

„Dostawa sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina”

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu komputerowego i oprogramowania w ramach projektu grantowego „Cyfrowa Gmina” - Dostawa specjalistycznego oprogramowania do wykonania kopii zapasowych wraz z wdrożeniem

Wymagania ogólne:

1. Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowiło naruszenia majątkowych praw autorskich osób trzecich.
2. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem nowym to znaczy nigdy nie używanym, nie aktywowanym przez innego użytkownika w wersji aktualnej na dzień poprzedzający dzień składania ofert.
3. Dla zaoferowanego oprogramowania należy dostarczyć: licencje, nośniki instalacyjne oraz instrukcje obsługi.
4. Zamawiający wymaga by dostarczone licencje były wystawione na użytkownika końcowego, którym jest Urząd Miejski w Czarnej Białostockiej.
5. Miejscem świadczenia usług gwarancyjnych jest siedziba Urzędu Miejskiego w Czarnej Białostockiej ul. Torowa 14A, 16-020 Czarna Białostocka.

Elementy składowe Części II zamówienia	ilość
Oprogramowanie do backupu	1
Usługa backupu do chmury	1

ROZWIĄZANIE BACKUPU

Nazwa zaproponowanego rozwiązania backupu:

.....

.....

.....

Powyższa nazwa rozwiązania backupu powinna zawierać wszystkie nazwy produktów składowych i oprogramowania. W nazwach rozwiązania i częściach składowych rozwiązania proszę wypisać dla każdego oprogramowania: nazwę producenta, nazwę oprogramowania, rodzaj licencji, ilość licencji, lub inne istotne parametry i opisy.

Zakup i wdrożenie rozwiązania backupu realizowane jest przez Urząd Miejski w Czarnej Białostockiej w celu zabezpieczenia posiadanych systemów, zminimalizowania ryzyka utraty ciągłości działania wywołanymi awariami oraz szybkiego przywrócenia do działania kluczowych systemów po katastrofie.

Zawartość opracowania:

- I. Opis przedmiotu zamówienia, minimalnych i opcjonalnych funkcji.
- II. Cel wdrożenia.
- III. Opis infrastruktury.
- IV. Domyślna konfiguracja backupu (harmonogramy backupu).

- V. Projekt i harmonogram wdrożenia.
- VI. Czynności wdrożeniowe.
- VII. Szkolenie i dokumentacja powdrożeniowa.

I. Opis przedmiotu zamówienia, minimalnych i opcjonalnych funkcji

1.	Akceptowalny poziom utraty danych (RPO) oraz czas przywrócenia po awarii (RTO)	Rozwiązanie backupowe powinno być zgodne z poniżej zdefiniowanymi maksymalnymi parametrami RTO (Recovery Time Objective) i RPO (Recovery Point Objective). RTO definiuje czas w jakim należy przywrócić procesy po wystąpieniu awarii. RPO definiuje akceptowalny poziom utraty danych wyrażony w czasie. <u>Systemy krytyczne:</u> ▪ RTO – 6 godziny ▪ RPO – 4 godziny <u>Dla pozostałych systemów:</u> ▪ RTO – 10 godzin ▪ RPO – 12 godzin Aby zachować wymagane poziomy RTO i RPO Wykonawca musi uwzględnić posiadaną przez Zamawiającego infrastrukturę teleinformatyczną. Struktura i wielkość infrastruktury teleinformatycznej Zamawiającego została opisana w rozdziale III – opis infrastruktury. Zamawiający dopuszcza odtwarzanie równoległe większej ilości systemów, jednak obciążenie nie powinno wpłynąć na działanie pracujących systemów produkcyjnych np. usług AD, serwera plików,
----	--	--



		serwerów aplikacji i baz danych.
2.	Licencje i platforma sprzętowa	Wykonawca dostarczy wszelkie licencje niezbędne do uruchomienia rozwiązania backupu. Platforma sprzętowa Zamawiającego: a) serwer – specyfikacja zawarta w Części I SWZ. b) serwer NAS – specyfikacja zawarta w Części I SWZ.
3.	Wirtualizacja	Oprogramowanie musi backupować środowisko Hyper-V, tj. wykonywać kopię maszyn wirtualnych pracujących w środowisku produkcyjnym Zamawiającego bez przerywania ich działania zachowując zdefiniowane RTO i RPO. Opis środowiska teleinformatycznego do backupu znajduje się w rozdziale III – opis infrastruktury.
4.	Obsługiwane systemy operacyjne	Oprogramowanie powinno oferować backup serwerów fizycznych, wirtualnych oraz stacji roboczych pracujących pod systemami operacyjnymi, co najmniej: a) Windows Server w wersjach co najmniej: 2008 R2, 2012 R2, 2016, 2019; b) Centos w wersjach co najmniej 6.5; c) Debian 10 d) Windows 10 Pro
5.	Agenci	Backup środowiska wirtualnego powinien odbywać się bez wykorzystania agentów. Zamawiający dopuszcza zastosowanie agentów dla serwerów fizycznych, stanowisk komputerowych pracowników (desktopów i notebooków) oraz do zaawansowanego backupu (od wewnątrz) serwerów wirtualnych, baz danych, serwerów pocztowych oraz środowiska Active Directory.

6.	Backup	a) Rozwiązanie backupowe musi realizować procesy backupu oraz odzyskiwania danych; b) Rozwiązanie backupowe musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów; c) Rozwiązanie backupowe musi zapewniać funkcjonalność automatycznego raportowania i powiadamiania administratora (mail) w zakresie statusu wykonywanych zadań backupowych oraz informacji o przyczynach w przypadku nieudanych zadań backupowych. d) Rozwiązanie backupowe musi umożliwić uruchomienie co najmniej 4 maszyn wirtualnych bezpośrednio ze zdeduplikowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych. Zamawiający dopuszcza realizację tej funkcjonalności poprzez dostarczenie urządzenia (storage - NAS) duplikującego; e) Rozwiązanie backupowe musi pozwalać na migrację on-line uruchomionych z backupu (w powyższy sposób) maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w Hyper-V. Jeżeli licencja na Hyper-V nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami; f) Rozwiązanie backupowe musi mieć możliwość odtworzenia plików z kopii bezpośrednio do maszyny wirtualnej; g) Rozwiązanie backupowe musi posiadać zintegrowane w systemie mechanizmy indeksowania i wyszukiwania plików. h) Rozwiązanie backupowe musi granularnie odzyskiwać dane, w tym pojedynczych plików z backupów całych systemów i maszyn, tj. wymieniony mechanizm nie może wymagać pełnego odtworzenia maszyny wirtualnej ani jej uruchomienia;
----	--------	---

		i) Rozwiązanie backupowe musi posiadać wbudowany mechanizm tworzenia kopii otwartych plików na platformie Windows i Linux; j) Rozwiązanie backupowe musi wspierać funkcjonalność odtwarzania fizycznego serwera do środowiska wirtualnego, minimum: dla serwera Windows do środowiska Hyper-V; k) Rozwiązanie backupowe musi potrafić przetwarzać kilka wirtualnych dysków jednocześnie; l) Rozwiązanie backupowe musi wspierać mechanizm CBT (Change Block Tracking) minimum dla Hyper-V; m) Oprogramowanie do backupu musi być dostępne w języku polskim lub angielskim.
7.	Kształtowanie pasma (OPCJONALNE, DODATKOWO PUNKTOWANE)	Dla dowolnego transferu danych z klienta lub zadania backupowego musi istnieć możliwość definiowania/ograniczania pasma dla transferu danych
8.	Backup do środowisk chmurowych (OPCJONALNE, DODATKOWO PUNKTOWANE)	Rozwiązanie backupowe musi umożliwiać pełne odtworzenie maszyny wirtualnej bezpośrednio do środowiska chmurowego.
9.	Przenoszenie backupu do środowisk chmurowych (OPCJONALNE, DODATKOWO PUNKTOWANE)	Rozwiązanie backupowe musi umożliwiać przenoszenie zdeduplikowanych kopii do środowiska chmurowego. Przenoszone dane w zakresie komunikacji i składowania danych muszą podlegać szyfrowaniu.
10.	Przeszukiwanie zbackupowanych plików (OPCJONALNE, DODATKOWO PUNKTOWANE)	Rozwiązanie backupowe musi przeszukiwać zbackupowane dane, w tym również wewnątrz plików, co najmniej dla: MS Office (minimum dla rozszerzeń plików: DOC, DOCX, PPT, PPTX, XLS, XLSX), PDF przeszukiwalny, plików tekstowych.
11.	Usługa backupu do chmury (OPCJONALNE, DODATKOWO PUNKTOWANE)	Wykonawca dostarczy rozwiązanie oparte o chmurę jako dodatkowe miejsce na przechowywania kopii baz danych systemów krytycznych poza głównym miejscem przetwarzania danych.



		Rozwiązanie musi zapewniać minimum: a) przechowywanie wszystkich plików w postaci zaszyfrowanej (dokumenty, kopie baz danych), b) automatyczny backup zgodnie z ustalonym harmonogramem, c) co najmniej 500 GB miejsca na backup, d) dostęp do panelu kontrolnego
12.	Backup środowiska Active Directory	Rozwiązanie backupowe musi umożliwiać wykonanie kopii Active Directory bez przerywania jego działania.
13.	Deduplikacja	a) Rozwiązanie backupowe musi przechowywać jedynie unikalne bloki danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych; b) Deduplikacja blokowa musi obejmować dane backupowane; c) Deduplikacja musi odbywać się na źródle i na celu. Zamawiający dopuszcza również stosowanie deduplikacji globalnej tylko na źródle. d) Rozwiązanie backupowe musi pozwalać na instalację bazy deduplikacyjnej indeksów w układzie wysokiej dostępności (minimum na dwóch serwerach) w taki sposób, aby awaria pojedynczego serwera nie powodowała utraty możliwości deduplikacji i odtwarzania danych. Zamawiający dopuszcza rozwiązanie równoważne zapewniające wysoki poziom dostępności i bezawaryjności działania rozwiązania deduplikacyjnego. W ramach tego postępowania Zamawiający nie wymaga dostarczenia drugiego urządzenia. e) włączenie mechanizmów deduplikacji nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji;



14.	Bezpieczeństwo	a) Komunikacja pomiędzy składnikami (np. replikacja pomiędzy serwerami backupu) rozwiązania backupowego musi być szyfrowana (np. https); b) Wysyłanie danych zbackupowanych (także zdeduplikowanych) pomiędzy serwerami backupu (site-to-site replication lub site-to-cloud replication) musi odbywać się minimum na poziomie AES 256-bit; c) Komunikacja pomiędzy agentem a serwerem rozwiązania backupowego musi być szyfrowana (np. AES)
15.	Delegacja uprawnień (OPCJONALNE, DODATKOWO PUNKTOWANE)	Rozwiązanie backupowe musi zapewniać elastyczne delegowanie uprawnień oraz audytowanie działań użytkowników. Z tym, że delegowanie uprawnień musi pozwalać na przydział uprawnień per serwer czy per grupa serwerów, przydział uprawnień musi pozwalać na definiowanie uprawnień dla lokalnej bazy użytkowników systemu backupowego lub grup użytkowników z domeny AD.
16.	Dwuetapowe uwierzytelnianie (OPCJONALNE, DODATKOWO PUNKTOWANE)	Rozwiązanie backupowe musi pozwalać na skonfigurowanie mechanizmu dwuskładnikowego uwierzytelniania – do uruchomienia konsoli administracyjnej systemu backupowego potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod (OTP) wysyłany do administratora np. poprzez mail, sms, czy aplikację w telefonie komórkowym generującą OTP.
17.	Automatyczne sprawdzanie backupu (OPCJONALNE, DODATKOWO PUNKTOWANE)	Zaproponowane rozwiązanie musi umożliwiać warianty: I lub II weryfikacji poprawności wykonania zadań backupowych: Wariant I. a) Stworzenie laboratorium (izolowanego środowiska) dla Hyper-V używając wbudowanych mechanizmów dla uruchomienia wirtualnych maszyn bezpośrednio z backupu lub w przypadku zaoferowania urządzenia duplikującego Zamawiający dopuszcza uruchamianie maszyn na urządzeniu deduplikującym; b) Weryfikację z dowolnego backupu kilku maszyn wirtualnych jednocześnie w izolowanym



		środowisku Hyper-V lub na zaproponowanym urządzeniu według zdefiniowanego harmonogramu; c) Testowanie działania baz danych; d) Uruchamianie skryptów (np. odczytanie rekordu z bazy, otwarcie pliku, uruchomienie programu) testujących poprawność backupu; e) Wysyłanie na adres e-mail raportu podsumowującego przebieg testów (wszystkich lub grupy maszyn wirtualnych); f) Wysłanie na adres e-mail szczegółowego raportu o niepoprawności odtworzenia backupu; Zamawiający dopuszcza, aby Wykonawca dostarczył rozwiązanie sprzętowe do odtwarzania backupu spełniające powyższe wymagania. Zamawiający dopuszcza, aby urządzenie duplikujące mogło być wykorzystane do odtwarzania i sprawdzania backupu. Wariant II. Dostarczony system backupu będzie wykonywał auto-weryfikację wykonania każdego z zadań backupowych i zadań odtwarzania potwierdzonego odpowiednim Raportem składowanym w systemie. System backupu dla funkcji modułu sprawdzającego / raportującego musi być zdolny do wysłania odpowiedniego powiadomienia email do administratora systemu backupowego. Baza Raportów o statusie wykonania zadań backupu lub zadania przywracania powinna mieć filtry wyszukiwania: po harmonogramie lub źródle backupu; po czasie (od daty lub z przedziału czasu) Automatyczne sprawdzanie backupu zweryfikuje poprawność wykonania backupu oraz sprawdzenie czy wirtualny serwer nie ma błędów uniemożliwiających jego uruchomienie lub działanie po restarcie.
18.	Archiwizacja zaawansowana (OPCJONALNE, DODATKOWO)	Rozwiązanie backupowe realizuje archiwizację jako proces przenoszenia zasobów plikowych lub pocztowych do archiwum (repozytorium dyskowe) z pozostawieniem skrótów lub bez ich



	PUNKTOWANE)	pozostawiania.
19.	Indeksowanie pełnotekstowe (OPCJONALNE, DODATKOWO PUNKTOWANE)	Rozwiązanie backupowe musi umożliwić pełno tekstowe indeksowanie treści danych dla wybranych typów plików, indeksacja musi odbywać się dla danych znajdujących się już w systemie, co najmniej dla: MS Office (minimum dla rozszerzeń plików: DOC, DOCX, PPT, PPTX, XLS, XLSX), PDF przeszukiwalny, plików tekstowych.
20.	Raportowanie	a) Rozwiązanie backupowe musi mieć wbudowane predefiniowane zestawy alarmów którymi administrator może zarządzać i wskazywać do kogo i jakich okolicznościach będą wysyłane. b) Rozwiązanie backupowe musi mieć rozbudowany system powiadamiania o zdarzeniach poprzez e-mail; c) Rozwiązanie backupowe musi mieć rozbudowany system raportowania dla administratorów, przy czym minimalny zestaw dostępnych raportów dot. działania rozwiązania backupu powinien zawierać: wykorzystanie licencji, wykonanie zadań backupowych, działanie serwera, działanie bazy danych, bazy indeksów, bazy deduplikacji i replikacji; d) Rozwiązanie backupowe musi mieć możliwość wysyłania raportów wg harmonogramu dla określonych grup serwerów; e) Rozwiązanie backupowe musi mieć możliwość automatycznego zapisywania raportów w jednym z formatów: PDF; CSV; HTML; f) Rozwiązanie backupowe musi mieć możliwość generowania / wysyłania alertów per zadanie backupowe lub zadanie odtwarzania danych Rozwiązanie backupowe musi mieć możliwość wysyłania alertów minimum poprzez mail.
21.	Centralna konsola	Rozwiązanie backupowe powinno posiadać jedną konsolę do administracji i zarządzania wszystkimi opisanymi funkcjonalnościami.



22.	Backup końcówek	a) Rozwiązanie backupowe musi obsługiwać co najmniej następujące systemy: Windows 10 PRO 32bit/64bit; b) Rozwiązanie backupowe musi zapewniać backup laptopów i desktopów; c) Dla backupu laptopów i desktopów system backupowy musi umożliwić skonfigurowanie zadania backupowego, tak by było wykonane w przedziale czasowym w czasie gdy dana laptop / desktop jest w zasięgu systemu backupowego lokalnie lub zdalnie w oddziale (oddział i centrala połączone site-to-site VPN lub dedykowany/prywatny WAN). d) Rozwiązanie backupowe musi oferować konsolę odzyskiwania dla wyznaczonego / uprawnionego użytkownika któremu uprawnienia nadał administrator główny. e) Z konsoli odzyskiwania administrator/użytkownik powinien móc odzyskać dowolne pliki umiejscowione na serwerze plików do których posiada zdefiniowany dostęp (pliki z dysków sieciowych oraz z przekierowanych folderów); Zamawiający posiada 47 szt. komputerów posiadających w sumie ok. 1 TB danych.
23.	Gwarancja i wsparcie techniczne	Dostarczone rozwiązanie backupowe musi być objęte co najmniej 36 - miesięczną gwarancją i wsparciem technicznym producenta urządzenia/oprogramowania obejmującym wszystkie jego elementy. Zamawiający wymaga aby wsparcie techniczne było świadczone na następującym poziomie: a) Nieograniczony dostęp (24 godziny na dobę, 7 dni w tygodniu) do dedykowanej przez producenta urządzenia strony www pozwalający na uzyskanie pomocy technicznej, wykonywanie aktualizacji dostarczonego oprogramowania, b) Nieograniczony dostęp (24 godziny na dobę, 7 dni w tygodniu) do wsparcia producenta drogą telefoniczną,

II. Wdrożenie

Celem wdrożenia systemu do backupu jest zabezpieczenie posiadanego przez Zamawiającego środowiska, rozwiązaniem backupowym umożliwiającym wykonanie kopii danych oraz odtworzenie danych z zabezpieczonych serwerów oraz stacji roboczych użytkowników w przypadku wystąpienia awarii lub potrzeby cofnięcia się do konkretnego (wcześniejszego) punktu wykonywania backupu. Zakłada się, że system backupowy zabezpieczy środowisko informatyczne Zamawiającego w zakresie:

- a) Zabezpieczenia wszystkich danych z posiadanych serwerów Windows i Linux oraz wybranych/wskazanych zasobów stacji roboczych z systemem operacyjnym Windows;
- b) Zabezpieczenia aplikacji i baz danych, w szczególności Active Directory;
- c) Zabezpieczenia maszyn wirtualnych;
- d) Zabezpieczenia fizycznych serwerów z systemem Windows Server oraz Hyper-V Server;
- e) Możliwości zabezpieczenia w przyszłości uruchomionych i eksploatowanych serwerów i stacji roboczych.

Wdrożenie powinno być zrealizowane przez certyfikowanego informatyka (posiadającego certyfikaty producenta rozwiązania) w obsłudze, konfiguracji i administrowaniu zaproponowanym rozwiązaniem backupowym. Zamawiający dopuszcza możliwość pracy zdalnej pracowników Wykonawcy w zakresie uzgodnionym z Zamawiającym.

Realizowane przez Wykonawcę czynności podczas wdrożenia nie powinny wpłynąć negatywnie na działanie środowiska Zamawiającego w godzinach pracy urzędu. Zadania czynności mające wpływ na systemu produkcyjne powinny być wykonywane wg zaplanowanych działań i zgłoszone do administratora tych systemów. Wykonawca zobowiązany jest do natychmiastowego usunięcia negatywnych skutków czynności wdrożeniowych.

III. Opis infrastruktury



1.	Lokalizacje i godziny pracy	Lokalizacje: a) 16-020 Czarna Białostocka, ul. Torowa 14A b) 16-020 Czarna Białostocka, ul. Torowa 9 Godziny pracy Zamawiającego: ▪ 7.30 – 15.30 Zamawiający dopuszcza aby prace wymagające zatrzymania środowiska produkcyjnego odbywały się poza godzinami pracy Zamawiającego.
2.	Łącza Internetowe	Lokalizacje: a) 16-020 Czarna Białostocka, ul. Torowa 14A - 100/100Mb b) 16-020 Czarna Białostocka, ul. Torowa 9 – 100/100Mb Obie lokalizacje połączone są ze sobą Tunelem VPN
3.	Serwery fizyczne i przestrzeń dyskowa	a) Serwer Actina Solar – Windows serwer 2008 R2 – przestrzeń dyskowa 400GB (zajętość 166GB), 2 maszyny wirtualne b) Serwer HP Prolinat 350e – Windows Serwer 2012 R2 – przestrzeń dyskowa 420GB (zajętość 245GB), c) Serwer Dell R330 – Windows Serwer Hyper-V 2019 core – przestrzeń dyskowa 1,6TB (zajętość 334GB) , 4 maszyny wirtualne



4.	Stacje robocze i przestrzeń dyskowa	Zamawiający posiada 47 szt. komputerów posiadających w sumie ok. 1 TB danych.
----	-------------------------------------	---

IV. Domyślna konfiguracja backupu

1.	Harmonogram backupu.	Podany poniżej harmonogram backupu jest ustawieniem domyślnym. Zamawiający zastrzega sobie możliwość modyfikacji poniższych harmonogramów po przygotowaniu przez Wykonawcę projektu backupu. Domyślny harmonogram backupu: a) kopie dzienne (pn, wt, śr, cz, pt) wykonywane raz dziennie i przechowywane 5 dni b) kopie tygodniowe wykonywane pierwszego dnia tygodnia i przechowywane przez 4 tygodnie c) kopie miesięczne wykonywane ostatniego lub pierwszego dnia miesiąca i przechowywane przez 2 miesiące d) kopie roczne wykonywane ostatniego lub pierwszego dnia roku i przechowywane przez 2 lata
2.	Systemy krytyczne (kluczowe)	Lista systemów krytycznych wraz z podanymi szacowanymi obecnymi wielkościami: a) Środowisko domenowe Windows Server (ok. 0,1 TB) b) System FK, Kadrowo-Płacowy QNT (ok. 0,1 TB) c) System elektronicznego obiegu dokumentów EZD (ok. 0,5 TB)



		d) System FISKUS (ok. 0,2 TB) Pozostałe systemy serwerowe z maszynami Windows i Linux (ok. 0,5 TB)
--	--	--

V. Projekt i harmonogram wdrożenia.

1.	Projekt	Wykonawca przygotuje i przedstawi koncepcję wdrożenia backupu dla środowiska Zamawiającego z uwzględnieniem wymaganych funkcjonalności oraz wszystkich lokalizacji. Projekt musi zawierać schemat backupu środowiska we wszystkich lokalizacjach; Wszelkie czynności wynikające z projektu powinny znaleźć się w harmonogramie prac. Termin dostarczenia projektu backupu powinien zostać ustalony między Wykonawcą a Zamawiającym na etapie akceptacji harmonogramu prac.
2.	Harmonogram prac	Wykonawca we współpracy z Zamawiającym przedstawi najpóźniej w ciągu 10 dni roboczych, liczonych od daty podpisania Umowy, szczegółowy harmonogram wdrożenia. Wstępną propozycję harmonogramu Zamawiający otrzyma nie później niż 5 dni roboczych od daty podpisania Umowy. Zamawiający może zgłosić uwagi do wstępnej propozycji harmonogramu oraz harmonogramu ostatecznego w ciągu 3 dni od dnia otrzymania. Harmonogram powinien zawierać wszelkie wymagane we wdrożeniu czynności wraz z podziałem na czynności należące do Wykonawcy i Zamawiającego. Zamawiający deklaruje, iż może zrealizować następujące czynności: a) konfigurację sieci LAN i WAN w infrastrukturze Zamawiającego (switchy, UTM); b) konfigurację serwera NAS – specyfikacja zawarta w Części I SWZ.

		c) konfigurację backupu do chmury
--	--	-----------------------------------

VI. Czynności wdrożeniowe

1.	Instalacja i konfiguracja systemu backupowego	Wykonawca skonfiguruje oprogramowanie zaproponowanego rozwiązania backupowego. Wykonawca wykona niezbędną do działania rozwiązania backupowego konfigurację NAS, oraz oprogramowania backupowego. Jeżeli będzie taka potrzeba Wykonawca dokona modyfikacji konfiguracji już istniejącego sprzętu i oprogramowania znajdującego się u Zamawiającego.
2.	Lokalizacje backupów	Zamawiający przekaze Wykonawcy informacje do projektu o planowanych przez niego lokalizacjach backupów po podpisaniu umowy.
3.	Zadania backupowe	Wykonawca skonfiguruje zadania backupowe zgodnie z harmonogramem backupu, z rozdziału IV, dla poszczególnych systemów.
4.	Testowanie backupów	Wykonawca wykona konfigurację pozwalającą na: a) Testowe wykonanie backupów według ustalonego harmonogramu; b) Wysłanie raportu na maila do wskazanej grupy administratorów o niepowodzeniu zadania backupowego; c) Wysłanie raz dziennie zbiorczego raportu o stanie systemu backupowego; Test backupu środowisk wirtualizacji powinien obejmować co najmniej:

		a) Poprawność uruchomienia się wirtualnej maszyny; b) Dostępność ważnych dla niej usług; c) Odczytanie rekordu z bazy danych; d) Sprawdzenie dostępności maszyny z zewnątrz; Testy mogą być realizowane poprzez przygotowane przez Wykonawcę skrypty.
5.	Raportowanie	Wykonawca przygotowuje co najmniej następujące raporty i alerty: a) Raport wykonania zadań backupowych - raport generowany raz dziennie musi zawierać podsumowanie wszystkich zadań backupowych; b) Alert informujący o problemach z rozwiązaniem backupu – alert wysyłany niezwłocznie po wykryciu problemu;
6.	Przetestowanie poprawności działania systemu backupowego	a) Wykonawca przetestuje poprawność działania zaimplementowanej polityki backupowej poprzez odtworzenie kilku wybranych (min. 2) maszyn wirtualnych; b) Wykonawca przetestuje odtworzenie Microsoft Active Directory;

VII. Szkolenie i dokumentacja powdrożeniowa.

1.	Szkolenie powdrożeniowe	Wykonawca w ramach wdrożenia przeprowadzi minimum 8 godzinne (realizowane w 1 lub 2 dni) szkolenie dla administratora Zamawiającego z wdrożonego rozwiązania do backupu, które obejmie swoim zakresem przedstawienie wszystkich wdrożonych funkcjonalności. Szkolenie powinno być przeprowadzone na koniec wdrożenia. Wykonawca może skorzystać z wdrożonego środowiska lub przygotować samodzielnie
----	-------------------------	--



		laboratorium (wirtualne maszyny). Szkolenie powinno być przeprowadzone przez certyfikowanego informatyka. Zamawiający zapewni salę szkoleniową wyposażoną w projektor, sieć i komputer. Termin szkolenia musi zostać uzgodniony z Zamawiającym, w ramach uzgodnionego harmonogramu.
2.	Dokumentacja	Dokumentacja powdrożeniowa musi zawierać: a) Opis/charakterystykę wdrożonego środowiska; b) Listę elementów składowych systemu backupu; c) Schemat backupu środowiska we wszystkich lokalizacjach; d) Dane administracyjne i ustawienia podstawowe systemu; e) Opis Konfiguracji wdrożenia systemu backupu; f) Procedury konfiguracji zadań backupowych oraz harmonogramów; g) Procedury w zakresie odtwarzania/przywracania zasobów z backupu; h) Procedury w zakresie administracji rozwiązaniem; i) Procedury w zakresie monitorowania i diagnostyki rozwiązania backupu; j) Procedury w zakresie kontaktu z serwisem, trybu zgłaszania problemów oraz obsługi zgłoszeń serwisowych. Wszelkie przygotowane dokumenty muszą być w języku polskim. Dokumenty powinny zawierać schemat rozwiązania backupowego z danymi sieciowymi, hasłami oraz innymi danymi kluczowymi do administrowania rozwiązaniem backupu. Dokumentacja powinna zostać dostarczona w formie papierowej (podpisana przez wykonawcę) i w edytowalnej formie elektronicznej (dokument docx).

Funkcjonalności dodatkowo punktowane

Lp.	Punkt w opisie przedmiotu zamówienia	Nazwa punktu
-----	--	--------------

1.	7	Kształtowanie pasma (OPCJONALNE, DODATKOWO PUNKTOWANE)
2.	8	Backup do środowisk chmurowych (OPCJONALNE, DODATKOWO PUNKTOWANE)
3.	9	Przenoszenie backupu do środowisk chmurowych (OPCJONALNE, DODATKOWO PUNKTOWANE)
4.	10	Przeszukiwanie zbackupowanych plików (OPCJONALNE, DODATKOWO PUNKTOWANE)
5.	11	Usługa backupu do chmury (OPCJONALNE, DODATKOWO PUNKTOWANE)
6.	15	Delegacja uprawnień (OPCJONALNE, DODATKOWO PUNKTOWANE)
7.	16	Dwuetapowe uwierzytelnianie (OPCJONALNE, DODATKOWO PUNKTOWANE)
8.	17	Automatyczne sprawdzanie backupu (OPCJONALNE, DODATKOWO PUNKTOWANE)
9.	18	Archiwizacja zaawansowana (OPCJONALNE, DODATKOWO PUNKTOWANE)
10.	19	Indeksowanie pełnotekstowe (OPCJONALNE, DODATKOWO PUNKTOWANE)



Rzeczpospolita
Polska



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego

