OPIS PRZEDMIOTU ZAMÓWIENIA

I. Przedmiot zamówienia

Przedmiotem umowy jest „Dostawa środowiska kopii bezpieczeństwa" polegająca na zaprojektowaniu, konfiguracji, uruchomieniu oraz przetestowaniu środowiska kopii zapasowych wraz z dostawą urządzeń informatycznych i oprogramowania w ramach wdrożenia rozwiązań "Cyberbezpiecznego Samorządu".

Rozwiązanie ma zapewnić wykonywanie kopii zapasowych zgodnie z zasadą 3-2-1 lub tożsamą zasadą (zgodną z dobrymi praktykami tworzenia kopii bezpieczeństwa), z wykorzystaniem trzech niezależnych miejsc składowania kopii: Serwer Kopii Bezpieczeństwa przeznaczony na kopie "pierwszej pomocy", macierz dyskowa, oraz napęd taśmowy (kopia offline/offsite).

II. Cel zamówienia

1. Zapewnienie odporności na awarie logiczne i sprzętowe, błędy ludzkie oraz incydenty ransomware poprzez:
   1) regularne kopie dzienne i tygodniowe,
   2) możliwość szybkiego odtworzenia,
   3) kopię długoterminową na taśmach (offline/offsite),
2. Wykonywanie testów odtworzeniowych,
3. Zbieranie logów,
4. Monitoring infrastruktury.
5. Opracowanie dokumentacji.

III. Wymagania ogólne:

1. Kopie muszą być wykonywane automatycznie wg harmonogramu,
2. Dostęp do repozytoriów kopii musi być ograniczony (least privilege),
3. Wykonawca przygotuje i przetestuje plany kopii oraz procedury odtwarzania.
4. Wykonawca będzie ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na sumę gwarancyjną min. 450 000,00 zł (słownie złotych: czterysta pięćdziesiąt tysięcy złotych 00/100).

IV. Środowisko Zamawiającego.

Środowisko produkcyjne, które należy objąć ochroną, składa się z dwóch serwerów fizycznych z systemami operacyjnymi Windows Server 2022 oraz serwerów wirtualnych (wirtualizator Hyper-V). Wielkość danych przeznaczonych do ochrony (stan na moment przygotowania OPZ):

• Serwer 1: ok. 3 TB danych.

• Serwer 2: ok. 12 TB danych.

Do zarządzania kopiami bezpieczeństwa wykorzystywane będzie oprogramowanie Acronis Cyber Protect - Backup Advanced Virtual Host, posiadane przez Zamawiającego. Zamawiający posiada również serwer plików, który zostanie wykorzystany jako dodatkowa przestrzeń dyskowa do gromadzenia logów z systemów IT.

V. Plan wdrożenia zadania: „Dostawa środowiska kopii bezpieczeństwa”

1. Wykonawca przygotuje koncepcję środowiska kopii bezpieczeństwa (zwaną dalej koncepcją). W terminie do czternastu dniu od daty podpisania umowy, Wykonawca przekaże Zamawiającemu kompletną koncepcję, Zamawiający w przeciągu czterech dni roboczych dokona analizy koncepcji. Zamawiający ma prawo do wnoszenia uwag do koncepcji, Wykonawca uwzględni uwagi Zamawiającego w koncepcji. Zamawiający podpisze uzgodnioną koncepcję i przekaże ją Wykonawcy do realizacji. Założenia do przygotowania koncepcji środowiska kopii bezpieczeństwa:

   1.1. koncepcja będzie opracowana z uwzględnieniem najwyższych standardów bezpieczeństwa danych, w szczególności będzie uwzględniać zabezpieczenia danych przed utratą w wyniku działania szkodliwego oprogramowania i awarii, np.: z zastosowaniem zasady 3-2-1-1-0,

   1.2. koncepcja będzie zawierać wymagania wynikające z przepisów prawa, w szczególności wymagania na zgodność z normą PN-EN ISO/IEC 27001,

   1.3. koncepcja ma uwzględniać kluczowe wskaźniki w planowaniu ciągłości działania tj. Recovery Time Objective (RTO) i Recovery Point Objective (RPO) dla wszystkich kluczowych systemów Zamawiającego,

   1.4. koncepcja będzie opierać się na sprzęcie dostarczonym w ramach niniejszej umowy, Wykonawca dostarczy wszystkie elementy niezbędne do realizacji koncepcji (w szczególności: interfejsy, kable, wkładki światłowodowe itp.), nawet wtedy, gdy nie są wprost wymienione w OPZ,

   1.5. koncepcja będzie wykorzystywać zabezpieczenia sprzętowe tj. Write Once Read Many (WORM),

   1.6. koncepcja będzie opisywać fizyczne i logiczne połączenia pomiędzy dostarczonym sprzętem i sprzętem Zamawiającego (w szczególności: serwery fizyczne i wirtualne oraz przełączniki),

   1.7. Zamawiający posiada dwa redundantne przełączniki połączone w stos, Wykonawca uwzględni to w koncepcji oraz zaprojektuje segmentację sieci dedykowaną dla środowiska kopii bezpieczeństwa,

   1.8. za pomocą środowiska będzie można wykonać kopie bezpieczeństwa wszystkich serwerów fizycznych i wirtualnych Zamawiającego oraz nowych serwerów zakupionych w przyszłości,

   1.9. środowisko do tworzenia kopii będzie wykorzystywać oprogramowanie, które posiada Zamawiający, Wykonawca zaprojektuje i wdroży wszystkie plany kopii bezpieczeństwa,

1.10. koncepcja będzie uwzględniać okna serwisowe dla poszczególnych systemów Zamawiającego oraz wielkość kopii danych,

1.11. koncepcja będzie zawierać opis wykonania testu kopii bezpieczeństwa oraz testowego uruchomienia serwerów wirtualnych z kopii,

1.12. koncepcja będzie uwzględniała sposób postępowania z nośnikami, na których zapisane są kopie bezpieczeństwa, w szczególności opis postępowania z taśmami LTO,

1.13. koncepcja będzie uwzględniała wdrożenie centralnego systemu zapisywania i przechowywania logów,

1.14. koncepcja będzie uwzględniała wdrożenie systemu monitorowania i nadzorowania infrastruktury IT,

2. Wykonawca dostarczy wszystkie elementy niezbędne do wdrożenia koncepcji w tym: serwer, macierz dyskową, napęd taśmowy o parametrach z nie gorszych niż poniższy opis

2.1. Serwer, jedna sztuka.

Parametr	**Charakterystyka (wymagania minimalne)**
Obudowa	• Obudowa Rack o wysokości max 2U • 16 wnęk na dyski 2.5” • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 144 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. • Płyta główna powinna obsługiwać do 8TB pamięci RAM.
Procesor	• Zainstalowane dwa procesory min. 8-rdzeniowe, min. 3.5GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 170 w teście SPECspeed®2017_fp_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej oferowanego serwera.
RAM	• 128GB DDR5 RDIMM 6400MT/s,

Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający
	  ○ Min. 8GB nieulotnej pamięci cache,
	  ○ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
	  ○ Wsparcie dla dysków samoszyfrujących
	  ○ Obsługa dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS

Dyski twarde	• Zainstalowane:
	  ○ 2x dysk SSD SATA o pojemności min. 960GB, Hot-Plug
	  ○ 7x dysk SAS o pojemności min. 2.4TB, Hot-Plug
	Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.

Gniazda PCI	• Cztery sloty PCIe
Interfejsy sieciowe/FC/SAS	• 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) • Czteroportowa karta 12Gb SAS HBA

Wbudowane porty	• 4 porty USB w tym min:
	  ○ 1 port USB 2.0 Type-C
	  ○ 2 porty USB 3.1
	  ○ 1 port USB 3.0 wewnątrz obudowy
	• Port VGA z tyłu obudowy

Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	• Redundantne, Hot-Plug min. 1100W klasy Titanium
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
System operacyjny/ dodatkowe oprogramowanie	• Ze względu na konieczność zachowania kompatybilności z posiadanym przez Zamawiającego systemem informatycznym wymagane jest dostarczenie licencji Windows Server Standard w najnowszej wersji z możliwością instalacji wersji 2022 (licencja na wszystkie rdzenie procesorów w zaoferowanym serwerze).
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0

	• Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port RJ-45 Gigabit Ethernet
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklarację CE.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta na okres minimum 2 lat. • W przypadku awarii dysków uszkodzone nośniki danych pozostają u Zamawiającego. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych, a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym od zgłoszenia (NBD). • Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.

	• Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu, oświadczenia że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.

2.2. Macierz dyskowa, jedna sztuka.

Parametr	**Charakterystyka (wymagania minimalne)**
Procesor	Procesor 64-bitowy x86 o taktowaniu nie mniejszym niż 5.1 GHz
Zainstalowana pamięć RAM	Min. 32 GB ECC DDR5, możliwość rozbudowy do 192 GB
Pamięć Flash	Min. 5 GB
Liczba zatok na dyski	Min. 14 szt., w tym min. 12 x 3,5-calowych SATA oraz min. 2 x M.2 2280 NVMe
Obsługiwane dyski twarde	3.5" SATA, 2.5" SATA oraz M.2 NVMe SSD
Zainstalowane dyski twarde	Min. 7 szt. dysków o pojemności 8TB Dostarczone dyski muszą być przeznaczone do pracy w dostarczonej macierzy dyskowej.
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Min. 2 szt.
Porty LAN 10 GbE	Min. 2 szt.
Porty LAN 25 GbE SFP28	Min. 2 szt.
Porty USB 3.2 Gen2	Min. 2 szt.
Port PCiE	Min. 3 szt.
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 2U

Zasilanie	Dwa zasilacze redundantne
Agregacja łączy	Tak
Obsługiwane systemy plików	EXT4, ZFS lub BTRFS
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Poziomy RAID: Pojedynczy Dysk, 0, 1, 5, 6, 10, 50, 60, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer Monitoringu

VPN	VPN client / VPN server Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Warunki gwarancji	Wymagane min. 2 lata gwarancji producenta urządzenia. W przypadku awarii dysków uszkodzone nośniki danych pozostają u Zamawiającego.

2.3. Napęd taśmowy, jedna sztuka.

Parametr	**Charakterystyka (wymagania minimalne)**
Obudowa	Urządzenie nie może przekraczać rozmiaru 2U w podstawowej konfiguracji. Urządzenie musi być wyposażone w zestaw umożliwiający jej zamontowanie w szafie Rack 19”.

Napędy i obsługiwane nośniki	Urządzenie musi być wyposażone w minimum jeden napęd w technologii LTO9. Minimalna pojemność taśmy bez kompresji 18TB. Urządzenie musi posiadać interfejs SAS o prędkości minimum 12Gb/s.
Kieszenie na nośniki (sloty)	Biblioteka musi mieć minimum 8 kieszeni na nośniki, jeśli ich obsługa wymaga dodatkowych licencji, wymagane jest dostarczenie takiej licencji.
Zarządzanie	Biblioteka musi być wyposażona w moduł zdalnego zarządzania. Biblioteka musi udostępniać funkcję monitorowania napędów. Biblioteka powinna mieć również możliwość zdalnego monitorowania urządzenia i wychwytywania błędów bezpośrednio przez inżynierów producenta za pomocą odpowiedniego oprogramowania.
Pozostałe wymagania	Urządzenie musi posiadać czytnik kodów kreskowych do identyfikacji taśm. Wraz z urządzeniem należy dostarczyć 10 taśm LTO9 i 1 taśmę czyszczącą.
Warunki gwarancji	Urządzenie musi być objęte minimum 2 letnią gwarancją i wsparciem producenta z możliwością zgłaszania awarii w trybie 5x8 z czasem dostawy części w trybie następnego dnia roboczego z usługą wymiany części na miejscu. W okresie serwisu zamawiający musi mieć dostęp do zdalnej pomocy technicznej, poprawek i nowych wersji oprogramowania i sterowników oferowanego urządzenia.

2.4. Interfejsy sieciowe dla serwerów produkcyjnych Zamawiającego.

Parametr	**Charakterystyka (wymagania minimalne)**
Interfejs sieciowy dla serwera produkcyjnego 1	Serwer produkcyjny należy doposażyć w minimum 2 interfejsy sieciowe, minimum 10Gb Ethernet każdy, w standardzie minimum SFP+. Wykonawca dostarczy wszystkie wkładki światłowodowe (dla serwera i przełączników) oraz kable światłowodowe, niezbędne do prawidłowego działania połączeń.
Interfejs sieciowy dla serwera produkcyjnego 2	Serwer produkcyjny należy doposażyć w minimum 2 interfejsy sieciowe, minimum 10Gb Ethernet każdy, w standardzie minimum SFP+. Wykonawca dostarczy wszystkie wkładki światłowodowe (dla serwera i przełączników) oraz kable światłowodowe, niezbędne do prawidłowego działania połączeń.

3. Wykonawca przeprowadzi wdrożenie ustalonej koncepcji oraz przeprowadzi wszelkie niezbędne prace potrzebne do uruchomienia środowiska kopi bezpieczeństwa.

   Zamawiający wymaga wykonania wraz z dostawą w/w urządzeń następujących prac inżynieryjnych po stronie Wykonawcy. Zamawiający zaznacza, że prace wykonywane mogą być wyłącznie w siedzibie Zamawiającego, a prace wymagające przerw komponentów infrastruktury Zamawiającego muszą być wykonywane poza godzinami urzędowana organizacji Zamawiającego.

Parametr	Charakterystyka (wymagania minimalne)
Instalacja i konfiguracja serwera (1 sztuka)	• Wymaga, aby Wykonawca dokonał montażu dostarczonego serwera we wskazanej przez Zamawiającego szefie Rack. • Wymaga się od Wykonawcy dokonania wstępnej konfiguracji urządzenia w zakresie interfejsu zarządzania zdalnego. • Wymaga się od Wykonawcy konfiguracji pul dyskowych w zakresie RAID1 dla dysków przeznaczonych na system operacyjny oraz RAID5 przeznaczone na dane. • Wymaga się od Wykonawcy dokonania instalacji systemu operacyjnego dostarczonego razem z serwerem • Wymaga się od Wykonawcy dokonania instalacji niezbędnych sterowników i dokonania niezbędnych aktualizacji. • Wymaga się od Wykonawcy podłączenia serwera do produkcyjnej sieci Zamawiającego za pomocą wbudowanych w serwer interfejsów SFP28.
Instalacja i konfiguracja macierzy dyskowej	• Wymaga, aby Wykonawca dokonał montażu dostarczonej macierzy dyskowej we wskazanej przez Zamawiającego szefie Rack. • Wymaga się od Wykonawcy dokonana wstępnej konfiguracji urządzenia w zakresie interfejsu zarządzania zdalnego. • Wymaga się od Wykonawcy podłączenia macierzy dyskowej do produkcyjnej sieci Zamawiającego za pomocą wbudowanych w serwer interfejsów SFP28. • Wymaga się od Wykonawcy konfiguracji pul dyskowych w zakresie RAID5 dla dostarczonych wraz z urządzeniem dysków twardych. • Wymaga się od Wykonawcy konfiguracji udostępnionego zasobu sieciowego przeznaczonego na magazyn kopii zapasowych tworzonych przez posiadane przez Zamawiającego oprogramowanie Acronis Backup.
Instalacja i konfiguracja urządzenia taśmowego	• Wymaga, aby Wykonawca dokonał montażu dostarczonego urządzenia taśmowego we wskazanej przez Zamawiającego szefie Rack. • Wymaga się od Wykonawcy dokonana wstępnej konfiguracji urządzenia w zakresie interfejsu zarządzania zdalnego. • Wymaga się od Wykonawcy podłączenia napędu taśmowego do dostarczonego serwera. • Wymaga się od Wykonawcy dokonania zainicjowania dostarczonych nośników LTO9 w urządzeniu.
Migracja środowiska Acronis Cyber Protect – Backup (będącego w	• Wykonawca wykona instalację serwera zarządzania Acronis Cyber Protect – Backup na dostarczonym serwerze.

posiadaniu Zamawiającego)	• Wykonawca przeniesie posiadane przez Zamawiającego licencje rozwiązania Acronis do nowo zainstalowanego serwera zarządzania. • Wykonawca wykona reinstalację agentów Acronis przenosząc ich relację zarządzania do nowego serwera Acronis. • Wykonawca dokona inwentaryzacji maszyn wirtualnych wymagających ochrony. • Wykonawca dokona konfiguracji magazynów przechowywania kopii zapasowych bazując na trzech obszarach: o Lokalne dyski serwera zarządzania. o Zasób SMB udostępniony z dostarczonej macierzy dyskowej o Urządzenie taśmowe. • Wykonawca zdefiniuje, po konsultacji z Zamawiającym plany ochrony „krótkoterminowy" i zastosuje je na zinwentaryzowanych maszynach wirtualnych. Plan ten ma przechowywać kopie zapasowe na macierzy dyskowej, a jego harmonogram ma gwarantować maksymalnie częste wykonywanie kolejnych kopii. • Wykonawca zdefiniuje, po konsultacji z Zamawiającym plany ochrony „długoterminowy" i zastosuje je na zinwentaryzowanych maszynach wirtualnych. Plan ten ma przechowywać kopie zapasowe na lokalnych zasobach serwera zarządzania oraz na napędzie taśmowym, a jego harmonogram ma gwarantować maksymalnie długie składowanie kopii zapasowych.
Instalacja interfejsów sieciowych dla serwerów produkcyjnych 1 i 2.	Wykonawca wykona instalację i konfigurację dodatkowych interfejsów sieciowych w serwerach produkcyjnych Zamawiającego.

4. Wykonawca wdroży centralny system zapisywania i przechowywania logów.

4.1. Wymagania związane z rozwiązaniem centralnego zapisywania i przechowywania logów:

4.1.1. System operacyjny powinien być na licencji Open Source.

4.1.2. Platformą sprzętowa dla rozwiązania centralnego składowania dzienników jest wirtualny serwer w środowisku Hyper-V.

4.1.3. Architektura systemu powinna bazować na komponentach o licencjonowaniu Open Source

4.1.4. Zamawiający na wyżej wymieniony cel planuje przeznaczyć serwer wirtualny o parametrach procesor (CPU) 2 rdzeni, pamięć RAM 16 GB oraz dysk twardy (HDD) 2TB.

4.1.5. Tworzenie użytkowników w systemie centralnego składowania logów może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.

4.1.6. System centralnego składowania dzienników zdarzeń powinien mieć możliwość zdefiniowania dowolnie wielu i dowolnie skonfigurowanych źródeł danych, wśród których znajdują się m.in.: Sysloga UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Konfiguracja źródeł danych powinna pozwalać na zdefiniowanie dowolnego portu komunikacji, np. Syslog UDP 514 lub/i Syslog UDP 10514.

4.1.7. System centralnego składowania dzienników zdarzeń powinien mieć możliwość ekstrakcji fragmentów wpisów logów z możliwością wykorzystania ich do filtrowania danych, budowania zapytań dla powiadomień i alarmów czy widoków w ramach dashboardów oraz ich import jak i eksport.

4.1.8. System centralnego składowania dzienników zdarzeń powinien udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trypie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV czy urządzeniach z dowolną przeglądarką WWW.

4.1.9. System centralnego składowania dzienników zdarzeń powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego.

4.1.10. System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów).

4.2. W zakresie wdrożenie proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania dzienników zdarzeń:

4.2.1. Instalacja systemu operacyjnego na wybranym przez Zamawiającego serwerze wirtualnym.

4.2.2. Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do Centralnego systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca zaproponuje rozwiązanie pozwalające na uspójnienie zegarów czasów sieci Zamawiającego.

4.2.3. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracja parametrów podstawowej pracy, w tym polityki dostępu dla informatyków Zamawiającego.

4.2.4. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktów prawnych i dobrych praktyk występujących w środowisku Zamawiającego.

4.2.5. Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły:

- (1x) Urządzenie klasy UTM firmy Stormshield,
- (10x) Przełączników zarządzalnych firmy Netgear,
- (9x) Serwery Windows,
- (3x) Serwery Linux,
- (130x) stacji roboczych Windows 10 i 11,
- (1x) Aplikację centralnego zarządzania ESET Endpoint Security, EDR,
- (3x) Serwery wirtualizacji Hyper V,
- (1x) Aplikację Axence nVision,
- (1x) System środowiskowy Vutlan,

4.2.6. Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.

4.2.7. Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.

4.2.8. Wykonanie rekonfiguracji rozwiązania Axence nVision w celu umożliwienia interakcji między rozwiązaniami, która umożliwi przesyłanie i analizę logów z wyżej wymienionego rozwiązania. Rekonfiguracja ma umożliwić pobieranie logów takich jak:

- Aktywność Administratorów w konsoli centralnego zarządzania, z klasyfikacją wykonanych czynności;
- Listę zdarzeń co do których nVision ogłasza alarm, z klasyfikacją na typ zdarzenia, istotność oraz źródło problemu;

4.2.9. Automatyzacja analizy napływających logów poprzez zbudowanie dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.

4.2.10. Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.

4.2.11. Konfiguracja wysyłania powiadomień poprzez maila lub Microsoft Teams w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.

4.2.12. Wprowadzenie informatyków Zamawiającego do obsługi wdrożonego systemu.

4.3. Asysta techniczna:

4.3.1. Zamawiający wymaga, aby Wykonawca w czasie do 12 miesięcy od wdrożenia rozwiązania zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.

4.3.2. Zamawiający wymaga, aby Wykonawca w okresie do 12 miesięcy od wdrożenia rozwiązania świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów.

4.3.3. Zamawiający wymaga, aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 16.00.

4.3.4. Zamawiający akceptuje fakt, że każda interwencja wymagać będzie od niego zgłoszenia potrzeby pomocy drogą elektroniczną, a wskazany kanał komunikacji będzie wyznaczony przez Wykonawcę, i może to być system zgłoszeń elektronicznych lub komunikacja mailowa.

4.4. Wymagania dotyczące doświadczenia wykonawcy:

4.4.1. Zamawiający wymaga, aby Wykonawca posiadał certyfikaty producenta potwierdzające ukończone szkolenia z proponowanego rozwiązania.

5. Wykonawca wdroży system nadzorowania infrastruktury IT.

5.1. Wymagania związane z rozwiązaniem klasy SIEM/XDR:

5.1.1. Zamawiający wymaga, aby system operacyjny hostujący centralną część wdrażanego rozwiązania SIEM/XDR był oparty o licencji Open Source.

5.1.2. Platformą sprzętowa dla rozwiązania SIEM/XDR jest w sieci Zamawiającego wirtualna serwer w środowisku Hyper-V o parametrach procesor (CPU) 2 rdzeni, pamięć RAM 16 GB oraz dysk twardy (HDD) 1 TB.

5.1.3. Architektura rozwiązania SIEM/XDR powinna bazować na komponentach o licencjonowaniu Open Source, której strukturę można podzielić na cztery zasadnicze części: usługę indeksowania danych, usługę analizowania danych usługę wizualizacji danych, czyli GUI do codziennej pracy oraz usługa agent monitorującego serwery i stacje robocze w sieci Zamawiającego.

5.1.4. Usługa indeksowania danych powinna wspierać osadzenie jej na serwerze z systemem Ubuntu w wersji 22.04 lub nowszym i powinna zapewnić stabilną prace przy przydzielonych parametrach 8 GB pamięci RAM i 8 rdzeniach.

5.1.5. Usługa analizowania danych powinna wspierać osadzenie jej na serwerze z systemem Ubuntu w wersji 22.04 lub nowszym i powinna zapewnić stabilną prace przy przydzielonych parametrach 4 GB pamięci RAM i 2 rdzeniach.

5.1.6. Usługa wizualizacji danych powinna wspierać osadzenie jej na serwerze z systemem Ubuntu w wersji 22.04 lub nowszym i powinna zapewnić stabilną prace przy przydzielonych parametrach 4 GB pamięci RAM i 2 rdzeniach.

5.1.7. Zamawiający wymaga, aby usługa agenta monitorującego była kompatybilna w jego środowisku z następującymi systemami:

- Windows 10 i nowszy
- Windows Server 2016 i nowszy
- Linux ContOS 6 i nowszy
- Linux Fedora 22 i nowszy
- Linux Ubuntu 12 i nowszy
- Linux Mint 22 i nowszy

5.1.8. Tworzenie użytkowników w systemie SIEM/XDR powinno odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.

5.1.9. Rozwiązanie powinno oferować możliwość analizy napływających logów zgodnie z metodyką MITRE ATT&CK w kontekście wykrywania i opisywania możliwych ataków i naruszeń.

5.1.10. Rozwiązanie powinno oferować możliwość oceny poziomu bezpieczeństwa i poprawności konfiguracji urządzeń zgodnie z metrykami CIS Control.

5.1.11. Rozwiązanie powinno oferować możliwość wykrywania konfiguracji sprzętowej urządzeń objętych monitoringiem w zakresie minimum architektury, procesora, pamięci RAM czy numeru seryjnego urządzenia.

5.1.12. Rozwiązanie powinno oferować możliwość wykrywania zainstalowanych aplikacji na urządzeniach objętych monitoringiem.

5.1.13. Rozwiązanie powinno oferować możliwość wykrywania i oceny podatności zgodnie z metodykami CVE MITRE dla systemów operacyjnych i wyrywnych aplikacji.

5.1.14. Rozwiązanie powinno pozwalać na generowanie raportów i exportu danych z każdego dostępnego w nim widoku

5.1.15. Rozwiązanie powinno pozwalać na zdefiniowanie akcji alarmowych, które mogę być wysyłana przynajmniej na mail lub komunikator MS Teams.

5.1.16. Rozwiązanie powinno zapewniać wsparcie dla realizacji regulacji prawnych w zakresie RODO, PCI DSS, HIPAA czy NIST.

5.2. W zakresie wdrożenie proponowanego rozwiązania Wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu SIEM/XDR:

5.2.1. Instalacja systemu operacyjnego będącego bazą systemu na wybranych przez Zamawiającego serwerze.

5.2.2. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracja parametrów podstawowej pracy, w tym polityki dostępu dla informatyków Zamawiającego.

5.2.3. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów polityk bezpieczeństwa Zamawiającego.

5.2.4. Konfiguracji mechanizmów powiadamiania informatyków Zamawiającego o zagrożeniach w oparciu o komunikację mail.

5.2.5. Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi monitorowania urządzeń typu serwery i stacje robocze. Zamawiający informuje, że w jego środowisku znajduję się:

- 12 x Serwer Windows
- 3 x Serwery Linux
- 130 x stacji roboczych Windows 10 i 11

5.2.6. Zdefiniowanie mechanizmów oceny konfiguracji stacji roboczych i serwerów objętych pracą agenta oraz usług osadzonych na serwerach z metrykami CIS Control.

5.2.7. Zdefiniowanie mechanizmów wykrywana podatności w zakresie systemów operacyjnych oraz aplikacji dla urządzeń z zaimplementowanym agentem zgodnie ze standardem CVE MITRE.

5.2.8. Zdefiniowanie mechanizmów wykrywania działania szkodliwego oprogramowanie, w tym Malware czy Ransomware. Mechanizm ten powinien działać w oparciu o metodyki oceny konfiguracji bezpieczeństwa monitorowanego urządzenia (SCA), „Rootchecks” czy monitoring integralności plików (FIM).

5.2.9. Zdefiniowanie mechanizmów analizy logów w oparciu o metodykę MITRE ATT&CK dla danych napływających od urządzeń z zaimplementowanym agentem.

Mechanizm powinien gwarantować opisywanie logów w kontekście taktyk i technik ataków wraz z ich klasyfikacją dla napływających danych.

5.2.10. Wykonanie korelacji danych między wdrażanym rozwiązaniem, a rozwiązaniem do centralnego systemu zapisywania i przechowywania logów.

5.3. Asysta techniczna systemu SIEM/XDR:

5.3.1. Zamawiający wymaga, aby Wykonawca w czasie do 12 miesięcy od wdrożenia rozwiązania zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.

5.3.2. Zamawiający wymaga, aby Wykonawca w okresie do 12 miesięcy od wdrożenia rozwiązania świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów.

5.3.3. Zamawiający wymaga, aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 16.00.

5.3.4. Zamawiający akceptuje fakt, że każda interwencja wymagać będzie od niego zgłoszenia potrzeby pomocy drogą elektroniczną, a wskazany kanał komunikacji będzie wyznaczony przez Wykonawcę, i może to być system zgłoszeń elektronicznych lub komunikacja mailowa.

6. Wykonawca wdroży system monitorowania o następujących wymaganiach:

6.1. System operacyjny będący bazą rozwiązania powinien być na licencji Open Source.

6.2. Platformą sprzętowa dla rozwiązania do monitoringu systemów IT jest wirtualny serwer środowiska Hyper-V w sieci Zamawiającego.

6.3. Architektura systemu powinna bazować na komponentach o licencjonowaniu Open Source

6.4. Zamawiający na wyżej wymieniony cel planuje przeznaczyć serwer wirtualny o parametrach procesor (CPU) 2 rdzeni, pamięć RAM 16 GB oraz dysk twardy (HDD) 1TB.

6.5. W zakresie monitorowania infrastruktury Zamawiającego wymaga się od rozwiązania, aby:

6.5.1. Rozwiązanie powinno pozwalać na dodanie do niego nielimitowanej liczny obiegów, czyli monitorowanych urządzeń na podstawie ich adresu IP.

6.5.2. Rozwiązanie powinno pozwalać na monitorowanie serwerów fizycznych i wirtualnych (Windows, Linux/Unix).

6.5.3. Rozwiązanie powinno pozwalać na monitorowanie urządzeń sieciowych (routery, przełączniki, firewalle) poprzez protokoły standardowe (min. SNMP v1/v2c/v3).

6.5.4. Rozwiązanie powinno pozwalać na monitorowanie usług sieciowych (HTTP/HTTPS, SMTP, DNS, FTP, SSH, RDP, itp.).

6.5.5. Rozwiązanie powinno pozwalać na monitorowanie baz danych (w tym MS SQL, PostgreSQL, MySQL).

6.5.6. Rozwiązanie powinno pozwalać na monitowanie parametrów systemowych, tj. CPU, pamięć RAM, przestrzeń dyskowa, I/O, interfejsy sieciowe, procesy i usługi systemowe.

6.5.7. Rozwiązanie powinno pozwalać na obsługę monitoringu poprzez: agentów instalowanych na hostach Windows oraz Linux, metody bezagentowe (SNMP, WMI, SSH, API).

6.5.8. Rozwiązanie powinno oferować możliwość monitorowania urządzeń poprzez linkowanie (stosowanie) gotowych wzorców monitorowania, a same wzorce powinny dawać możliwość ich korekty, edycji czy też tworzenia własnych wzorców.

6.6. W zakresie interfejsu i raportowania rozwiązanie powinno:

6.6.1. Oferować zarządzanie procesem monitorowania infrastruktury Zamawiającego w oparciu o przeglądarkę WWW, bez konieczności instalowania na stacjach roboczych żadnych dodatkowych aplikacji do zarządzania.

6.6.2. Tworzenie użytkowników w systemie monitorowania systemów IT może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.

6.6.3. Zapewnić dostęp wielopoziomowy na bazie ról i uprawnień.

6.6.4. Oferować możliwość tworzenia nieskończenie wielu pulpitów nawigacyjnych, czyli tzw. dashboardów operatorskich. A wspomniane dashboardy powinny mieć możliwość automatycznego przełączania widoków w ramach kolejnych widoków grupowanych w nim.

6.6.5. Oferować generowanie raportów okresowych (PDF/CSV).

6.6.6. Zapewnić wizualizację danych historycznych (wykresy, trendy) dla każdego z monitorowanych szablonami obszarów.

6.6.7. Oferowane rozwiązanie powinno pozwalać na dynamiczną zmianę wersji językowej, bazując na zaimplementowanych wersjach językowych w systemie operacyjnych platformy na jakiej działa rozwiązanie. Wymagane jest minimum zapewnienie polskiej i angielskiej wersji językowej.

6.7. Wymaganie niefunkcjonalne oczekiwane w rozwiązaniu to:

6.7.1. System musi być rozwiązaniem rozwijanym i wspieranym przez producenta lub społeczność Open Source.

6.7.2. Musi posiadać dokumentację techniczną w języku polskim lub angielskim.

6.7.3. Musi umożliwiać aktualizację bez utraty konfiguracji.

6.7.4. Musi umożliwiać przechowywanie danych historycznych przez minimum 24 miesiące (przy odpowiedniej konfiguracji zasobów).

6.7.5. System musi wspierać minimum 1000 monitorowanych hostów (z możliwością rozbudowy).

6.7.6. System musi być rozwiązaniem skalowalnym i umożliwiać architekturę rozproszoną (serwer centralny + proxy/sondy zdalne) w razie przyszłej rozbudowy o jednostki podległe Zamawiającemu.

6.7.7. Obsługiwać szyfrowanie komunikacji między komponentami.

6.8. W zakresie wdrożenia proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu monitorowania infrastruktury IT:

6.8.1. Instalacja systemu operacyjnego na wybranym przez Zamawiającego serwerze lub maszynie wirtualnej.

6.8.2. Weryfikacja źródła czasu na wszystkich urządzeniach/systemach objętych monitorowaniem. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca zaproponuje rozwiązanie pozwalające na uspójnienie zegarów czasów sieci Zamawiającego.

6.8.3. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracja parametrów podstawowej pracy, w tym polityki dostępu dla informatyków Zamawiającego.

6.8.4. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktów prawnych i dobrych praktyk występujących w środowisku Zamawiającego.

6.8.5. Zarejestrowanie w rozwiązaniu wykazu urządzeń z sieci IT Zamawiającego (na podstawie otrzymanej na wdrożeniu listy urządzeń (Nazwa urządzenia, Typ urządzenia, Adres IP). Zamawiający wymaga, aby w zakresie minimalnym prace objęły rejestrację urządzeń w zakresie:

- (1x) Urządzenie klasy UTM firmy Stormshield
- (10x) Przełączniki zarządzalne firmy Netgear
- (9x) Serwery Windows
- (3x) Serwery Linux
- (130x) stacji roboczych Windows 10 i 11
- (3x) Serwery wirtualizacji Hyper V

6.8.6. Zdefiniowanie monitoringu dla wskazanej infrastruktury poprzez dopasowanie odpowiednich szablonów monitorowania, a w przypadku ich braku dokonania analizy i opracowania wzorców monitoringu.

6.8.7. Wykonanie analizy napływających z monitoringu danych i opracowanie widoków analitycznych (pulpitów nawigacyjnych poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i/lub graficznej. Wykonanie analizy napływających z monitoringu danych i opracowanie widoków analitycznych (pulpitów nawigacyjnych prezentujących dane w postaci tabelarycznej i/lub graficznej. Zamawiający wymaga zaprojektowania pulpitów nawigacyjnych tematycznych oraz minimum jednego zbiorczego pulpitu, który będzie wyświetlany 24/7 w pomieszczeniu informatyków na posiadanych przez Zamawiającego ekranie.

6.8.8. Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych danych pomiarowych.

6.8.9. Konfiguracja wysyłania powiadomień poprzez maila lub Microsoft Teams w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.

6.8.10. Szkolenie pracowników informatyków Zamawiającego z zarządzania i administracji wdrożonym rozwiązaniem do monitoringu systemów IT.

6.9. Asysta techniczna:

6.9.1. Zamawiający wymaga, aby Wykonawca w czasie do 12 miesięcy od wdrożenia rozwiązania zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.

6.9.2. Zamawiający wymaga, aby Wykonawca w okresie do 12 miesięcy od wdrożenia rozwiązania świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów.

6.9.3. Zamawiający wymaga, aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 16.00.

6.9.4. Zamawiający akceptuje fakt, że każda interwencja wymagać będzie od niego zgłoszenia potrzeby pomocy drogą elektroniczną, a wskazany kanał komunikacji będzie wyznaczony przez Wykonawcę, i może to być system zgłoszeń elektronicznych lub komunikacja mailowa.

7. Wykonawca przeprowadzi Testy dostarczonego i wdrożonego środowiska kopii zgodnie z przedstawioną koncepcją oraz ogólnymi założeniami przestawionymi poniżej.

7.1. Wykonawca wykona kopię zapasową każdej chronionej maszyny wirtualnej, w ramach każdego ze zdefiniowanych planów i dla każdego z magazynów kopii.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

7.2. Wykonawca wykona testowe odtworzenie każdej utworzonej w czasie testu kopii zapasowej. Odtworzenie musi być wykonane albo poza godzinami pracy urzędu albo w sposób niekolizyjny dla produkcyjnych maszyn Zamawiającego.

8. Wykonawca przeprowadzi Szklenia dla informatyków Starostwa powiatowego w Ciechanowie, obejmujące wszystkie dostarczone i wdrożone elementy.
9. Wykonawca przygotuje dokumentację powykonawczą środowiska kopii bezpieczeństwa.

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl