

Część 5 – Zakup backup w chmurze

I. Charakterystyka ogólna i architektura rozwiązania

Przedmiotem zamówienia jest dostawa oraz wdrożenie zintegrowanego systemu klasy **Hybrid Cloud Backup**, łączącego funkcjonalność tworzenia kopii zapasowych z mechanizmami aktywnej ochrony przed cyberzagrożeniami. Zamawiający wymaga, aby oferowane rozwiązanie opierało się na architekturze hybrydowej, w której proces zarządzania realizowany jest za pośrednictwem centralnej konsoli dostępnej w modelu chmurowym (SaaS – Software as a Service), niewymagającej instalacji dedykowanych serwerów zarządzających w infrastrukturze lokalnej Zamawiającego.

System musi realizować politykę bezpieczeństwa poprzez instalację lekkich agentów na urządzeniach końcowych, które będą odpowiedzialne za wykonywanie kopii zapasowych, ich szyfrowanie oraz replikację do chmury. Rozwiązanie musi umożliwiać składowanie danych w dwóch lokalizacjach jednocześnie (zgodnie z regułą 3-2-1):

1. **Lokalnie:** na zasobach dyskowych Zamawiającego (macierze NAS, udziały sieciowe, dyski USB) w celu zapewnienia szybkiego czasu odtwarzania (RTO).
2. **W chmurze:** w dedykowanej, bezpiecznej przestrzeni dyskowej dostarczonej przez producenta rozwiązania, służącej jako zabezpieczenie na wypadek awarii krytycznej (Disaster Recovery).

II. Wymagania funkcjonalne w zakresie backupu i odtwarzania

Oprogramowanie musi charakteryzować się szeroką kompatybilnością systemową, zapewniając pełne wsparcie techniczne producenta (zarówno w zakresie wykonywania backupu, jak i odzyskiwania danych) dla środowisk heterogenicznych. W szczególności system musi obsługiwać stacje robocze pracujące pod kontrolą systemów Microsoft Windows (wersje od XP SP3, przez Windows 7, 8, aż do 10 i 11) oraz macOS. W zakresie systemów serwerowych wymagana jest obsługa rodziny Microsoft Windows Server (wersje od 2003/2003 R2, przez 2008, 2012, 2016, 2019, aż do 2022) oraz systemów z rodziny Linux (kernel 2.6.x i nowsze). Ponadto oprogramowanie musi wspierać edycje specjalistyczne, takie jak Windows SBS 2011 czy Windows Storage Server.

W zakresie tworzenia kopii zapasowych system musi umożliwiać wykonywanie pełnych obrazów dysków i partycji (image-based backup), co pozwoli na odtworzenie całego systemu operacyjnego wraz z konfiguracją, jak również kopii na poziomie plików i folderów. Rozwiązanie musi posiadać mechanizmy zapewniające spójność kopii dla aplikacji biznesowych i baz danych (technologia Application-Aware), w tym dla Microsoft Exchange, SQL Server, SharePoint, Active Directory oraz Oracle DB. W celu optymalizacji wykorzystania łącza internetowego i przestrzeni dyskowej, proces backupu musi być wspierany przez mechanizmy deduplikacji danych realizowanej na źródle (przed wysłaniem danych do sieci) oraz kompresji.

Proces odtwarzania danych musi być elastyczny i umożliwiać przywracanie zarówno pojedynczych plików, folderów czy obiektów aplikacji (np. pojedynczych wiadomości e-mail lub tabel SQL), jak i całych systemów operacyjnych na „czysty” sprzęt (Bare Metal Restore). Kluczową funkcjonalnością musi być technologia Universal Restore, pozwalająca na skuteczne uruchomienie odtworzonego obrazu systemu na innej platformie sprzętowej niż pierwotna, poprzez automatyczne wstrzykiwanie odpowiednich sterowników.

III. Zintegrowane mechanizmy cyberbezpieczeństwa

Zamawiający wymaga, aby dostarczony agent backupu posiadał wbudowane, aktywne mechanizmy ochrony stacji roboczych i serwerów, wykraczające poza standardowe kopiowanie danych. Oprogramowanie musi być wyposażone w moduł ochrony przed atakami typu Ransomware, działający w oparciu o analizę behawioralną i sztuczną inteligencję, a nie tylko sygnatury. System ten musi automatycznie wykrywać procesy próbujące nielegalnie szyfrować dane, natychmiastowo je blokować oraz automatycznie przywracać uszkodzone pliki z lokalnej pamięci podręcznej lub kopii zapasowej.

Dodatkowo agent musi posiadać funkcjonalność skanowania podatności (Vulnerability Assessment), która będzie cyklicznie weryfikować system operacyjny i zainstalowane aplikacje pod kątem znanych luk bezpieczeństwa (CVE) i prezentować administratorowi raport z oceną ryzyka dla każdego urządzenia.

IV. Wymogi dotyczące chmury i bezpieczeństwa danych (RODO)

Wszelkie dane przesyłane do chmury publicznej producenta muszą być składowane w Centrach Przetwarzania Danych zlokalizowanych fizycznie na terenie **Unii Europejskiej (UE) lub Europejskiego Obszaru Gospodarczego (EOG)**. Wykonawca gwarantuje, że dane nie będą transferowane do państw trzecich niespełniających wymogów RODO. Centrum danych musi legitymować się certyfikatem bezpieczeństwa ISO/IEC 27001.

Bezpieczeństwo danych musi być realizowane poprzez silne szyfrowanie (algorytm AES-256 lub wyższy) zarówno w trakcie transmisji, jak i podczas spoczynku w magazynie chmurowym (Data-at-Rest). System musi zapewniać mechanizm, w którym klucz szyfrujący jest generowany i przechowywany wyłącznie przez Zamawiającego, a dostawca usługi chmurowej nie posiada technicznej możliwości odszyfrowania treści składowanych plików (zasada Zero-Knowledge Encryption).

V. Model licencjonowania i ilości

Zamawiający wymaga dostarczenia subskrypcji na oprogramowanie na okres **12 miesięcy**. Model licencjonowania musi być oparty na liczbie chronionych urządzeń (Per Workload), bez limitów transferu danych. W ramach zamówienia Wykonawca dostarczy licencje dla następującej liczby systemów:

1. **Licencje Serwerowe:** dla 3 sztuk serwerów fizycznych lub wirtualnych (obsługujących systemy Windows Server lub Linux).
2. **Licencje Workstation:** dla 80 sztuk stacji roboczych (komputerów PC/Laptop z systemem Windows lub macOS).
3. **Przestrzeń Chmurowa:** dedykowana pula dyskowa o pojemności **min. 4 TB**, współdzielona dynamicznie (w ramach jednej puli/quota) przez wszystkie licencjonowane urządzenia Zamawiającego.

VI. Wdrożenie systemu

W ramach ceny oferty, Wykonawca zobowiązany jest do przeprowadzenia kompleksowego wdrożenia Systemu w środowisku informatycznym Zamawiającego. Usługa zostanie zrealizowana w formie **zdalnej asysty technicznej** (z wykorzystaniem bezpiecznego połączenia szyfrowanego) w wymiarze niezbędnym do uruchomienia pełnej funkcjonalności rozwiązania, jednak nie mniejszym niż **8 roboczogodzin**.

Wdrożenie musi obejmować następujące etapy:

1. Etap I – Inicjalizacja i Konfiguracja Środowiska Centralnego

Załącznik nr 1.5

- a. Utworzenie i aktywacja dedykowanej instancji (konta) Zamawiającego w chmurze producenta.
- b. Konfiguracja globalnych ustawień bezpieczeństwa konsoli zarządzającej, w tym włączenie uwierzytelniania dwuskładnikowego (2FA) dla kont administratorów.
- c. Zdefiniowanie struktury organizacyjnej w konsoli (np. podział na lokalizacje, działy lub typy urządzeń: Serwery, Stacje Robocze).
- d. **Generowanie kluczy szyfrujących:** Asysta przy generowaniu unikalnych kluczy szyfrujących dla magazynów danych. Wykonawca przeszkoli Zamawiającego z procedury bezpiecznego przechowywania kluczy, gwarantując, że dostęp do danych posiada wyłącznie Zamawiający (zgodnie z zasadą *Zero-Knowledge Encryption*).

2. Etap II – Instalacja Agentów i Konfiguracja Polityk

- a. Przygotowanie paczek instalacyjnych agentów dostosowanych do systemów operacyjnych Zamawiającego.
- b. Instruktaż i asysta przy masowej dystrybucji agentów (np. poprzez GPO Active Directory lub skrypty instalacyjne) lub ręczna instalacja agentów na grupie reprezentatywnej **minimum 10 urządzeń** wskazanych przez Zamawiającego (np. 1 serwer fizyczny, 1 maszyna wirtualna, 3 stacje robocze o różnej konfiguracji).
- c. Utworzenie i wdrożenie **Polityk Ochrony** dedykowanych dla serwerów i stacji roboczych, uwzględniających:
 - i. Harmonogramy wykonywania kopii (np. Grandfather-Father-Son).
 - ii. Retencję danych (czas przechowywania kopii).
 - iii. Ścieżki zapisu: lokalnie (na wskazany zasób sieciowy NAS) oraz replikację do chmury.
 - iv. Wykluczenia plików tymczasowych i systemowych w celu optymalizacji miejsca.
- d. Aktywacja modułów Cyberbezpieczeństwa: konfiguracja ochrony anty-ransomware (Active Protection) oraz harmonogramu skanowania podatności.

3. Etap III – Testy Funkcjonalne Weryfikacja poprawności działania systemu poprzez przeprowadzenie wspólnie z administratorem Zamawiającego testów odtworzeniowych:

- a. **Test 1:** Odtworzenie pojedynczego pliku z chmury na stację roboczą.
- b. **Test 2:** Odtworzenie bazy danych (np. SQL lub pliku PST/Exchange) do nowej lokalizacji.
- c. **Test 3:** Symulacja awarii krytycznej (Disaster Recovery) – testowe odtworzenie całego systemu operacyjnego (Bare Metal Recovery) na maszynę wirtualną lub inny sprzęt fizyczny.

4. Etap IV – Transfer Wiedzy (Szkolenie Stanowiskowe) Przeprowadzenie warsztatu dla administratorów Zamawiającego (min. 2 osoby) obejmującego:

- a. Codzienne zarządzanie konsolą i monitorowanie statusu zadań.
- b. Procedurę dodawania nowych urządzeń do ochrony.
- c. Interpretację raportów błędów i logów systemowych.
- d. Procedurę zgłaszania incydentów do wsparcia technicznego producenta.

Załącznik nr 1.5

5. Dokumentacja Powykonawcza Zakończenie wdrożenia musi zostać potwierdzone podpisaniem **Protokołu Odbioru Wdrożenia**. Warunkiem podpisania protokołu jest przekazanie Zamawiającemu dokumentacji powykonawczej (w formie elektronicznej PDF), zawierającej co najmniej:

- a. Dane dostępowe do konta administracyjnego.
- b. Opis skonfigurowanych polityk backupu i retencji.
- c. Raport z przeprowadzonych testów odtworzeniowych potwierdzający ich skuteczność.

VII. Asysta techniczna, SLA i warunki serwisu

Wykonawca zapewnia świadczenie asysty technicznej oraz prawo do aktualizacji oprogramowania (maintenance) przez cały okres trwania umowy (12 miesięcy). Wsparcie techniczne musi być realizowane przez wykwalifikowanych inżynierów w języku polskim, za pośrednictwem dedykowanego portalu zgłoszeniowego, poczty e-mail oraz infolinii telefonicznej.

Usługi wsparcia oraz przyjmowanie zgłoszeń muszą być realizowane w **dni robocze (od poniedziałku do piątku), z wyłączeniem dni ustawowo wolnych od pracy, w godzinach pracy Zamawiającego, tj. od 07:30 do 15:30.**

Wykonawca gwarantuje dostępność usługi chmurowej na poziomie min. 99,0% w skali miesiąca. W przypadku wystąpienia awarii, Wykonawca zobowiązuje się do podjęcia działań naprawczych (Czas Reakcji) w następujących terminach liczonych w godzinach świadczenia asysty:

Priorytet (Kategoria błędu)	Definicja Błędu	Gwarantowany Czas Reakcji*
KRYTYCZNY (A)	Całkowity brak dostępności usługi. Niemożność wykonania backupu lub odzyskania danych z chmury dla wszystkich lub kluczowych systemów (Serwery). Zagrożenie utraty danych.	do 4 godzin roboczych
WYSOKI (B)	Ograniczona funkcjonalność. Backup/Restore nie działa dla pojedynczych stacji roboczych. Błędy w działaniu agentów uniemożliwiające poprawną pracę, ale niezatrzymujące procesów krytycznych.	do 8 godzin roboczych (do końca następnego dnia roboczego)
NORMALNY (C)	Błędy niekrytyczne, pytania o konfigurację, prośba o wyjaśnienie funkcji, problemy z raportowaniem, drobne błędy interfejsu.	do 24 godzin roboczych

1.

W przypadku niedotrzymania gwarantowanych czasów reakcji lub poziomu dostępności usługi, Zamawiający ma prawo naliczyć kary umowne określone we wzorze umowy.