**Załącznik nr 1.3 do SWZ**

**LICENCJE SYSTEMU KOPII ZAPASOWYCH**

**Dane identyfikacyjne (wypełnia Wykonawca):**  
• Nazwa: …  
• Typ/model/nr katalogowy: …  
• Producent / kraj pochodzenia: …  
• Rok produkcji: …

**Tabela: Wymagania minimalne dla systemu kopii zapasowych – licencje**

| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **Parametry oferowanego sprzętu**  **PODAĆ** |
| --- | --- | --- | --- |
| 1. | **Wymagania ogólne** | 1.1. Oprogramowanie przeznaczone do środowisk klasy DataCenter. 1.2. Obsługa platform wirtualizacyjnych: VMware vSphere 6.x, 7.x, 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 – pełna funkcjonalność na każdej z platform. 1.3. Obsługa backupu z sieciowych zasobów plikowych NAS (SMB/CIFS/NFS) i bezpośrednio z serwerów Windows/Linux. |  |
| 2. | **Koszty całkowite i niezależność sprzętowa** | 2.1. Oprogramowanie nie może wymagać dedykowanego sprzętu. 2.2. Archiwa backupowe samowystarczalne – nie wymagają dodatkowej bazy metadanych. 2.3. Backupy deduplikowane i kompresowane – bez utraty funkcjonalności. 2.4. Metadane deduplikacji przechowywane w plikach backupu, nie w centralnej bazie. 2.5. Możliwość utworzenia jednej wirtualnej puli pamięci masowej dla backupu – bez limitu urządzeń. 2.6. Obsługa repozytoriów w chmurze: Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi oraz archiwizacji do Azure Archive Blob i Amazon Glacier. 2.7. Wsparcie niezmienności backupów (Immutable Backups) – zabezpieczenie przed ransomware. |  |
| 3. | **Architektura i zarządzanie** | 3.1. Brak konieczności instalowania agentów wewnątrz maszyn wirtualnych. 3.2. Portal samoobsługowy umożliwiający odzyskiwanie danych przez użytkowników końcowych (maszyny wirtualne, MS Exchange, MS SQL, Oracle, PostgreSQL). 3.3. Delegacja uprawnień przywracania danych. 3.4. Wbudowane RESTful API do integracji z innymi systemami. 3.5. Backup konfiguracji systemu – automatyczny. 3.6. Szyfrowanie danych backupu i transmisji – bez ograniczeń funkcjonalnych. 3.7. Mechanizmy zabezpieczające przed utratą hasła szyfrowania. 3.8. Architektura klient-serwer, wiele konsol administracyjnych. 3.9. Wbudowane MFA (uwierzytelnianie wieloskładnikowe) do konsoli. |  |
| 4. | **Wymagania RPO – backup i replikacja** | 4.1. Certyfikowane mechanizmy CBT (Change Block Tracking) dla platform wirtualizacyjnych. 4.2. Śledzenie zmienionych plików dla udziałów sieciowych. 4.3. Możliwość kontroli obciążenia storage'u produkcyjnego z poziomu backupu. 4.4. Backup z wykorzystaniem snapshotów macierzowych – bez hostów proxy. 4.5. Wsparcie VMware vSAN – potwierdzone certyfikacją. 4.6. Backup i archiwizacja na taśmach. 4.7. Wsparcie retencji GFS. 4.8. Integracja z urządzeniami deduplikacyjnymi (Dell DataDomain, HPE StoreOnce, ExaGrid, itp.). 4.9. Obsługa BlockClone API (ReFS, XFS). 4.10. Wbudowana akceleracja WAN do replikacji backupów. 4.11. Replikacja asynchroniczna między hostami (VMware, Hyper-V). 4.12. Replikacja ciągła z VMware VAIO z RPO logiem. 4.13. Wsparcie „replica seeding” i punktów przywracania dla replik. 4.14. Obsługa wszystkich trybów transportu hypervisora. |  |
| 5. | **Wymagania RTO – szybkie przywracanie** | 5.1. Uruchamianie wielu VM bezpośrednio ze skompresowanego backupu – bez kopiowania danych na storage. 5.2. Obsługa instant recovery z backupów wykonanych na innych platformach (np. fizycznych, chmury). 5.3. Migracja uruchomionych VM do storage produkcyjnego (vMotion, Storage Migration lub natywne mechanizmy backupu). 5.4. Prezentowanie pojedynczego dysku do działającej VM. 5.5. Instant recovery dla plików SMB, MS SQL, Oracle – z migracją online. 5.6. Pełne odtwarzanie maszyn wirtualnych, plików i dysków. 5.7. Odtwarzanie bezpośrednio do: Microsoft Azure, Azure Stack, Amazon EC2, GCP. 5.8. Granularne odzyskiwanie plików bez agenta VM – przez API/PowerShell. 5.9. Obsługa systemów plików: Windows, Linux, Mac, BSD, Solaris, Novell. 5.10. Granularne odtwarzanie Active Directory, Exchange, SQL, Sharepoint, Oracle, PostgreSQL, SAP HANA, SAP Oracle, Microsoft SQL VDI – z backupu jednoprzebiegowego. 5.11. Obsługa „reverse CBT” i odzysku przez SAN. |  |
| 6. | **Ograniczenie ryzyka** | 6.1. Tworzenie wirtualnych laboratoriów do testowania backupu w środowisku izolowanym (VMware, Hyper-V). 6.2. Testy odtwarzalności VM z backupu – w pełni automatyczne, wg harmonogramu. 6.3. Skanowanie backupu przez AV (min. Windows Defender, ESET, Symantec). 6.4. Automatyczne odtwarzanie VM z wykonaniem skryptu pre/post. |  |
| 7. | **Środowiska fizyczne** | 7.1. Wsparcie backupu dla Windows, Linux, macOS (również klient i serwer). 7.2. Obsługa dystrybucji Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE. 7.3. Odtwarzanie plików z fizycznych maszyn – dowolny OS. 7.4. Wsparcie Microsoft Failover Cluster. 7.5. Bare metal recovery, odzysk wolumenów, plików, folderów. 7.6. Backup dysków USB, DAS, NAS, chmura obiektowa (S3/Blob). 7.7. Deduplikacja i kompresja na źródle. 7.8. Kontrola pasma, ograniczenie backupu w sieciach WiFi/VPN. 7.9. Śledzenie zmienionych bloków (CBT), certyfikacja Microsoft. 7.10. Obsługa BitLocker, odzysk z nośnika awaryjnego. 7.11. Granularne odtwarzanie aplikacji: Exchange, AD, Sharepoint, SQL, Oracle, PostgreSQL – w trybie jednoprzebiegowym. 7.12. Obsługa point-in-time recovery. 7.13. Publikowanie baz danych bezpośrednio z backupu (MS SQL, Oracle). |  |

***należy podpisać***

***kwalifikowanym podpisem elektronicznym***

***lub podpisem zaufanym lub podpisem osobistym***