Nr sprawy: BOA.383.1.2026

KUJAWSKO-POMORSKI FUNDUSZ POŻYCZKOWY SP. Z O.O.

ZAPYTANIE OFERTOWE

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

## Załącznik nr 1: Specyfikacja techniczna

### 1. Przedmiot zamówienia

Przedmiotem zamówienia jest realizacja usługi Security Operations Center w zakresie cyberbezpieczeństwa wraz z zapleczem teleinformatycznym w modelu usługowym wraz z usługami uzupełniającymi, zwana dalej Usługą. Usługa składa się z Usługi Podstawowej i Usług Dodatkowych.

### 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

### 2. 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 zapewnieniem dostępu do bezpiecznej i wysokodostępnej infrastruktury teleinformatycznej w modelu usługowym.

### 2.1 W ramach Usługi Wykonawca zobowiązuje się:

1) świadczyć przez cały okres trwania umowy usługę SOC w zakresie cyberbezpieczeństwa, wraz z dostarczeniem i utrzymaniem systemu SIEM na własnej infrastrukturze PaaS.
2) zapewnić na czas realizacji umowy administrowanie usługą AD wraz z obsługą dla wszystkich Użytkowników w terminie do 10 dni roboczych od dnia podpisania umowy;
3) dostarczyć system do realizacji kopii zapasowych dla środowisk Zamawiającego;
4) dostarczyć system antywirusowy dla wskazanych systemów Zamawiającego.

## 3. Szczegółowy opis Usługi

### 3.1. Security Operations Center wraz z ochroną antywirusową,

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. Usługa SOC musi zawierać poniższe elementy do realizacji:
   a) 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.
   b) 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.
   c) Zadania realizowane przez zespół cyberbezpieczeństwa SOC:
      a. monitoring zdarzeń bezpieczeństwa w godzinach 7-19 5 dni w tygodniu
      b. klasyfikację i priorytetyzację alertów bezpieczeństwa,
      c. reakcję na incydenty zgodnie z przyjętymi procedurami,
      d. informowanie klienta o wykrytych zdarzeniach i rekomendowanych działaniach,

e. analizę złożonych incydentów bezpieczeństwa,
f. administrację, utrzymanie i rozwój systemu SIEM,
g. wsparcie w tworzeniu i rozwój procedu i reakcję na incydenty,
h. analizy powłamaniowe (forensic),
i. threat hunting- proaktywne wyszukiwanie zagrożeń,
j. analizę złośliwego oprogramowania,
k. wsparcie przy zgłoszeniu incydentów do S46.

d) Zakres monitoringu:
a. Serwery wirtualne w ilości: do 15,
b. Stacje robocze w ilości: do 100,
c. Urządzenia sieciowe w ilości: do 15,
d. Usługi Microsoft w tym MS 365,
e. W tym pozostałe system zdolne wysłać sys.log

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.

a. ochrony Zamawiającego przed instalacją złośliwego oprogramowania w udostępnionych Zamawiającemu usługach,

b. prowadzenia aktualnego rejestru: przeglądów, incydentów, awarii i usterek.

3. Zamawiający oczekuje dostarczenia sytemu monitoringu dla infrastruktury Zamawiającego z wykorzystaniem systemu SIEM, wdrożonego i utrzymywanego w infrastrukturze Wykonawcy, zgodnie z wymaganiami CPD.

4. Zamawiający oczekuje nadzoru nad infrastrukturą teleinformatyczną przez Wykonawcę. Wykonawca zobowiązany jest:

a. zapewnić niezbędne oprogramowanie i/lub licencje oraz infrastrukturę teleinformatyczną związane z realizacją Usługi,

b. skonfigurować ochronę na styku z Internetem w warstwie sieciowej i aplikacyjnej,

c. skonfigurować bezpieczne połączenie VPN między infrastruktura Zamawiającego a Wykonawcy,

d. skonfigurować i udostępnić repozytorium zbierania i przechowania logów zdarzeń z urządzeń styku z siecią Internet na okres 12 miesięcy.

e. świadczyć usługę administrowania uruchomionymi systemem bezpieczeństwa (SIEM) do poziomu systemu operacyjnego w trybie 24/7/.

f. Zamawiający oczekuje że cały system bezpieczeństwa będzie zabezpieczony kopią zapasową,

g. 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 w CPD w zakresie:

h. instalacji i konfiguracji elementów niezbędnych do zapewnienia środowiska wysokiej dostępności HA;

i. aktualizacji oprogramowania ze względu na błędy bezpieczeństwa;

j. utrzymania infrastruktury pod kątem wydajności, bezpieczeństwa;
k. realizacji bieżących czynności administracyjnych maszyn wirtualnych;
l. analiz incydentów oraz problemów wraz pełnym przywracaniem funkcjonalności.

### 3.2. Kopia zapasowa

1. Zamawiający oczekuje dostarczenia i wdrożenia systemu kopii zapasowej dla wskazanej infrastruktury Zamawiającego. Zamawiający wymaga, aby dane przechowywane była w oparciu , w infrastrukturze CPD.
2. Zakres usługi kopii zapasowej obejmuje 10 szt. serwerów wirtualnych z opcją zwiększenia o 50%, 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. Obecna wielkość kopii zapasowej to 36 TB
3. Zamawiający oczekuje realizacji harmonogramu retencji danych kopii zapasowych zgodnie z poniższym zestawieniem:
    a. dzienna – 7 dni,
    b. miesięczna – 6 miesięcy,
    c. roczna – 1 rok.
4. Zamawiający oczekuje realizacji wykonywania kopii zapasowych w dni pracujące w oknie w godzinach od 17.00 do 6.00.
5. 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).
6. Zamawiający oczekuje dostarczenia rozwiązania, które w sposób automatyczny będzie testowało w sposób jednoznaczny poprawność wykonania kopii zapasowej.
7. Zamawiający oczekuje dostarczenia rozwiązania, które w sposób półautomatyczny dokona testowego odtworzenia kopii zapasowej i weryfikacji spójności wszystkich odtwarzanych danych. Testy mają być wykonywane raz na kwartał lub wezwanie Zamawiającego.
8. Zamawiający oczekuje realizacji RTO na poziomie 30 min. dla pojedynczej maszyny wirtualnej oraz 24h dla całego środowiska oraz RPO zgodnie z przyjętym harmonogramem.
9. 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, Hyper-V.
    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.

### 3.3. 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

## 4. Wymogi w zakresie SLA, czasu reakcji oraz wymagań CPD

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) Wymagania dla reakcji na zdarzenia bezpieczeństwa:

| Klasyfikacja zdarzeń bezpieczeństwa i czas reakcji | | | |
|---|---|---|---|
| 1 | LOW | Niski poziom zagrożenia<br>Czas reakcji do 24h | Potencjalne zagrożenia bez znaczącego wpływu, mogące wymagać monitorowania, ale niekoniecznie natychmiastowej reakcji, charakteryzujące się minimalnymi zakłóceniami w funkcjonowaniu systemu. |
| 2 | MEDIUM | Średni poziom zagrożenia<br>Czas reakcji do 12h | Potencjalne zagrożenia z umiarkowanym wpływem, wymagające średniej pilności w reakcji i konieczność podjęcia działań zaradczych w rozsądnym czasie. |
| 3 | HIGH | Wysoki poziom zagrożenia<br>Czas reakcji do 4h | Konkretne i potencjalnie poważne zagrożenia, wymagające natychmiastowej reakcji i skoordynowanego działania, cechujące się |

| | | | |
|---|---|---|---|
| | | | konieczności szybkiego działania w celu zminimalizowania szkód. |
| 4 | CRITICAL | Krytyczny poziom zagrożenia<br>Czas reakcji do 1h | Krytyczne zagrożenia z potencjalnie katastrofalnymi skutkami, wymagające natychmiastowej, zdecydowanej i kompleksowej reakcji, działające jako najwyższy priorytet,<br>a wszelkie środki zaradcze są wdrożone natychmiast. |

Wymagania CPD w zakresie bezpieczeństwa i parametrów, pozwalające wyeliminować wskazane zagrożenia:

| Parametr | Wyeliminowanie zagrożenia |
|---|---|
| **1. Obiekt i lokalizacja** | |
| CPD zlokalizowane na terenie UE, a wszystkie dane Zamawiającego będą gromadzone i przetwarzane wyłączenie na terenie UE lub Lichtensteinu, Islandii, Norwegii. | Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak spełnienie wymagań RODO / GDPR. |
| CPD posiada ogrodzony zamknięty teren wraz z ograniczoną strefą wejść. | Brak podstawowej kontroli fizycznego dostępu do infrastruktury IT oraz innych urządzeń (elementy zasilania, chłodzenia, wentylacji). |
| CPD jest usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie. | Zagrożenie nieprzerwanej pracy infrastruktury IT oraz innych urządzeń (elementy zasilania, chłodzenia, wentylacji) w wyniku działań działania sił natury. |
| CPD jest położony nie mniej niż 5 metrów powyżej poziomu wody stuletniej | Zagrożenie długotrwałego zalania. Wysoka intensywność oddziaływania sytuacji krytycznych. |
| CPD jest oddalony nie mniej niż 1 km 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). Zagrożenie fizycznego uszkodzenia infrastruktury IT oraz innych urządzeń wskutek eksplozji zewnętrznej. |
| CPD jest oddalony nie mniej niż 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, | Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko |

| | |
|---|---|
| centra handlowe, miejsca organizacji imprez masowych dla 10 tys. osób i więcej). | niekontrolowanego zachowania tłumów, ryzyko zamieszek, zniszczeń. |
| CPD nie posiada ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z urządzeniami serwerowymi. | Zagrożenie przecieków, zalania infrastruktury IT lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności). |
| CPD posiada nie mniej niż 15 metrów oddalenia urządzeń serwerowych udostępnionych Zamawiającemu od źródeł pól zakłócających takich jak transformatory SN i WN. | Zagrożenie uszkodzenia urządzeń i danych w wyniku niekorzystnego oddziaływania półzakłócających pracę urządzeń elektrycznych i magnetycznych. |
| CPD posiada podłogę techniczną w pomieszczeniu z serwerami. | Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych. |
| CPD spełnienia 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. |
| 2. Węzły telekomunikacyjne | |
| CPD posiada połączenie światłowodowe z niezależnymi operatorami telekomunikacyjnymi, w tym nie mniej niż 2 operatorów o zasięgu krajowym jest podłączonych niezależnymi drogami światłowodowymi. | Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia usług transmisji danych przez operatora zewnętrznego. |
| Dojścia połączeń CPD wykonane są dwoma niezależnymi trasami kablowymi. | Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem. |
| CPD posiada węzeł dostępowy do sieci Internet dopięty do minimum 2 różnych operatorów z zaimplementowanym protokołem BGP oraz ochroną DDoS. | Zapewnienie niezawodności i jakości transmisji danych w ramach sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet. |
| CPD posiada węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,99%. | Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet. |

| | |
|---|---|
| CPD posiada węzeł telekomunikacyjny wyposażony w redundantny system firewall. | Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej. |
| CPD posiada węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci. | Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy. |
| 3. Zasilanie energetyczne | |
| CPD posiada dostępność roczną systemu zasilania energetycznego na poziomie nie niższym niż 99,999% | Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń. |
| CPD posiada nie mniej niż dwie niezależne linie zasilania dostępne dla infrastruktury IT. | Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego przywracania ciągłości zasilania. |
| CPD posiada 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. |
| CPD posiada redundantny system agregatów prądotwórczych. | Zagrożenie braku zachowania zasilania. |
| System zasilaczy awaryjnych UPS w CPD gwarantuje podtrzymanie zasilania urządzeń serwerowych oraz infrastruktury towarzyszącej, przeznaczonej dla Zamawiającego przez przynajmniej 15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się agregatów i ich 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. |
| Agregaty prądotwórcze CPD posiadają 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. |
| 4. Bezpieczeństwo | |

| | |
|---|---|
| CPD jest wyposażone w system sygnalizacji włamania i napadu, system wykrywania wody i zalania. | Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu. |
| CPD posiada ochronę całego obiektu realizowaną przez profesjonalną zewnętrzną licencjonowaną firmę ochrony mienia. Ochrona realizowana jest w trybie 24/7. | Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej. |
| CPD posiada system CCTV, który zapewnia ciągły 24/7 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. |
| System CCTV w CPD powinien zapewnić: rejestrację z zapisem aktualnej daty i godziny, archiwizacja zapisanego materiału przez okres nie krótszy niż 21 dni. | Element zapewniający możliwość określenia chronologii zdarzeń zapisanych w systemie monitorującym oraz odtworzenie zapisu zdarzeń po wykryciu zagrożeń. |
| System SKD (System Kontroli Dostępu) w CPD obejmuje nie mniej niż trzy strefy dostępu. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po terenie i obiekcie. |
| Dostęp do strefy I (teren w otoczeniu obiektu) w CPD podlega identyfikacji na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów) wkraczających na ogrodzony teren w otoczeniu obiektu. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |
| Dostęp do strefy II (strefa technologiczna) w CPD możliwy jest wyłącznie przy użyciu unikalnej i osobistej karty identyfikacyjnej współpracującej z SKD. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |
| Dostęp do strefy III (pomieszczenia ze sprzętem serwerowym Zamawiającego) w CPD możliwy jest wyłącznie przy użyciu łącznie 2 elementów identyfikacji: SKD, | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |

| | |
|---|---|
| osobistej karty identyfikacyjnej, hasła (kodu) lub elementu biometrycznego. | |
| CPD posiada system gaszenia bezpieczny dla ludzi i sprzętu komputerowego oraz serwerowego. | Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia. |
| CPD posiada 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. |
| 5. Monitoring | |
| CPD posiada elektroniczny system przyjmowania zgłoszeń dotyczących awarii dostępny w trybie 24/7. | Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej. |
| CPD posiada stałe i całodobowe 24/7 monitorowanie poprawności pracy infrastruktury 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. |

5. Wymogi w zakresie kompetencji Wykonawcy

Wymagania obligatoryjne:

a) Wymagania dot. posiadania odpowiedni certyfikatów

1. Wdrożona norma ISO 22301 od 5 lat na oferowane usługę będąca przedmiotem zamówienia potwierdzona ważnym certyfikatem.
2. Wdrożona norma ISO 27001 od 5 lat na oferowane usługę będącą przedmiotem zamówienia potwierdzona ważnym certyfikatem
3. Doświadczenie w co najmniej 1 wdrożeniach systemu SIEM wraz z obsługą SOC
4. Doświadczenie w co najmniej 5 wdrożeniach polegających na dostarczeniu rozwiązania dla umiejscowienia kopii zapasowej

b) Wymagania dotyczące zespołu analityków SOC / Pentesterów

Zamawiający wymaga, aby Wykonawca wykazał, że dysponuje ZESPOŁEM, w skład którego wchodzą, w szczególności:
a) KIEROWNIK ZESPOŁU

Zamawiający wymaga, aby osoba pełniąca funkcję Kierownika Zespołu posiadała kwalifikacje audytora wiodącego systemu zarządzania bezpieczeństwem informacji zgodnego z normą ISO/IEC 27001 oraz systemu zarządzania ciągłością działania zgodnego z normą ISO
22301 lub równoważne oraz posiadała co najmniej 2-letnie doświadczenie zawodowe w zakresie zarządzania projektami lub usługami związanymi z cyberbezpieczeństwem, w tym brała udział w realizacji co najmniej jednego projektu obejmującego wdrożenie lub utrzymanie
systemów monitorowania bezpieczeństwa IT (np. SIEM, SOC, systemy analizy zdarzeń);
b) PENTESTER
co najmniej 1 osoba posiadająca:

- doświadczenie w prowadzeniu testów penetracyjnych lub analiz podatności,
- certyfikat OSCP (ang. OffSec Certified Professional) lub GPEN (GIAC Penetration Tester Certification) lub równoważny;

c) INŻYNIER BEZPIECZEŃSTWA
co najmniej 1 osoba posiadająca:

- doświadczenie w projektowaniu lub nadzorze nad bezpieczeństwem systemów IT,
- certyfikat OSDA (ang. OffSec Defense Analyst) lub GIAC Security Operations Certified lub równoważny.

d) ANALITYK BEZPIECZEŃSTWA
co najmniej 5 osób posiadających:

- doświadczenie w monitorowaniu bezpieczeństwa lub analizie zdarzeń (SOC/SIEM),
- certyfikat np. CompTIA Security+ lub BTL1 (ang. Blue Team Level 1) lub równoważny;

e) ARCHITEKT BEZPIECZEŃSTWA
co najmniej 1 osoba posiadająca:

- doświadczenie w projektowaniu lub nadzorze nad bezpieczeństwem systemów IT,
- certyfikat CISSP (ang. Certified Information Systems Security Professional) lub Comptia SecurityX lub równoważny;

f) INŻYNIER SYSTEMU SIEM
co najmniej 2 osoby posiadające

- doświadczenie w zakresie wdrożenia lub utrzymania systemów SIEM,
- certyfikaty inżynierski producenta oferowanego systemu SIEM lub równoważne, potwierdzające kompetencje w zakresie wdrożenia i utrzymania systemów SIEM.

g) Inżynier systemu Kopii zapasowych.
Co najmniej 1 osoba posiadająca certyfikat Inżyniera wdrażanego sytemu kopii zapasowej.

Certyfikaty, o których mowa w pkt a), Wykonawca zobowiązany jest przedłożyć wraz z ofertą, w formie umożliwiającej Zamawiającemu dokonanie oceny spełnienia określonych wymagań.
Wymagania, o których mowa w pkt b), tj. dotyczące wykształcenia, kwalifikacji, doświadczenia zawodowego oraz dysponowania osobami skierowanymi do realizacji zamówienia stanowią wymagania dotyczące potencjału osobowego Wykonawcy i podlegają

weryfikacji przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia oraz na każdym etapie realizacji Umowy.

Zamawiający jest uprawniony, na każdym etapie postępowania o udzielenie zamówienia oraz w okresie realizacji Umowy, do żądania od Wykonawcy dokumentów potwierdzających spełnienie wymagań dotyczących osób skierowanych do realizacji zamówienia, w szczególności dokumentów potwierdzających:

- wykształcenie;
- posiadane kwalifikacje i uprawnienia;
- doświadczenie zawodowe;
- udział w projektach odpowiadających wymaganiom określonym przez Zamawiającego;
- aktualne zatrudnienie, współpracę lub pozostawanie w dyspozycji Wykonawcy osób wskazanych do realizacji zamówienia.

Wykonawca zobowiązany jest zapewnić przez cały okres realizacji Umowy dysponowanie osobami posiadającymi kwalifikacje, doświadczenie i certyfikaty wymagane dla poszczególnych funkcji określonych w niniejszym rozdziale.

Zamawiający jest uprawniony do żądania w każdym czasie, w szczególności w toku realizacji Umowy, przedstawienia dokumentów potwierdzających spełnienie wymagań dotyczących członków zespołu, w tym dokumentów dotyczących ich wykształcenia, doświadczenia, kwalifikacji oraz posiadanych certyfikatów.

W przypadku stwierdzenia, że osoba skierowana do realizacji zamówienia nie spełnia wymaganych warunków lub Wykonawca nie dysponuje wymaganą liczbą osób o określonych kwalifikacjach, Wykonawca zobowiązany jest, w terminie wskazanym przez Zamawiającego, zapewnić osobę spełniającą wymagania określone w niniejszym rozdziale.

Zmiana osób skierowanych do realizacji zamówienia w trakcie realizacji Umowy wymaga zapewnienia przez Wykonawcę osoby posiadającej kwalifikacje, doświadczenie i certyfikaty nie niższe niż wymagane dla osoby zastępowanej.

## 6. 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, 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 cyberbezpieczeństwa 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.

## 7. 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.

## 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 nieskorzystania 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., 3) OPZ – maksymalnie dodatkowo 10 nowych stacji roboczych.
2. Kopia zapasowa zgodnie z parametrami w punkt 3.2 OPZ – maksymalnie dodatkowo 5 nowych urządzeń

## 9. Harmonogram realizacji uruchomienia i świadczenia usługi

1. Rozpoczęcie prac nastąpi z chwilą podpisania Umowy.

2. Uruchomienie przedmiotu zamówienia, o którym mowa w Rozdziale 3, przygotowanie i uruchomienie infrastruktury IaaS wraz z systemem kopii zapasowych musi zostać wykonane w terminie wskazanym w ofercie przez Wykonawcę, ale nie później niż 14 dni kalendarzowych od dnia podpisania Umowy, z tym zastrzeżeniem, że uruchomienie systemu SIEM i monitoringu SOC musi zostać wykonane w terminie wskazanym w ofercie przez Wykonawcę, ale nie później niż 30 dni kalendarzowych od podpisania umowy.

3. Zamawiający w ciągu 7 dni kalendarzowych jest zobowiązany do dokonania odbioru lub zgłoszenia uwag i wyznaczenia terminu na ich usunięcie, po czym przystąpi do ponownego odbioru.

Termin wykonania przedmiotu zamówienia: Wykonawca zobowiązany jest do świadczenia usługi w terminie 12 miesięcy liczonych od dnia obowiązywania niniejszej umowy, tj. od dnia 1 września 2026 r.

.....

Data i podpis (pieczęć/nazwa)