Załącznik nr 9

Załącznik nr 1 do Umowy

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

„Dostawa, wdrożenie, konfiguracja i uruchomienie infrastruktury teleinformatycznej wraz z zabezpieczeniami w obszarze ochrony przed cyberzagrożeniami.”

Spis treści

1 Definicje i skróty ... 3
2 Obowiązujące przepisy prawne i wytyczne ... 4
3 Informacja o projektach ... 4
4 Przedmiot zamówienia ... 5
5 Szczegółowy zakres prac ... 6
5.1 Dostarczenie infrastruktury teleinformatycznej 6
5.2 Dostarczenie rozwiązania kopii zapasowych 8
5.3 Dostarczenie powierzchni kolokacyjnej 10
5.4 Dostarczenie połączeń sieciowych 10
5.5 Zabezpieczenie łańcucha dostaw w obszarze bezpieczeństwa i cyberzagrożeń 12
5.6. Dostawa licencji 21
5.7. Szkolenia wdrożeniowe 21
6. Wymogi w zakresie SLA i czasu reakcji ... 22
7. Wymogi w zakresie świadczenia asysty technicznej ... 22
8. Wdrożenie i odbiór ... 23
8.1. Harmonogram realizacji uruchomienia i świadczenia usługi 23
8.2. Dokumentacja techniczna 23
8.3. Zobowiązania Wykonawcy 23
8.4. Zobowiązania Zamawiającego 24

1 Definicje i skróty

Użyte w niniejszym 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 lub infrastrukturą i odpowiadająca za jego lub jej sprawne działanie oraz posiadająca uprawnienia do części administracyjnych.
Alert Bezpieczeństwa SOC	Alert pojawiający się automatycznie w systemie monitorowania bezpieczeństwem klasy SIEM.
Awaria	Nieplanowane zdarzenie powodujące całkowity brak dostępu do infrastruktury, skutkujące przerwaniem podstawowej jej funkcjonalności.
HA	(High Availability) – Wysoka dostępność - określenie systemu informatycznego o wysokiej niezawodności i dostępności na poziomie nie mniejszym niż SLA 99,9% czasu w skali roku, który nie posiada pojedynczego punktu awarii.
IaaS	(Infrastructure as a Service) – Infrastruktura teleinformatyczna dostarczana w modelu chmury obliczeniowej.
Incydent	Nieplanowane zdarzenie powodujące lub mogące powodować obniżenie jakości infrastruktury np. ograniczone możliwości wprowadzania zmian, edycji lub modyfikacji, ale nie powodujące przerwy w działalności podstawowej jej funkcjonalności.
Incydent Bezpieczeństwa SOC	Zdarzenie, które doprowadziło do naruszenia lub utraty poufności danych, integralności systemów lub wycieku danych.
Ostrzeżenie Bezpieczeństwa SOC	Powiadomienie z innych dostępnych źródeł informacji, które może mieć wpływ na bezpieczeństwo.
PDC	(Primary Data Center) – podstawowy ośrodek przetwarzania danych.
RTO	(Recovery Time Objective) – czas w jakim należy przywrócić procesy po wystąpieniu awarii.
RPO	(Recovery Point Objective) – akceptowalny poziom utraty danych wyrażony w czasie.
SDC	(Secondary Data Center) – zapasowy ośrodek przetwarzania danych.
SIEM	System zarządzania i analizowania informacji z obszaru cyberbezpieczeństwa.
SLA	(Service Level Agreement) – gwarantowanym poziom dostępności w skali roku.
SOAR	System automatyzacji i orkiestracji w zakresie narzędzi z obszaru cyberbezpieczeństwa.
SOC	(Security Operations Center) – zestaw narzędzi teleinformatycznych i procedur zapewniających monitoring zdarzeń wykrywających i przeciwdziałających cyberzagrożeniom.
VM	Maszyna wirtualna.
Zamawiający	Urząd Marszałkowski Województwa Kujawsko-Pomorskiego w Toruniu.
Zdarzenie Bezpieczeństwa SOC	Potwierdzony Alert Bezpieczeństwa, który może prowadzić do zagrożenia bezpieczeństwa informacji, systemów lub sieci.

2 Obowiązujące przepisy prawne i wytyczne

Realizacja przedmiotu zamówienia musi uwzględniać wymagania wymienione w poniżej wskazanych dokumentach. Wykonawca zobowiązany jest do zapoznania się z treścią poniższych dokumentów w celu przygotowania prawidłowej oferty oraz realizacji w sposób prawidłowy przedmiotu zamówienia:

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 27.04.2016 r.(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.).
7. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. z 4.04.2019r. Dz. U. z 2019 poz. 700).

3 Informacja o projektach

1. Realizacja przedmiotu zamówienia współfinansowana jest ze środków Programu Regionalnego Fundusze Europejskie dla Kujaw i Pomorza 2021-2027 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego, w ramach następujących projektów:
   1) „Infostrada Kujaw i Pomorza 3.0” – Projekt zapewni wsparcie gospodarcze i społeczne Województwa Kujawsko-Pomorskiego poprzez podniesienie efektywności działań administracji samorządowej oraz jakości usług publicznych. Ponadto umożliwi dostarczenie spójnej, kompleksowej informacji o przestrzeni dla celu dostępu publicznego (front office) oraz dla celu prowadzonych postępowań administracyjnych (back office). Produkty projektu będą stanowić wsparcie dla urzędników w ramach obsługi klientów na różnych poziomach administracji, a równocześnie umożliwią zwiększenie zakresu usług publicznych dostępnych z poziomu obywatela.
   2) „Kultura w zasięgu 3.0” – Projekt umożliwi poprawę stanu rozwoju technologii informacyjnych w systemie społeczno-gospodarczym województwa poprzez rozwój usług publicznych w zakresie e-kultury. W ramach projektu planuje się przeprowadzenie digitalizacji, udostępnianie oraz wytworzenie cyfrowych kanałów komunikacji z odbiorcami, w celu zapewnienia większej dostępności zasobów dziedzictwa regionalnego i kultury dla obywateli, przedsiębiorstw, organizacji badawczych i instytucji publicznych.
   3) „Kujawsko – Pomorskie e-Zdrowie 3.0” – W ramach projektu planuje się wykorzystanie nowoczesnych technologii informacyjnych poprzez stworzenie infrastruktury technicznej, informatycznej i środowiska umożliwiających wprowadzenie specjalistycznych e-usług medycznych w ochronie zdrowia, co poprawi skuteczność opieki medycznej oraz zapewni łatwiejszy i szybszy dostęp do świadczeń medycznych. W ramach planowanego projektu zostanie wzmocnione działanie jednostek medycznych z terenu województwa kujawsko-pomorskiego poprzez dostarczenie nowoczesnych i efektywnych narzędzi informatycznych w tym rozszerzona zostanie funkcjonalność Regionalnego Repozytorium Danych Medycznych m. in. o moduły telemedycyny, telemonitoringu.
   4) „Generator Wniosków o Dofinansowanie wspomagający rozliczanie projektów w ramach perspektywy 2014-2020”.

2. Celem głównym przedmiotu zamówienia jest dostawa infrastruktury teleinformatycznej w modelu chmury obliczeniowej, umożliwiająca bezpieczną i efektywną realizację projektów informatycznych związanych z rozwojem systemów i aplikacji w obszarze cyfryzacji województwa kujawsko-pomorskiego.
3. Realizacja celów poszczególnych projektów zapewni wsparcie gospodarcze i społeczne rozwoju województwa kujawsko-pomorskiego poprzez podniesienie poziomu bezpieczeństwa przetwarzania i gromadzenia danych cyfrowych, w tym danych osobowych.
4. Mając na uwadze wymagania w zakresie Cyberbezpieczeństwa, a także konieczność uproszczenia i cyfryzacji kontaktów z dostawcą usług (ze względu na ciągły postęp technologiczny oraz konieczność zapewnienia odporności administracji publicznej na kryzysy takie jak pandemia COVID-19), w ramach wszystkich projektów niezbędne jest kontynuowanie przeniesienia kluczowych funkcjonalności do chmury obliczeniowej. W efekcie nastąpi wzmocnienie bezpieczeństwa świadczenia e-usług poprzez budowę oraz modernizację istniejących systemów o zasięgu regionalnym i lokalnym w zakresie Cyberbezpieczeństwa.

4 Przedmiot zamówienia

1. Przedmiotem Zamówienia jest:
   1) Etap I (Dostawa, wdrożenie, konfiguracja i uruchomienie infrastruktury teleinformatycznej wraz z zabezpieczeniami w obszarze ochrony przed cyberzagrożeniami), na który składa się dostawa, wdrożenie, konfiguracja i uruchomienie infrastruktury teleinformatycznej w modelu chmury obliczeniowej wraz z zabezpieczeniami w obszarze ochrony przed cyberzagrożeniami w celu spełnienia przez Zamawiającego wymogów bezpieczeństwa w obszarze łańcucha dostaw oraz realizacja niezbędnych działań uzupełniających, zgodnie z wymaganiami określonymi w dalszej części OPZ, w tym:
      a) realizacja kompleksowego zadania polegającego na dostarczeniu infrastruktury teleinformatycznej w modelu chmury obliczeniowej, w ramach którego zostanie przygotowane i uruchomione środowisko teleinformatyczne IaaS wraz niezbędnym oprogramowaniem i jego dalszą asystą techniczną związaną z prawidłowym funkcjonowaniem na potrzeby systemów i aplikacji Zamawiającego,
      b) realizacja kompleksowego zadania polegającego na dostarczeniu rozwiązania kopii zapasowych, w ramach którego zostanie przygotowane i uruchomione środowisko teleinformatyczne IaaS wraz niezbędnym oprogramowaniem i jego dalszą asystą techniczną związaną z prawidłowym funkcjonowaniem na potrzeby realizacji testowych odtworzeń wykonywanych kopii zapasowych Zamawiającego,
      c) realizacja kompleksowego zadania polegającego na dostarczeniu powierzchni kolokacyjnej na potrzeby kolokowania urządzeń teleinformatycznych Zamawiającego,
      d) realizacja kompleksowego zadania polegającego na zestawieniu i uruchomieniu połączeń sieciowych, które są niezbędne do prawidłowej realizacji zadań, o których mowa w lit. a-c) powyżej,
      e) zapewnienie bezpieczeństwa i ochrony przed cyberzagrożeniami, które są niezbędne do prawidłowej realizacji zadań, o których mowa w lit. a-d) powyżej, w celu spełnienia przez Zamawiającego wymogów bezpieczeństwa w obszarze łańcucha dostaw zgodnie z obowiązującymi przepisami prawnymi i wytycznymi w tym zakresie,
   2) Etap II (Asysta techniczna), na który składa się świadczenie asysty technicznej dla dostarczonych w ramach etapu I zasobów teleinformatycznych oraz realizacja niezbędnych działań uzupełniających, zgodnie z wymaganiami określonymi w dalszej części OPZ, w tym:
      a) zapewnienie doradztwa technicznego,
      b) zapewnienie niezbędnych licencji,
      c) przeprowadzenie szkoleń wdrożeniowych.
2. Realizacja przedmiotu zamówienia, o którym mowa w ust. 1 pkt. 1) lit. a-d) powyżej musi zostać przygotowana technologicznie w sposób umożliwiający zwiększanie ilości poszczególnych komponentów środowiska teleinformatycznego o 50% bez wpływu na ciągłość działania całego środowiska teleinformatycznego dostarczanego w ramach przedmiotu Zamówienia tzn. bez wykonywania przerwy w działaniu i dostępie do środowiska w związku z jego rozbudową lub zwiększeniem.
3. Realizacja przedmiotu zamówienia, o którym mowa w ust. 1 pkt. 1) lit. a-d) powyżej (przygotowanie i uruchomienie infrastruktury IaaS i rozwiązania kopii zapasowych, przekazanie do użytku powierzchni

kolokacyjnej oraz zestawienie połączeń sieciowych) musi zostać wykonana najpóźniej w terminie do 30 dni kalendarzowych od dnia podpisania Umowy.

4. Wykonawca na etapie składania oferty zobowiązany jest dołączyć własną dokumentację, w tym:
   1) szczegółową dokumentację techniczną proponowanego rozwiązania, zawierającą m. in.: schematy planowanego środowiska teleinformatycznego, diagramy, opisy słowne, tabele i zestawienia potrzebne do pełnego zrozumienia prezentowanej prawidłowej koncepcji funkcjonowania infrastruktury teleinformatycznej planowanej do dostarczenia przez Wykonawcę,
   2) plan wyjścia (exit plan) dla przedmiotu zamówienia, o którym mowa w ust. 1 pkt 1) lit. a-c) powyżej, uwzględniający szczegółowy opis działań związanych z postępowaniem z danymi Zamawiającego po zakończeniu Umowy.
5. Wykonawca ponosi pełną odpowiedzialność za wszelkie błędy konfiguracyjne i instalacyjne w infrastrukturze, która jest przedmiotem zamówienia, które spowodują utratę danych z systemów i aplikacji Zamawiającego na etapie migracji z obecnej infrastruktury Zamawiającego do infrastruktury Wykonawcy.

5 Szczegółowy zakres prac

5.1 Dostarczenie infrastruktury teleinformatycznej

1. Wykonawca zobowiązany jest dostarczyć infrastrukturę teleinformatyczną w modelu chmury obliczeniowej wraz z zapewnieniem dostępność HA wszystkich dostarczonych zasobów IaaS na czas trwania Umowy, w tym min.:
   1) zgodnie z bieżącymi potrzebami Zamawiającego konfigurować i utrzymywać instancje serwerowe (w tym VM), gotowe do instalacji własnych aplikacji i systemów Zamawiającego lub podmiotów przez niego wskazanych,
   2) zgodnie z bieżącymi potrzebami Zamawiającego instalować, utrzymywać i aktualizować na instancjach serwerowych (w tym VM) systemy operacyjne (Windows Server, Linux (w tym Kubernetes),
   3) skonfigurować i utrzymywać wewnętrzne połączenia sieciowe pomiędzy poszczególnymi instancjami serwerowymi oraz pozostałymi komponentami,
   4) skonfigurować i udostępnić dedykowane łącza telekomunikacyjne zgodnie z określonymi w OPZ minimalnymi parametrami pozwalającymi w sposób niezakłócony realizować operacje i zadania ze wszystkich instancji serwerowych oraz pozostałych komponentów zlokalizowanych w środowisku teleinformatycznym dostarczonym przez Wykonawcę,
   5) skonfigurować i udostępnić łącza do sieci Internet, zgodnie z określonymi w OPZ minimalnymi parametrami pozwalającymi w sposób niezakłócony realizować operacje i zadania ze wszystkich instancji serwerowych oraz pozostałych komponentów zlokalizowanych w środowisku teleinformatycznym dostarczonym przez Wykonawcę,
   6) skonfigurować i utrzymywać ochronę na styku z Internetem w warstwie sieciowej i aplikacyjnej,
   7) skonfigurować i utrzymywać na każdej instancji serwerowej, na której będzie to wskazane, oprogramowanie antywirusowe, aktualizowane na bieżąco, zarządzane z jednej konsoli administracyjnej, zabezpieczającej przed zagrożeniami należącymi do kategorii zagrożeń wirusowych systemów informatycznych,
   8) udostępnić system zbierania i przechowania logów zdarzeń z urządzeń sieciowych w celu stałego monitorowania wydajności rozwiązania,
   9) świadczyć usługę administrowania uruchomionymi instancjami serwerowymi (w tym VM) do poziomu systemu operacyjnego włącznie (Windows Server, Linux (w tym Kubernetes), zgodnie z wytycznymi i bieżącymi potrzebami Zamawiającego,
   10) zapewnić niezbędne licencje i oprogramowanie związane z realizacją przedmiotu zamówienia,
   11) świadczyć obsługę wsparcia zgodnie z określonymi parametrami wskazanymi w OPZ,
   12) świadczyć asystę techniczną zgodnie z określonymi parametrami wskazanymi w OPZ.
2. Zamawiający oczekuje dostarczenia infrastruktury teleinformatycznej w modelu chmury obliczeniowej z lokalizacji PDC, spełniającej minimalne wymogi bezpieczeństwa opisane w OPZ.
3. Zmawiający oczekuje zapewnienia pełnego wsparcia eksperckiego, merytorycznego i administracyjnego w zakresie realizacji przedmiotu zamówienia, zgodnie z najlepszymi praktykami i zgodnie z najnowszymi wytycznymi branżowymi i technologicznymi w tym zakresie, jak również wytycznymi z audytów

przeprowadzanych przez instytucje zewnętrzne, którym podlega Zamawiający przez cały okres obowiązywania Umowy.

4. Zamawiający oczekuje udostępnienia stałego dostępu do modułu zarządzania środowiskiem wirtualnym chmury obliczeniowej będącej przedmiotem zamówienia, w celu bezpośredniego monitorowania lub weryfikowania jego parametrów.
5. Zamawiający oczekuje instalacji systemów operacyjnych Windows Server lub Linux (w tym Kubernetes) z zapewnieniem ich aktualizacji do najnowszych wersji dla każdej VM w ramach realizowanego przedmiotu zamówienia oraz możliwości samodzielnego stałego monitorowania brzegu sieci infrastruktury teleinformatycznej dla połączeń VM. Szczegółową listę VM wraz z rodzajem wymaganego systemu operacyjnego Zamawiający będzie przekazywał Wykonawcy zgodnie z bieżącym zapotrzebowaniem.
6. Zamawiający oczekuje uruchomienie infrastruktury teleinformatycznej w modelu chmury obliczeniowej wraz z niezbędnym do prawidłowego działania oprogramowaniem systemowym i narzędziowym o parametrach nie gorszych niż określone poniżej i pozwalających wykreować dowolną ilość maszyn wirtualnych (VM) o dowolnych parametrach każda (CPU, RAM, HDD, SSD), w ramach przydzielonej poniżej puli zasobów. Zamawiający zakłada coroczny przyrost zapotrzebowania na przestrzeń storage (SSD, HDD, HDD S3) na poziomie 5%, przez cały okres trwania Umowy. Wymagana pula zasobów na dzień rozpoczęcia Umowy została wskazana poniżej:
   1) procesor CPU w ilości: 1 200 szt.,
   2) pamięć operacyjna RAM w ilości: 3 875 GB,
   3) przestrzeń dyskowa SSD (nie mniej niż 100 000 IOPS) w ilości: 90 TB,
   4) przestrzeń dyskowa HDD (nie mniej niż 1 000 IOPS) w ilości: 280 TB,
   5) przestrzeń dyskowa HDD S3 (z wykorzystaniem protokołu S3) w ilości: 550 TB,
   6) publiczne adresy IPv4 w ilości adresów użytecznych: 256 szt.,
   7) odseparowane sieci vLAN w ilości: dowolna ilość,
   8) powołane maszyny wirtualne wraz z zainstalowanym systemem operacyjnym w ilości: 190 szt., w tym: Windows Server: 55 szt.; Linux: 75 szt.; Kubernetes: 5 środowisk, a w nich łącznie: 60 VM z Linux.
7. W ramach chmury obliczeniowej Wykonawca jest także zobowiązany dostarczyć zasoby infrastruktury teleinformatycznej HA w postaci 4 szt. serwerów dedykowanych z lokalizacji PDC, o parametrach nie gorszych niż wymienione poniżej, w tym:
   1) klaster dwóch sztuk serwerów fizycznych dedykowanych dla bazy danych Oracle, na którym zostanie zainstalowany system wirtualizacyjny Vmware i zmigrowana baza danych z obecnej infrastruktury Zamawiającego, o parametrach technicznych każdego z serwerów fizycznych, nie gorszych niż:
      a) CPU: Intel Xeon Silver 4215R 3.2Ghz 1 szt. lub odpowiednik posiadający nie więcej niż 8 core,
      b) RAM: 64GB RDIMM,
      c) SSD: 960GB SSD SATA 6Gbps 2.5" hot-plug – 2 sztuki,
      d) Kontroler dyskowy: PERC H750 lub równoważny (potrzebny tylko do RAID 1),
      e) Obudowa 1U, szyny montażowe bez menedżera okablowania, pozwalające na pełne wysunięcie serwera z szafy rack, kable zasilające C13/C14,
      f) Zasilanie: podwójne zasilacze, hot-plug,
      g) Licencja na zarządzanie serwerem w wersji advanced,
      h) Sieć ETH: 1Gb Eth – 2 porty,
      i) Sieć FO: 10GbE SFP+ – 2 porty,
      j) Sieć FC: 16Gb FC HBA – 2 porty,
      k) TPM 2.0,
   2) klaster dwóch sztuk serwerów fizycznych dedykowanych dla bazy danych Oracle, na którym zostanie zainstalowany system wirtualizacyjny zgodny z licencjonowaniem Oracle (cpu pining) i zmigrowana baza danych z obecnej infrastruktury Zamawiającego, o parametrach technicznych każdego z serwerów fizycznych, nie gorszych niż:
      a) CPU: Intel Xeon Gold 5222 3.8Ghz 1 szt. lub odpowiednik posiadający nie więcej niż 4 core,
      b) RAM: 64GB RDIMM,
      c) SSD: 960GB SSD SATA 6Gbps 2.5" hot-plug – 2 sztuki,
      d) Kontroler dyskowy: PERC H750 lub równoważny (potrzebny tylko do RAID 1),
      e) Obudowa 1U, szyny montażowe bez menedżera okablowania, pozwalające na pełne wysunięcie serwera z szafy rack, kable zasilające C13/C14,

f) Zasilanie: podwójne zasilacze, hot-plug,
g) Licencja na zarządzanie serwerem w wersji advanced,
h) Sieć ETH: 1Gb Eth – 2 porty,
i) Sieć FO: 10GbE SFP+ – 2 porty,
j) Sieć FC: 16Gb FC HBA – 2 porty,
k) TPM 2.0.

8. Zamawiający oczekuję, że do zadań realizowanych przez Wykonawcę w ramach dostarczonej infrastruktury należeć będzie administracyjna zasobami informatycznymi (instancjami serwerowymi) wraz z nadzorem nad posiadaną przez Zamawiającego infrastrukturą chmurową zlokalizowaną w PDC i SDC, m. in. w zakresie:
   1) utrzymania i aktualizacji całego środowiska,
   2) instalacji i konfiguracji systemów operacyjnych,
   3) instalacji i konfiguracji elementów niezbędnych do zapewnienia środowiska HA,
   4) aktualizacji oprogramowania ze względu na błędy bezpieczeństwa,
   5) utrzymania infrastruktury pod kątem wydajności, bezpieczeństwa,
   6) realizacji bieżących czynności administracyjnych,
   7) przyjmowania zgłoszeń technicznych,
   8) analiz incydentów oraz problemów wraz z pełnym przywracaniem funkcjonalności.

5.2 Dostarczenie rozwiązania kopii zapasowych

1. Zadanie musi obejmować wszystkie VM i serwery fizyczne, będące składnikami środowiska teleinformatycznego Zamawiającego oraz, które Wykonawca dostarczy dodatkowo przez cały okres trwania Umowy w ramach dostarczonych przez Wykonawcę zasobów teleinformatycznych.
2. Zamawiający oczekuje realizacji zadania z infrastruktury teleinformatycznej z lokalizacji PDC spełniającej minimalne wymogi bezpieczeństwa opisane w OPZ, a także częściowo z lokalizacji SDC.
3. Wykonawca zapewni niezbędne licencje i oprogramowanie związane z realizacją zadania.
4. Wykonawca zapewni realizację migracji obecnie posiadanych kopii zapasowych Zamawiającego do infrastruktury Wykonawcy, będącej przedmiotem zamówienia.
5. Zakres realizacji zadania z lokalizacji PDC bez replikacji do lokalizacji SDC obejmuje:
   1) 190 szt. VM (serwerów wirtualnych) z możliwością zwiększenia ilości sztuk w trakcie Umowy,
   2) 370 TB danych cyfrowych z rocznym przyrostem na poziomie 5%,
   3) Zamawiający oczekuje realizacji harmonogramu kopii zapasowych wykonywanych jeden raz dziennie z retencją 7 dni wstecz,
   4) Zamawiający oczekuje dostarczenia rozwiązania, które w sposób zautomatyzowany umożliwi dokonanie na żądnie Zamawiającego odtworzenia kopii zapasowej wybranej VM z PDC i weryfikacji spójności wszystkich odtwarzanych danych. Wszelkie zasoby niezbędne do odtworzenia kopii zapasowej musi zapewnić Wykonawca,
   5) Wykonawca zabezpieczy i dostarczy infrastrukturę IaaS w ramach niniejszego zamówienia na potrzeby wykonania testowego odtworzenia,
   6) Wykonawca będzie realizował pełne wsparcie eksperckie, merytoryczne i administracyjne w zakresie prawidłowego działania systemu kopii zapasowych i zarządzania całością systemu kopii zapasowych, zgodnie z najlepszymi praktykami i zgodnie z najnowszymi wytycznymi w tym zakresie, jak również wytycznymi z audytów przeprowadzanych przez instytucje zewnętrzne, którym podlega Zamawiający przez cały okres realizacji usługi.
6. Zakres realizacji usługi z lokalizacji PDC wraz z replikacją do lokalizacji SDC obejmuje:
   1) 98 szt. VM (serwerów wirtualnych),
   2) 12 szt. serwerów fizycznych,
   3) 175 imiennych kont usługi Microsoft 365,
   4) repozytorium 195 TB w PDC z rocznym przyrostem na poziomie 5%,
   5) repozytorium 195 TB w SDC z rocznym przyrostem na poziomie 5%,
   6) Zamawiający oczekuje dostarczenia i skonfigurowania połączeń sieciowych, umożliwiających wykonywanie kopii zapasowych z lokalizacji wskazanych przez Zamawiającego do PDC oraz wykonywania replikacja z PDC do SDC, zgodnie z wymogami wskazanymi w OPZ,

7) Zamawiający oczekuje uruchomienia i udostępnienia konsoli do samodzielnego zarządzania wykonywanymi kopiami zapasowymi, ich ustawianiami retencji, harmonogramów oraz odtworzeniem wraz z przeszkoleniem osób oddelegowanych przez Zamawiającego do zarządzania konsolą,
8) Zamawiający oczekuje samodzielnej możliwości wykonania testowego odtworzenia z PDC kopii zapasowych wybranych VM na żądanie. Odtworzenie może zostać zrealizowane samodzielnie przez Zamawiającego w dowolnym terminie w czasie trwania Umowy. Wykonawca dostarczy infrastrukturę IaaS w ramach niniejszego zamówienia na potrzeby wykonania testowego odtworzenia o parametrach nie mniejszych niż:
   a) procesor CPU w ilości: 64 szt.,
   b) pamięć operacyjna RAM w ilości: 256 GB,
   c) przestrzeń dyskowa SSD (nie mniej niż 100 000 IOPS) w ilości: 30 TB.

7. Zamawiający oczekuje, aby wszystkie dane były szyfrowane kluczem szyfrującym o długości co najmniej 4096 bit oraz algorytmem szyfrującym powszechnie uznanym za bezpieczny.
8. Zamawiający oczekuje dostarczenia monitoringu, który charakteryzuje się następującymi parametrami:
   1) interwały sprawdzania poprawności działania powinny być częstsze niż 5 min,
   2) system musi w czasie rzeczywistym informować o aktualnym stanie kopii zapasowej,
   3) system musi w czasie rzeczywistym raportować o wolnej przestrzeni dyskowej,
   4) system musi w czasie rzeczywistym monitorować wszystkie ustalone z Wykonawcą w trakcie wdrożenia parametry, jak np. czas wykonania kopii zapasowej czy ilość przetworzonych danych (rozmiar).
9. Zamawiający oczekuje, że w ramach realizacji systemu będzie możliwe osiągniecie RTO na poziomie 1h dla pojedynczej VM oraz RPO 24h dla całego środowiska kopii zapasowych.
10. Wykonawca zobligowany jest do dostarczenia systemu, który posiada następujący minimalny zestaw funkcjonalności w ramach dostarczonego rozwiązania:
    1) rozwiązanie musi w pełni obsługiwać VM oparte o rozwiązanie Oracle oraz Vmware,
    2) rozwiązanie musi umożliwić wykonywanie kopii zapasowej pakietu Microsoft 365, w szczególności Exchange, SharePoint, OneDrive, Teams,
    3) rozwiązanie musi umożliwiać odtworzenie całej VM, jak również pojedynczych plików bezpośrednio z kopii zapasowej (bez konieczności przywracania w całości VM, aby odzyskać pojedynczy plik), niezależnie od systemu operacyjnego maszyny wirtualnej,
    4) rozwiązanie musi być wyposażone w wewnętrzne mechanizmy kompresji i deduplikacji – wykluczone jest stosowanie narzędzi innych, niż producenta rozwiązania systemu kopii zapasowej,
    5) mechanizm kompresji i deduplikacji musi być dostępny tylko dla danych nie zaszyfrowanych zarówno po stronie systemu operacyjnego VM i serwerów fizycznych oraz zaszyfrowanych przez dostarczony system kopii zapasowych,
    6) rozwiązanie musi mieć możliwość pracy z dowolnym typem urządzeń przechowujących dane w dowolnej ilości lokalizacji,
    7) rozwiązanie musi umożliwiać odkładanie kopii danych w różnych lokalizacjach geograficznych i logicznych, przy zachowaniu pełnej funkcjonalności systemu,
    8) rozwiązanie musi umożliwiać pełne uruchomienie VM z kopii zapasowej w przypadku awarii oraz równoczesną realizację jej przywracania. Równolegle muszą mieć możliwość działać dwa procesy: (1) proces przywracania VM z kopii zapasowej, (2) proces jej poprawnego, pełnego funkcjonowania w trakcie operacji przywracania,
    9) rozwiązanie musi umożliwiać przywracanie pojedynczych elementów aplikacyjnych z kopii zapasowych bez konieczności wcześniejszego przywrócenia całej VM. Do tych elementów zaliczają się co najmniej: pojedyncze wiadomości email lub pojedyncze wiersze i tabele baz danych,
    10) rozwiązanie musi być wyposażone w funkcję zaawansowanego monitorowania i raportowania infrastruktury, posiadać inteligentną diagnostykę i możliwość wykorzystywania infrastruktury i planowania mocy obliczeniowej, jak również musi umożliwiać analizę danych pierwotnych i dostosowywanie raportów, w tym tworzenie raportów umożliwiających konsolidowanie danych z wielu raportów w jednym zbiorczym zestawieniu.

5.3 Dostarczenie powierzchni kolokacyjnej

1. Zadanie musi obejmować przygotowanie i przekazanie Zamawiającemu powierzchni (przestrzeni) kolokacyjnej wraz z relokacją infrastruktury sprzętowej Zamawiającego, znajdującej się w Toruniu (87-100 Toruń) dla 11 sztuk urządzeń rack o wielkości 16 U i łącznej mocy znamionowej nie przekraczającej 2600 W.
2. Zadnie musi obejmować wykonanie i utrzymanie połączeń sieciowych opisanych w OPZ.
3. Zadanie musi obejmować dostawę gwarantowanego zasilania w energię elektryczną infrastruktury sprzętowej Zamawiającego.
4. Zadanie musi być realizowane z wykorzystaniem powierzchni kolokacyjnej spełniającej wymogi dla PDC określone w OPZ.
5. Zamawiający w ramach realizacji zadania oczekuje m. in.:
   1) przygotowania i przekazania miejsca kolokacyjnego we własnej szafie rack Wykonawcy, która musi spełniać wymogi bezpieczeństwa dla tego typu przeznaczenia, musi być zamykana na klucz i nie może być współdzielona z innymi urządzeniami, które nie są urządzeniami Zamawiającego,
   2) zaprojektowania rozmieszczenia sprzętu w szafie kolokacyjnej wraz z połączeniami sieciowymi i sporządzeniem dokumentacji połączeń sieciowych,
   3) demontażu i przygotowania infrastruktury sprzętowej Zamawiającego do transportu, wraz z realizacją transportu do miejsca kolokacji Wykonawcy. Zamawiający zastrzega, że Wykonawca zobowiązany będzie do dokonania demontażu, zabezpieczenia, transportu i instalacji infrastruktury sprzętowej Zamawiającego, z tym zastrzeżeniem, że działania te muszą zostać wykonane w godzinach od 20.00 do 6.00 rano dnia następnego (sobota i niedziela) w celu ograniczenia do minimum przerw w ciągłości działania,
   4) świadczenia wsparcia technicznego typu „zdalne ręce" w trybie 24/7/365, obejmującego swym zakresem m. in. restart kolokowanych urządzeń, odczyt informacji, wymianę okablowania z czasem reakcji do 1h od przyjęcia zgłoszenia,
   5) dostępu do przestrzeni kolokacyjnej w trybie 24/7/365 dla osób każdorazowo wskazanych przez Zamawiającego,
   6) monitoringu przestrzeni kolokacyjnej system telewizji przemysłowej CCTV (okres przechowywania nagrań musi wynosić nie mniej niż 28 dni),
   7) systemu kontroli biometrycznej do strefy przestrzeni kolokacyjnej (pomieszczenia kolokacyjnego),
   8) systemu alarmowego wraz z ochroną fizyczną obiektu w trybie 24/7/365 przez licencjonowane służby ochrony osób i mienia,
   9) utrzymania parametrów w przestrzeni kolokacyjne: temperatura powietrza od 15 do 28°C oraz wilgotność powietrza względna od 20 do 80% wraz z przekazywaniem Zamawiającemu raportów z zachowania ww. parametrów na każde jego wezwanie,
   10) automatycznego systemu gaszenia w przestrzeni kolokacyjnej gazem neutralnym dla ludzi np. typu FM 200,
   11) redundantnego systemu zasilania kolokowanej infrastruktury sprzętowej w energię elektryczną, za pomocą dwóch torów zasilających w obrębie jednej szafy rack.
6. Wykonawca ponosi pełną odpowiedzialność materialną za urządzenia Zamawiającego będące przedmiotem kolokacji podczas całego procesu ich relokacji do wartości ich zakupu księgowego.
7. Wykonawca zobowiązany jest dostarczyć opis sposobu autoryzacji osób wskazywanych przez Zamawiającego, które będą miały dostęp do przestrzeni kolokacyjnej, w tym także pozostałych osób trzecich, nie będących pracownikami Wykonawcy, które będą miały dostęp do przestrzeni kolokacyjnej na każdorazowe wskazanie Zamawiającego.
8. Zamawiający oczekuję stałego dobowego monitoringu infrastruktury będącej przedmiotem kolokacji, w trybie 24/7/365 przez zespół pracowników Wykonawcy, który będzie przebywał w obiekcie Wykonawcy na miejscu w trybie 24/7.

5.4 Dostarczenie połączeń sieciowych

1. Wykonawca ma obowiązek dostarczyć na potrzeby zadań, o których mowa w Rozdziale 4, ust. 1 pkt. 1, lit. a) oraz lit. c) połączenia telekomunikacyjne i sieciowe pozwalające na płynne działanie wszystkich systemów i rozwiązań umieszczonych w środowisku teleinformatycznych Wykonawcy, w tym:

1) zapewnić połączenia do sieci Internet za pomocą co najmniej 2 niezależnych operatorów telekomunikacyjnych o zasięgu co najmniej krajowym,
2) dostępna dla całej dostarczonej infrastruktury przepustowość łącza do Internetu musi wynosić co najmniej 4 Gbps (łącze symetryczne) bez limitu transferu przesyłanych danych oraz musi umożliwiać techniczną rozbudowę przepustowości do wartości co najmniej 10 Gbps (łącze symetryczne), bez potrzeby wyłączania na czas wykonania rozszerzenia,
3) zapewnić ochronę 24/7/365 przed atakami DDoS w pełnym zakresie przepustowości dla dostarczanych łącz, o których mowa pkt. 1) powyżej,
4) zapewnić połączenia między VM na interfejsach co najmniej 10G Ethernet. Każdy serwer fizyczny używany do wystawienia zasobów w ramach środowiska teleinformatycznego musi być połączony dwoma niezależnymi drogami, do dwóch niezależnych przełączników sieciowych, co najmniej 1 połączeniem 10G Ethernet na każdej drodze. Połączenia do macierzy dyskowych muszą być zrealizowane na portach co najmniej 16G FC. Każda macierz używana do wystawienia zasobów w ramach środowiska teleinformatycznego musi być połączona dwoma niezależnymi drogami, do dwóch niezależnych przełączników sieciowych FC, co najmniej 2 połączeniami 16G FC. Dostarczona w ten sposób przestrzeń dyskowa musi pochodzić od co najmniej 4 niezależnych macierzy dyskowych opartych w pełni o dyski NVMe (tzw. macierze all-flash),
5) zapewnić połączenia zarządzające serwerami, macierzami oraz innymi urządzeniami fizycznymi służącymi do utrzymania środowiska teleinformatycznego na bazie osobnej sieci fizycznej i osobnych urządzeniach sieciowych na portach co najmniej 1G Ethernet,
6) Zamawiający dysponuje dwoma urządzeniami brzegowymi Fortigate 1100E, przez które musi być zrealizowane połączenie środowiska teleinformatycznego z Internetem, siecią łączy VPN do partnerów których wskaże Zamawiający oraz łączami dedykowanymi punkt-punkt (transmisje danych bez dostępu do Internetu),
7) połączenie środowiska teleinformatycznego z urządzeniami brzegowymi Zamawiającego musi być zrealizowane co najmniej 2 łączami po 10G Ethernet każde, dwoma niezależnymi drogami, na interfejsach co najmniej 10G Ethernet z możliwością rozbudowy do 40G Ethernet za pośrednictwem dwóch niezależnych urządzeń sieciowych,
8) zapewnić dostarczenie, wdrożenie, konfigurację i wsparcie systemu typu WAF (ang. Web Application Firewall) monitorującego i filtrującego ruch do aplikacji i systemów Zmawiającego, które będzie spełniało poniższe wymogi:
    a) minimalny ruch jaki musi gwarantować rozwiązanie to obsłużenie 4000 jednoczesnych połączeń SSL/TLS i ruch o przepustowości zgodnej z wymogami połączeń opisanych w OPZ,
    b) rozwiązanie musi umożliwiać terminowanie połączeń SSL do klienta oraz serwera aplikacji. W celu zmniejszenia czasu odpowiedzi serwera możliwe jest stałe utrzymywanie puli połączeń do serwera aplikacji, które mogą być wykorzystane przez zapytania wysłane przez klienta,
    c) rozwiązanie musi zapewniać tryb, który umożliwia szyfrowanie protokołu HTTP w imieniu serwera aplikacyjnego zamieniając wszystkie zapytania i odpowiedzi HTTP na HTTPS, bez wprowadzania zmian i modyfikacji po stronie aplikacji lub serwera aplikacyjnego,
    d) rozwiązanie musi utrzymywać pewną liczbę połączeń, które mogą być wykorzystane to wysyłania zapytań do aplikacji bez potrzeby inicjowania nowych połączeń,
    e) rozwiązanie musi oferować tryb detekcji (logowania informacji o wykrytych zagrożeniach bez blokowania), w którym reguły bezpieczeństwa posiadają takie same ustawienia jak w trybie prewencji. System zabezpieczeń musi umożliwiać konfigurację trybu w sposób szczegółowy dla poszczególnych części aplikacji takich jak URL, parametry formularza etc.,
    f) rozwiązanie musi obsługiwać następujące możliwości blokowania: resetowanie połączenia, wysyłanie wybranego kodu błędu, przekierowanie żądania, modyfikacja ciała odpowiedzi lub zablokowanie adresów klienckich IP na określony czas,
    g) rozwiązanie musi umożliwiać automatyczne limitowanie liczby żądań – rate limiting,
    h) rozwiązanie musi zapewniać funkcję przepisywania HTML. Musi być możliwe dodawanie, usuwanie i edycja nagłówków zapytań i odpowiedzi HTML, translacji kodowania znaków spacji w URL, przepisywania i przekierowania URL w zapytaniu oraz przepisywania części body w odpowiedzi. Wyrażenia regularne, muszą być dostępne dla wymaganych manipulacji tekstem,

i) rozwiązanie musi pozwolić administratorowi ograniczyć dostęp do różnych metod HTTP i WEBDAV, w tym HEAD, CONNECT, TRACE itp. dla poszczególnych adresów URL,
j) rozwiązanie musi mieć możliwość zastosowania różnych zasad ograniczeń do różnych części żądania,
k) rozwiązanie musi obsługiwać negatywny model bezpieczeństwa, w którym ataki wykrywane są poprzez dopasowanie wyrażenia regularnego względem przychodzących żądań do adresów URL,
l) rozwiązanie musi wspierać pozytywny model bezpieczeństwa, który pozwala na określenie „białej listy" wartości w różnych elementach polityki bezpieczeństwa, podczas gdy wszystkie inne wartości są odrzucane,
m) rozwiązanie musi umożliwiać tworzenie wirtualnych serwisów/usług (które odpowiadają docelowym aplikacjom). Ponadto musi być możliwe stworzenie indywidualnych profili konfiguracyjnych dla każdej aplikacji,
n) Wykonawca zapewni wsparcie administracyjne, nadzór nad poprawnym działaniem usługi, monitorowaniem ruchu, analizą błędów i proaktywnym podejmowaniem działań mających na celu optymalizację konfiguracji, jak również zapobieganie atakom.

2. Wykonawca ma obowiązek dostarczyć na potrzeby zadania kopii zapasowej, o którym mowa w Rozdziale 4, ust. 1 pkt. 1, lit b) połączenia telekomunikacyjne i sieciowe pozwalające na płynne działanie wszystkich systemów i rozwiązań umieszczonych w środowisku teleinformatycznych Wykonawcy, w tym:
   1) połączenie z PDC za pomocą technologii światłowodowej z obecną infrastrukturą sprzętową Zamawiającego (Plac Teatralny 2, 87-100 Toruń). Połączenie musi zapewnić co najmniej 2 linki światłowodowe, zrealizowane za pomocą usługi ciemnego włókna (link nr 1) oraz za pomocą usługi transmisji (link nr 2) doprowadzone dwoma niezależnymi relacjami fizycznymi między obecną infrastrukturą sprzętową Zamawiającego, a środowiskiem teleinformatycznym PDC dostarczonym przez Wykonawcę w ramach zamówienia. Wykonawca jest zobowiązany do przedstawienia dokładnego przebiegu połączeń fizycznych na etapie składania oferty,
   2) połączenie pomiędzy PDC a SDC za pomocą technologii łącza dedykowanego o przepustowości co najmniej 10 Gbps o parametrze RTT na poziomie 5 ms lub lepszym (krótszym), bez limitu transferu ilości przesyłanych danych oraz umożliwić rozbudowę do 20 Gbit/s w ramach oferowanej usługi bez przerwy w świadczeniu usługi,
   3) połączenia sieciowe wewnętrzne w ramach infrastruktury teleinformatycznej Wykonawcy i środowisk teleinformatycznych udostępnionych Zamawiającemu (połączenia pomiędzy serwerami i routerami) o przepustowości nie mniejszej niż 10 Gbps, bez limitu transferu przesyłanych danych.
3. Wykonawca ma obowiązek dokonać migracji konfiguracji urządzenia FortiGate 1100E z środowiska obecnego dostawcy infrastruktury teleinformatycznej na 2 urządzenia fizyczne FortiGate 1100E Zamawiającego, działające w klastrze, które są przedmiotem kolokacji w OPZ, w tym:
   1) zaplanować i przeprowadzić migrację konfiguracji,
   2) zapewnić dalszą konfigurację, wsparcie i utrzymanie zgodnie z wykupionym wsparciem producenta w ramach dostarczonej licencji wsparcia, o której mowa w OPZ.
4. Wykonawca ma obowiązek dostarczyć łącza telekomunikacyjne i świadczyć wsparcie na czas trwania Umowy.

5.5 Zabezpieczenie łańcucha dostaw w obszarze bezpieczeństwa i cyberzagrożeń

1. Zgodnie z Dyrektywą 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, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) Zamawiający wymaga od Wykonawcy uruchomienia i wdrożenia infrastruktury teleinformatycznej w modelu chmury obliczeniowej wraz z zapewnieniem rozwiązań w obszarze bezpieczeństwa i ochrony przed cyberzagrożeniami w celu spełnienia przez Zamawiającego wymogów bezpieczeństwa w obszarze łańcucha dostaw.
2. Zamawiający oczekuje, że infrastruktura teleinformatyczna i sieciowa PDC Wykonawcy, niezbędna do realizacji zadań będących przedmiotem Zamówienia oraz systemy wewnętrzne Wykonawcy związane z zarządzaniem nimi (infrastruktura zarządzająca Wykonawcy) będą objęte monitoringiem i ochroną SOC, która zostanie zapewniona przez Wykonawcę przez cały okres trwania Umowy. Wykonawca w ramach realizacji zamówienia zapewni własną infrastrukturę teleinformatyczną wraz z niezbędnym

oprogramowaniem do świadczenia ochrony SOC m. in.: przestrzeń dyskową na potrzeby zbierania logów, serwery wirtualne, oprogramowanie oraz inne niezbędne zasoby do prawidłowego świadczenia usługi.

3. Zamawiający oczekuje, że infrastruktura teleinformatyczna, niezbędna do realizacji zadań, o których mowa w Rozdziale 4, ust. 1 pkt. 1, lit. a-d) oferowane z PDC będzie objęta ochroną SOC, która zostanie zapewniona przez Wykonawcę przez cały okres trwania Umowy.
4. Zamawiający oczekuje, że w ramach ochrony SOC będą realizowane poniższe zadania, przez cały okres trwania Umowy:
   1) przeprowadzenie wstępnej analizy bezpieczeństwa (skanowania w celu wykrycia podatności zgodnie ze standardem Critical-Severity CVSS (Common Vulnerability Scoring System) v3.0 Service Vulnerability) dostarczonej infrastruktury teleinformatycznej wraz z oprogramowaniem na niej zainstalowanym oraz opracowanie i przekazanie Zamawiającemu raportu z przeprowadzonej analizy – w terminie do 30 dni od daty odbioru Etapu I,
   2) prowadzenie monitoringu infrastruktury teleinformatycznej wraz z oprogramowaniem na niej zainstalowanym pod kątem zagrożeń cyberbezpieczeństwa zgodnie z ust. 6 poniżej – w trybie 24/7 od daty odbioru Etapu I,
   3) wykrywanie anomalii w zakresie zagrożeń cyberbezpieczeństwa zgodnie z ust. 6 poniżej – w trybie 24/7 od daty odbioru Etapu I,
   4) przyjmowanie i rejestrację zgłoszeń dotyczących zagrożeń cyberbezpieczeństwa zgodnie z zapisami w Rozdziale 6 ust. 1 pkt. 2) . – w trybie 24/7 od daty odbioru Etapu I,
   5) cykliczne raporty dobowe o zdarzeniach cyberbezpieczeństwa – w trybie raz dziennie, od daty odbioru Etapu I,
   6) cykliczne raporty miesięczne o zdarzeniach cyberbezpieczeństwa – w trybie raz w miesiącu, od daty odbioru Etapu I,
   7) cykliczne skanowanie w celu wykrycia podatności i zagrożeń cyberbezpieczeństwa zgodnie ze standardem wymienionym w pkt 1) powyżej oraz opracowanie i przekazanie Zamawiającemu raportu z przeprowadzonej analizy – w trybie raz w kwartale od daty odbioru Etapu I,
   8) analiza zdarzeń bezpieczeństwa – w trybie 24/7 od daty odbioru Etapu I, zgodnie z klasyfikacją priorytetów i czasami reakcji wskazanymi poniżej:

1	**Niski (Low)**	Niski poziom zagrożenia Czas reakcji do 24h	Potencjalne zagrożenia bez znaczącego wpływu, mogące wymagać monitorowania, ale niekoniecznie natychmiastowej reakcji, charakteryzujące się minimalnymi zakłóceniami w funkcjonowaniu systemu np. wiadomości email zawierające elementy z wyłudzaniem danych.
2	**Średni (Medium)**	Średni poziom zagrożenia Czas reakcji do 12h	Potencjalne zagrożenia z umiarkowanym wpływem, wymagające średniej pilności w reakcji i konieczność podjęcia działań zaradczych w rozsądnym czasie np. próby skanowania portów niezakłócające prawidłowego działania systemów IT.
3	**Wysoki (High)**	Wysoki poziom zagrożenia Czas reakcji do 6h	Konkretne i potencjalnie poważne zagrożenia, wymagające natychmiastowej reakcji i skoordynowanego działania, cechujące się koniecznością szybkiego działania w celu zminimalizowania szkód np. wykryta luka w zabezpieczeniach systemu IT, dostępna publicznie i wykorzystywana aktywnie przez osoby trzecie.
4	**Krytyczny (Critical)**	Krytyczny poziom zagrożenia Czas reakcji do 1h	Krytyczne zagrożenia z potencjalnie katastrofalnymi skutkami, wymagające natychmiastowej, zdecydowanej i kompleksowej reakcji, działające, jako najwyższy priorytet, a wszelkie środki zaradcze są wdrożone

			natychmiast np. skutecznie zainicjowany atak szyfrujący dane typu ransomware szyfrujący dane cyfrowe.

5. Zamawiający oczekuje, że w ramach ochrony SOC otrzyma także dostęp na prawach odczytu do konsoli prezentującej wybrane informacje z rozwiązania klasy SIEM:
   1) licznik: suma alertów w określonym czasie (do 30 dni wstecz),
   2) licznik: suma zdarzeń w określonym czasie (do 30 dni wstecz),
   3) wykres (oś czasu): ile alertów w ciągu jednego dnia z ostatnich 30 dni,
   4) wykres (oś czasu): ile zdarzeń w ciągu jednego dnia z ostatnich 30 dni,
   5) tabelę ostatnich alertów z ostatnich 30 dni,
   6) tabelę ostatnich zdarzeń z ostatnich 30 dni,
   7) generowanie raportu zwierającego podsumowanie ilości i typów alertów oraz zdarzeń z ostatnich 30 dni.
6. Ochrona SOC musi uwzględniać rozwiązania klasy SIEM dla dostarczonej infrastruktury teleinformatycznej w warstwie sprzętowej (m.in.: macierze, serwery, przełączniki sieciowe) oraz w warstwie oprogramowania na niej zainstalowanego (m.in. systemy operacyjne, aplikacje, bazy danych), spełniające poniższe wymagania:
   1) system musi posiadać wsparcie producenta wraz z możliwością zakładania zgłoszeń serwisowych na portalu producenta przez cały okres trwania Umowy,
   2) system SIEM ma mieć możliwość integracji z zewnętrznym systemem SOAR,
   3) musi posiadać możliwości integracji z komercyjnymi bazami zagrożeń,
   4) system musi zapewniać skalowalną architekturę spełniającą następujące wymagania:
      a) system SIEM musi dostarczać elementy zapewniający możliwość zbierania zdarzeń bezpieczeństwa z maszyn wirtualnych oraz innych systemów i urządzeń wskazanych przez Zamawiającego,
      b) zadaniem elementów zbierających jest przesyłanie zebranych informacji (zdarzeń bezpieczeństwa) do warstwy przechowującej i analizującej w celu wykrycia zagrożeń,
      c) element zbierający musi mieć możliwość ograniczenia ilości przesyłanych zdarzeń do systemu SIEM,
      d) system SIEM powinien mieć możliwość kompresji danych zdarzeń,
      e) komunikacja pomiędzy elementami zbierającymi a warstwami przechowującej i analizującej musi być szyfrowana w wypadku awarii elementu zbierającego, element zbierający zastępczy może być uruchomiony poprzez jego zarejestrowanie,
      f) wydajność systemu SIEM nie może być mniejsza niż 5 000 EPS (zdarzeń na sekundę odbieranych w trybie ciągłym),
      g) system SIEM musi być w stanie przetwarzać informacje otrzymywane z wykorzystaniem protokołu Syslog,
      h) system SIEM musi być w stanie aktualizować oraz tworzyć nowe dekodery,
      i) system SIEM musi być w stanie aktualizować oraz tworzyć nowe reguły wykrywania zagrożeń,
      j) elementy zbierające mają mieć możliwość aktualizacji wersji swojego oprogramowania z warstwy zarządzającej,
   5) warstwa przechowywania i analizy, od tego miejsca określana, jako Klaster SIEM, ma spełniać następujące wymagania:
      a) klaster SIEM powinien używać metody load-balancingu do obsługi otrzymywanych zdarzeń elementów zbierających,
      b) w przypadku przechowywania danych na dysku lokalnym lub udziale NFS ma być możliwe stworzenie architektury redundantnej, w której w przypadku awarii jednego z komponentu nie wpływa ona na pracę systemu SIEM,
      c) rozwiązanie ma wspierać system wirtualizacji: VMWare, Hyper-V, KVM, AWS, Azure,
      d) klaster SIEM musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych (Virtual Appliance - VA). Wspomniana skalowalność ma być realizowana również poprzez:
         (1) przeprowadzaną w czasie rzeczywistym korelację reguł,
         (2) dystrybuowanie pomiędzy elementami klastra SIEM analizy danych,
      e) klaster SIEM nie może posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i danych w przestrzeni storage,

f) klaster SIEM nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.),
g) dane zbieranych zdarzeń (events) mogą być gromadzone na dyskach VM podczas działania w oparciu o pojedynczą maszynę wirtualną lub też pracy w trybie klastra (wiele VM),
h) klaster SIEM musi mieć możliwość obsłużenia (potencjalną możliwość docelowego wyskalowania do) nie mniej niż 50 tysięcy EPS,
i) klaster SIEM musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log), jak i w formie sparsowanych danych (parsed event log)/danych znormalizowanych,
j) musi istnieć możliwość konfiguracji warstwy zarządzania, jako klastra złożonego z większej liczby instancji, nie mniejszej niż 3, zabezpieczającego przed awarią tej funkcji,
k) maszyny wirtualne systemu SIEM mają działać w oparciu o system Linux, który ma mieć możliwość aktualizacji,

6) rozwiązanie SIEM musi mieć możliwość zbierania danych z monitorowanych urządzeń, również innych niż logi, co ma być osiągalne poprzez nie mniej niż:
a) wykrywanie urządzeń wewnątrz sieci bez wykorzystania dodatkowego oprogramowania typu agent,
b) zdolność do monitorowania statusu oraz dostępności usług takich jak np.: DNS, FTP, TCP, UDP, ICMP, LDAP, SMTP, IMAP, POP3, POP3S, SSH, HTTP, HTTPS,
c) możliwość automatycznego przypisania wirtualnych maszyn do poszczególnych grup, np.: grupa linux, grupa windows,
d) automatyczne wykrywanie aplikacji działających na poszczególnych urządzeniach,
e) monitorowanie metryk wydajnościowych ma dotyczyć nie mniej niż:
(1) obciążenia CPU,
(2) wykorzystania pamięci,
(3) wykorzystania przestrzeni dyskowej,
7) rozwiązanie SIEM musi dostarczać zunifikowane narzędzia analityczne dzięki, którym możliwe jest wykonywanie zapytań w oparciu o ten sam język zarówno dla logów/zdarzeń zbieranych z urządzeń, jak i dla danych wydajnościowych,
8) wymagane jest, aby elementy zbierające systemu SIEM pozwalały na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne. Mechanizm ten nie może mieć żadnego wpływu na model licencjonowania,
9) zarówno dane w stanie surowym, jak i te sparsowane lub wzbogacone muszą być możliwe do przesłania do rozwiązania SIEM z elementów zbierających,
10) przetwarzanie danych związanych z poszczególnymi zdarzeniami (events) wykonywane jest poprzez parsery systemowe,
11) musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów,
12) tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI),
13) rozwiązanie SIEM musi mieć możliwość zbierania zdarzeń (event) z systemów Windows oraz Linux w oparciu o aplikacje typu agent,
14) rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości:
a) centralne zarządzanie i możliwość aktualizacji z głównej konsoli systemu SIEM,
b) możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows,
c) możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application,
d) zdolność do monitorowania integralności plików,
e) zdolność do monitorowania rejestru systemowego,
f) zdolność do monitorowania urządzeń zewnętrznych (removable devices),
g) zdolność do wykonywania poleceń PowerShell wraz z odsyłaniem wyniku ich działania w postaci logów,
h) agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany,
i) musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu,

j) agent Windows musi mieć możliwość buforowania zbieranych zdarzeń w wypadku utraty komunikacji z pozostałymi elementami klastra SIEM,
k) musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych, np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS,

15) rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Linux (Linux Agent), które posiadają nie mniej niż następujące możliwości:
a) centralne zarządzanie i możliwość aktualizacji z głównej konsoli systemu SIEM,
b) możliwość zbierania logów z wykorzystaniem protokołu syslog,
c) możliwość zbierania logów z plików tekstowych,
d) zdolność do monitorowania integralności plików,
e) zdolność do monitorowania pliku w oparciu o jego sumę kontrolną,
f) musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu,
16) system SIEM musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI,
17) muszą być wspierane zewnętrzne metody uwierzytelniania użytkowników SIEM, nie mniej niż: Active Directory lub LDAP,
18) musi istnieć integracja z zewnętrznymi bazami o zagrożeniach (Threat Inteligence Feeds - TI):
a) wymagane jest, aby każda z zewnętrznych baz zagrożeń była w stanie wesprzeć do 200 tysięcy wpisów,
b) system SIEM musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym. Korelacja ta ma odbywać się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data),
c) system musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np. VirusTotal, w tym również pochodzących od producenta samego systemu SIEM,
d) system musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK w oparciu o wbudowane reguły, których ilość w tym kontekście ma wynosić nie mniej niż 900,
19) system SIEM musi pozwalać na eksportowanie i importowanie pulpitów administracyjnych (dashboards), raportów oraz reguł,
20) pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji,
21) dane w ramach pulpitów administracyjnych muszą pozwalać na następujące formy prezentacji: Bar, Pie, Line, Table, Gauges, Geographical Map,
22) system SIEM musi:
a) posiadać możliwość uruchamiania skryptów w odpowiedzi na wybrane zdarzenia bezpieczeństwa,
b) posiadać możliwość integracji w oparciu o API z zewnętrznymi systemami do obsługi zgłoszeń (ticketingsystems) takimi jak ServiceNow, ConnectWise lub Jira,
c) mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system),
23) możliwości w zakresie analityki:
a) wyszukiwania zdarzeń (events) w czasie rzeczywistym,
b) wyszukiwania w oparciu o słowa kluczowe,
c) wyszukiwania historycznego,
d) tworzenia harmonogramu raportów i dostarczania ich pocztą elektroniczną,
e) możliwości eksportowania raportów do formatów CSV, PDF, skalowania możliwości analitycznych poprzez dodawanie do systemu SIEM kolejnych maszyn wirtualnych bez konieczności wyłączania całego klastra SIEM,
f) korelowania użytkownika z jego lokalizacją i adresem IP.

7. Ochrona SOC musi uwzględniać rozwiązania antywirusowe VM, spełniającą minimalny zakres funkcjonalności obejmujący:
1) pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami IT,
2) pomoc techniczną, interfejs oraz dokumentację w języku polskim,
3) wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, phishing, narzędzi hakerskich, backdoor, itp.,
4) wbudowaną technologie do ochrony przed rootkitami,

5) automatyczną, inkrementacyjną aktualizację baz wirusów i innych zagrożeń,
6) dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej,
7) wbudowaną zaporę osobistą, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego,
8) możliwość tworzenia list sieci zaufanych,
9) możliwość dezaktywacji funkcji zapory sieciowej,
10) moduł ochrony przeciwko zagrożeniom typu ransomware.

8. W ramach dokumentacji po uruchomieniu ochrony SOC Wykonawca w terminie 60 dni od dnia odbioru Etapu I dostarczy:
   1) architekturę rozwiązania wraz z opisem,
   2) szczegółową procedurę reagowania na incydenty, przygotowaną w porozumieniu z Zamawiającym.
9. Zamawiający z uwagi na ograniczenie ryzyk siły wyższej zastrzega, że PDC i SDC nie mogą być powiązane kapitałowo, ani należeć do tej samej grupy właścicielskiej. Wykonawca zobowiązany jest wskazać w ofercie lokalizację gromadzonych i przetwarzanych danych będących przedmiotem Umowy (adresy lokalizacji PDC i SDC) oraz załączyć oświadczenie o braku powiązań właścicielskich i kapitałowych pomiędzy PDC i SCD.
10. Zamawiający z uwagi na ograniczenie ryzyk siły wyższej zastrzega, że odległość pomiędzy PDC i SDC nie może być mniejsza niż 100 km w linii prostej w celu zachowania dostępności danych na wypadek klęski i zniszczenia jednego z nich (PDC lub SDC).
11. Zamawiający z uwagi na ograniczenie ryzyk siły wyższej zastrzega, że odległość pomiędzy siedzibą Zamawiającego (Plac Teatralny 2, 87-100 Toruń), a PDC nie może być większa niż 50 km w linii prostej (średni czas dojazdu do 1h), w celu szybkiego dostępu do danych, aplikacji i systemów Zamawiającego na wypadek długotrwałej awarii łącza dostępowego po stronie Zamawiającego. Z uwagi na powyższe Zamawiający oczekuje w trakcie całego trwania okresu Umowy zapewnienia dostępu do pomieszczenia biurowego na terenie PDC o powierzchni nie mniejszej niż 21 m2 wraz z dostępem do 3 stanowisk pracy (biurko z krzesłem), wyposażonego w bezpośrednie połączenie sieciowe umożliwiające wydajne połączenie z aplikacjami i systemami przechowującym dane Zamawiającego w PDC.
12. Z uwagi na potrzebę wysokiej dostępności całej infrastruktury będącej przedmiotem zamówienia wraz z wszystkimi systemami towarzyszącymi, Zamawiający oczekuje, aby proponowane rozwiązanie spełniało najwyższe, dostępne na terenie Unii Europejskiej standardy bezpieczeństwa teleinformatycznego. Wymagania dla ośrodka PDC i SDC są obligatoryjne. Wykluczone jest częściowe spełnianie któregokolwiek wymogu. Zamawiający na etapie wyboru oferty, a także realizacji umowy zastrzega możliwość weryfikacji i wezwania Wykonawcy do udokumentowania spełniania każdego z wymogów określonych poniżej:
   1) PDC i SDC posiada odpowiednie zabezpieczenia fizyczne i organizacyjne zapewniające bezpieczeństwo przetwarzanych danych Zamawiającego. Wykonawca ponosi odpowiedzialność w zakresie bezpieczeństwa informacji i danych przechowywanych na wykorzystanej infrastrukturze teleinformatycznej PDC i SDC,
   2) PCD i SDC posiadają zabezpieczenia 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,
      e) ochrony świadczonej przez licencjonowaną firmę ochroniarską w trybie 24/7,
   3) PDC realizuje profesjonalne utrzymanie i konserwację posiadanej infrastruktury teleinformatycznej w postaci:
      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) prowadzenia aktualnego rejestru: przeglądów, incydentów, awarii i usterek.

4) PDC spełnia wymagania bezpieczeństwa w zakresie parametrów powalających wyeliminować wskazane zagrożenia:

Parametr	Wyeliminowanie zagrożenia
1. Obiekt i lokalizacja	
PDC zlokalizowane 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.
PDC posiada ogrodzony zamknięty teren wraz z ograniczoną strefą wejść.	Brak podstawowej kontroli fizycznego dostępu do infrastruktury IT oraz innych urządzeń (elementy zasilania, chłodzenia, wentylacji).
PDC 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.
PDC jest położony nie mniej niż 5 metrów powyżej poziomu wody stuletniej	Zagrożenie długotrwałego zalania. Wysoka intensywność oddziaływania sytuacji krytycznych.
PDC 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 w skutek eksplozji zewnętrznej.
PDC jest oddalony nie mniej niż 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, centra handlowe, miejsca organizacji imprez masowych dla 10 tys. osób i więcej).	Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów, ryzyko zamieszek, zniszczeń.
PDC 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).
PDC 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 pół zakłócających pracę urządzeń elektrycznych i magnetycznych.
PDC posiada podłogę techniczną w pomieszczeniu z serwerami.	Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych.

PDC 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	
PDC 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 PDC wykonane są dwoma niezależnymi trasami kablowymi.	Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem.
PDC 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.
PDC posiada węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,99%.	Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet.
PDC posiada węzeł telekomunikacyjny wyposażony w redundantny system firewall.	Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej.
PDC 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	
PDC posiada dostępność roczną systemu zasilania energetycznego na poziomie nie niższym niż 99,999%	Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń.
PDC 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.
PDC 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.
PDC posiada redundantny system agregatów prądotwórczych.	Zagrożenie braku zachowania zasilania.

System zasilaczy awaryjnych UPS w PDC 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 PDC 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	
PDC 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.
PDC 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.
PDC 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 PDC 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 PDC 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 PDC 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 PDC 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 PDC możliwy jest wyłącznie przy użyciu łącznie 2 elementów identyfikacji: SKD, osobistej karty identyfikacyjnej, hasła (kodu) lub elementu biometrycznego.	Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń.
PDC posiada system gaszenia bezpieczny dla ludzi i sprzętu komputerowego oraz serwerowego.	Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia.
PDC 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	
PDC 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.
PDC 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.

5.6. Dostawa licencji

1. Wykonawca dostarczy licencje wparcia producenta dla 4 sztuk urządzeń FortiGate 1100E, w tym:
   1) licencje typu: Unified Threat Protection (UTP), (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium,
   2) dla 2 sztuk urządzeń, znajdujących się w siedzibie Zamawiającego (Plac Teatralny 2, 87-100 Toruń), licencje muszą być ważne na czas od dnia 25.09.2024 roku do końca trwania Umowy,
   3) dla 2 sztuk urządzeń podlegających kolokacji w ramach niniejszego zamówienia, licencje muszą być ważne na czas od dnia 03.10.2024 roku do końca trwania Umowy.
2. W przypadku wycofania przez producenta urządzenia wsparcia na urządzenie, o którym mowa w ust. 1, pkt. 1) powyżej, Wykonawca dostarczy na pozostały okres trwania Umowy urządzenia o parametrach i funkcjonalności nie gorszej niż parametry urządzenia, o którym mowa w ust. 1, pkt. 1) powyżej, wraz z wsparciem producenta.
3. Wykonawca dostarczy 1 licencję obejmującą wszystkie aplikacje usługi Adobe Creative Cloud. Licencja musi być ważna na czas od dnia 01.12.2024 roku minimum do końca trwania Umowy.
4. Wykonawca dostarczy licencję na Cloudflare PRO. Licencja musi być ważna na czas od dnia 05.10.2024 roku minimum do końca trwania Umowy.

5.7. Szkolenia wdrożeniowe

1. Wykonawca, w terminie uzgodnionym z Zamawiającym zobowiązany jest do przeprowadzenia szkoleń wdrożeniowych, potrzebnych do realizacji przedmiotu Umowy, dla wskazanych przez Zamawiającego osób (nie więcej niż 15 osób):
   1) z zakresu technologii wirtualizacji,
   2) z zakresu technologii kopii zapasowej,
   3) z zakresu technologii bezpieczeństwa sieci (np. z obsługi firewall NG),

4) z zakresu monitorowania zdarzeń SIEM.
5. Szkolenia będą prowadzone przez specjalistów Wykonawcy, którzy zajmują się bezpośrednim utrzymaniem systemów i usług realizowanych w ramach Zamówienia.
6. Szkolenia odbędą się w siedzibie Zamawiającego. Zamawiający dopuszcza formę zdalną przeprowadzenia szkoleń.
7. Każdy z uczestników może odbyć szkolenie w innym terminie.
8. Uczestnicy szkolenia otrzymają bezzwrotne materiały szkoleniowe.
9. Szkolenia zostaną przeprowadzone w języku polskim.
10. Po zakończeniu szkolenia uczestnicy otrzymają zaświadczenie o ukończeniu szkolenia.
11. Realizacja cyklu szkoleń będzie następowała w dni robocze Zamawiającego tj. od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy.

6. 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, o której mowa w Rozdziale 4, ust.1, pkt. 1), lit. a-e) nie niższą niż SLA na poziomie dostępności 99,9% i więcej w skali roku, licząc od daty podpisania Umowy, w tym:
   1) obsługa utrzymania i zarządzania oferowanego rozwiązania musi być realizowana w trybie 24/7/365,
   2) przyjmowanie zgłoszeń serwisowych musi być realizowane w trybie 24/7/365 w sposób autoryzowany w systemie online Wykonawcy, który umożliwia podgląd wszystkich dokonanych zgłoszeń, czas ich realizacji oraz bieżący ich status, wraz z historią wszystkich zgłoszeń,
   3) Czas reakcji na zgłoszenie musi wynosić nie więcej niż 60 minut od przyjęcia zgłoszenia, z zastrzeżeniem pkt 6),
   4) Czas usunięcia Awarii musi wynosić do 24 godzin od przyjęcia zgłoszenia,
   5) Czas usunięcia Incydentu musi wynosić do 5 dni roboczych od przyjęcia zgłoszenia,
   6) Czasy reakcji na analizy zdarzeń bezpieczeństwa muszą być realizowane zgodnie z czasami wskazanymi w tabeli w Rozdziale 5, podrozdział 5.5. ust. 4, pkt. 8.
2. Wykonawca składa raport z dostępności SLA w terminie 5 dni kalendarzowych po zakończeniu roku kalendarzowego, a w przypadku ostatniego roku obowiązywania Umowy, w terminie 5 dni od jej zakończenia.

7. Wymogi w zakresie świadczenia asysty technicznej

1. Do zadań realizowanych przez Wykonawcę w ramach usług asysty technicznej należeć będzie obsługa administracyjna zasobów teleinformatycznych wraz z nadzorem nad posiadaną przez Zamawiającego infrastrukturą zlokalizowaną PDC i SDC w zakresie:
   1) instalacji i konfiguracji systemów operacyjnych, licencji i innych niezbędnych komponentów,
   2) instalacji i konfiguracji elementów niezbędnych do zapewnienia wysokiej dostępności (HA),
   3) aktualizacji oprogramowania ze względu na błędy bezpieczeństwa,
   4) utrzymania infrastruktury pod kątem wydajności, bezpieczeństwa,
   5) realizacji bieżących czynności administracyjnych,
   6) analiz incydentów oraz problemów wraz pełnym przywracaniem funkcjonalności.
2. W zakresie tych czynności, o których mowa w ust. 1, które Wykonawca będzie wykonywał na podstawie zleceń Zamawiającego składanych w udostępnionym przez Wykonawcę systemie typu helpdesk. Wykonawca winien przystąpić do wykonania zlecenia w ciągu maksymalnie 24 godzin i wykonać zlecenie w terminie maksymalnie 168 godzin.
3. Niezależnie od powyższego zakresu czynności, do dyspozycji w ramach świadczonej usługi asysty technicznej Wykonawca udostępni zasoby ludzkie w postaci 100 roboczogodzin rocznie pracy specjalistów IT na prace zlecone przez Zamawiającego związane z kreowaniem, przenoszeniem, zabezpieczaniem, testowaniem, przywracaniem, aktualizacją, bieżącym utrzymaniem systemów w środowisku infrastrukturalnym, wsparciem systemów funkcjonujących w środowisku infrastrukturalnym oraz innymi obszarami funkcjonowania instancji serwerowych przez cały czas trwania usługi wynikającej z przedmiotowego Zamówienia.

4. Niezależnie od powyższego zakresu czynności, do dyspozycji w ramach świadczonej usługi asysty technicznej Wykonawca udostępni zasoby ludzkie w postaci 100 roboczogodzin rocznie pracy specjalistów IT z zakresu: technologii wirtualizacji, wykonywania kopii zapasowych, połączeń sieciowych i bezpieczeństwa IT w celu wykonywania doradztwa i konsultacji technicznych w zakresie wdrażanych aplikacji i systemów, w tym przy udziale zewnętrznych wykonawców i dostawców Zamawiającego.
5. Wykonawca na wezwanie Zamawiającego będzie każdorazowo składał raport nt. ilości godzin już wykorzystanych przez Zamawiającego oraz godzin pozostałych do dyspozycji.

8. Wdrożenie i odbiór

8.1. Harmonogram realizacji uruchomienia i świadczenia usługi

1. Rozpoczęcie prac nastąpi z chwilą podpisania Umowy.
2. Etap I (Dostawa, wdrożenie, konfiguracja i uruchomienie infrastruktury teleinformatycznej wraz z zabezpieczeniami w obszarze ochrony przed cyberzagrożeniami) musi nastąpić nie później niż w terminie zaoferowanym przez Wykonawcę, ale nie dłużej niż 30 dni kalendarzowych od daty zawarcia Umowy i musi obejmować zadania wskazane w Rozdziale 4, ust. 1 pkt.1, lit. a-e).
3. Wykonawca zgłosi gotowość do obioru Etapu I na 1 dzień kalendarzowy przed terminem zakończenia Etapu I.
4. Zamawiający w ciągu 60 dni kalendarzowych jest zobowiązany do dokonania odbioru Etapu I lub zgłoszenia uwag i wyznaczenia terminu na ich usunięcie, po czym przystąpi do ponownego odbioru. W przypadku nie usunięcia uwag wskazanych przez Wykonawcę, Zamawiający ma prawo do wstrzymania płatności za wykonanie Etapu I do czasu całkowitego usunięcia uwag.
5. Etap II (Asysta techniczna) rozpocznie się od momentu protokolarnego odbioru (częściowego) bez uwag Etapu I i będzie trwał do dnia 30 listopada 2027 r.
6. Wykonawca udzieli Zamawiającemu nieodpłatnej gwarancji na przedmiot zamówienia, która zostanie udzielona na okres 1 miesiąca, począwszy od daty protokolarnego odbioru (końcowego) bez uwag Etapu II.
7. Po odbiorze (częściowym) Etapu I, zostanie dokonana płatność w wysokości 20% całego zamówienia, natomiast pozostała część wynagrodzenia za realizację Etapu II będzie rozliczana proporcjonalnie w ramach płatności rocznych (w wysokości 20% całego zamówienia) po zakończeniu każdego roku kalendarzowego i protokolarnego odbioru (częściowego) bez uwag realizacji Etapu II w danym roku kalendarzowym, a w przypadku ostatniego roku po protokolarnym odbiorze (końcowym) bez uwag realizacji Etapu II dokonanego po zakończeniu trwania Umowy.

8.2. Dokumentacja techniczna

1. W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest do opracowania dokumentacji powykonawczej z wdrożenia w terminie do 30 dni kalendarzowych od dnia uruchomienia usługi.
2. Dokumentacja musi zawierać co najmniej:
   1) opis parametrów systemu mających wpływ na jego funkcjonowanie,
   2) architekturę logiczną i fizyczną zastosowanych rozwiązań,
   3) schemat połączeń sieciowych.
3. Wykonawca zobowiązany jest zapewnić w ramach realizacji przedmiotu zamówienia wszelkie prawa umożliwiające Zamawiającemu korzystanie z opracowanej oraz dostarczonej w ramach realizacji Dokumentacji wdrożenia.

8.3. 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. Wykonawca zobowiązany będzie skierować do realizacji przedmiotu zamówienia zespół projektowy, składający się z osób wskazanych w ofercie. W przypadku zmian w składzie zespołu Wykonawca zobowiązuje się do zapewnienia osób do zespołu projektowego, o co najmniej takich samych kwalifikacjach i doświadczeniu, jakie posiadać będą osoby wskazane w ofercie.

4. Zamawiający wymaga zatrudnienia przez Wykonawcę, jak i podwykonawcę, na podstawie umowy o pracę osób wykonujących w zakresie realizacji zamówienia czynności polegające na wykonywaniu pracy w sposób określony w art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy (tj. Dz. U. z 2018r. poz. 917 z późn. zm.), tj. osób wykonujących następujące czynności:
   1) opracowywanie założeń i architektury systemów informatycznych,
   2) administrowanie urządzeniami sieciowymi,
   3) administrowanie serwerami w środowisku wirtualnym,
   4) administrowanie systemami operacyjnymi,
   5) administrowanie systemami bezpieczeństwa.
5. Sposób dokumentowania zatrudniania osób, o których mowa powyżej, uprawnienia Zamawiającego w zakresie kontroli spełniania przez Wykonawcę wymagań z tytułu zatrudnienia na podstawie umowy o pracę oraz sankcje z tytułu niespełnienia tych wymagań zostały określone we wzorze Umowy.

8.4. 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.