

Załącznik nr 1 do SWZ

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.

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.

I. Wymagania systemu do wykonywania kopii zapasowych (lub równoważne):**Ogólne:**

1. Oprogramowanie może być dostarczane w dwóch scenariuszach:
 - 1) Cloud(Software as Service),
 - 2) On-premise.
2. Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud.
3. Interfejs systemu dostępny jest w języku:
 - 1) polskim,
 - 2) angielskim,
4. Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych,
5. Oprogramowanie może być uruchomione w kontenerze docker,
6. Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:
 - 1) Debian: 9+
 - 2) Ubuntu: 16.04+
 - 3) Fedora: 29+
 - 4) CentOS: 7+
 - 5) RHEL: 6+
 - 6) openSUSE: 15+
 - 7) SUSE Enterprise Linux (SLES): 12 SP2+

- 8) Windows Client: 7, 8.1, 10 (1607+)
- 9) Windows Server: 2008 R2+,
7. System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji,
8. Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju),

Wsparcie techniczne:

1. Pomoc techniczna w językach:

- 1) polskim,
- 2) angielskim.

2. Materiały samopomocowe:

- 1) Baza wiedzy:
 - a) polski,
 - b) angielski

Zarządzanie:

1. Zarządzanie całością działania systemu (backup, przywracanie) z poziomu jednej konsoli dostępnej z poziomu przeglądarki internetowej,
2. Zarządzanie całym systemem poprzez dashboardy,
3. Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego,
4. System posiada wbudowane predefiniowane zadania backupowe,
5. System umożliwia tworzenie zadań backupowych w oparciu o kalendarz.
6. Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem,
7. Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem,
8. Monitorowanie postępu działania zadania,
9. Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach:
 - 1) Zadanie zostało zakończone pomyślnie,
 - 2) Zadanie zostało zakończone z ostrzeżeniami,
 - 3) Zadanie zostało zakończone z błędem,
 - 4) Zadanie zostało anulowane,
- 5) Zadanie nie zostało uruchomione.
10. System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego.
11. Możliwość zdefiniowania okna backupowego dla każdego z zadań,
12. Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów,
13. System pozwala na klonowanie planów kopii zapasowych,
14. System umożliwia reset hasła administratora w przypadku jego utraty,
15. Oprogramowanie umożliwia definiowanie retencji według schematów:
 - 1) GFS (Grandfather-Father-Son),
 - 2) FIFO (First-In, First-Out).
16. Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami,

17. Konta użytkowników mogą być tworzone poprzez import pliku CSV,
18. Oprogramowanie umożliwia tworzenie grup urządzeń,
19. Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
20. System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.:

- 1) System Administrator,
- 2) Backup operator,
- 3) Restore operator,
- 4) Viewer.

Składowanie danych:

1. Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie z poziomu jednej konsoli,
2. System umożliwia składowanie danych:
 - 1) Lokalnie:
 - Zasób SMB,
 - Zasób NFS,
 - Zasób ISCSI,
 - Zasób S3,
 - Katalog zabezpieczonego urządzenia.
 - 2) W chmurze:
 - Amazon Web Service,
 - Magazyn zgodny z S3,
 - Dostarczanej bezpośrednio przez producenta.
3. System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji,
4. System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.

Odtwarzanie:

1. Odtwarzanie granularne:
 - 1) Pojedynczych plików z kopii obrazu dysku,
 - 2) Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365,
2. Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów:
 - 1) Windows: 7+,
 - 2) Windows Server: 2008 R2+,
3. Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
4. Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a,
5. Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V.

6. Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK),
 7. Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL),
 8. Odtwarzanie zasobów plikowych z prawami dostępu,
 9. Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows),
 10. Odtwarzanie danych według harmonogramu,
 11. Przywracanie danych z określonego urządzenia/użytkownika,
 12. Przywracanie kopii z wybranego magazynu.
 13. Przywracanie danych Microsoft 365:
 - 1) do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku:
 - pst,
 - mbox.
 - 2) do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji),
 14. System posiada możliwość nieodwracalnego kasowania danych,
 15. Przywracanie repozytoriów GIT:
 - 1) przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket),
 - 2) przywracanie między kontami.
- Backup:
16. Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla:
 - 1) Systemów operacyjnych:
 - Alpine 3.10+,
 - Debian: 9+,
 - Ubuntu: 16.04+,
 - Fedora: 29+,
 - CentOS: 7+,
 - RHEL: 6+,
 - openSUSE: 15+,
 - SUSE Enterprise Linux(SLES): 12 SP2+,
 - macOS: 10.13+,
 - Windows: 7, 8.1, 10(1607+),
 - Windows Server: 2008 R2+,
 - 2) Środowisk wirtualnych:
 - Hyper-V,
 - VMware: 6.7+.
 - Dowolne inne w sposób agentowy
 - 3) Repozytoriów GIT:
 - GitHub,
 - Bitbucket.
 17. Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla:
 - 1) Baz danych:
 - Microsoft SQL,
 - MySQL,
 - PostgreSQL,

- Firebird,
- Dowlolnych innych przez podpięcie skryptów pre/post.

18. Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:

- 1) 128 bit,
- 2) 192 bit,
- 3) 256 bit.

19. Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów:

- 1) ZStandard,
- 2) LZ4.

20. Oprogramowanie umożliwia zarządzanie poziomem kompresji,

21. Wykonywanie kopii zapasowej otwartych plików(VSS),

22. System umożliwia uruchamianie skryptów przed i po backupie,

23. System umożliwia uruchamianie skryptów po wykonaniu migawki VSS,

24. System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów,

25. Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT,

26. Backup plikowy,

27. Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe,

28. Oprogramowanie umożliwia konsolidację wersji kopii zapasowych,

29. Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia,

30. Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego.

31. Oprogramowanie pozwala na backup zaszyfrowanych partycji.

GIT

32. Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych),

33. Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki).

Licencjonowanie:

Sposób licencjonowania opiera się na:

- 1) Ilości serwerów/endpointów- dla fizycznych urządzeń,
- 2) Ilości maszyn wirtualnych,
- 3) Ilości repozytoriów - dla GIT,
- 4) ilości użytkowników dla ekosystemu Microsoft Office 365.

Licencje umożliwiają :

- 1) wieczyste zabezpieczenie fizycznych 40szt. komputerów używanych w urzędzie,
- 2) wieczyste zabezpieczenie 8 maszyn wirtualnych,
- 3) przechowywanie danych w chmurze bezpośrednio przez producenta oprogramowania wraz z przestrzenią min. 100GB przez min. 2 lata

Wsparcie techniczne:

- 1) Świadczone jest w języku polskim, bezpośrednio przez główną siedzibę producenta,

- 2) Zapewnia dostęp do aktualizacji oprogramowania,
- 3) Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego,

Obowiązuje przez okres minimum 24 miesiące.

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:

- 1) Zabezpieczenia wskazanych przez Zamawiającego danych z posiadanych serwerów Windows i Linux oraz wybranych/wskazanych zasobów stacji roboczych z systemem operacyjnym Windows;
- 2) Zabezpieczenia wskazanych przez Zamawiającego aplikacji i baz danych,;
- 3) Zabezpieczenia wskazanych przez Zamawiającego maszyn wirtualnych;
- 4) Zabezpieczenia wskazanych przez Zamawiającego fizycznych serwerów z systemem Windows Server oraz Hyper-V Server;
- 5) Możliwości zabezpieczenia w przyszłości uruchomionych i eksploatowanych serwerów i stacji roboczych.

Wdrożenie powinno być zrealizowane przez certyfikowanego informatyka 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 systemy 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

- 1) 16-020 Czarna Białostocka, ul. Torowa 14A
- 2) 16-020 Czarna Białostocka, ul. Torowa 9

Godziny pracy Zamawiającego:

Poniedziałek 07:30-16:00

Wtorek, Środa, Czwartek 07:30-15:30

Piątek 07:30-15:00

Zamawiający dopuszcza aby prace wymagające zatrzymania środowiska produkcyjnego odbywały się poza godzinami pracy Zamawiającego.

2. Łącza Internetowe Lokalizacje:

- 1) 16-020 Czarna Białostocka, ul. Torowa 14A - 100/100Mb

- 2) 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
- 1) Serwer HP Prolinat 350e – Windows Serwer 2012 R2 – przestrzeń dyskowa 420GB (zajętość 245GB),
- 2) 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.
5. Serwer Dell R550 – przestrzeń dyskowa 4TB (zajętość 140 GB) 2 maszyny wirtualne

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:

- 1) kopie dzienne (pn, wt, śr, cz, pt) wykonywane raz dziennie i przechowywane 5 dni
- 2) kopie tygodniowe wykonywane pierwszego dnia tygodnia i przechowywane przez 4 tygodnie
- 3) kopie miesięczne wykonywane ostatniego lub pierwszego dnia miesiąca i przechowywane przez 2 miesiące
- 4) 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:

- 1) Środowisko domenowe Windows Server (ok. 0,1 TB)
- 2) System FK, Kadrowo-Płacowy QNT (ok. 0,1 TB)
- 3) System elektronicznego obiegu dokumentów EZD (ok. 0,5 TB)
- 4) 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 przygotowuje 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.

3. 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:

- 1) konfigurację sieci LAN i WAN w infrastrukturze Zamawiającego (switche, UTM);
- 2) konfigurację serwera NAS – specyfikacja zawarta w Części I SWZ.
- 3) 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 przekaże 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 poprawność uruchomienia się wirtualnej maszyny;

Testy mogą być realizowane poprzez przygotowane przez Wykonawcę skrypty.