

Rzeczpospolita
PolskaDofinansowane przez
Unię Europejską

Opis przedmiotu zamówienia (OPZ)
(charakterystyka i minimalne wymagania)

Przedmiot zamówienia: **Nowe systemy cyberbezpieczeństwa w Gminie Dzierzgoń**

Element 1 – Zakup i wdrożenie bezpiecznego systemu przechowywania danych wraz z systemem backupu

Przedmiotem zamówienia w zakresie części 1, jest podniesienie poziomu cyberbezpieczeństwa poprzez zakup i wdrożenie bezpiecznego systemu przechowywania danych wraz z systemem backupu, dla systemów serwerowych oraz 50 stacji roboczych z utworzeniem bezpiecznej przestrzeni backupowej NAS oraz usługą konfiguracji i weryfikacji odtwarzania celem niwelowania skutków ataku ransomware, wraz z gwarancją producenta na 36 miesięcy i szkoleniem stanowiskowym z obsługi wdrożonego systemu. Dostawa obejmuje komplet sprzętu i urządzeń wraz z odpowiednim oprogramowaniem, spełniających poniższe minimalne parametry i wymagania:

Lp.	Element zadania	Ilość
I.	Macierz	2 sztuki
II.	Oprogramowanie do backupu	1 komplet
III.	Serwer do oprogramowania do backupu	1 sztuka
IV.	Oprogramowanie systemowe do serwera backupu	1 komplet
V.	Przełącznik zarządzalny	1 sztuka

I. Macierz - 2 sztuki**Dostawa 2 sztuk macierzy ze wsparciem producenta i gwarancją na 36 miesięcy**

Lp.	Element konfiguracji	Wymagania minimalne
1	Obudowa	<ol style="list-style-type: none"> System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19" Macierz nie może być prototypem, wszystkie podzespoły muszą pochodzić od jednego producenta
2	Pojemność	<ol style="list-style-type: none"> System musi zostać dostarczony w konfiguracji zawierającej minimum: <ol style="list-style-type: none"> 12 dysków 1800GB SAS 10k posiadać możliwość rozbudowy o kolejne dyski System musi wspierać dyski: <ol style="list-style-type: none"> SAS: 900GB do 1800GB SATA/NL-SAS: od 4TB do 16TB SSD: 800GB do 15 300GB Budowa systemu musi umożliwiać rozbudowę do modeli wyższych bez potrzeby kopiowania/migrowania danych. (zamawiający przez model wyższy rozumie inny model macierzy danego producenta z większą pamięcią cache oraz mocniejszymi procesorami). System musi mieć możliwość rozbudowy do 500 dysków w obrębie pary kontrolerów lub w obrębie klastra wielu kontrolerów (scale-out) w zależności od sposobu realizacji rozbudowy dla oferowanego rozwiązania. W przypadku klastrowania kontrolerów macierzy, system musi działać pod kontrolą jednego systemu operacyjnego od jednego producenta, nie dopuszczalne jest zestawienie systemu klastrowego poprzez wykorzystanie serwerów pośredniczących i oprogramowania dodatkowego. Dla rozwiązań wykorzystujących klastrowanie (scale-out) musi być możliwość rozbudowy rozwiązania do co najmniej 12 kontrolerów w klastrze. Rozwiązanie musi pozwalać na rozbudowę o dyski lub kontrolery wykonane w technologii NVMe do min 1120 dysków w technologii NVME. Zamawiający dopuszcza zaoferowanie rozwiązania, które nie posiada takiej możliwości w przypadku gdy całość zasobów zostanie dostarczona na dyskach flash/SSD.
3	Kontroler	<ol style="list-style-type: none"> Dwa kontrolery wyposażone w przynajmniej 64GB cache oparte o RAM na kontroler dodatkowa pamięć Flash minimum 1024GB pamięci na kontroler (wbudowana w kontroler lub formie dodatkowych dysków Flash skonfigurowanych w RAID 10).

		<p>2. System musi pozwalać na rozbudowę pamięci Cache opartej o RAM do 3072GB za pomocą dodatkowych modułów pamięci RAM lub poprzez rozbudowę o kolejne kontrolery.</p> <p>3. Procesory macierzy powinny być wykonane w technologii wielordzeniowej z przynajmniej 8 rdzeniami na każdy kontroler dla procesorów AMD i Intel. Dla innych rodzajów procesorów min 64 rdzenie.</p> <p>4. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub poprzez zrzut na pamięć nieulotną.</p> <p>5. Macierz musi pozwalać na poszerzenie pamięci Cache za pomocą dysków SSD do 6TB.</p>
4	Interfejsy	<p>Oferowana macierz musi posiadać minimum:</p> <ol style="list-style-type: none"> 1) 8 portów 25GbE SFP 2) 4 porty 32Gb FC 3) 4 porty 1GbE 4) 6 portów 12Gb SAS
5	RAID	System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii minimum trzech dysków w grupie RAID.
6	Kopie migawkowe	<ol style="list-style-type: none"> 1. Macierz musi być wyposażona w system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy. System kopii migawkowych nie może powodować spadku wydajności macierzy +/-5%. 2. Zamawiający dopuszcza rozwiązanie, które ma wpływ na wydajność przy stosowaniu kopii migawkowych przy zapisie, przy założeniu zaoferowania całej pojemności na dyskach SSD/Flash/NVME.
7	Obsługiwane protokoły	Macierz musi obsługiwać jednocześnie protokoły FC, iSCSI, CIFS i NFS, S3 (macierz obiektowa) - jeśli wymagane są licencje zamawiający wymaga dostarczenia ich wraz z macierzą.
8	Wsparcie systemów	Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Win 2018 i nowsze, Linux, Vmware, Unix.
9	Zarządzanie wolumenami	<ol style="list-style-type: none"> 1. Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie 2. Macierz musi posiadać funkcjonalność priorytetyzacji zadań.
10	Kompresja danych	Macierz musi posiadać funkcjonalność kompresji danych w trybie in-line oraz off-line na każdym rodzaju danych.
11	Deduplikacja	Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych którą można stosować na macierzy/danych produkcyjnej dla wszystkich rodzajów danych. Macierz powinna mieć możliwość czynności odwrotnej tzn. Cofnięcia procesu deduplikacji na zdeduplikowanym wolumenie.
12	Replikacja	Macierz musi posiadać funkcjonalność replikacji synchronicznej i asynchronicznej pomiędzy macierzami tego samego producenta. Funkcjonalność replikacji danych musi być natywnym narzędziem macierzy. Przed procesem replikacji macierz

		musi umożliwiać włączenie procesu deduplikacji danych w celu optymalizacji wykorzystania łącza dla replikowanych zasobów. Macierz musi posiadać funkcję replikacji zaszyfrowanych danych.
13	Funkcjonalności bezpieczeństwa anty Ransomware	System musi posiadać specjalny moduł do zabezpieczenia przez atakiem Ransomware w szczególności: <ol style="list-style-type: none"> 1) musi informować administratora w przypadku nie standardowego zachowania systemu oraz danych 2) wykonywać prewencyjną kopię migawkową „snapshot” w przypadku zagrożenia atakiem ransomware 3) monitorować niestandardowe zachowanie użytkowników serwera plików
14	Funkcjonalności bezpieczeństwa WORM	Macierz musi posiadać zaimplementowaną funkcjonalność WORM. Jeżeli rozwiązanie wymaga do tego licencji zamawiający wymaga jej dostarczenia.
15	Mechanizmy bezpieczeństwa	W celach bezpieczeństwa macierz musi posiadać funkcjonalność wieloetapowej akceptacji wybranych operacji tj. operacje takie jak: Skasowanie LUN/Wolumeny, skasowanie Snapshotu, wyłączenie replikacji. System musi pozwalać by wykonanie w/w operacji było akceptowane przez przynajmniej dwóch administratorów w celu zwiększenia bezpieczeństwa i uniknięcia błędów ludzkich.
16	Audyt danych	System musi posiadać moduł do audytu zasobów plikowych na wyspecyfikowanej macierzy po kątem przechowywanych danych wrażliwych/osobowych. W szczególności moduł mu posiadać: <ol style="list-style-type: none"> 1) Możliwość przeszukiwania zasobów plikowych <ol style="list-style-type: none"> a) na wyspecyfikowanej macierzy b) innych serwerach plików jak Windows File server, SYnology File sever, QnapFille server, Google drive, Onedrive, Azure files, c) baz danych: Oracle, MySQL, MS SQL, PostgreSQL, Mongo DB, SAP HANA d) system musi pozwalać na utworzenie kategorii przeszukanych plików na: <ul style="list-style-type: none"> - niewrażliwe (ogólne informacje o pracowniku) - dane osobiste (numer NIP, Pesel) - dane wrażliwe (dane zdrowotne, informacje o wynagrodzeniu) 2) System musi być zgodny z europejskimi przepisami GDPR (Rodo) w tym móc przeszukiwać i kategoryzować dane po: <ol style="list-style-type: none"> a) NIP/Regon b) Pesel c) Adresie Email d) Kontach bankowych

17	Automatyzacja informacji dla administratora	Macierz musi posiadać możliwość automatycznego informowania przez macierz i przesyłania przez pocztę elektroniczną raportów o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne macierzy.
18	Wirtualne klony	Macierz musi posiadać funkcjonalność wykonania wirtualnych klonów, które nie wymagają kopiowania bloków danych.
19	Monitoring i raportowanie	Z macierzą zamawiający wymaga dostarczenia oprogramowania które pozwala na: <ol style="list-style-type: none"> 1) monitoring wykorzystania przestrzeni na macierzy 2) monitoring grup RAIDowych 3) monitoring wykonywanych backupów/replikacji danych między macierzami 4) monitoring wydajności macierzy 5) analizę i diagnozę spadku wydajności
20	Licencje	Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy.
21	Portal zarządzający	Producent musi dostarczyć usługę w postaci portalu WWW lub dodatkowego oprogramowania umożliwiającą następujące funkcjonalności: <ol style="list-style-type: none"> 1) Narzędzie do tworzenia procedury aktualizacji oprogramowania macierzowego. <ol style="list-style-type: none"> a) procedura musi opierać się na aktualnych danych pochodzących z macierzy oraz najlepszych praktykach producenta. b) procedura musi uwzględniać systemy zależne np, macierze replikujące c) procedura musi umożliwiać generowanie planu cofnięcia aktualizacji. 2) Wyświetlanie statystyk dotyczących wydajności, użycia, oszczędności uzyskanych dzięki funkcjonalnościom macierzy. 3) Wyświetlanie konfiguracji macierzy oraz porównywanie jej z najlepszymi praktykami producenta w celu usunięcia błędów konfiguracji.
22	Zastrzeżenie funkcjonalności	Zamawiający wymaga by wszystkie opisane funkcjonalności macierzy działały wspólnie tj. włączenie jednej funkcjonalności nie eliminowało innej.
23	Funkcjonalności dodatkowo punktowane	<ol style="list-style-type: none"> 1. Producent musi oferować możliwość zainstalowania wirtualnej instancji systemu operacyjnego macierzy na jednym z dostępnych systemów wirtualizacyjnych na rynku jak: Vmware, MS HyperV, XEN, KVM 2. Macierz musi posiadać licencję na tiering oraz replikację zimnych danych na dowolny zasób S3 (Chmura AWS/Azure/Google/ALibaba . lub dowolną macierz obiektową) 3. Zamawiający wymaga potwierdzenia funkcjonalności oferowanego rozwiązania oświadczeniem producenta złożonym wraz z ofertą

II. Oprogramowanie do backupu – 1 komplet

Zamawiający wymaga licencji wieczystych, umożliwiających zabezpieczenie co najmniej 50 stacji roboczych i 3 serwerów fizycznych lub 20 maszyn wirtualnych z suportem, minimum na 36 miesięcy w trybie 24/7.

Lp.	Element konfiguracji	Wymagania minimalne
1	Wymagania ogólne	<ol style="list-style-type: none"> Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5, rozwiązanie nie może być rozwiązaniem prototypowym, autorskim, mieć konfigurację specjalną. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
2	Całkowite koszty posiadania	<ol style="list-style-type: none"> Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej. Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.

		<p>7. Oprogramowanie musi wspierać niezmienną kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.</p> <p>8. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.</p> <p>9. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time).</p> <p>10. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.</p> <p>11. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.</p> <p>12. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.</p> <p>13. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiegokolwiek funkcjonalności wymienionej w tej specyfikacji.</p> <p>14. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.</p> <p>15. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.</p> <p>16. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.</p> <p>17. Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora).</p> <p>18. Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS).</p> <p>19. Oprogramowanie musi posiadać integracje z systemami typu SIEM.</p> <p>20. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.</p>
3	Wymagania RPO	<p>1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.</p> <p>2. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.</p> <p>3. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastora.</p>

		<p>4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.</p> <p>5. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.</p> <p>6. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).</p> <p>7. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).</p> <p>8. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.</p> <p>9. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.</p> <p>10. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.</p> <p>11. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.</p> <p>12. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.</p> <p>13. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.</p> <p>14. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).</p> <p>15. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).</p>
4	Wymagania RTO	<p>1. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.</p> <p>2. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).</p>

		<ol style="list-style-type: none"> 3. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami. 4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre. 5. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. 6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków. 7. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. 8. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików. 9. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. 10. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell. 11. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM. 12. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. 13. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. 14. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. 15. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. 16. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
--	--	--

		<p>17. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.</p> <p>18. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.</p> <p>19. Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji.</p> <p>20. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.</p> <p>21. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle.</p> <p>22. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI.</p> <p>23. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2.</p> <p>24. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.</p>
5	Ograniczenie ryzyka	<p>1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchamianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).</p> <p>2. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.</p> <p>3. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.</p> <p>4. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.</p> <p>5. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware.</p> <p>6. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania.</p> <p>7. Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków.</p>

		8. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
6	Środowiska fizyczne	<ol style="list-style-type: none"> 1. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego 2. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych 3. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE 4. Rozwiązanie musi wspierać system operacyjny macOS 5. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix 6. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) 7. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster 8. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów 9. Rozwiązanie musi wspierać backup podłączonych dysków USB 10. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym 11. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) 12. Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone 13. Rozwiązanie musi wspierać kontrolę pasma sieciowego 14. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych 15. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN 16. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft 17. Rozwiązanie musi wspierać technologię BitLocker 18. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania

		<p>19. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednorazowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych</p> <p>20. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych</p> <p>21. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.</p> <p>22. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform</p> <p>23. Rozwiązanie musi wspierać szyfrowanie</p> <p>24. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne</p> <p>25. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego</p> <p>26. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej</p> <p>27. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych</p>
7	Monitoring	<p>1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich</p> <p>2. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie</p> <p>3. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.</p> <p>4. System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter</p> <p>5. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn</p> <p>6. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel</p> <p>7. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk</p>

	<p>8. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora</p> <p>9. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów</p> <p>10. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)</p> <p>11. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna</p> <p>12. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego</p> <p>13. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta</p> <p>14. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.</p> <p>15. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.</p> <p>16. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware</p> <p>17. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4</p> <p>18. Raportowanie</p> <p>19. System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie</p> <p>20. System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.</p> <p>21. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.</p> <p>22. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V</p> <p>23. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF</p> <p>24. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc</p>
--	--

		<p>25. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach</p> <p>26. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów</p> <p>27. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych</p> <p>28. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych</p> <p>29. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury</p> <p>30. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta</p> <p>31. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.</p> <p>32. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.</p> <p>33. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware</p> <p>34. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)</p> <p>35. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.</p>
--	--	--

III. Serwer do oprogramowania do backupu – 1 sztuka

Serwer do oprogramowania do backupu z gwarancją i wsparciem producenta na 36 miesięcy.

Lp.	Element konfiguracji	Wymagania minimalne
1	Obudowa	Obudowa Rack o wysokości max 1 U z możliwością instalacji min. 10 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
2	Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

3	Procesor	1 procesor 8 rdzeni, 2,8 GHz, 12MB Cache
4	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
5	Pamięć RAM	128 GB RAM DDR5 ECC RDIMM 4800MT/s
6	Kontroler RAID	1. Sprzętowy kontroler dyskowy obsługujący transfer 6Gb/s, 12Gb/s i 22,5Gb/s, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, and 60. Kontroler musi umożliwiać konfigurację JBOD. Kontroler musi posiadać 8G pamięci podręcznej DDR4. Głębokość kolejki kontrolera musi być większa niż 8000. Kontroler musi wspierać automatyczną odbudowę dysków Hot Spare, kontroler musi umożliwiać automatyczne wznowienie pracy podczas odbudowy macierzy. 2. Kontroler musi obsługiwać dyski logiczne o pojemności większej niż 2TB. Kontroler musi posiadać wsparcie dla dysków samoszyfrujących.
7	Interfejsy sieciowe	1. Dwa interfejsy 10 Gbit Ethernet 2. Jeden interfejs 1 Gbit Ethernet
8	Dyski twarde	1. Możliwość instalacji dysków SATA/SAS 2. Zainstalowane 2 dyski SSD SATA o pojemności min. 960 GB, 6Gb, 2,5" Hot- Plug o parametrach min. 1 DWPD i skonfigurowane fabrycznie w RAID1
9	Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
10	Zdalne zarządzanie	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: 1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej; 2) zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); 3) szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; 4) możliwość podmontowania zdalnych wirtualnych napędów; 5) wirtualną konsolę z dostępem do myszy, klawiatury; 6) wsparcie dla IPv6; 7) wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;

		8) możliwość zdalnego monitorowania w czasie rzeczywistym 9) poboru prądu przez serwer; 10) możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; 11) integracja z Active Directory; 12) możliwość obsługi przez dwóch administratorów jednocześnie; 13) wsparcie dla dynamic DNS; 14) wysyłanie do administratora maila z powiadomieniem o awarii; 15) możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera.
11	Diagnostyka	Wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
12	Zasilacze	Redundantne, Hot-Plug min. 700W każdy
13	Wspierane systemy operacyjne	Oferowany serwer musi wspierać następujące systemy operacyjne: 1) Canonical Ubuntu Server LTS 2) Microsoft Windows Server with Hyper-V 3) Red Hat Enterprise Linux 4) SUSE Linux Enterprise Server 5) VMware vSAN/ESXi
14	Certyfikaty	1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. 2. Serwer musi posiadać deklarację CE. 3. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów, Microsoft Windows 2019, Microsoft Windows 2022.
15	Gwarancja	1. 3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 2. Zamawiający wymaga od Wykonawcy wykupienia opcji wymiany dysku uszkodzonego, z warunkiem pozostawienia uszkodzonych dysków u Zamawiającego., tym samym w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego, przez cały okres udzielonej gwarancji.

		3. Serwis serwera świadczony będzie przez autoryzowany serwis producenta.
--	--	---

IV. Oprogramowanie systemowe do serwera backupu – 1 komplet

Lp.	Element konfiguracji	Wymagania minimalne
1	Rodzaj systemu operacyjnego	Komercyjny, serwerowy system operacyjny umożliwiający uruchomienie minimum 2 maszyn wirtualnych
2	Typ licencji	Licencja perpetual na min 16 core procesora
3	Dodatkowe wymogi	Licencja musi umożliwiać prawidłowe współdziałanie z wykorzystywanym przez Zamawiającego systemem Windows Server 2022 (oraz wersje starsze), w sposób zgodny z zasadami licencjonowania Microsoft. Przez prawidłowe działanie należy rozumieć możliwość wykorzystania wszystkich funkcjonalności systemu Windows Server 2022 (oraz wersje starsze), bez konieczności jakiegokolwiek ingerencji w konfigurację tego systemu.

V. Przełącznik zarządzalny – 1 sztuka**Przełącznik zarządzalny 1 szt. z gwarancją producenta na 36 miesięcy**

Lp.	Element konfiguracji	Wymagania minimalne
1	Typ przełącznika	Przełącznik zarządzalny warstwy L3, 1U, stackowalny
2	Ilość portów	24 porty 10 GBit 10 base T, 4 25GBASE-X SFP28 uplinks
3	Port konsoli	RJ 45
4	Przepustowość	przepustowość rutowania/przełączania: 650 Gbit/s
5	Wielkość pamięci bufora pakietów	32 MB
6	Wielkość pamięci flash	512MB NAND 8-bit ECC

7	Opóźnienia dla portów 10 GBit 10 base T	<2.20μs
8	Standardy komunikacyjne	IEEE 802.1D, IEEE 802.1Q, IEEE 802.1Qav, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3ak, IEEE 802.3bz, IEEE 802.3u
9	Obsługiwane protokoły	OSPF, OSPFv2, OSPFv3, RIP, RIP-1, RIP-2
10	Ilość VLAN	4000
11	Gwarancja i wsparcie producenta	3 lata
12	Okablowanie	Niezbędne okablowanie do podłączenia serwera, przełącznika i macierzy

Usługi instalacyjne i wdrożeniowe systemu backupu – wymagania dodatkowe:

1. Zamawiający wymaga wykonania wdrożenia zintegrowanego systemu backupowego obejmującego dwie macierze NAS, serwer backupu wraz z oprogramowaniem systemowym i zainstalowanym na nim oprogramowaniem do wykonywania backupu oraz zarządzalny przełącznik sieciowy służący do podłączenia zakupionej infrastruktury. Macierze umieszczone zostaną, jedna w ośrodku podstawowym, druga w ośrodku zapasowym. Na pierwszą macierz przeniesione zostaną wszystkie zasoby z serwerów Gminy, w tym środowisko maszyn wirtualnych. Pomiędzy macierzami zostanie uruchomiona replikacja asynchroniczna tj. dane niezduplikowane będą automatycznie przekopiowywane na drugą macierz w centrum zapasowym. Zamawiający wymaga uruchomienia mechanizmów kryptograficznych na macierzach dyskowych, oraz systemu RAID umożliwiającego pracę macierzy przy uszkodzeniu trzech dysków. Zadaniem systemu backupu jest regularne tworzenie kopii zapasowych danych aplikacji i maszyn wirtualnych a także zabezpieczenie bezpieczeństwa plików systemowych, logów systemowych i dzienników systemowych poprzez regularne wykonywanie kopii na zakupionej macierzy. Dodatkowo, wszystkim komputerom biurowym udostępniony zostanie poprzez protokół CIFS zasób na macierzy, tj. każdy użytkownik będzie składował swoje dane na chronionym udziale macierzowym. W celu optymalizacji danych wykonawca uruchomi na macierzach funkcjonalności deduplikacji i kompresji danych. W ramach budowy systemu wykonawca uruchomi systemy antyransomware chroniące na macierzy dane przed atakami ransomware oraz mechanizmy WORM. Wykonawca opracuje i wdroży procedury backupu oraz odtwarzania w przypadku awarii i ataku ransomware. Wykonawca uruchomi funkcję autosupport tj. zabezpieczone łącze diagnostyczne do producenta macierzy. Przeprowadzi testy odtwarzania oraz wykona przeszkolenie stanowiskowe i dokumentację powdrożeniową.
2. Żaden z dostarczanych elementów nie może być prototypem sprzętowym, ani oprogramowaniem autorskim.
3. Przedmiot umowy będzie objęty serwisem Wykonawcy przez 36-miesięczny okres gwarancyjny.