Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia

NR REF. TARRSA/IT/1/2021

OPIS PRZEDMIOTU ZAMÓWIENIA

Kod i nazwa zamówienia według Wspólnego Słownika Zamówień (CPV)

48800000-6 - Systemy i serwery informacyjne
72415000-2 - Usługi hostingowe dla stron WWW
72317000-0 - Usługi przechowywania danych
72253200-5 - Usługi w zakresie wsparcia systemu
72611000-6 - Usługi w zakresie wsparcia technicznego

1. Definicje i skróty

Użyte w niniejszym Opisie Przedmiotu Zamówienia (OPZ) i załącznikach wszelkie nazwy własne, normy, aprobaty, specyfikacje techniczne, systemy referencji technicznych, procesy charakteryzujące produkt lub usługę, należy rozumieć każdorazowo jak opatrzone dopiskiem **„lub równoważne”**.

Definicja/skrót	Opis
Active Directory, AD	Usługa katalogowa (hierarchiczna baza danych) dla systemów Windows będąca implementacją protokołu LDAP
Administrator	Osoba, zespół osób lub jednostka zajmująca się zarządzaniem systemem wirtualizacji i maszynami wirtualnymi, odpowiadająca za ich sprawne działanie i posiadająca uprawnienia dostępowe do części administracyjnych systemu.
Backup	System kopi zapasowy danych cyfrowych.
Baza danych	Część architektury systemu, program komputerowy pozwalający na gromadzenie i zarządzanie zbiorem danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej systematyki lub metody.
CPD	Centrum przetwarzania danych
HA	(High Availability) - określenie systemu informatycznego o wysokiej niezawodności i dostępności bez pojedynczego punktu awarii.
IaaS	Infrastruktura jako usługa – infrastruktura teleinformatyczna.
NBD	(Next Business Day) – następny dzień roboczy od przyjętego zgłoszenia
PaaS	Platforma jako usługa – platforma informatyczna.
RTO	(Recovery Time Objective) - czas w jakim należy przywrócić procesy po wystąpieniu awarii.
RPO	(Recovery Point Objective) - akceptowalny poziom utraty danych wyrażony w czasie.

SLA	(Service Level Agreement) - umowa o gwarantowanym poziomie świadczenia usług, wyrażona jako dostępność usług mierzona w skali roku, począwszy od dania zawarcia umowy.
Środowisko produkcyjne	Wydzielone, dedykowane środowisko teleinformatyczne obejmujące odpowiednie zasoby obliczeniowe oraz oprogramowanie, służące do realizacji testów zatwierdzających oraz produkcyjnego uruchomienia systemów i aplikacji.
Środowisko testowe	Wydzielone środowisko teleinformatyczne obejmujące odpowiednie zasoby obliczeniowe oraz oprogramowanie, służące do realizacji testów funkcjonalności i usług w ramach testów dopuszczeniowych systemów i aplikacji przed wdrożeniem produkcyjnym.
Usługa podstawowa	Usługa podstawowa ma charakter usługi będącej głównym przedmiotem.
Usługa dodatkowa	Usługa uzupełniająca ma charakter Prawa Opcji.
Użytkownik	Pracownik Zamawiającego lub osoba wskazana.
VM	Maszyna wirtualna
Zamawiający	Toruńska Agencja Rozwoju Regionalnego S.A.

2. Przedmiot zamówienia

Przedmiotem zamówienia jest kompleksowa usługa zapewnienia dostępu do bezpiecznej i wysokodostępnej infrastruktury teleinformatycznej w modelu usługowym wraz z usługami uzupełniającymi, a także świadczenie usługi tzw. pierwszej linii wsparcia (HelpDesk) w godzinach 8:00-16:00 w dni robocze z czasem reakcji na zgłoszenie do 1 godziny oraz faktyczne usunięcie zgłoszonych usterek w terminie do 6 godzin roboczych zwana dalej Usługą. Usługa składa się z Usługi podstawowej i Usług dodatkowych.

2.1 W ramach Usługi podstawowej Wykonawca zobowiązuje się:

a) udostępnić infrastrukturę teleinformatyczną CPD wraz z mocą obliczeniową i przestrzenią dyskową oraz oprogramowaniem zgodnie z określonymi przez Zamawiającego wymaganiami w terminie do 10 dni roboczych od dnia podpisania Umowy;
b) zapewnić pełną obsługę i realizację bezprzerwowej migracji systemów teleinformatycznych i aplikacji oraz danych cyfrowych z obecnie wykorzystywanych zasobów teleinformatycznych Zamawiającego do zasobów Wykonawcy dostarczonych w ramach przedmiotowego zamówienia w terminie do 10 dni roboczych od dnia podpisania Umowy, wraz z późniejszym utrzymaniem i zarządzaniem dostarczoną infrastrukturą teleinformatyczną w celu prawidłowego działania Usługi zgodnie z określonymi parametrami;
c) zapewnić ochronę maszyn wirtualnych, komputerów i urządzeń końcowych przed atakami i instalacją złośliwego oprogramowania oraz zapewnić mechanizmy i narzędzia do zbierania i przechowania logów zdarzeń z urządzeń styku z siecią Internet (syslog) w terminie do 10 dni roboczych od dnia podpisania Umowy;
d) zapewnić dostęp do aplikacji biurowych z pocztą email i jej uruchomieniem uwzględniającym migrację danych z obecnie wykorzystywanego systemu poczty email w terminie do 10 dni roboczych od dnia podpisania Umowy;

e) zapewnić usługę AD wraz z obsługą dla wszystkich Użytkowników w terminie do 10 dni roboczych od dnia podpisania umowy;
f) zapewnić łącza do sieci Internet w terminie do 10 dni roboczych od podpisania Umowy;
g) zapewnić dedykowane łącza światłowodowe pomiędzy CPD a siedzibą Zamawiającego w terminie do 10 dni roboczych od podpisania Umowy.

2.2. W ramach Usług dodatkowych Wykonawca zobowiązuje się:

na każdorazowe wezwanie Zamawiającego w trybie NBD dostarczyć usługi dodatkowe wymienione w pkt. 2.1. lit c), d), ponad ilości wskazane w ramach szczegółowego opisu Usługi podstawowej poniżej, ale nie przekraczające ilości wskazanych w ramach szczegółowego opisu Usługi uzupełniającej poniżej.

3. Szczegółowy opis Usługi podstawowej

3.1. Wymagania dla ośrodka CPD

Z uwagi na potrzebę wysokiej dostępności całej infrastruktury teleinformatycznej CPD wraz z mocą obliczeniową oraz przestrzenią dyskową Zamawiający oczekuje, aby proponowane rozwiązanie spełniało najwyższe, dostępne na terenie Unii Europejskiej standardy bezpieczeństwa informatycznego w trakcie trwania realizacji całego zamówienia. Wymagania CPD są obligatoryjne. Wykluczone jest częściowe spełnianie któregokolwiek wymogu. Zamawiający na etapie oceny ofert, a także realizacji Usługi zastrzega sobie możliwość weryfikacji i udokumentowania spełniania każdego z wymogów określonych w OPZ.

Tabela nr 1. Centrum przetwarzania danych.

OBIEKT I LOKALIZACJA			
L.p.	Parametr lub kryterium	Wyeliminowanie zagrożenia	Wykonawca spełnia (TAK / NIE)
1	Centrum przetwarzania danych zlokalizowane na terenie na terenie UE lub Lichtenstainu, Islandii, Norwegii. Wszystkie dane Zamawiającego będą gromadzone i przetwarzane na terenie UE lub Lichtenstainu, Islandii, Norwegii.	Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak spełnienie wymagań RODO / GDPR.	
2	Ogrodzony teren centrum przetwarzania danych.	Brak podstawowej kontroli fizycznego dostępu do infrastruktury ośrodka.	
3	Teren usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie.	Zagrożenie nieprzerwanej pracy urządzeń serwerowych oraz innych urządzeń architektury ośrodka (elementy zasilania, agregaty) w wyniku działań działania sił natury.	
4	Teren powinien być położony co najmniej 5 metrów powyżej poziomu wody stuletniej	Zagrożenie długotrwałego zalania ośrodka. Wysoka intensywność oddziaływania sytuacji krytycznych.	
5	Minimum 1 km od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne,	Zagrożenie powstania sytuacji zagrażających zdrowiu lub życiu osób fizycznie obsługujących urządzenia,	

	wybuchowe, żrące, również od stacji paliw lub składowisk paliw płynnych oraz baz wojskowych.	długotrwałego skażenia terenu lub długotrwałych działań służb zapobiegających zdarzeniom krytycznym (np. odcięcie terenu przez straż pożarną, wojsko).	
6	Minimum 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, centra handlowe, miejsca organizacji imprez masowych na minimum 10 tys. osób).	Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów, ryzyko zamieszek, zniszczeń.	
8	Brak ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z serwerami.	Zagrożenie, przecieków, zalania urządzeń lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności).	
9	Minimum 15 m oddalenia urządzeń komputerowych udostępnionych Zamawiającemu od źródeł pól zakłócających (transformatory SN i WN).	Zagrożenie uszkodzenia urządzeń i danych w wyniku niekorzystnego oddziaływania pół zakłócających pracę urządzeń elektrycznych i magnetycznych.	
10	Wysokość technologiczna wewnątrz pomieszczenia serwerowni z serwerami: min 2,5 m - wysokość mierzona od podłogi technicznej do sufitu; lub funkcjonujące korytarze ciepłego i zimnego powietrza	Zagrożenie zachowania odpowiedniej cyrkulacji powietrza, zachowania stref gorącej i zimnej, zmian parametrów środowiskowych.	
11	Wysokość technologiczna podłogi technicznej w pomieszczeniu serwerowni min 0,7 m	Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych.	
12	Odseparowane pomieszczenie na przechowywanie nośników magnetycznych wyposażone w sejf. Sejf powinien posiadać atesty odporności ogniowej S120DIS zgodnie z EN 1047-1 oraz I klasę odporności włamaniowej zgodnie z EN 1143-1.	Przeciwdziałanie zagrożeniu fizycznego uszkodzenia, zniszczenia lub utraty nośników magnetycznych.	
13	Spełnienie wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie :budownictwa, energetyki	Przeciwdziałanie zagrożeniom budowlanym, pożarowym lub zagrożeniu życia i zdrowia ludzi w wyniku niezastosowania przepisów BHP, stosowania odrębnych od powszechnie	

	oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej.	stosowanych oznaczeń, błędów instalacji energetycznej.	
WĘZŁY TELEKOMUNIKACYJNE			
1	Podłączenie w pełni niezależnymi drogami światłowodowymi do co najmniej dwóch różnych operatorów telekomunikacyjnych o zasięgu krajowym	Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia usług transmisji danych przez operatora.	
2	Dojścia połączeń do ośrodka wykonane min. dwoma niezależnymi trasami kablowymi.	Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem.	
3	Węzeł dostępowy do sieci Internet dopięty do minimum 2 różnych operatorów z zaimplementowanym protokołem BGP	Zapewnienie niezawodności i jakości transmisji danych w ramach sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet.	
4	Węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,9%	Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet.	
5	Węzeł telekomunikacyjny wyposażony w redundantny system firewall	Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej.	
6	Węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci.	Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy.	
ZASILANIE			
1	Dostępność roczna systemu zasilania 99,9%	Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń.	
2	Minimum dwie niezależne linie zasilania dostępne dla sprzętu IT	Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego przywracania ciągłości zasilania.	
3	System zasilania awaryjnego UPS osobno na każdą linię zasilającą	Zagrożenie dla zachowania nieprzerwanego zasilania urządzeń lub skrócenia pracy urządzeń na zasilaniu awaryjnym poniżej czasu bezpiecznego.	
4	Redundantny system agregatów prądotwórczych	Zagrożenie braku zachowania zasilania	

5	System zasilaczy awaryjnych UPS winien podtrzymać zasilanie urządzeń komputerowych przeznaczonych dla Zamawiającego przez przynajmniej 15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatu i jego synchronizacji z siecią energetyczną	Zagrożenie ciągłości pracy urządzeń w wyniku niedostosowania czasu pracy na zasilaniu awaryjnym do czasu reakcji na awarię zasilania i uruchomienia agregatów. Zagrożenie dla utraty lub uszkodzenia danych w wyniku niedostosowania czasu pracy urządzeń do czasu bezpiecznego zamknięcia wykonywanych na urządzeniach procesów.	
6	Agregat prądotwórczy ma posiadać zapas paliwa pozwalający na autonomiczną pracę bez konieczności uzupełniania zbiorników przez co najmniej 8 godzin. Agregat musi umożliwiać uzupełnienie paliwa w trakcie jego pracy.	Zagrożenie powstania przerw w zasilaniu wynikających z zatrzymania pracy agregatów.	
BEZPIECZEŃSTWO			
1	Wyposażenie w system telewizji przemysłowej CCTV, okres archiwizacji min. 21 dni, system kontroli dostępu (SKD).	Zagrożenie braku kontroli i monitorowania fizycznego dostępu do urządzeń. Zagrożenie braku materiałów dowodowych w przypadku naruszenia fizycznego bezpieczeństwa urządzeń.	
2	Wyposażenie w system sygnalizacji włamania i napadu, System wykrywania wody i zalania.	Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu.	
3	Ochrona realizowana przez licencjonowaną firmę ochroniarską w trybie 24/7 .	Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej.	
4	System CCTV zapewnia ciągły 365/7/24 dozór obszarów i rejestrację zdarzeń z zachowaniem następujących parametrów funkcjonalnych: monitorowane wszystkie wejścia do obiektu – kamery wewnętrzne, monitorowane wszystkie pomieszczenia technologiczne.	Element zapewnienia wczesnego wykrywania i ostrzegania przed zagrożeniem naruszenia bezpieczeństwa fizycznego obiektu oraz zabezpieczenia materiału dowodowego na wypadek zaistnienia naruszenia, w tym identyfikacji osób.	
5	System CCTV powinien zapewnić: rejestrację z zapisem aktualnej daty i godziny, archiwizacja zapisanego materiału przez okres co najmniej 21 dni.	Element zapewniający możliwość określenia chronologii zdarzeń zapisanych w systemie monitorującym oraz odtworzenie zapisu zdarzeń po wykryciu zagrożeń.	

6	Dostęp do pomieszczenia ze sprzętem komputerowym Zamawiającego możliwy wyłącznie przy użyciu łącznie 2 elementów identyfikacji SKD - osobistej karty identyfikacyjnej i hasła (kodu) lub elementu biometrycznego.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	
7	System gaszenia w pomieszczeniu z serwerami powinien być bezpieczny dla ludzi i sprzętu komputerowego.	Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia.	
8	Ściany, stropy części technologicznej o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń technologicznych o odporności ogniowej 60 minutowej.	Zapewnienie oporności ogniowej do czasu reakcji służb ratowniczych w celu ograniczenia skutków wystąpienia pożaru. Przeciwdziałanie zagrożenia rozprzestrzeniania się pożaru.	
MONITOROWANIE			
1	System przyjmowania zgłoszeń dotyczących awarii działający w trybie 365/24/7	Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej.	
2	Stałe i całodobowe (24/7/365) monitorowanie poprawności pracy infrastruktury ośrodka i urządzeń komputerowych udostępnianej Zamawiającemu. Pomiary mają dotyczyć minimum: wykresy przebiegów temperatury, wykres przebiegu wilgotności.	Zagrożenie braku kontroli parametrów pracy ośrodka oraz długich reakcji niekorzystne zmiany warunków pracy urządzeń.	
CERTYFIKACJA			
1	certyfikat potwierdzający zarządzanie ciągłością działania w organizacji minimum w zakresie świadczenia usług w modelu cloud computing i backupu danych	Minimalizacja zagrożenia przerw w dostępie do usług, określenie wymogów wobec zapobiegania incydentom zakłócającym pracę, zmniejszenia prawdopodobieństwa ich wystąpienia.	
2	certyfikat potwierdzający bezpieczeństwo informacji minimum w zakresie świadczenia usług w modelu cloud computing i backupu danych	Zwiększenie poziomu zabezpieczeń przetwarzanych danych, określenie procedury bezpieczeństwa IT.	

CPD musi posiadać zabezpieczenia fizyczne i organizacyjne zapewniające bezpieczeństwo danych przetwarzanych. Ośrodek ponosi odpowiedzialność w zakresie bezpieczeństwa informacji przechowywanych na wykorzystanej infrastrukturze serwerowej.

Tabela 2. Bezpieczeństwo sprzętu informatycznego.

	Zakres	Wykonawca spełnia (TAK / NIE)
1	Izolacja sprzętu krytycznego	
2	Ochrona przed uszkodzeniem	
3	Rejestr wejść i wyjść do obszaru, w którym umieszczony jest sprzęt przeznaczony do obsługi Zamawiającego	
4	Ochrona przed dostępem dla osób nieupoważnionych	
5	Ochrona infrastruktury przed instalacją złośliwego oprogramowania.	

Tabela 3. Naprawy i konserwacja sprzętu.

	Zakres	Wykonawca spełnia (TAK / NIE)
1	Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu.	
2	Obsługa i naprawy muszą być dokonywane przez personel posiadający kwalifikacje zgodnie z zaleceniami producenta sprzętu i wewnętrznymi procedurami Ośrodka.	
3	Należy usuwać nośniki danych przed przekazaniem sprzętu do naprawy.	
4	Należy stosować bezpieczne zbywanie lub przekazywanie sprzętu do ponownego użycia, w tym skuteczne usuwanie danych z nośników (wraz z systemami operacyjnymi i danymi licencyjnymi).	
5	Należy wykonywać przeglądy techniczne zgodnie z wymaganiami producenta sprzętu i procedurami wewnętrznymi Ośrodka.	
6	Należy prowadzić rejestr incydentów, awarii i usterek.	
7	Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu.	

3.2. Warunki ciągłości działania SLA i czas reakcji

1. Dostępność Usługi musi wynosi minimum SLA 99,9% w skali roku.
2. Obsługa infrastruktury teleinformatycznej CPD musi być realizowana w trybie 24/7/365.
3. Czas reakcji na zgłoszenie musi wynosić do 60 min.
4. Czas usunięcia awarii krytycznej – awarii powodującej stałą niedostępność Usługi trwającej dłużej niż 60 min - należy wykonać w terminie do 6 godzin od zgłoszenia awarii.
5. Czas usunięcia awarii zwykłej – awarii powodującej chwilową niedogodność w dostępie do Usługi lub krótkie przerwy w jej dostępności – należy usunąć w terminie 1 dni roboczych od zgłoszenia awarii.

6. Przyjmowanie zgłoszeń serwisowych musi być realizowane w trybie 24/7/365.

3.3. Uruchomienie infrastruktury teleinformatycznej

Wykonawca jest zobowiązany:

1. przygotować i udostępnić Zamawiającemu maszyny wirtualne wraz z systemami operacyjnymi i bazodanowymi (wraz z zapewnieniem niezbędnego oprogramowania i/lub licencji na czas trwania Usługi);
2. zapewnić niezbędne pozostałe oprogramowanie i/lub licencje oraz infrastrukturę teleinformatyczną związane z realizacją Umowy;
3. skonfigurować połączenia sieciowe pomiędzy poszczególnymi maszynami wirtualnymi;
4. przygotować i udostępnić fizycznie wydzielony serwer plików
5. skonfigurować i udostępnić dedykowane łącze światłowodowe od serwera plików do siedziby Zamawiającego zgodnie z określonymi parametrami;
6. skonfigurować i udostępnić łącze do sieci Internet, zgodnie z określonymi parametrami;
7. skonfigurować ochronę na styku z Internetem w warstwie sieciowej i aplikacyjnej;
8. skonfigurować i udostępnić system Backup do wykonywania kopii bezpieczeństwa wszystkich serwerów i bazy danych;
9. skonfigurować i udostępnić system zbierania i przechowania logów zdarzeń z urządzeń styku z siecią Internet;
10. świadczyć usługę administrowania uruchomionymi maszynami wirtualnymi do poziomu systemu operacyjnego w trybie 24/7/365, zgodnie z określonymi parametrami i czasem reakcji.
11. zapewnić bezprzerwową migrację z obecnych serwerów wirtualnych Zamawiającego i ich konfigurację w środowisku Wykonawcy.

3.4. Maszyny wirtualne i serwer plików

Wykonawca musi udostępniać maszyny wirtualne i serwer plików oraz oprogramowanie systemowe i narzędziowe o parametrach nie gorszych niż określone w Tabeli 4. Wykonawca musi zapewnić niezawodność i ciągłość pracy serwerów wirtualnych i serwera plików w ramach rozwiązania HA - w przypadku awarii pojedynczego komponentu (m.in. serwer fizyczny, dysk) musi następować automatyczne bezprzerwowe przełączenie urządzeń w celu utrzymania ciągłości pracy dostarczonych zasobów. Do zadań realizowanych przez Wykonawcę w ramach usług utrzymaniowych infrastruktury teleinformatycznej należeć będzie bieżąca obsługa administracji IT zasobów informatycznych (instancji serwerowych) wraz z nadzorem nad posiadaną przez Zamawiającego infrastrukturą zlokalizowaną CPD w zakresie:

a) migracji usług do infrastruktury chmurowej i ich utrzymania;
b) instalacji i konfiguracji systemów operacyjnych;
c) instalacji i konfiguracji elementów niezbędnych do zapewnienia środowiska wysokiej dostępności HA;
d) aktualizacji oprogramowania ze względu na błędy bezpieczeństwa;
e) utrzymania infrastruktury pod kątem wydajności, bezpieczeństwa;
f) realizacji bieżących czynności administracyjnych maszyn wirtualnych;

g) analiz incydentów oraz problemów wraz pełnym przywracaniem funkcjonalności.

Wymagana jest regularna realizacja usługi backupowej całego środowiska serwerów wirtualnych i serwera plików według harmonogramu: 1 kopia raz dziennie, retencja 7 dni w trakcie całego czasu trwania umowy.

Zamawiający oczekuje realizacji RTO na poziomie 6 godzin dla pojedynczej maszyny wirtualnej oraz 6 godzin dla całego środowiska oraz RPO zgodnie z przyjętym harmonogramem.

Wymagany jest monitoring środowiska w zakresie wydajności (zajętość dysków, dostępność usług, ważność certyfikatów) w trakcie całego czasu trwania umowy.

Niezależnie od powyższego zakresu czynności, do dyspozycji w ramach świadczonej usługi wsparcia administracyjnego Wykonawca udostępni zasoby ludzkie w postaci 40 roboczogodzin pracy Administratorów i Specjalistów IT na prace zlecone przez Zamawiającego związane z kreowaniem, przenoszeniem, zabezpieczaniem, testowaniem, przywracaniem, aktualizacją, bieżącym utrzymaniem systemów w środowisku infrastrukturalnym, wsparciem systemów funkcjonujących w środowisku infrastrukturalnym oraz innymi obszarami funkcjonowania instancji serwerowych przez cały czas trwania usługi wynikającej z przedmiotowego Zamówienia.

Tabela 4. Parametry techniczne serwerów wirtualnych

1	Serwer wirtualny (www) x 1 szt.	Minimalne wymagania Zamawiającego
a	Architektura	x86-64
b	Pamięć podstawowa	4 GB DDR3 1333MHz
c	Procesor/Procesory	4 x 2,40GHz (E5-2630 V.3) min. 10 000 punktów w teście PassMark
d	Skalowalność	Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50%
e	Interfejsy sieciowe	2 x 10Gb
f	Moduł zarządzania	Wymagany
g	System operacyjny	Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny
h	Przestrzeń dyskowa	200 GB (200.000 IOPS)
i	Adres zewnętrzny	1 x IPv4
j	Backup	Kopia zapasowa serwera wirtualnego: 1 szt. x 200 GB HDD
k	Antywirus	Ochrona antywirusowa serwera wirtualnego: 1 szt.
2	Serwer wirtualny (aplikacji) x 2 szt.	Minimalne wymagania Zamawiającego
a	Architektura	x86-64
b	Pamięć podstawowa	4 GB DDR3 1333MHz
c	Procesor/Procesory	2 x 2,40GHz (E5-2630 V.3) min. 10 000 punktów w teście PassMark
d	Skalowalność	Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50%
e	Interfejsy sieciowe	2 x 10Gb
f	Moduł zarządzania	Wymagany

g	System operacyjny	Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny
h	Przestrzeń dyskowa	100 GB (200.000 IOPS)
I	Adres zewnętrzny	2 x IPv4
J	Backup	Kopia zapasowa serwera wirtualnego: 1 szt. x 100 GB HDD
K	Antywirus	Ochrona antywirusowa serwera wirtualnego: 1 szt.
3	Serwer wirtualny (aplikacja) x 1 szt.	Minimalne wymagania Zamawiającego
a	Architektura	x86-64
b	Pamięć podstawowa	2 GB DDR3 1333MHz
c	Procesor/Procesory	2 x 2,40GHz (E5-2630 V.3) min. 10 000 punktów w teście PassMark
d	Skalowalność	Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50%
e	Interfejsy sieciowe	2 x 10 Gb
f	Moduł zarządzania	Wymagany
g	System operacyjny	Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny
H	Przestrzeń dyskowa	100 GB (200.000 IOPS)
I	Adres zewnętrzny	1 x IPv4
J	Backup	Kopia zapasowa serwera wirtualnego: 1 szt. x 100 GB HDD
K	Antywirus	Ochrona antywirusowa serwera wirtualnego: 1 szt.
4	Serwer wirtualny (aplikacja) x 1 szt.	Minimalne wymagania Zamawiającego
a	Architektura	x86-64
b	Pamięć podstawowa	4 GB DDR3 1333MHz
c	Procesor/Procesory	2 x 2,40GHz (E5-2630 V.3) min. 10 000 punktów w teście PassMark
d	Skalowalność	Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50%
e	Interfejsy sieciowe	2 x 10Gb
f	Moduł zarządzania	Wymagany
g	System operacyjny	Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny
h	Przestrzeń dyskowa	200 GB (200.000 IOPS)
I	Adres zewnętrzny	1 x IPv4
J	Backup	Kopia zapasowa serwera wirtualnego: 1 szt. x 200 GB HDD
K	Antywirus	Ochrona antywirusowa serwera wirtualnego: 1 szt.
5	Serwer wirtualny (aplikacja) x 1 szt.	Minimalne wymagania Zamawiającego
a	Architektura	x86-64
b	Pamięć podstawowa	4 GB DDR3 1333MHz
c	Procesor/Procesory	4 x 2,40GHz (E5-2630 V.3) min. 10 000 punktów w teście PassMark

d	Skalowalność	Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50%
e	Interfejsy sieciowe	2 x 10Gb
f	Moduł zarządzania	Wymagany
g	System operacyjny	Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny
h	Przestrzeń dyskowa	100 GB (200.000 IOPS)
I	Adres zewnętrzny	1 x IPv4
J	Backup	Kopia zapasowa serwera wirtualnego: 1 szt. x 100 GB HDD
K	Antywirus	Ochrona antywirusowa serwera wirtualnego: 1 szt.
6	Serwer wirtualny (aplikacja) x 3 szt.	Minimalne wymagania Zamawiającego
a	Architektura	x86-64
b	Pamięć podstawowa	2 GB DDR3 1333MHz
c	Procesor/Procesory	2 x 2,40GHz (E5-2630 V.3) min. 10 000 punktów w teście PassMark
d	Skalowalność	Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50%
e	Interfejsy sieciowe	2 x 10Gb
f	Moduł zarządzania	Wymagany
g	System operacyjny	Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny
h	Przestrzeń dyskowa	100 GB (200.000 IOPS)
I	Adres zewnętrzny	1 x IPv4
J	Backup	Kopia zapasowa serwera wirtualnego: 1 szt. x 100 GB HDD
K	Antywirus	Ochrona antywirusowa serwera wirtualnego: 1 szt.
7	Serwer wirtualny (aplikacja) x 2 szt.	Minimalne wymagania Zamawiającego
a	Architektura	x86-64
b	Pamięć podstawowa	4 GB DDR3 1333MHz
c	Procesor/Procesory	2 x 2,40GHz (E5-2630 V.3) min. 10 000 punktów w teście PassMark
d	Skalowalność	Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50%
e	Interfejsy sieciowe	2 x 10Gb
f	Moduł zarządzania	Wymagany
g	System operacyjny	Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny
h	Przestrzeń dyskowa	100 GB (200.000 IOPS)
I	Adres zewnętrzny	1 x IPv4
J	Backup	Kopia zapasowa serwera wirtualnego: 1 szt. x 100 GB HDD
K	Antywirus	Ochrona antywirusowa serwera wirtualnego: 1 szt.
8	Serwer wirtualny (AD) x 2 szt.	Minimalne wymagania Zamawiającego

a	Architektura	x86-64
b	Pamięć podstawowa	4 GB DDR3 1333MHz
c	Procesor/Procesory	2 x 2,40GHz (E5-2630 V.3) min. 10 000 punktów w teście PassMark
d	Skalowalność	Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50%
e	Interfejsy sieciowe	2 x 10Gb
f	Moduł zarządzania	Wymagany
g	System operacyjny	Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny
h	Przestrzeń dyskowa	100 GB (200.000 IOPS)
i	Backup	Kopia zapasowa serwera wirtualnego: 1 szt. x 100 GB HDD
j	Antywirus	Ochrona antywirusowa serwera wirtualnego: 1 szt.
9	Serwer wirtualny (OCSIP) x 1 szt.	Minimalne wymagania Zamawiającego
a	Architektura	x86-64
b	Pamięć podstawowa	2 GB DDR3 1333MHz
c	Procesor/Procesory	2 x 2,40GHz (E5-2630 V.3) min. 10 000 punktów w teście PassMark
d	Skalowalność	Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50%
e	Interfejsy sieciowe	2 x 10Gb
f	Moduł zarządzania	Wymagany
g	System operacyjny	Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny
h	Przestrzeń dyskowa	100 GB (200.000 IOPS)
i	Backup	Kopia zapasowa serwera wirtualnego: 1 szt. x 100 GB HDD
j	Antywirus	Ochrona antywirusowa serwera wirtualnego: 1 szt.
10	Serwer wirtualny (Update) x 1 szt.	Minimalne wymagania Zamawiającego
a	Architektura	x86-64
b	Pamięć podstawowa	2 GB DDR3 1333MHz
c	Procesor/Procesory	2 x 2,40GHz (E5-2630 V.3) min. 10 000 punktów w teście PassMark
d	Skalowalność	Możliwość zwiększenia pamięci operacyjnej i wydajności obliczeniowej procesorów min. o 50%
e	Interfejsy sieciowe	2 x 10Gb
f	Moduł zarządzania	Wymagany
g	System operacyjny	Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny
h	Przestrzeń dyskowa	100 GB (200.000 IOPS)
i	Backup	Kopia zapasowa serwera wirtualnego: 1 szt. x 100 GB HDD
j	Antywirus	Ochrona antywirusowa serwera wirtualnego: 1 szt.
11	Fizyczny serwer plików	Minimalne wymagania Zamawiającego

a	Pamięć RAM	co najmniej 2 GB
b	Dyski twarde	co najmniej 4 dyski twarde o pojemności 4TB każdy z interfejsem SATA III dedykowane do pracy w urządzeniach typu NAS
c	Ilość kieszeni na dyski	co najmniej 4 kieszenie dyskowe obsługujące dyski 3.5" oraz 2,5”, obsługujących dyski z interfejsem SATA III, kieszenie z funkcją hot-swap
d	Sieć	co najmniej 1 port Gigabit LAN
e	Złącza dodatkowe	co najmniej 2 x USB 3.0, 1 x eSATA
f	Wskaźniki LED	co najmniej zasilanie, HDD 1-4, Status
g	Obsługa trybów RAID	co najmniej RAID 10, RAID 6, RAID 5, RAID 1, RAID 0, JBOD
h	Montaż	montaż w szafie rack, szyny montażowe w zestawie. umożliwiające montaż w szafie rack.
i	Zasilanie	co najmniej 2 zasilacze redundantne o mocy pozwalającej na poprawną pracę urządzenia przy maksymalnym obłożeniu kieszeni na dyski
j	Obsługiwane systemy operacyjne	co najmniej Windows, Mac OSX, Linux
k	System plików	Dla dysków wewnętrznych obsługa co najmniej ext4 i btrfs, dla dysków zewnętrznych btrfs, ext3, ext4, fat, ntfs
l	Protokoły sieciowe	Dla obsługi plików co najmniej CIFS, AFP, NFS, FTP, WebDAV
ł	Konfiguracja sieci	TCP / IP, stały lub dynamiczny adres
m	Mechanizm szyfrowania sprzętowego	Tak
n	Zarządzanie systemem	poprzez przeglądarkę internetową
o	Logi systemowe	co najmniej inf. o użytkownikach, alarmach, błędach, połączeniach
p	ilość użytkowników	do 2048
r	ilość grup	do 256
s	ilość folderów udostępnionych	do 512
t	ilość jednoczesnych połączeń	do 500
u	Język interfejsu	co najmniej polski i angielski

Tabela 5. Podsumowanie ilości komponentów serwerów wirtualnych

	Komponent	Ilość
1	Serwery wirtualne (maszyny wirtualne)	15 szt.
2	Pamięć podstawowa - DDR3 1333MHz	48 GB
3	Procesor 2,40GHz (E5-2630 V.3) min. 500 punktów w teście PECint_rate_2006	34 vCPU
4	Razem system operacyjny - Windows Server 2016 z możliwością upgrade do nowszej wersji lub równoważny	15 szt.
5	Razem adres zewnętrzny IPv4	15 szt.
6	Razem sieć wewnętrzna vLAN	15 szt.
7	Razem przestrzeń dyskowa 200.000 IOPS	1 800 GB
8	Razem Backup maszyn wirtualnych	15 szt.
9	Razem przestrzeń HDD Backup	1 800 GB

10.	Razem ochrona antywirusowa serwerów wirtualnych	15 szt.

Opis równoważności Windows Server 2016.

Minimalne funkcjonalności:

1. możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
2. możliwość dokonywania uaktualnień sterowników urządzeń przez Internet witrynę producenta systemu;
3. darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat);
4. wymagane podanie nazwy strony serwera www;
5. internetowa aktualizacja zapewniona w języku polskim;
6. wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami ip v4 i v6;
7. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe;
8. możliwość uruchomienia kontrolera domeny będącego w pełni zgodnym z wdrożoną u Zamawiającego domeną AD pracującą w oparciu o system Windows Server 2012 R2 (poziom funkcjonalności AD DS Windows Server 2012 R2);
9. możliwość uruchomienia kontrolera domeny tylko do odczytu;
10. możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny i w pełni zgodnego z serwerami DNS Zamawiającego pracującymi w oparciu Windows Server 2012 R2 Enterprise;
11. możliwość uruchomienia serwera usług terminalowych (RemoteApp) zgodnego z Windows Server 2012 R2; obsługa zdalnego pulpitu;
12. możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
13. obsługa wirtualizatora Hyper-V
14. obsługa PowerShell 4.0
15. obsługa certyfikatów w AD;
16. obsługa Microsoft Office 2013;
17. obsługa drzewa katalogowego Microsoft Active Directory.

3.5. Ochrona antywirusowa

Wdrożenie ochrony antywirusowej dla 70 stacji roboczych.

Tabela nr 6. Wymagania dla ochrony antywirusowej

Lp.	Minimalne wymagania
1	Systemy Operacyjne Windows ● Windows 10 ● Windows 8.1 ● Windows 8
2	Środowiska Microsoft Exchange ● Exchange Server 2016 z rolą Edge Transport

	lub Mailbox ● Exchange Server 2013 z rolą Edge Transport lub Mailbox ● Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox ● Exchange Server 2007 z rolą Edge Transport, Hub Transport lub Mailbox
3	Wymagania funkcjonalno-użytkowe: 1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim. 3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 4. Wbudowana technologia do ochrony przed rootkitami. 5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". 7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 8. Możliwość skanowania dysków sieciowych i dysków przenośnych. 9. Skanowanie plików spakowanych i skompresowanych. 10. Możliwość umieszczenia na liście wykluczenia ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach i procesów. 11. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express. 12. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 13. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 14. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 15. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. 16. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 17. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać. 18. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS. 19. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 20. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło. 21. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : O programie" możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony. 22. Możliwość pobrania płyty ratunkowej, do uruchomienia z niej komputera i przeskanowania dysków umieszczonych w komputerze. 23. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.

	24. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien pracować w trybie graficznym. 25. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. 26. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 27. Praca programu musi być niezauważalna dla użytkownika. 28. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej. 29. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet. 30. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej. 31. Możliwość odblokowania ustawień programu po wpisaniu hasła 32. Posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu modułu Super użytkownika 33. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie) 34. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, z bazy danych urządzeń podłączanych przez użytkowników do komputerów. 35. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp. 36. Funkcja Ochrony danych konfigurowana zdalnie przez administratora. 37. Jedna wersja instalacyjna na stacje robocze i serwery plików. 38. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego. 39. Możliwość zainstalowania silnika pełnego, lekkiego z sprawdzaniem reputacji plików w chmurze, lub skanowanie przez centralny serwer bezpieczeństwa. 40. Możliwość tworzenia list sieci zaufanych. 41. Możliwość dezaktywacji funkcji zapory sieciowej. 42. Możliwość ochrony systemu bez instalacji na stacji roboczej silnika antywirusowego. Jego role przejmuje centralny serwer bezpieczeństwa odpowiedzialny za proces skanowania plików. 43. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu. 44. Dodatkowy moduł ochrony przeciwko zagrożeniom typu ransomware.

3.6. Poczta email i pakiet aplikacji biurowych

Tabela nr 7. Wymagania dla poczty email dla 10 kont technicznych.

Lp.	Minimalne wymagania dla pojedynczego konta
1	Powierzchnia dysku w chmurze pojedynczego użytkownika 10 GB
2	Maksymalny rozmiar załącznika w jednej wiadomości email 50 MB
3	Środowisko MS Exchange
4	Dostęp do OWA (Outlook Web Aplication)
5	ActiveSync dla smartfonów i tabletów
6	Dostęp przez IMAP
7	Integracja z firmowym Active Directory
8	Ochrona antyspamowa i antywirusowa na serwerze
9	Własna domena firmowa

10	MS Outlook aktualizowane do najnowszych wersji oprogramowania

Tabela nr 8. Wymagania dla poczty email dla 60 użytkowników.

Lp.	Minimalne wymagania dla pojedynczego Użytkownika
1	Powierzchnia dysku w chmurze pojedynczego użytkownika 50 GB
2	Maksymalny rozmiar załącznika w jednej wiadomości email 150 MB
3	Środowisko MS Exchange
4	Dostęp do OWA (Outlook Web Aplication)
5	ActiveSync dla smartfonów i tabletów
6	Dostęp przez IMAP
7	Integracja z firmowym Active Directory
8	Ochrona antyspamowa i antywirusowa na serwerze
9	Własna domena firmowa
10	MS Outlook aktualizowane do najnowszych wersji oprogramowania
11	Prywatny i współdzielony kalendarz

Tabela nr 9. Wymagania dla aplikacji biurowych dla 60 użytkowników.

Lp.	Minimalne wymagania dla pojedynczego Użytkownika
1	Pełne, instalowane i zawsze aktualne wersje programów Outlook, Word, Excel, PowerPoint i OneNote dla systemu Windows lub dla komputerów Mac (oraz programów Access i Publisher tylko dla komputerów PC)
2	Każdy użytkownik może zainstalować aplikacje pakietu Office na maksymalnie 5 komputerach PC
3	Internetowe wersje aplikacji Word, Excel, PowerPoint i OneNote
4	Możliwość centralnego zarządzania użytkownikami – konto administratora do zarządzania licencjami MS 365 Business STD
5	Podłączenie komputerów lokalnych użytkowników do Active Directory.
6	Dostęp do aplikacji umożliwiającej komunikację z innymi użytkownikami wewnątrz i na zewnątrz firmy, a także tworzenie konferencji
7	Internetowa wersja aplikacji Outlook
8	Dostęp do usługi katalogowej w chmurze typu SharePoint o pojemności 1TB

Warunki dla Share Point.

Serwer systemu wyszukiwania i gromadzenia danych (SWGD) musi zapewniać:

1. Publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych i zewnętrznych.
2. Zarządzanie strukturą portalu i treściami WWW.
3. Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej.
4. Udostępnienie formularzy elektronicznych.
5. Tworzenie repozytoriów wzorów dokumentów.
6. Tworzenie repozytoriów dokumentów.

7. Wspólną, bezpieczną pracę nad dokumentami.
8. Wersjonowanie dokumentów (dla wersji roboczych).
9. Organizację pracy grupowej.
10. Wyszukiwanie treści.
11. Dostęp do danych w relacyjnych bazach danych.
12. Analizę danych wraz z graficzną prezentacją danych.
13. Możliwość wykorzystania mechanizmów portalu do budowy systemu zarządzania eszkoleniami (e-learning).
14. Możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.
15. Mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów.

Serwery SWGD muszą posiadać następujące cechy dostępne bezpośrednio, jako wbudowane właściwości produktu:

1) Interfejs użytkownika:
   a) Praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji w specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu).
   b) Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0.
   c) Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów.
   d) Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego.
   e) Możliwość pracy off-line z plikami przechowywanymi w repozytoriach portalu.
   f) Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy).
2) Uwierzytelnianie – wbudowane mechanizmy wspierające uwierzytelnianie na bazie:
   a) Oświadczeń (claim-based authentication) z wykorzystaniem:
      i) Open Authorization 2.0 dla uwierzytelniania aplikacji,
      ii) Uwierzytelniania w trybie server-to-server,
      iii) SAML iv. Windows claims.
   b) Pojedynczego logowania domenowego (single-sign on).
   c) Na bazie formularzy (Form-based).
3) Projektowanie stron:
   a) Wbudowane intuicyjne narzędzia projektowania wyglądu stron.
   b) Wsparcie dla narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML.
   c) Wsparcie dla ASP.NET, Apache, C#, Java i PHP.
   d) Możliwość osadzania elementów iFrame w polach HTML na stronie.
4) Integracja z pozostałymi modułami rozwiązania oraz innymi systemami:
   a) Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili.
   b) Dostęp poprzez interfejs portalowy do całości bądź wybranych elementów skrzynek pocztowych użytkowników w komponencie poczty elektronicznej, z zapewnieniem podstawowej funkcjonalności pracy z tym systemem w zakresie czytania, tworzenia, przesyłania elementów.
   c) Możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili.
   d) Integracja z systemem obsługującym serwis WWW w zakresie publikacji treści z repozytoriów wewnętrznych firmy na zewnętrzne strony serwisu WWW (pliki, strony).

e) Integracja z usługą katalogową w zakresie prezentacji informacji o pracownikach. Dane typu: imię, nazwisko, stanowisko, telefon, adres, miejsce w strukturze organizacyjnej mają stanowić źródło dla systemu portalowego.
f) Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services.
g) Mechanizm jednokrotnej identyfikacji (single sign-on) pozwalający na autoryzację użytkowników portalu i dostęp do danych w innych systemach biznesowych, niezintegrowanych z systemem LDAP.
h) Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym z możliwością wydzielenia danych.

5) Zarządzanie treścią i wyglądem portalu powinno opierać się o narzędzia umożliwiające prostą i intuicyjną publikację treści w formacie HTML w trybie WYSIWYG, bez konieczności znajomości języka HTML i innej wiedzy technicznej przez autorów treści:
a) Możliwość formatowania tekstu w zakresie zmiany czcionki, rozmiaru, koloru, pogrubienia, wyrównania do prawej oraz lewej strony, wyśrodkowania, wyjustowania.
b) Proste osadzenie i formatowanie plików graficznych, łącz (linków) różnych typów, tabel, paragrafów, wypunktowań itp. w treści artykułów publikowanych w intranecie (stron HTML).
c) Spójne zarządzanie wyglądem stron intranetu, głównie pod kątem formatowania tekstu: możliwość globalnego zdefiniowania krojów tekstu, które mogą być wykorzystywane przez edytorów treści, możliwość wklejania treści przy publikacji stron intranetu z plików tekstowych lub edytorów tekstu (np. MS Word) z zachowaniem lub z usunięciem formatowania oryginalnego.
d) Zarządzanie galeriami zasobów elektronicznych (pliki graficzne, filmy video, dokumenty), wykorzystywanymi przy tworzeniu stron intranetu i przechowywanymi w intranetowym repozytorium treści. Możliwość współdzielenia tych zasobów na potrzeby stron umiejscowionych w różnych obszarach portalu intranetowego. Podstawowe funkcjonalności związane z wersjonowaniem i wyszukiwaniem tych zasobów.
e) Definiowanie szablonów dla układów stron (tzw. layout'ów), określających ogólny układ stron intranetu oraz elementy wspólne dla stron opartych na tym samym szablonie. Możliwość stworzenia wielu szablonów na potrzeby różnych układów stron w zależności od potrzeb funkcjonalnych w różnych częściach intranetu. Możliwość generalnej zmiany wyglądu utworzonych już stron poprzez modyfikację szablonu, na którym zostały oparte.
f) Możliwość wielokrotnego wykorzystania elementów zawartości intranetu (części treści publikowanych na stronach) w różnych częściach portalu, tzn. modyfikacja zawartości w jednym miejscu powoduje jej faktyczną zmianę na wszystkich stronach intranetu, gdzie dana treść została opublikowana
g) Możliwość odwzorowania w systemie CMS przyjętej wizualizacji portalu intranetowego (projekt graficzny i funkcjonalny).
h) Możliwość osadzania na stronach narzędzia do odtwarzania materiałów audio i wideo,

6) Organizacja i publikacja treści:
a) Wersjonowanie treści stron intranetu, działające automatycznie przy wprowadzaniu kolejnych modyfikacji przez edytorów treści.
b) Zastosowanie procesów zatwierdzania zawartości przez publikacją, tzn. Udostępnieniem jej dla szerokiego grona pracowników. Możliwość zdefiniowania przynajmniej dwóch poziomów uprawnień edytorów (edytor i recenzent), przy czym treści publikowane przez edytorów muszą uzyskać pozytywną akceptację recenzenta przed Udostępnieniem jej wszystkim użytkownikom intranetu.
c) Możliwość budowania hierarchicznej struktury stron portalu z prostym przenoszeniem stron i sekcji w ramach struktury nawigacji.
d) Automatyczne tworzenie nawigacji na stronach intranetu, odwzorowujące obecną hierarchię.
e) Automatyczne generowanie mapy stron portalu.
f) Możliwość definiowania nawigacji w oparciu o centralne zarządzanie metadanymi.
g) Umożliwienie zarządzania poszczególnymi obszarami portalu osobom nietechnicznym, pełniącym rolę edytorów bądź administratorów merytorycznych. Istotne jest nieangażowanie zespołu IT w proces zarządzania treścią intranetu.
h) Definiowanie uprawnień użytkowników niezależnie do poszczególnych sekcji i stron intranetu, np. do obszarów poszczególnych spółek, dywizji, biur. Dotyczy to zarówno uprawnień do odczytu zawartości,

jak i edycji oraz publikacji (różni edytorzy zawartości intranetu w zależności od jego części). Definiowanie uprawnień powinno być dostępne dla administratorów merytorycznych poszczególnych obszarów portalu w sposób niezależny od pracowników działu IT.

i) Automatyczne dołączanie do publikowanych stron informacji o autorze (edytorze) i dacie publikacji.
j) Możliwość personalizacji i filtrowania treści w intranecie w zależności od roli lub innych atrybutów pracownika (np. stanowiska, działu, pionu lub spółki). Funkcjonalność ta ma być niezależna od mechanizmów zarządzania uprawnieniami użytkownika do zawartości, i ma mieć na celu dostarczenie pracownikowi adekwatnych, skierowanych do niego informacji.
k) Wsparcie dla obsługi różnych wersji językowych wybranych zawartości intranetu oraz zapewnienie automatycznego tłumaczenia na wybrane języki.

7) Repozytoria dokumentów:
   a) Możliwość prostej publikacji dokumentów w intranecie przez edytorów portalu. Prosty sposób publikacji dokumentów, funkcjonalny dostęp użytkowników intranetu do opublikowanych dokumentów.
   b) Wykorzystanie do publikacji, edycji i przeglądania dokumentów w repozytorium narzędzi znanych użytkownikom np. pakiety biurowe czy przeglądarka internetowa.
   c) Możliwość tworzenia wielu tematycznych repozytoriów dokumentów w różnych częściach intranetu.
   d) Możliwość publikacji plików w strukturze katalogów.
   e) Możliwość publikacji materiałów wideo oraz audio.
   f) Możliwość definiowania metryki dokumentu, wypełnianej przez edytora przy publikacji pliku.
   g) Możliwość nawigacji po repozytorium dokumentów (lub całym portalu) w oparciu o metadane z metryk dokumentów.
   h) Prosty, elastyczny i niezależny od działu IT mechanizm zarządzania uprawnieniami do publikowanych dokumentów w ramach istniejących uprawnień. Możliwość definiowania różnych poziomów uprawnień przez administratorów merytorycznych, np. uprawnienia do odczytu, publikacji, usuwania.
   i) Zarządzanie wersjonowaniem dokumentów: obsługa głównych oraz roboczych wersji (np.: 1.0, 1.1, 1.x… 2.0), automatyczna kontrola wersji przy publikacji dokumentów.
   j) Możliwość zdefiniowania w systemie procesu zatwierdzania nowych lub modyfikowanych dokumentów. System informuje użytkowników recenzujących materiały o oczekujących na nich elementach do zatwierdzenia i pozwala podjąć decyzję o ich publikacji lub odrzuceniu.
   k) Możliwość tworzenia specjalnych repozytoriów lub katalogów przeznaczonych do przechowywania specyficznych rodzajów treści, np. galerie obrazów dla plików graficznych.
   l) Możliwość definiowania polityk cyklu życia dokumentu oraz retencji dokumentów.
   m) Możliwość tworzenia specjalnych repozytoriów przeznaczonych na raporty osadzone w arkuszach kalkulacyjnych w formacie ISO/IEC 29500:2008. Serwer powinien generować na podstawie tych arkuszy kalkulacyjnych raporty dostępne do oglądania przez przeglądarkę Internetową bez zainstalowanych innych narzędzi klienckich.
   n) Możliwość automatyzacji usuwania duplikatów dokumentów.

8) Wyszukiwanie treści:
   a) Pełnotekstowe indeksowanie zawartości intranetu w zakresie różnych typów treści publikowanych w portalu, tj. stron portalu, dokumentów tekstowych (w szczególności dokumentów XML), innych baz danych oraz danych dostępnych przez webservice.
   b) Centralny mechanizm wyszukiwania treści dostępny dla użytkowników intranetu.
   c) Opcja wyszukiwania zaawansowanego, np. wyszukiwanie wg typów treści, autorów, oraz zakresów dat publikacji.
   d) Możliwość budowania wielu wyszukiwarek w różnych częściach portalu, służących do przeszukiwania określonych obszarów intranetu wg zadanych kryteriów, np. wg typów dokumentów.
   e) Możliwość definiowania słownika słów wykluczonych (często używanych).
   f) Możliwość tworzenia „linków sponsorowanych”, prezentowanych wysoko w wynikach wyszukiwania w zależności od słów wpisanych w zapytaniu.
   g) Podświetlanie w wynikach wyszukiwania odnalezionych słów kluczowych zadanych w zapytaniu.
   h) Przedstawianie w wynikach duplikatów plików.
   i) Statystyki wyszukiwanych fraz.

9) Administracja intranetem i inne funkcje:
   a) Możliwość definiowania ról / grup uprawnień, w ramach których definiowane będą uprawnienia i funkcje użytkowników. Przypisywanie użytkowników do ról w oparciu o ich konta w LDAP lub poprzez grupy domenowe. Funkcjonalność zarządzania uprawnieniami dostępna dla administratorów merytorycznych intranetu, niewymagająca szczególnych kompetencji technicznych.
   b) Możliwość określania uprawnień do poszczególnych elementów zawartości intranetu tj. sekcja, pojedyncza strona, repozytorium dokumentów, katalogu dokumentów, pojedynczego dokumentu.
   c) Generowanie powiadomień pocztą elektroniczną dla użytkowników intranetu z informacją o publikacji najbardziej istotnych treści.
   d) Definiowanie metryk opisujących dokumenty w poszczególnych repozytoriach portalu oraz centralnie zarządzanego zbioru metadanych z wyznaczonym administratorem merytorycznym.
   e) Możliwość definiowania zewnętrznych źródeł danych takich jak bazy danych i webservice oraz wykorzystywania ich do opisywania dokumentów.
   f) Konfigurowanie procesów zatwierdzania publikowanych stron i dokumentów. Możliwość odrębnej konfiguracji w poszczególnych częściach portalu tj. definiowanie różnych edytorów i recenzentów w ramach różnych obszarów intranetu.
   g) Statystyki odwiedzin poszczególnych części i stron intranetu – analiza liczby odsłon w czasie. Opcjonalnie zaawansowane statystyki i analizy.
   h) Funkcjonalności wspierające pracę grupową - do wykorzystania na najniższym poziomie intranetu do celów pracy działów i zespołów zadaniowych. Funkcjonalności wspierające gromadzenie dokumentów, wsparcie komunikacji, planowanie zadań i wydarzeń
   i) Funkcjonalność publikowania na portalu formularzy elektronicznych XML i przetwarzanych na aplikację webową dostępną dla użytkowników przez przeglądarkę Internetową. Dane z wypełnionego formularza mają być zapisywane w formacie XML zgodnie z definicją formularza.
   j) Mechanizmy wspierające przepływy pracy (workflow) wraz z funkcjonalnością definiowania procesów obiegu dokumentów, integracji przepływów z web-services, wywoływania web-services z poziomu workwlow bez konieczności kodowania przy wykorzystaniu prostych w obsłudze narzędzi portalu.

3.7. Podłączenie do serwera OCSIP

Podłączenie każdego Użytkownika końcowego Zamawiającego w ramach Usługi podstawowej i Usług dodatkowych do serwera OCS.

3.8. Zestawienie bezpiecznego połączenia VPN

Zestawienie i uruchomienie dla każdego Użytkownika końcowego Zamawiającego w ramach Usługi podstawowej i Usług dodatkowych bezpiecznego połączenia VPN i zestawienie komunikacji, umożliwiającej realizację pracy zdalnej.

3.9. System uprawnień AD

Dostawa, wdrożenie i utrzymanie usługi systemu uprawnień typu Active Directory dla każdego Użytkownika końcowego Zamawiającego w ramach Usługi podstawowej i Usług dodatkowych.

Tabela nr 10. Wymagania AD.

1) System równoważny do Active Directory musi spełniać następujące wymagania: a) umożliwia scentralizowane zarządzanie obiektami (serwery, drukarki czy udostępnione pliki), a także przypisywanie uprawnień do tychże zasobów, b) umożliwiająca uwierzytelnienie obiektów (np. użytkowników, komputerów) i autoryzacja (lub jej odmowa) dostępu do innych obiektów (dowolnych, np. kontenera lub obiektu użytkownika) oraz do zasobów innych, w tym dyskowych, sieciowych oraz aplikacji, c) umożliwia konfigurację obiektów,

d) możliwość działania w rozproszonych sieciach,
e) możliwość działania w środowisku Microsoft Windows Server,
f) możliwość konfiguracji za pomocą narzędzi graficznych i z linii komend,
g) możliwość tworzenia skryptów,
h) aktywne wsparcie protokołu LDAP (Lightweight Directory Access Protocol).

2) Obiekty:
a) Konto użytkownika – obiekt zawierający informacje o użytkowniku,
b) Kontakt – obiekt zawierający informacje kontaktowe użytkowników,
c) Komputer – obiekt zawierający informacje o komputerze,
d) Drukarka – obiekt zawierający odniesienie (wskaźnik) do drukarek sieciowych,
e) Udział sieciowy – obiekt zawierający odniesienie do udostępnionych folderów w sieci,
f) Grupa – obiekt zawierający kolekcję innych obiektów, stosowany do zarządzania uprawnieniami,
g) Jednostka organizacyjna – obiekt administracyjny obejmujący inne obiekty, stasowany do zarządzania konfiguracją,
h) Domena – podstawowa struktura systemu, w ramach której zdefiniowane są pozostałe obiekty,
i) Kontroler Domeny – obiekt zawierający informację o serwerze pełniącym funkcję kontrolera domeny,
j) Lokalizacja (Site) – obiekt zawierający informację o podsieciach w danej lokalizacji,
k) Builtin – grupy o predefiniowanych uprawnieniach do wykonywania czynności administracyjnych,
l) Relacja zaufania – obiekt zawierający informację o relacjach zaufania pomiędzy domenami.

4. Łącza internetowe

1. Łącza do sieci publicznej (Internet)
   Przepustowość symetrycznego łącza, zapewnionego w ramach realizacji Usługi, musi być nie mniejsza niż 1 Gbps. Łącze musi posiadać ochronę przed atakami DDoS.

2. Łącze światłowodowe
   Wykonawca zapewni dedykowane łącze światłowodowe z CPD do siedziby Zamawiającego wraz z niezbędnymi urządzeniami aktywnymi. Przesyłanie danych będzie odbywać się poza siecią publiczną. W ramach realizacji usługi zamawiający zestawi połącznie pomiędzy serwerem plików a siedzibą Zamawiającego.

5. Usługi dodatkowe

Usługa dodatkowa ma charakter Prawa Opcji. Oznacza to, że Zamawiający ma prawo złożyć zamówienie na te usługi lecz nie ma takiego obowiązku. W przypadku nie skorzystania przez Zamawiającego z Usług dodatkowych Wykonawcy nie będzie przysługiwało roszczenie o ich wykonanie jaki żadne roszczenie finansowe. W przypadku skorzystania z Usług dodatkowych Wykonawca otrzyma wynagrodzenie odpowiadające iloczynowi ceny jednostkowej określonej w Ofercie dla każdej Usługi dodatkowej i liczby usług faktycznie zrealizowanych.

5.1. Ochrona antywirusowa zgodnie z parametrami w pkt. 3.5. OPZ – maksymalnie dodatkowo 30 nowych stacji roboczych.

5.2. Poczta email i pakiet aplikacji biurowych zgodnie z parametrami w pkt. 3.6. OPZ - maksymalnie dodatkowo 30 nowych kont pocztowych.

6. Usługa typu helpdesk

Wymagany zakres wparcia:

1. świadczenie usługi 1 linii wsparcia w godzinach 8:00-16:00 w dni robocze z czasem reakcji na zgłoszenie do 1 godziny oraz faktyczne usunięcie zgłoszonych usterek w terminie do 6 godzin roboczych, a w przypadku braku możliwości fizycznego usunięcia usterki we wskazanym terminie - ustalenie z Zamawiającym innego terminu na usunięcie niesprawności (np. w razie konieczności wymiany/zamówienia nowego sprzętu); przyjmowanie zgłoszeń od użytkowników i ich obsługa w ramach zakresu realizowanych prac helpdesk;
3. przyjmowanie zgłoszeń od użytkowników i ich przekazywanie do firm trzecich w zakresie prac realizowanych przez te firmy, a wykraczającym poza zakres realizowanych prac helpdesk;
4. prowadzenie ewidencji zgłoszeń wraz z ich statusem i ewidencją czasu reakcji oraz realizacji;
5. instalacja, konserwacja, konfiguracja i administracja stacjami roboczymi stacjonarnymi i mobilnymi oraz urządzeniami biurowymi (drukarki, skanery, projektory, UPS biurowe)/ w tym możliwość zdanego wykonania tych prac na stacjach roboczych Zamawiającego;
6. wsparcie użytkowników w zakresie instalacji oraz konfiguracji oprogramowania na stacjach roboczych użytkowników końcowych;
7. pomoc użytkownikom końcowym w zakresie obsługi systemów i oprogramowania (dopuszczalna/zalecana forma w postaci zdalnej konfiguracji z użyciem dedykowanego, zabezpieczonego łącza VPN);
8. koordynacja napraw sprzętu komputerowego oraz biurowego w zakresie obsługiwanym w ramach helpdesk;
9. realizacja podłączeń sieciowych urządzeń końcowych do wskazanego urządzenia sieciowego w ramach punktu dystrybucji sieci;
10. techniczne wsparcie wykorzystania urządzeń audiowizualnych i systemów komputerowych;
11. prowadzenie inwentaryzacji urządzeń końcowych oraz biurowych wraz z oprogramowaniem.
12. naprawy, wymiany gniazd komputerowych RJ 45, naprawa i instalacja okablowania sieciowego, wymiana przewodów sieciowych łączących laptopy, komputery PC z siecią (gniazdo RJ 45). Koszty materiałów ponosi Zamawiający.
13. wsparcie przy sporządzaniu dokumentacji (OPZ) dotyczącej zakupów nowych stacji roboczych stacjonarnych i mobilnych oraz urządzeń biurowych (drukarki, skanery, projektory, UPS biurowe); określenie parametrów sprzętu do OPZ oraz weryfikacja zgodności parametrów sprzętu zaproponowanego w ofertach i przy odbiorze. Powyższe zakupy mogą być dokonywane w oparciu o przepisy ustawy Prawo zamówień publicznych i w związku z tym Wykonawca zapewni w tym zakresie personel posiadający wiedzę i doświadczenie w stosowaniu ww. ustawy i wytycznych w zakresie kwalifikowalności.

7. Zamówienia podobne na podstawie art. 214 ust. 1 pkt 7 ustawy pzp.

Zamawiający przewiduje udzielanie zamówienia, o którym mowa w art. 214 ust. 1 pkt 7 ustawy pzp. Zamawiający przewiduje możliwość udzielenia wybranemu wykonawcy zamówienia podobnego do 20% wartości zamówienia podstawowego (Usługa podstawowa + Usługa dodatkowa). Zamówienie może być udzielone w terminie 3 lat od zawarcia umowy o zamówienie podstawowe. Przedmiotem zamówienia uzupełniającego mogą być wszystkie usługi będące przedmiotem zamówienia podstawowego lub tylko niektóre z nich, z możliwością zmian ilości, realizowane w zakresie i na warunkach zamówienia podstawowego. Umowa o zamówienie podobne będzie udzielona na warunkach określonych we wzorze umowy dla zamówienia podstawowego.

8. Obowiązek zatrudnienia na podstawie stosunku pracy

Zamawiający wymaga zatrudnienia przez Wykonawcę, jak i podwykonawcę, na podstawie stosunku pracy osób wykonujących w zakresie realizacji zamówienia czynności polegające na wykonywaniu pracy w sposób określony w art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy (t.j. Dz.U. z 2018r. poz. 917 z późń. zm.), tj. osób wykonujących następujące czynności:

a) opracowywanie założeń i architektury systemów informatycznych,

b) administrowanie urządzeniami sieciowymi,

c) administrowanie serwerami w środowisku wirtualnym,

d) administrowanie systemami operacyjnymi.

Sposób dokumentowania zatrudniania osób, o których mowa powyżej, uprawnienia Zamawiającego w zakresie kontroli spełniania przez Wykonawcę wymagań z tytułu zatrudnienia na podstawie stosunku pracy oraz sankcje z tytułu niespełnienia tych wymagań zostały określone w załączniku do SIWZ - "Wzór umowy".