Załącznik nr 1 do SWZ

Opis Przedmiotu Zamówienia (OPZ)

Realizacja usługi Security Operations Center w zakresie cyberbezpieczeństwa wraz z zapleczem teleinformatycznym w modelu usługowym.

Tryb postępowania:

Postępowanie o udzielenie zamówienia prowadzone jest w trybie przetargu nieograniczonego, o którym mowa w art. 132 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych, zwanej dalej „ustawą Pzp".

CPV

72220000-3 Usługi doradcze w zakresie systemów i doradztwo techniczne

72240000-9 Usługi analizy systemu i programowania

72254100-1 Usługi w zakresie testowania systemu

72265000-0 Usługi konfiguracji oprogramowania

72320000-4 Usługi bazy danych

72611000-6 Usługi w zakresie wsparcia technicznego

72317000-0 Usługi przechowywania danych

Zamówienie realizowane jest zgodnie z poniższymi przepisami i Dyrektywami PE i Rady UE

1) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).
2) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L Nr.119).
3) Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr. 159, poz. 948).
4) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz. U. 2006 Nr. 206 poz. 1518).
5) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE z dnia 27.04.2016r.(Dz. Urz. UE. L Nr 119) RODO. Ustawa z dnia 10.05.2018r. o ochronie danych osobowych (Dz. U. z 2018r.poz.1000).
6) Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. Nr. 128, poz. 1402, z późn. zm.).

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
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	Kopia zapasowa 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.
SOC	Security Operations Center – element organizacyjny realizujący operacje związane z zapewnieniem bezpieczeństwa systemów teleinformatycznych.
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	Kujawsko-Pomorski Fundusz Pożyczkowy sp. z o.o. ul. Sienkiewicza 38, 87-100 Toruń

2. Przedmiot zamówienia

Przedmiotem zamówienia jest kompleksowa usługa w zakresie cyberbezpieczeństwa wraz z zapewnienia dostępu do bezpiecznej i wysokodostępnej infrastruktury teleinformatycznej w modelu usługowym wraz z usługami uzupełniającymi, zwana dalej Usługą. Usługa składa się z Usługi Podstawowej i Usług Dodatkowych.

2.1 W ramach Usługi Podstawowej Wykonawca zobowiązuje się:

1) świadczyć przez cały okres trwania umowy usługę SOC w zakresie cyberbezpieczeństwa, mającą na celu ochronę przed cyberzagrożeniami;
2) udostępnić na czas realizacji umowy 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;

3) 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;

4) zapewnić na czas realizacji umowy usługę kopii zapasowej udostępnionej infrastruktury teleinformatycznej zgodnie z określonymi przez Zamawiającego wymaganiami w terminie do 10 dni roboczych od dnia podpisania umowy;

5) zapewnić na czas realizacji umowy dostęp do aplikacji biurowych wraz z pocztą email i jej uruchomieniem w terminie do 10 dni roboczych od dnia podpisania Umowy oraz przeprowadzić migrację z obecnie wykorzystywanego systemu poczty email;

6) zapewnić na czas realizacji umowy usługę AD wraz z obsługą dla wszystkich Użytkowników w terminie do 10 dni roboczych od dnia podpisania umowy;

7) zapewnić na czas realizacji umowy łącza internetowe w terminie do 10 dni roboczych od podpisania umowy.

2.2. W ramach Usług Dodatkowych Wykonawca zobowiązuje się:

Na każdorazowe wezwanie Zamawiającego w trybie następnego dnia roboczego dostarczyć Usługi Dodatkowe wymienione w pkt. 2.1. 5), 6), 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. Security Operations Center

1. Z uwagi na potrzebę ochrony przed cyberzagrożeniami Zamawiający oczekuję realizacji usługi SOC. Usługa musi być realizowana w oparciu o narzędzia i systemy teleinformatyczne funkcjonujące w ramach infrastruktury CPD spełniającej wymogi określone dla CPD w pkt. 3.2. Usługa SOC musi zawierać poniższe elementy do realizacji:
    a) Audyt bezpieczeństwa infrastruktury IT w siedzibie głównej Zamawiającego – wykonanie 2 audytów w okresie trwania umowy, w terminie uzgodnionym z Zamawiający. Zakres audytu musi obejmować:
        a. przeprowadzenie weryfikacji oraz identyfikacji całej infrastruktury lokalnej w celu określenia wszelkich usług oraz oprogramowania wykorzystywanych w sieci lokalnej;
        b. weryfikację sposobu segmentacji sieci lokalnej oraz ruchu w celu weryfikacji czy poufne dane są przesyłane w odpowiedni sposób, np. z wykorzystaniem szyfrowania;
        c. przeprowadzenie analizy wykorzystywanego oprogramowania oraz sprzętu w infrastrukturze pod kątem aktualności zabezpieczeń oraz luk bezpieczeństwa;
        d. przeprowadzenie weryfikacji testowego, kontrolowanego wykorzystania znanych podatności w oprogramowaniu oraz usługach;
        e. identyfikację mechanizmów uwierzytelniania stosowanego w sieci lokalnej, które zostaną następnie poddane weryfikacji, w szczególności weryfikacji czy nie są wykorzystywane słabe hasła lub też domyślne ustawione poświadczenia przez producenta sprzętu;
        f. przeprowadzenie weryfikacji stosowania zasad bezpieczeństwa na wybranych stacjach roboczych użytkowników;
        g. wykonanie dokumentacji zidentyfikowanych podatności oraz przedstawienie rekomendacji w raporcie końcowym;
        h. wszystkie testy mogą być wykonane za pomocą technik manualnych lub z wykorzystaniem automatycznych narzędzi do odnajdywania luk w zabezpieczeniach.

b) Audyt bezpieczeństwa sieci bezprzewodowych w siedzibie głównej Zamawiającego – wykonanie 2 audytów w okresie trwania umowy, w terminie uzgodnionym z Zamawiający. Zakres audytu musi obejmować:

   a. identyfikację wszystkich sieci bezprzewodowych w infrastrukturze;

   b. identyfikację standardów szyfrowania wykorzystywanych sieci bezprzewodowych;

   c. przeprowadzenie weryfikacji oraz próbę przełamania zidentyfikowanych zabezpieczeń;

   d. wykonanie analizy w kontekście izolacji sieci bezprzewodowej od zasobów wewnętrznych;

   e. wykonanie dokumentacji zidentyfikowanych podatności oraz przedstawienie rekomendacji w raporcie końcowym;

   f. wszystkie testy mogą być wykonane za pomocą technik manualnych lub z wykorzystaniem automatycznych narzędzi do odnajdywania luk w zabezpieczeniach.

c) Testy socjotechniczne – wykonanie 2 testów w okresie trwania umowy, w terminie uzgodnionym z Zamawiający. Zakres testu musi obejmować:

   a. wykonanie pełnej identyfikacji adresów e-mail pracowników organizacji;

   b. zarejestrowanie fałszywych domen internetowych;

   c. stworzenie stron internetowych, mając imitować strony produkcyjne Zamawiającego;

   d. wysyłkę wiadomości mailowych nakłaniających użytkowników do kliknięcia w złośliwy odnośnik lub też otwarcie załącznika wiadomości;

   e. wykonanie dokumentacji interakcji pracowników oraz wykorzystywanych przez nich haseł, co pozwoli zidentyfikować zachowanie użytkowników w przedmiotowych, testowanych sytuacjach;

   f. zaproponowanie działań zapobiegawczych w celu ograniczenia zidentyfikowanego ryzyka;

   g. testy mogą być wykonane za pomocą technik manualnych lub z wykorzystaniem automatycznych narzędzi do tworzenia kampanii socjotechnicznych

   h. po wykonaniu testu Wykonawca sporządzi i dostarczy raport, w którym zostaną udokumentowane interakcje pracowników, siła stosowanych haseł, zestawienia statystyczne oraz działania zapobiegawcze w celu ograniczenia zidentyfikowanego ryzyka.

d) Skanowanie infrastruktury wewnętrznej pod kątem podatności – usługa ma być realizowana w trybie ciągłym w trakcie trwania umowy. Usługa ma na celu wykrywanie podatności z wykorzystaniem trybów skanowania:

   a. skanowania sieciowego – identyfikacja otwartych portów, działających usług, analiza możliwych podatności, weryfikacja usług wykorzystujących domyślne poświadczenia.

   b. skanowania z poświadczeniami – poprzez przekazanie poświadczeń do wewnętrznych systemów skaner musi przeprowadzić czynności identyfikujące wewnętrzne podatności bezpieczeństwa, możliwe do ujawnienia tylko z poziomu zaufanego pracownika (koncepcja zero trust).

      Wykonywanie skanowania wewnętrznej infrastruktury musi być realizowane pod kątem zgodności z wymaganiami i normami bezpieczeństwa. Wykonawca będzie dostarczał Zamawiającemu raportu na żądanie, nie częściej niż raz na kwartał, w którym zostaną przedstawione udokumentowane, zidentyfikowane podatności. W przypadku wykrycia podatności przez Wykonawcę, Zamawiający jest niezwłocznie informowany o zaistniałym fakcie oraz otrzymuje rekomendacje bezpieczeństwa.

e) Analiza infrastruktury zewnętrznej pod kątem luk bezpieczeństwa – usługa ma być realizowana w trybie ciągłym w trakcie trwania umowy. Usługa ma na celu realizację stałego monitoringu infrastruktury zewnętrznej pod kątem:

   a. usług związanych z przemysłowymi systemami sterowania,

   b. wykonywania skanowania zewnętrznych usług sieciowych,

   c. usług powiązanych z urządzeniami Internetu Rzeczy,

d. naruszonych usług związanych ze złośliwym oprogramowaniem,

e. nowo otwartych portów oraz usług,

f. usług baz danych, która nie wymagają uwierzytelniania,

g. usług używających wygasłego certyfikatu ssl,

h. usług, które nie powinny być dostępnie publiczne,

i. usług posiadających zidentyfikowane podatności.

Wykonawca będzie dostarczał Zamawiającemu raportu na żądanie, nie częściej niż raz na kwartał, w którym zostaną przedstawione udokumentowane, zidentyfikowane podatności. W przypadku wykrycia podatności przez Wykonawcę, Zamawiający jest niezwłocznie informowany o zaistniałym fakcie oraz otrzymuje rekomendacje bezpieczeństwa.

2. Z uwagi na potrzebę ochrony przed cyberzagrożeniami Zamawiający oczekuję w terminie do 10 dni roboczych od podpisania umowy wdrożenia ochrony antywirusowej dla 80 szt. stacji roboczych. Wymagania dla ochrony antywirusowej:

a) Obsługa systemu operacyjnego Windows 10 i nowsze;

b) Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

c) Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim.

d) Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.

e) Wbudowana technologia do ochrony przed rootkitami.

f) Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

g) Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".

h) Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.

i) Możliwość skanowania dysków sieciowych i dysków przenośnych.

j) Skanowanie plików spakowanych i skompresowanych.

k) Możliwość umieszczenia na liście wykluczenia ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach i procesów.

l) Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.

m) 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).

n) Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.

o) Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.

p) Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator.

q) Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.

r) Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.

s) Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.

t) Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.

u) 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.

v) 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.

w) Możliwość pobrania płyty ratunkowej, do uruchomienia z niej komputera i przeskanowania dysków umieszczonych w komputerze.

x) System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.

y) System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien pracować w trybie graficznym.

z) Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.

aa) Praca programu musi być niezauważalna dla użytkownika.

bb) Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.

cc) Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.

dd) Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.

ee) Możliwość odblokowania ustawień programu po wpisaniu hasła

ff) Posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu modułu Super użytkownika

gg) 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)

hh) Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, z bazy danych urządzeń podłączanych przez użytkowników do komputerów.

ii) Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.

jj) Funkcja Ochrony danych konfigurowana zdalnie przez administratora.

kk) Jedna wersja instalacyjna na stacje robocze i serwery plików.

ll) Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.

mm) Możliwość zainstalowania silnika pełnego, lekkiego z sprawdzaniem reputacji plików w chmurze, lub skanowanie przez centralny serwer bezpieczeństwa.

nn) Możliwość tworzenia list sieci zaufanych.

oo) Możliwość dezaktywacji funkcji zapory sieciowej.

pp) Możliwość ochrony systemu bez instalacji na stacji roboczej silnika antywirusowego. Jego role przejmuje centralny serwer bezpieczeństwa odpowiedzialny za proces skanowania plików;

qq) Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.

rr) Dodatkowy moduł ochrony przeciwko zagrożeniom typu ransomware.

3.2. Infrastruktura teleinformatyczna CPD

1) Z uwagi na potrzebę wysokiej dostępności infrastruktury teleinformatycznej CPD na potrzeby świadczonych usług, 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 wiarygodnego udokumentowania przez Wykonawcę spełniania każdego z wymogów określonych w OPZ w punkcie 5 poniżej. Wymogi CPD muszą być spełnione przez cały okres trwania umowy.
2) Zamawiający oczekuje, że CPD posiada odpowiednie zabezpieczenia fizyczne i organizacyjne zapewniające m.in. bezpieczeństwo przetwarzanych danych Zamawiającego. Wykonawca ponosi odpowiedzialność w zakresie bezpieczeństwa informacji i danych przechowywanych na wykorzystanej infrastrukturze teleinformatycznej CPD.
3) Zamawiający oczekuje, że CPD posiadają wysokie bezpieczeństwo sprzętu teleinformatycznego w postaci:
    a. izolacji sprzętu krytycznego (dedykowana przestrzeń wyłącznie dla urządzeń serwerowych),
    b. ochrony przed uszkodzeniem infrastruktury serwerowej w postaci zamykanych szaf rack,
    c. prowadzenia rejestru wejść i wyjść do obszaru, w którym umieszczony jest sprzęt przeznaczony do obsługi Zamawiającego,
    d. ochrony przed dostępem dla osób nieupoważnionych w trybie 24/7.
4) Zamawiający oczekuje, że CPD zapewnia profesjonalne utrzymanie i konserwację wykorzystywanej infrastruktury, w postaci m.in:
    a. posiadania i stosowania procedury kontroli, regularnych przeglądów zgodnie z zaleceniami producentów, konserwacji i naprawy sprzętu teleinformatycznego, energetycznego i klimatyzacyjnego,
    b. napraw dokonywanych przez personel posiadający kwalifikacje zgodnie z zaleceniami producenta sprzętu i wewnętrznymi procedurami lub autoryzowane serwisy zewnętrzne,
    c. usuwaniem nośników danych ze sprzętu teleinformatycznego przed przekazaniem do naprawy lub serwisu,
    d. stosowania bezpiecznej utylizacji lub przekazywania sprzętu do ponownego użycia, w tym skuteczne usuwanie danych z nośników (wraz z systemami operacyjnymi i danymi licencyjnymi),
    e. ochrony Zamawiającego przed instalacją złośliwego oprogramowania w udostępnionych Zamawiającemu usługach,
    f. prowadzenia aktualnego rejestru: przeglądów, incydentów, awarii i usterek.
5) Zamawiający oczekuje, że CPD musi spełniać poniższe wymagania:

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 500 metrów od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, również od stacji paliw lub składowisk paliw płynnych oraz baz wojskowych.	Zagrożenie powstania sytuacji zagrażających zdrowiu lub życiu osób fizycznie obsługujących urządzenia, 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.	
7	Minimum 100 m oddalenie od linii wysokiego napięcia i elektrowni.	Zagrożenie spowodowania uszkodzeń wynikających z awarii linii wysokiego napięcia, ryzyko wybuchów, ryzyko pożarów. Zagrożenie długotrwałego ograniczenia dostępu do ośrodka wynikającego z wykonywanych napraw.	
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 3,5 m - wysokość mierzona od podłogi technicznej do sufitu	Zagrożenie zachowania odpowiedniej cyrkulacji powietrza, zachowania stref gorącej i zimnej, zmian parametrów środowiskowych.	

11	Wysokość technologiczna podłogi technicznej w pomieszczeniu serwerowni min 1,0 m	Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych.	
12	Spełnienie wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie :budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej.	Przeciwdziałanie zagrożeniom budowlanym, pożarowym lub zagrożeniu życia i zdrowia ludzi w wyniku niezastosowania przepisów BHP, stosowania odrębnych od powszechnie 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 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 99,99%	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 99,99%	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 przez zewnętrzną licencjonowaną firmę.	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	Element zapewnienia wczesnego wykrywania i ostrzegania przed zagrożeniem naruszenia bezpieczeństwa fizycznego obiektu oraz zabezpieczenia materiału dowodowego na wypadek	

	wszystkie wejścia do obiektu – kamery wewnętrzne, monitorowane wszystkie pomieszczenia technologiczne.	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	System SKD dzieli centrum przetwarzania danych wraz z terenem na minimum IV strefy dostępu z zastrzeżeniem, że teren bezpośrednio przyległy do obiektu stanowi strefę I.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po ośrodku.	
7	Dostęp do strefy I (teren obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów).	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	
8	Dostęp do strefy II (część administracyjno-biurowa obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości ze zdjęciem.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	
9	Dostęp do strefy III (strefa technologiczna) możliwy wyłącznie przy użyciu unikalnej i osobistej karty identyfikacyjnej współpracującej z SKD.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.	
10	Dostęp do strefy IV (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.	
11	System gaszenia powinien być bezpieczny dla ludzi i sprzętu komputerowego.	Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia.	
12	Ściany, stropy części technologicznej o odporności	Zapewnienie oporności ogniowej do czasu reakcji służb ratowniczych w celu	

	ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń technologicznych o odporności ogniowej 60 minutowej.	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.	

6) Zamawiający oczekuje uruchomienia infrastruktury teleinformatycznej przez Wykonawcę. Wykonawca zobowiązany jest:
    a. przygotować i udostępnić Zamawiającemu maszyny wirtualne wraz z systemami operacyjnymi i bazodanowymi (wraz z zapewnieniem niezbędnego oprogramowania i/lub licencji na czas trwania Usługi);
    b. zapewnić niezbędne pozostałe oprogramowanie i/lub licencje oraz infrastrukturę teleinformatyczną związane z realizacją Umowy;
    c. skonfigurować połączenia sieciowe pomiędzy poszczególnymi maszynami wirtualnymi;
    d. skonfigurować i udostępnić dedykowane łącza zgodnie z określonymi parametrami;
    e. skonfigurować i udostępnić łącze do sieci Internet, zgodnie z określonymi parametrami;
    f. skonfigurować ochronę na styku z Internetem w warstwie sieciowej i aplikacyjnej;
    g. skonfigurować i udostępnić system Backupu do wykonywania kopii bezpieczeństwa wszystkich serwerów i bazy danych;
    h. skonfigurować i udostępnić system zbierania i przechowania logów zdarzeń z urządzeń styku z siecią Internet;
    i. świadczyć usługę administrowania uruchomionymi maszynami wirtualnymi do poziomu systemu operacyjnego w trybie 24/7/ zgodnie z określonymi parametrami i czasem reakcji.
7) Wykonawca musi udostępniać maszyny wirtualne i serwer plików oraz oprogramowanie systemowe i narzędziowe. 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.
8) 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.

9) Zamawiający oczekuje udostępnienia środowiska chmurowego w modelu IaaS. Zamawiający oczekuje udostępnienia w ramach środowiska chmurowego IaaS puli zasobów wirtualnych wraz z niezbędnym do prawidłowego działania oprogramowaniem systemowym i narzędziowym o parametrach nie gorszych niż określone poniżej i pozwalających wykreować dowolną ilość maszyn wirtualnych w ramach przydzielonej puli zasobów:

a. architektura: x86-64;

b. pamięć podstawowa: 28 GB;

c. procesory: 17 vCPU;

d. system operacyjny: Windows Standard 2019 z możliwością podniesienia do najnowszej wersji lub równoważny dla każdej maszyny wirtualnej;

e. przestrzeń dyskowa S3 Object Storage: 4 TB;

f. przestrzeń dyskowa HDD: 1 TB;

g. przestrzeń dyskowa SSD: 1TB;

h. adres IP: 8x IPv4 adresów użytecznych;

i. łącze do sieci Internet: 1 Gbit/s z ochroną przed atakami DDoS, bez limitu transferu;

j. możliwości samodzielnego zarządzania środowiskiem wirtualnym, w tym powoływanie VM;

k. możliwość zarządzanie brzegiem sieci;

l. możliwość zwiększenia ilości zasobów o min. 40% w ramach dodatkowego zamówienia uzupełniającego;

3.3. Migracja

Wykonawca musi zapewnić bezprzerwową migrację z obecnych serwerów wirtualnych Zamawiającego i ich konfigurację w środowisku Wykonawcy.

3.4. Kopia zapasowa

1. Zamawiający oczekuje aby usługa kopii zapasowej była realizowana w oparciu o CPD, w infrastrukturze CPD.
2. Wykonawca zobowiązany jest wskazać w ofercie lokalizację gromadzonych i przetwarzanych danych będących przedmiotem umowy (adres lokalizacji CPD).
3. Zamawiający z uwagi na ograniczenia ryzyka siły wyższej oraz z uwagi na ograniczenie ryzyka związanego z wydłużonym czasem dojazdu do CPD zastrzega, że odległość pomiędzy siedzibą Zamawiającego (adres siedziby głównej Zamawiającego), a CPD nie może być większa niż 50 km (średni czas dojazdu do 1h). Z uwagi na powyższe, w szczególności w przypadku długotrwałej awarii łącza dostępowego u Zamawiającego, Zamawiający oczekuje dostępu do pomieszczenia biurowego w CPD o powierzchni nie mniejszej niż 21 m^2 wraz z dostępem do 3 stanowisk pracy wyposażonych w bezpośrednie połączenie umożliwiające wydajne połączenie z systemem przechowującym dane.
4. Zakres usługi kopii zapasowej obejmuje 10 szt. serwerów wirtualnych z opcją zwiększenia o 50% w ramach dodatkowego zamówienia uzupełniającego, 1 TB przestrzeni na dane kopii zapasowych. Zamawiający oczekuje, aby wszystkie dane w ramach usługi kopii zapasowej były szyfrowane kluczem szyfrującym o długości co najmniej 4096 bit oraz algorytmem szyfrującym powszechnie uznanym za bezpieczny.

5. Zamawiający oczekuje realizacji harmonogramu retencji danych kopii zapasowych zgodnie z poniższym zestawieniem:
    a. dzienna – 7 dni,
    b. miesięczna – 6 miesięcy,
    c. roczna – 1 rok.
6. Zamawiający oczekuje realizacji wykonywania kopii zapasowych w dni pracujące w oknie w godzinach od 17.00 do 6.00.
7. Zamawiający oczekuje dostarczenia monitoringu usługi kopii zapasowej, który charakteryzuje się następującymi parametrami:
    a. interwały sprawdzania poprawności działania usługi powinny być częstsze niż 5 min,
    b. system musi w czasie rzeczywistym informować o aktualnym stanie kopii zapasowej,
    c. system musi w czasie rzeczywistym raportować o wolnej przestrzeni dyskowej,
    d. system musi w czasie rzeczywistym monitorować wszystkie ustalone z Wykonawcą w trakcie wdrożenia parametry usługi, jak np. czas wykonania kopii zapasowej czy ilość przetworzonych danych (rozmiar).
8. Zamawiający oczekuje dostarczenia rozwiązania, które w sposób automatyczny będzie testowało w sposób jednoznaczny poprawność wykonania kopii zapasowej.
9. Zamawiający oczekuje dostarczenia rozwiązania, które w sposób zautomatyzowany dokona testowego odtworzenia kopii zapasowej i weryfikacji spójności wszystkich odtwarzanych danych.
10. Zamawiający oczekuje możliwości realizacji testowego odtworzenia kopii zapasowej z częstotliwością nie rzadziej niż raz w roku przez Wykonawcę na żądanie Zamawiającego, w środowisku chmury obliczeniowej dostarczonym przez Wykonawcę w ramach niniejszego zamówienia. Wykonawca na żądanie Zamawiającego dostarczy raport z przeprowadzonego odtworzenia.
11. Zamawiający oczekuje realizacji RTO na poziomie 30 min. dla pojedynczej maszyny wirtualnej oraz 24h dla całego środowiska oraz RPO zgodnie z przyjętym harmonogramem.
12. Wykonawca zobligowany jest do dostarczenia usługi, która posiada następujący minimalny zestaw funkcjonalności w ramach dostarczonego rozwiązania:
    a. rozwiązanie musi w pełni obsługiwać maszyny wirtualne oparte o rozwiązanie Vmware,
    b. rozwiązanie musi umożliwiać odtworzenie całej maszyny wirtualnej jak również pojedynczych plików bezpośrednio z kopii zapasowej (bez konieczności przywracania w całości maszyny wirtualnej, aby odzyskać pojedynczy plik), niezależnie od systemu operacyjnego maszyny wirtualnej,
    c. rozwiązanie musi być wyposażone w wewnętrzne mechanizmy kompresji i deduplikacji - wykluczone jest stosowanie narzędzi innych, niż producenta rozwiązania systemu kopii zapasowej,
    d. mechanizm kompresji i deduplikacji musi być dostępny tylko dla danych nie zaszyfrowanych zarówno po stronie systemu operacyjnego maszyn wirtualnych i serwerów fizycznych oraz zaszyfrowanych przez dostarczony system kopii zapasowych,
    e. rozwiązanie musi mieć możliwość pracy z dowolnym typem urządzeń przechowujących dane w dowolnej ilości lokalizacji,
    f. rozwiązanie musi umożliwiać odkładanie kopii danych w różnych lokalizacjach geograficznych i logicznych, przy zachowaniu pełnej funkcjonalności systemu,
    g. rozwiązanie musi umożliwiać pełne uruchomienie maszyny wirtualnej z kopii zapasowej w przypadku awarii oraz równoczesną realizację jej przywracania. Równolegle muszą mieć możliwość działać dwa procesy: (1) proces przywracania maszyny wirtualnej z kopii zapasowej, (2) proces jej poprawnego, pełnego funkcjonowania w trakcie operacji przywracania,

h. rozwiązanie musi umożliwiać przywracanie pojedynczych elementów aplikacyjnych z kopii zapasowych bez konieczności wcześniejszego przywrócenia całej maszyny wirtualnej. Do tych elementów zaliczają się co najmniej: pojedyncze wiadomości email lub pojedyncze wiersze i tabele baz danych.

3.5. Aplikacje biurowe

1) Zamawiający oczekuje dostarczenia aplikacji biurowych i poczty email w ramach pakietów Microsoft MS365 dla 75 użytkowników, w tym:
   a. wersja MS365 Standard dla 25 użytkowników;
   b. wersja MS365 Basic dla 50 użytkowników.

3.6. 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.

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

3.7. Łącza

1) Wykonawca ma obowiązek dostarczyć na potrzeby realizacji przedmiotowej usługi łącza telekomunikacyjne pozwalające na płynne działanie wszystkich systemów i usług umieszczonych w środowiskach teleinformatycznych.
2) Wykonawca zapewni połączenie głównej siedziby zamawiającego z CPD za pomocą technologii światłowodowej z obecną infrastrukturą sprzętową Zamawiającego.
3) Wykonawca zapewni połączenie do sieci Internet za pomocą co najmniej 2 niezależnych operatorów telekomunikacyjnych o zasięgu co najmniej krajowym. Dostępna dla całej dostarczonej infrastruktury przepustowość łącza do Internetu musi wynosić co najmniej 1 Gbit/s (łącze symetryczne) oraz musi umożliwiać rozbudowę przepustowości do wartości co najmniej 10 Gbit/s (łącze symetryczne). Wykonawca do dostarczonego połączenia zapewni ochronę AntiDDoS w pełnym zakresie przepustowości dostarczanego w danym momencie łącza.
4) Wykonawca zapewni ponadto łącza do sieci Internet do oddziałów Zamawiającego, zapewniając odpowiednią przepustowość pozwalającą na możliwość wykorzystania udostępnionych w ramach zamówienia zasobów w tym:
    a. Lokalizacja nr 1, ul. Sienkiewicza 38, 87-100 Toruń, przepustowość min. 100/100 Mbit/s
    b. Lokalizacja nr 2, ul. Przedzamcze 8, 87-100 Toruń, przepustowość min. 20/20 Mbit/s
    c. Lokalizacja nr 3, ul. Gimnazjalna 2a, 85-007 Bydgoszcz, przepustowość min. 20/20 Mbit/s
    d. Lokalizacja nr 4, ul. Jagiellońska 1, 85-067 Bydgoszcz, przepustowość (lokalizację należy objąć nadzorem technicznym)
    e. Lokalizacja nr 5, ul. Toruńska 30, 87-800 Włocławek, przepustowość min. 20/20 Mbit/s
    f. Lokalizacja nr 6, ul. Bechiego 2, 87-800 Włocławek, przepustowość 20/20 Mbit/s
    g. Lokalizacja nr 7, ul. Waryńskiego 4, 86-300 Grudziądz, przepustowość
5) Wykonawca ma obowiązek dostarczyć łącza telekomunikacyjne na czas trwania umowy.

4. Wymogi w zakresie SLA i czasu reakcji

1) Z uwagi na potrzebę wysokiej dostępności usług będących przedmiotem zamówienia wraz z wszystkimi systemami towarzyszącymi, Zamawiający oczekuje, aby rozwiązanie spełniało wysoki poziom SLA zaoferowany przez Wykonawcę tj. gwarancja dostępności usługi nie mniejsza niż 99,90% SLA skali roku.
2) Obsługa utrzymania i zarządzania oferowanego rozwiązania musi być realizowana w trybie 24/7/365.
3) Przyjmowanie zgłoszeń serwisowych musi być realizowane w trybie 24/7/365 w systemie online Wykonawcy, który umożliwia podgląd wszystkich dokonanych zgłoszeń, czas ich realizacji oraz bieżący ich status.
4) Czas reakcji na zgłoszenie musi wynosić nie więcej niż 60 minut.

5. Zobowiązania Wykonawcy

1. Wykonawca udzieli Zamawiającemu pełnej informacji na temat stanu realizacji przedmiotu zamówienia, na każde wezwanie Zamawiającego.
2. Wykonawca zobowiązany będzie współdziałać z osobami wskazanymi przez Zamawiającego.
3. Dostarczane komponenty cyfrowe, w szczególności infrastruktura w modelu chmury obliczeniowej, licencje, realizowane usługi muszą uwzględniać wszystkie wytyczne zawarte w Dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyber bezpieczeństwa na terytorium Unii.
4. Zgodnie z Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 usługi chmurowe powinny obejmować usługi cyfrowe umożliwiające administrowanie na żądanie skalowalnym i

elastycznym zbiorem rozproszonych zasobów obliczeniowych do wspólnego wykorzystania oraz szeroki dostęp zdalny do tego zbioru.

5. Zgodnie z Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 realizowane usługi przez Wykonawcę muszą być zgodne z wytycznymi CSIRT w celu odpowiedniej obsługi wszelkich incydentów, jakie mogą wystąpić na dostarczanych w ramach zamówienia komponentach cyfrowych.
6. Zgodnie z Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 realizowane usługi przez Wykonawcę muszą być zdolne do udostępnienia niezbędnych środków technicznych w celu zapewnienia monitorowania przez CSIRT infrastruktury będącej w posiadaniu lub wykorzystaniu przez Zamawiającego. Wykonawca zobowiązany jest do dostarczenia wszelkich środków technicznych i organizacyjnych do bezwarunkowego zapewnienia monitorowania wszystkich komponentów cyfrowych dostarczonych w ramach zamówienia.
7. Zgodnie z Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 realizowane usługi przez Wykonawcę muszą być zgodne z przyjętą polityką cyberhigieny o której mowa w Dyrektywie, stanowiącą podstawę pozwalającą chronić infrastrukturę sieci i systemów informatycznych, bezpieczeństwo sprzętu, oprogramowania i aplikacji internetowych oraz dane przedsiębiorstw lub użytkowników końcowych wykorzystywanych przez Zamawiającego.
8. Zgodnie z Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 realizowane usługi przez Wykonawcę muszą być zgodne z założeniami Dyrektywy dotyczącymi polityki promowania aktywnej cyberobrony: w przeciwieństwie do działania reaktywnego aktywna cyberobrona polega na aktywnym zapobieganiu naruszeniom bezpieczeństwa sieci, ich wykrywaniu, monitorowaniu, analizowaniu i ograniczaniu, w połączeniu z wykorzystaniem zdolności rozmieszczonych w sieci, która padła ofiarą ataku, i poza tą siecią.
9. Zgodnie z Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 realizowane usługi przez Wykonawcę muszą być zgodne z założeniami Dyrektywy dotyczącymi szybkiego identyfikowania podatności i ich eliminowania. Wykonawca musi zapewnić wszelkie środki techniczne i organizacyjne w celu pełnej realizacji założeń związanych z obsługą podatności, w szczególności rozliczalności, przejrzystości i szybkości ich obsługi w sytuacji wystąpienia w dostarczanych komponentach cyfrowych.
10. Zgodnie z Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 realizowane usługi przez Wykonawcę muszą być zgodne z założeniami Dyrektywy dotyczącymi współpracy w przypadku incydentów i sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę na poziomie Unii, co wymaga przygotowania do uczestnictwa w skoordynowanych działaniach w celu szybkiej i skutecznej reakcji.
11. Zgodnie z Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 realizowane usługi przez Wykonawcę muszą być zgodne z założeniami Dyrektywy dotyczącymi ewentualnej współpracy z EU-CyCLONe w przypadku wystąpienia sytuacji kryzysowych w cyberbezpieczeństwie na dużą skalę.

6. Zobowiązania Zamawiającego

1. Udostępnienie dokumentów, materiałów, danych, dokumentacji i informacji będących w posiadaniu Zamawiającego, niezbędnych do realizacji przedmiotu zamówienia.
2. Udzielanie Wykonawcy na bieżąco niezbędnych do realizacji przedmiotu zamówienia wyjaśnień oraz przekazywania niezbędnych informacji.
3. Zapewnienie, że dostarczone przez Zamawiającego informacje będą prawdziwe i kompletne.
4. Informowanie Wykonawcy o wszelkich czynnościach podejmowanych w związku z realizacją projektu, jeśli będą one miały związek z realizacją przedmiotu zamówienia przez Wykonawcę.
5. Konsultowanie i uzgadnianie wdrażanego systemu zgodnie z wymaganiami OPZ.

7. Asysta techniczna

1. Wykonawca zobowiązany jest do asysty technicznej.

2. Przez asystę techniczną Zamawiający rozumie wszelkie prace i operacje niezbędne do utrzymania w pełni funkcjonującej infrastruktury IT lokalnej w siedzibie głównej Zamawiającego. Do zadań realizowanych przez Wykonawcę w ramach asysty technicznej należeć będzie bieżąca obsługa IT urządzeń końcowych Zamawiającego w zakresie:
    a. instalacji i konfiguracji systemów operacyjnych;
    b. instalacji i konfiguracji elementów niezbędnych do zapewnienia bezpieczeństwa;
    h. aktualizacji oprogramowania ze względu na błędy bezpieczeństwa;
    i. utrzymania infrastruktury pod kątem wydajności, bezpieczeństwa;
    j. analiz incydentów oraz problemów wraz pełnym przywracaniem funkcjonalności.
3. Asysta techniczna będzie realizowana przez cały czas trwania umowy, w dni robocze w godzinach 8.00-16.00. Czas reakcji na zgłoszenie wynosi do 60 minut.

8. Prawo opcji

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. Zakres Usługi dodatkowej obejmuje:

1. Ochrona antywirusowa zgodnie z parametrami w pkt. 3.1., 2) OPZ – maksymalnie dodatkowo 50 nowych stacji roboczych.
2. Poczta email i pakiet aplikacji biurowych zgodnie z parametrami w pkt. 3.5. OPZ - maksymalnie dodatkowo 50 nowych kont pocztowych.