

**Załącznik Nr 1.7 do SWZ
OPZ –ZADANIE 7**

(Znak sprawy: SR.271.24.2025)

„Dostawa licencji oprogramowania kopii zapasowych z usługą instalacji i wdrożenia backupu” w ramach projektu grantowego "Cyberbezpieczny Samorząd" współfinansowanego ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II „Zaawansowane usługi cyfrowe” Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa”, tytuł projektu: „Podniesienie poziomu bezpieczeństwa infrastruktury informatycznej oraz poziomu wiedzy o cyberzagrożeniach w Urzędzie Gminy Dębe Wielkie”

Zakres projektu:

Dostawa licencji oprogramowania kopii zapasowych z usługą instalacji i wdrożenia backupu

Zakres prac obejmuje:

1. Dostarczenie licencji oprogramowania kopii zapasowych
2. Instalacja, konfiguracja i wdrożenie oprogramowania kopii zapasowych
3. Włączenie do systemu Infrastruktury IT urzędu objętej wdrożeniem:
 - 53 stanowisk PC
 - 3 serwery fizyczne
 - 8 serwerów wirtualnych
 - Subskrypcja – 12 miesięcy

Przedmiotem zamówienia jest dostawa licencji oprogramowania kopii zapasowych z usługą instalacji i wdrożenia backupu o parametrach minimalnych:

A. Oprogramowania do zabezpieczania danych poprzez mechanizm kopii zapasowych dedykowane dla środowisk stacji roboczych.

1. Oprogramowanie musi wspierać fizyczne i wirtualne komputery z systemem operacyjnym Windows XP i nowsze oraz systemy macOS.
2. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:
 - Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www.
 - Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego).
 - Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych.

- Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu).
- Możliwość definiowania uprawnień dla administratorów systemu kopii zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.).
- Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami.
- Wsparcie dla Single Sign On dla logowania do systemu.
- Możliwość zarządzania procesem tworzenia kopii zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT.
- Możliwość definiowania planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem).
- Możliwość tworzenia zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopii zapasowych.
- Możliwość zdalnej instalacji agentów kopii zapasowych z poziomu konsoli cyberochrony na maszynach z systemem operacyjnym Windows.
- Możliwość zdalnego uaktualniania agentów kopii zapasowych.
- Możliwość zdalnego zarządzania procesem wykonywania kopii zapasowej i odzyskiwania danych.
- Możliwość zdefiniowania dedykowanej maszyny, której agent kopii zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopii zapasowej).
- Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych.
- Centralny katalog wszystkich danych zapisanych w kopiach zapasowych.
- Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.

3. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:

- Kopie zapasowe całych dysków i partycji.
- Kopie zapasowe wybranych plików i folderów.
- Kopia zapasowa udziałów sieciowych.
- Zapis kopii zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczonym przez producenta systemu kopii zapasowych.
- Zapis kopii zapasowych na udziały sieciowe.
- Zapis kopii zapasowych na serwer SFTP.
- Zapis kopii zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana.
- Zapis kopii zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloaderzy).
- Możliwość wyszukiwania plików w kopiach zapasowych.

- Możliwość szyfrowania plików kopii zapasowych.
 - Wsparcia dla technologii VSS.
 - Deduplikacja kopii zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć.
 - Kompresja plików kopii zapasowych.
 - Możliwość replikacji kopii zapasowych na kolejne nośniki (dyski, magazyn chmurowy).
 - Możliwość replikacji kopii zapasowych na nośniki taśmowe.
 - Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopii zapasowych.
4. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:
- Odtworzenie całej maszyny (Windows, Mac) – tzw. Bare Metal Restore.
 - Odtworzenie całej maszyny (Windows, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową.
 - Odtworzenie poszczególnych plików i folderów.
 - Przywracanie przyrostu względem danych, które już się znajdują na dysku na który przywracana jest kopia zapasowa.
 - Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowaniu maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonana kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania).
5. Dodatkowe (obowiązkowe) wymagania związane ochroną danych dla systemów Windows 7 i nowszych:
- Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń
 - Skanowanie oprogramowania celem poszukiwania podatności. Podatności wypisane muszą być z minimum informacjami takimi jak nazwa produktu który zawiera podatność, maszyny na których znaleziono takie oprogramowanie, stopień ważności w skali CVSS.
6. Przestrzeń chmurowa dostarczana wraz z oprogramowaniem musi spełniać poniższe wymagania:
- W przypadku uzyskania uzasadnionej pewności, że doszło do naruszenia bezpieczeństwa, producent oprogramowania bez zbędnej zwłoki dostarczy informacje o takowym naruszeniu na adres e-mail podany podczas rejestracji konta.
 - W przypadku wyżej wymienionego naruszenia, producent podejmie kroki, aby udokumentować, naprawić i zminimalizować skutki naruszenia

bezpieczeństwa w odniesieniu do danych osobowych oraz aby zapobiec jego powtórzeniu

- Kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich repliki muszą być przechowywane na terenie Polski.
- Producent przechowuje dane osobowe klienta (dane osobowe oraz kopie zapasowe) przy użyciu technik szyfrowania, minimum AES-256.
- Producent nie wykorzystuje danych osobowych klienta bez anonimizacji w środowiskach programistycznych lub testowych.
- Producent oprogramowania przeprowadza okresowe oceny ryzyka i przeglądy co najmniej raz w roku.
- Infrastruktura (chmurowy magazyn kopii zapasowych) jest zaprojektowana zgodnie z podejściem N+1 (to, co niezbędne +1).
- Producent oprogramowania jest zgodny z standardem bezpieczeństwa ISO 27001 lub równoważne SOC 2 lub równoważne, a magazyn kopii zapasowych musi być zgodny z certyfikatami ISO 9001 lub równoważne, ISO 27001 lub równoważne oraz certyfikację DCOS lub równoważne na minimum 4 poziomie.
- Przestrzeń chmurowa dostarczana wraz z oprogramowaniem to minimum 50GB w ramach jednej licencji, na cały okres jej trwania.

7. Wymagania co do modelu licencjonowania rozwiązania

- Możliwość zakupu licencji subskrypcyjnych w okresie 1/3/5 lat
- Model licencjonowania oparty na maszynach fizycznych – brak limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji)

8. Wykaz usług:

Instalacji i wdrożenia backupu na 53 stacjach roboczych Windows.

B. Oprogramowania do zabezpieczania danych poprzez mechanizm kopii zapasowych dedykowane dla środowisk serwerowych.

1. Oprogramowanie musi wspierać co najmniej systemy operacyjne:

- Windows XP i nowsze.
- Windows Server 2003 i nowsze.
- Windows SBS 2011/2008, 2003/2003R2.
- Windows Storage Server 2012/2012R2, 2008R2/2008/2003.
- Windows MultiPoint Server 2012/2011/2010.
- Linux.

2. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:

- Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www.

- Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego).
- Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych.
- Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu).
- Możliwość definiowania uprawnień dla administratorów systemu kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.).
- Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami.
- Wsparcie dla Single Sign On dla logowania do systemu.
- Możliwość zarządzania procesem tworzenia kopii zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT.
- Możliwość definiowania planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem).
- Możliwość tworzenia zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopii zapasowych.
- Możliwość zdalnej instalacji agentów kopii zapasowych z poziomu konsoli cyberochrony na maszynach z systemem operacyjnym Windows.
- Możliwość zdalnego uaktualniania agentów kopii zapasowych.
- Możliwość zdalnego zarządzania procesem wykonywania kopii zapasowej i odzyskiwania danych.
- Możliwość zdefiniowania dedykowanej maszyny, której agent kopii zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopii zapasowej).
- Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych.
- Centralny katalog wszystkich danych zapisanych w kopiach zapasowych.
- Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.

3. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:

- Kopie zapasowe całych dysków i partycji.
- Kopie zapasowe wybranych plików i folderów.
- Kopia zapasowa udziałów sieciowych.
- Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory)
- Kopie zapasowe baz danych Oracle.

- Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczonym przez producenta systemu kopi zapasowych.
- Zapis kopi zapasowych na udziały sieciowe.
- Zapis kopi zapasowych na serwer SFTP.
- Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana.
- Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloader), wraz z wsparciem LTO-9.
- Możliwość wyszukiwania plików w kopiach zapasowych.
- Możliwość szyfrowania plików kopi zapasowych.
- Wsparcia dla technologii VSS.
- Deduplikacja kopii zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć.
- Kompresja plików kopi zapasowych.
- Możliwość replikacji kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy).
- Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.

4. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:

- Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore.
- Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową.
- Odtworzenie poszczególnych plików i folderów.
- Automatyzacja procesu odtwarzania całych maszyn – np.: po zbootowaniu maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania).
- Granularne odtwarzanie baz danych Microsoft Exchange.
- Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange.
- Wyszukiwanie i podgląd odtwarzanych wiadomości email.
- Granularne odtwarzanie baz danych Microsoft SQL.
- Możliwość granularnego odtwarzania witryn i plików Microsoft SharePoint.
- Odtwarzanie kontrolerów domeny Microsoft Active Directory.
- Granularne odtwarzanie baz danych Oracle.
- Przywracanie przyrostu względem danych, które już się znajdują na dysku na który przywracana jest kopia zapasowa.

5. Dodatkowe (obowiązkowe) wymagania związane ochroną danych dla systemów Windows 7 i nowszych:

- Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń.
 - Skanowanie oprogramowania celem poszukiwania podatności. Podatności wypisane muszą być z minimum informacjami takimi jak nazwa produktu który zawiera podatność, maszyny na których znaleziono takie oprogramowanie, stopień ważności w skali CVSS.
6. Przestrzeń chmurowa dostarczana wraz z oprogramowaniem musi spełniać poniższe wymagania:
- W przypadku uzyskania uzasadnionej pewności, że doszło do naruszenia bezpieczeństwa, producent oprogramowania bez zbędnej zwłoki dostarczy informacje o takowym naruszeniu na adres e-mail podany podczas rejestracji konta.
 - W przypadku wyżej wymienionego naruszenia, producent podejmie kroki, aby udokumentować, naprawić i zminimalizować skutki naruszenia bezpieczeństwa w odniesieniu do danych osobowych oraz aby zapobiec jego powtórzeniu
 - Kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich repliki muszą być przechowywane na terenie Polski.
 - Producent przechowuje dane osobowe klienta (dane osobowe oraz kopie zapasowe) przy użyciu technik szyfrowania, minimum AES-256.
 - Producent nie wykorzystuje danych osobowych klienta bez anonimizacji w środowiskach programistycznych lub testowych.
 - Producent oprogramowania przeprowadza okresowe oceny ryzyka i przeglądy co najmniej raz w roku.
 - Infrastruktura (chmurowy magazyn kopii zapasowych) jest zaprojektowana zgodnie z podejściem N+1 (to, co niezbędne +1).
 - Producent oprogramowania jest zgodny z standardem bezpieczeństwa ISO 27001 lub równoważne SOC 2 lub równoważne, a magazyn kopii zapasowych musi być zgodny z certyfikatami ISO 9001 lub równoważne, ISO 27001 lub równoważne oraz certyfikację DCOS lub równoważne na minimum 4 poziomie.
 - Przestrzeń chmurowa dostarczana wraz z oprogramowaniem to minimum 250GB w ramach jednej licencji, na cały okres jej trwania.
7. Wymagania co do modelu licencjonowania rozwiązania:
- Możliwość zakupu licencji subskrypcyjnych w okresie 1/3/5 lat
 - Model licencjonowania oparty na maszynach fizycznych – brak limitów na chronioną ilość danych i aplikacji.
8. Wykaz usług:
- Instalacji i wdrożenia backupu na 3 serwerach fizycznych.

C. Oprogramowania do zabezpieczania danych poprzez mechanizm kopii zapasowych dedykowane dla środowisk wirtualizacyjnych.

1. Oprogramowanie musi wspierać co najmniej systemy operacyjne:

- o Dla hosta:
 - VMware ESX/ESX(i) 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0.
 - Hyper-V.
 - Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6.
 - Red Hat Virtualization 4.0, 4.1.
 - Linux KVM.
 - Oracle VM Server 3.0, 3.3, 3.4.
- o Dla maszyn wirtualnych:
 - Windows XP (SP3) i nowsze.
 - Windows Server 2003 i nowsze.
 - Windows SBS 2011/2008, 2003/2003R2.
 - Windows Storage Server 2012/2012R2, 2008R2/2008/2003.
 - Windows MultiPoint Server 2012/2011/2010.
 - Linux OS.
 - macOS.

2. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:

- Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www.
- Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego).
- Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych.
- Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu).
- Definiowanie uprawnień dla administratorów system kopii zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.).
- Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami.
- Wsparcie dla Single Sign On dla logowania do systemu.
- Zarządzanie procesem tworzenia kopii zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT.
- Definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem).

- Tworzenie zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopii zapasowych.
- Możliwość zdalnej instalacji agentów kopii zapasowych z poziomu konsoli cyberochrony na maszynach z systemem operacyjnym Windows.
- Zdalne uaktualniania agentów kopii zapasowych.
- Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych.
- Możliwość zdefiniowania dedykowanej maszyny, której agent kopii zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopii zapasowej).
- Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych.
- Centralny katalog wszystkich danych zapisanych w kopiach zapasowych
- Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.

3. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:

- Kopie zapasowe całych dysków i partycji.
- Kopie zapasowe wybranych plików i folderów.
- Kopia zapasowa udziałów sieciowych.
- Technologia bezagentowego wykonywania kopii zapasowej dla maszyn wirtualnych (dotyczy Hyper-V i VMWare ESXi).
- Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory)
- Kopie zapasowe baz danych Oracle.
- Kopie zapasowe hostów Hyper-V i VMWare ESXi.
- Zapis kopii zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczonym przez producenta systemu kopii zapasowych.
- Zapis kopii zapasowych na udziały sieciowe.
- Zapis kopii zapasowych na serwer SFTP.
- Zapis kopii zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana.
- Zapis kopii zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloaderzy).
- Możliwość wyszukiwania plików w kopiach zapasowych.
- Szyfrowanie plików kopii zapasowych.
- Wsparcie dla technologii VSS.
- Deduplikacja kopii zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć.
- Kompresja plików kopii zapasowych.

- Replikacja kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy).
 - Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.
4. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:
- Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore
 - Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową.
 - Odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej platformie sprzętowej.
 - Odtworzenie poszczególnych plików i folderów.
 - Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowaniu maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonana kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania).
 - Granularne odtwarzanie baz danych Microsoft Exchange.
 - Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange.
 - Wyszukiwanie i podgląd odtwarzanych wiadomości email.
 - Granularne odtwarzanie baz danych Microsoft SQL.
 - Granularne odtwarzanie witryn i plików Microsoft SharePoint.
 - Odtwarzanie kontrolerów domeny Microsoft Active Directory.
 - Granularne odtwarzanie baz danych Oracle.
 - Przywracanie przyrostu względem danych, które już się znajdują na dysku na który przywracana jest kopia zapasowa.
 - Dla hostów VMware ESXi i Hyper-V – uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej bez konieczności odtwarzania całej maszyny na hoście. Możliwość docelowego odtworzenia uruchomionej maszyny z pliku kopii zapasowej na wybranym hoście bez przerywania jej pracy.
5. Dodatkowe (obowiązkowe) wymagania związane ochroną danych dla systemów Windows 7 i nowszych:
- Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń.
 - Skanowanie oprogramowania celem poszukiwania podatności. Podatności wypisane muszą być z minimum informacjami takimi jak nazwa produktu który zawiera podatność, maszyny na których znaleziono takie oprogramowanie, stopień ważności w skali CVSS.

6. Przestrzeń chmurowa dostarczana wraz z oprogramowaniem musi spełniać poniższe wymagania:
- W przypadku uzyskania uzasadnionej pewności, że doszło do naruszenia bezpieczeństwa, producent oprogramowania bez zbędnej zwłoki dostarczy informacje o takowym naruszeniu na adres e-mail podany podczas rejestracji konta.
 - W przypadku wyżej wymienionego naruszenia, producent podejmie kroki, aby udokumentować, naprawić i zminimalizować skutki naruszenia bezpieczeństwa w odniesieniu do danych osobowych oraz aby zapobiec jego powtórzeniu.
 - Kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich repliki muszą być przechowywane na terenie Polski.
 - Producent przechowuje dane osobowe klienta (dane osobowe oraz kopie zapasowe) przy użyciu technik szyfrowania, minimum AES-256.
 - Producent nie wykorzystuje danych osobowych klienta bez anonimizacji w środowiskach programistycznych lub testowych.
 - Producent oprogramowania przeprowadza okresowe oceny ryzyka i przeglądy co najmniej raz w roku.
 - Infrastruktura (chmurowy magazyn kopii zapasowych) jest zaprojektowana zgodnie z podejściem N+1 (to, co niezbędne +1).
 - Producent oprogramowania jest zgodny z standardem bezpieczeństwa ISO 27001 lub równoważne SOC 2 lub równoważne, a magazyn kopii zapasowych musi być zgodny z certyfikatami ISO 9001 lub równoważne, ISO 27001 lub równoważne oraz certyfikację DCOS lub równoważne na minimum 4 poziomie.
 - Przestrzeń chmurowa dostarczana wraz z oprogramowaniem to minimum 250GB w ramach jednej licencji, na cały okres jej trwania.
7. Wymagania co do modelu licencjonowania rozwiązania:
- Możliwość zakupu licencji subskrypcyjnych w okresie 1/3/5 lat
 - Model licencjonowania oparty na maszynach fizycznych i hostach – brak limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji
8. Wykaz usług:

Instalacji i wdrożenia backupu na 8 serwerach wirtualnych.