust. 1 pkt 1 ustawy, oraz w

	zintegrowanych kopiach baz danych, o których mowa w art. 4 ust. 1a pkt 8 ustawy, a także z systemem do elektronicznego zarządzania dokumentacją, o którym mowa w przepisach wydanych na podstawie art. 6 ust. 2b ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2011 r. Nr 123, poz. 698 i Nr 171, poz. 1016).
Użytkownik	Osoba, która jest pracownikiem Zamawiającego, posiada swój unikalny login i hasło i wykonuje za pomocą EZD lub systemu zasilającego.
Wada	Zakłócenie działania oprogramowania, sprzętu polegające na nienależytym działaniu jego części, nie ograniczające działania całego Systemu; nie mające istotnego wpływu na zastosowanie Systemu i nie będące Awarią lub Błędem
Web Service	Usługa sieciowa dostarczająca określoną funkcjonalność poprzez sieci Internet, niezależnie od platformy sprzętowej i implementacji.
Zdalny dostęp	możliwość realizacji usług wsparcia, wdrożenia i gwarancji związanych z systemem z dowolnego miejsca za pośrednictwem bezpiecznego połączenia internetowego.
XML	Format XML jest to obecnie powszechnie uznany standard publiczny, umożliwiający wymianę danych między różnymi systemami.