Numer referencyjny postępowania:

**WSZ-EP-53/2024**

**Załącznik nr 1 do SWZ**

**Pakiet 1 –** dostawa wsparcia producenta do licencji na posiadane przez Zamawiającego oprogramowanie, dostawa wsparcia technicznego producenta na posiadany przez Zamawiającego sprzęt, dostawa licencji oraz zakup subskrypcji producenta na posiadane przez Zamawiającego urządzenia i systemy operacyjne.

W ramach realizacji zamówienia Wykonawca:

1. dostarczy odnowienie wsparcia technicznego producenta dla posiadanych przez Zamawiającego licencji (zgodnie z punktem 1 OPZ) na okres do dnia 30.09.2025 r.

VEMS Account: 7001297096

Customer Name : WOJEWODZKI SZPITAL ZESPOLONY IM. DR . ROMANA OSTRZ SZPITALNA 45 KONIN,62-504,PL

**Wymagane warunki:**

Dostarczenie w formie pdf lub papierowej certyfikatu odnowienia wsparcia producenta.

1. dostarczy odnowienie wsparcia technicznego producenta dla posiadanych przez Zamawiającego serwerów, biblioteki taśmowej, macierzy dyskowych, przełączników SAN zgodnie z punktem 2 OPZ.

**Wymagane warunki:**

Dostarczenie w formie pdf lub papierowej dokumentu producenta sprzętu potwierdzającego odnowienie wsparcia technicznego.

1. dostarczy odnowienie licencji i wsparcie techniczne producenta dla posiadanych przez Zamawiającego urządzeń zgodnie z punktem 3 OPZ na okres 12 mc-y.

**Wymagane warunki:**

Dostarczenie w formie pdf lub papierowej dokumentu producenta sprzętu potwierdzającego odnowienie licencji i wsparcia technicznego.

1. dostarczy odnowienie subskrypcji producenta dla posiadanych przez Zamawiającego systemów operacyjnych zgodnie z punktem 4 OPZ na okres 12 mc-y.

**Wymagane warunki:**

Dostarczenie w formie pdf lub papierowej dokumentu producenta oprogramowania potwierdzającego odnowienie subskrypcji.

1. dostarczy licencje wraz ze wsparciem technicznym producenta do posiadanego przez Zamawiającego oprogramowania INFOSCALE zgodnie z punktem 5 OPZ na okres 12 mc-y.

**Wymagane warunki:**

Dostarczenie w formie pdf lub papierowej dokumentu producenta oprogramowania potwierdzającego zakup licencji i wsparcia technicznego dla Zamawiającego.

1. dostarczy licencję czasową do oprogramowania Oracle Database SE2 na 2 CPU (Zamawiający dopuszcza licencję typu application specific lub full use) na okres 12 mc-y.

**Wymagane warunki:**

Dostarczenie w formie pdf lub papierowej dokumentu producenta oprogramowania potwierdzającego zakup licencji i wsparcia technicznego dla Zamawiającego.

**Kryteria Równoważności dla Licencji Czasowej do Oprogramowania Oracle Database SE2:**

1. **Rodzaj Licencji**
	* Licencja powinna być typu czasowego, obejmującego 12-miesięczny okres użytkowania.
	* Dopuszcza się zarówno licencje "application specific", jak i "full use".
2. **Wersja i Funkcjonalność**
	* Oprogramowanie musi być równoważne do Oracle Database SE2, oferując identyczne lub wyższe funkcje i możliwości.
	* Wszystkie dostępne w Oracle Database SE2 funkcje muszą być w pełni dostępne w proponowanym oprogramowaniu.
3. **Zakres Obciążeń (Processing Capacity)**
	* Oprogramowanie musi wspierać co najmniej dwa fizyczne procesory (CPU).
	* Wydajność bazy danych oraz wsparcie dla liczby użytkowników muszą być takie same lub lepsze, jak w przypadku Oracle Database SE2.
4. **Zgodność Techniczna**
	* Oprogramowanie musi być zgodne z obecnymi systemami Zamawiającego, na których działa Oracle Database SE2, zarówno na poziomie systemu operacyjnego, jak i innych powiązanych komponentów.
	* Musi wspierać aktualne standardy SQL oraz integrację z systemami korzystającymi z Oracle Database SE2.
5. **Licencjonowanie**
	* Licencja powinna obejmować użytkowanie na równoważnych warunkach do licencji Oracle (w zakresie ograniczeń licencyjnych, liczby procesorów oraz użytkowników).
	* Licencja powinna zapewniać prawo do wykorzystania oprogramowania przez okres 12 miesięcy.
6. **Wsparcie Techniczne**
	* W okresie licencji musi być zapewnione wsparcie techniczne, które obejmuje aktualizacje i poprawki bezpieczeństwa, na podobnym poziomie jak wsparcie dostępne dla Oracle Database SE2.
7. **Bezpieczeństwo i Aktualizacje**
	* Oprogramowanie musi zapewniać regularne aktualizacje oraz poprawki bezpieczeństwa, zgodnie z obecnymi standardami dla oprogramowania bazodanowego.
8. **Środowisko Użytkownika**
	* Możliwość działania na istniejącej infrastrukturze sprzętowej Zamawiającego bez konieczności wprowadzania modyfikacji lub konieczności zakupu dodatkowego sprzętu.
9. Wykaz licencji posiadanych przez Zamawiającego, których dotyczy odnowienie wsparcia technicznego producenta:

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa** | **Ilość szt.** |
| 1. | ESSENTIAL 12 MONTHS RENEWAL FOR NETBACKUP PLATFORM BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREMISE STANDARD PERPETUAL LICENSE GOV DO 30.09.2025 | 3 |
| 2. | ESSENTIAL 12 MONTHS RENEWAL FOR NETBACKUP ENTERPRISE VIRTUAL CLIENT WLS CPU HARDWARE TIER 4 ONPREMISE STANDARD PERPETUAL LICENSE GOV DO 30.09.2025 | 4 |
| 3. | ESSENTIAL 12 MONTHS RENEWAL FOR INFOSCALE ENTERPRISE LNX 1 CORE ONPREMISE STANDARD PERPETUAL LICENSE GOV DO 30.09.2025 | 12 |

Kryteria równoważności do wsparcia producenta dla wymienionych licencji NetBackup i InfoScale. Kryteria te mają na celu zapewnienie pełnej zgodności pod względem funkcjonalności, jakości oraz warunków serwisowych:

**1. ESSENTIAL 12-MONTHS RENEWAL FOR NETBACKUP PLATFORM BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREMISE STANDARD PERPETUAL LICENSE GOV**

**Kryteria równoważności:**

* **Wsparcie techniczne:** 24/7 dostęp do wsparcia technicznego, z zapewnieniem reakcji w przypadku krytycznych incydentów.
* **Aktualizacje oprogramowania:** Dostęp do wszystkich aktualizacji i poprawek bezpieczeństwa w trakcie okresu wsparcia.
* **Kompatybilność:** Wsparcie dla platformy z funkcjonalnością obejmującą zarządzanie i archiwizację danych na poziomie 1 Front End TB w środowisku on-premise.
* **Zakres wsparcia:** Pełna obsługa wersji oprogramowania NetBackup Platform Base, w tym wsparcie dla konfiguracji standardowych oraz nietypowych.
* **Gwarancja dostępu do dokumentacji:** Pełny dostęp do dokumentacji technicznej, baz wiedzy oraz wsparcia w zakresie optymalizacji konfiguracji.

**2. ESSENTIAL 12-MONTHS RENEWAL FOR NETBACKUP ENTERPRISE VIRTUAL CLIENT WLS CPU HARDWARE TIER 4 ONPREMISE STANDARD PERPETUAL LICENSE GOV**

**Kryteria równoważności:**

* **Wsparcie techniczne:** Całodobowy dostęp do wsparcia technicznego dla klienckich maszyn wirtualnych na poziomie Enterprise, z reakcją priorytetową dla incydentów krytycznych.
* **Aktualizacje:** Prawo do otrzymywania najnowszych aktualizacji, poprawek i łat bezpieczeństwa przez cały okres trwania umowy.
* **Kompatybilność:** Wsparcie dla wirtualnych środowisk obliczeniowych zgodnych z WLS CPU Hardware Tier 4.
* **Zakres wsparcia:** Utrzymanie i serwisowanie instalacji z licencją wieczystą, zapewnienie kompatybilności z nowymi wersjami wirtualnych systemów operacyjnych.
* **Gwarancja działania:** Wsparcie dla optymalizacji konfiguracji i wydajności oprogramowania oraz zgodność z obowiązującymi standardami bezpieczeństwa.

**3. ESSENTIAL 12-MONTHS RENEWAL FOR INFOSCALE ENTERPRISE LNX 1 CORE ONPREMISE STANDARD PERPETUAL LICENSE GOV**

**Kryteria równoważności:**

* **Wsparcie techniczne:** 24/7 dostęp do wsparcia technicznego, obejmujący pomoc w zakresie instalacji, konfiguracji i rozwiązywania problemów.
* **Aktualizacje oprogramowania:** Pełny dostęp do aktualizacji i poprawek, które mają wpływ na stabilność i bezpieczeństwo systemu.
* **Kompatybilność:** Obsługa platformy Linux (LNX) dla minimum 1 rdzenia CPU, działającego w środowisku on-premise.
* **Zakres wsparcia:** Pomoc techniczna w zakresie utrzymania oprogramowania InfoScale Enterprise, w tym wsparcie dla wdrożeń standardowych oraz zaawansowanych konfiguracji.
* **Dokumentacja i wiedza:** Pełny dostęp do bazy wiedzy, dokumentacji oraz najlepszych praktyk dotyczących wdrożeń i utrzymania systemu.
1. Wykaz odnowienia wsparcia technicznego producenta dla posiadanych przez Zamawiającego serwerów, biblioteki taśmowej, macierzy dyskowych, przełączników SAN, ze wskazaniem okresu, na jaki wsparcie ma zostać odnowione:

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa** | **Ilość szt.** |
| 1. | WSPARCIE TECHNICZNE PRODUCENTA LENOVO SYSTEM SR650 (THINKSYSTEM) SN: J303R1BZ 9x5 NBD DO 30.09.2025 | 1 |
| 2. | WSPARCIE TECHNICZNE PRODUCENTA LENOVO SYSTEM SR650 (THINKSYSTEM) SN: J303R1C0 9x5 NBD DO 30.09.2025 | 1 |
| 3. | WSPARCIE TECHNICZNE PRODUCENTA LENOVO SYSTEM SR650 (THINKSYSTEM) SN: J303R1BX 9x5 NBD DO 30.09.2025 | 1 |
| 4. | WSPARCIE TECHNICZNE PRODUCENTA LENOVO SYSTEM SR650 (THINKSYSTEM) SN: J303R1BY 9x5 NBD DO 30.09.2025 | 1 |
| 5. | WSPARCIE TECHNICZNE PRODUCENTA LENOVO SYSTEM SR650 (THINKSYSTEM) SN: J303X1VT 24x7 fix24 + POZOSTAWIANIE USZKODZONYCH DYSKÓW U ZAMAWIAJĄCEGO DO 30.09.2025 | 1 |
| 6. | WSPARCIE TECHNICZNE PRODUCENTA IBM TS4300 SN: 7800E61 9x5 NBD DO 02.10.2025 | 1 |
| 7. | WSPARCIE TECHNICZNE PRODUCENTA IBM TS4300 SN: 7801D0C 9x5 NBD DO 02.10.2025 | 1 |
| 8. | WSPARCIE TECHNICZNE PRODUCENTA IBM SN: 781G5T3 24x7 fix24 + POZOSTAWIANIE USZKODZONYCH DYSKÓW U ZAMAWIAJĄCEGO DO 02.10.2025 | 1 |
| 9. | WSPARCIE TECHNICZNE PRODUCENTA IBM SN: 781G9B8 24x7 fix24 + POZOSTAWIANIE USZKODZONYCH DYSKÓW U ZAMAWIAJĄCEGO DO 02.10.2025 | 1 |
| 10. | WSPARCIE TECHNICZNE PRODUCENTA IBM SN: 781G6A0 24x7 fix24 + POZOSTAWIANIE USZKODZONYCH DYSKÓW U ZAMAWIAJĄCEGO DO 02.10.2025 | 1 |
| 11. | WSPARCIE TECHNICZNE PRODUCENTA IBM SN: 781G9B9 24x7 fix24 + POZOSTAWIANIE USZKODZONYCH DYSKÓW U ZAMAWIAJĄCEGO DO 02.10.2025 | 1 |
| 12. | WSPARCIE TECHNICZNE PRODUCENTA IBM SN: 753727A 9x5 NBD DO 02.10.2025 | 1 |
| 13. | WSPARCIE TECHNICZNE PRODUCENTA IBM SN: 753727P 9x5 NBD DO 02.10.2025 | 1 |
| 14. | WSPARCIE TECHNICZNE PRODUCENTA IBM/LENOVO SN: 06CTTCD 11x5 NBD DO 30.09.2025 | 1 |
| 15. | WSPARCIE TECHNICZNE PRODUCENTA IBM/LENOVO SN: 06CE769 11x5 NBD DO 31.12.2024 PO TYM OKRESIE WSPARCIE TECHNICZNE NIE PRODUCENTA DO 02.10.2025 ZGODNIE Z KRYTERIAMI RÓWNOWAŻNOŚCI | 1 |
| 16. | WSPARCIE TECHNICZNE PRODUCENTA IBM/LENOVO SN: 06CE770 11x5 NBD DO 02.10.2025 PO TYM OKRESIE WSPARCIE TECHNICZNE NIE PRODUCENTA DO 02.10.2025 ZGODNIE Z KRYTERIAMI RÓWNOWAŻNOŚCI | 1 |
| 17. | WSPARCIE TECHNICZNE PRODUCENTA IBM/LENOVO SN: S4ANH468 9x5 + POZOSTAWIANIE USZKODZONYCH DYSKÓW U ZAMAWIAJĄCEGO 30.09.2025 | 1 |

**Kryteria równoważności wsparcia technicznego dla sprzętu Lenovo ThinkSystem SR650 oraz IBM TS4300**

1. **Czas reakcji i typ wsparcia**:
	* Dla urządzeń **Lenovo ThinkSystem SR650** wsparcie producenta w trybie **9x5** (9 godzin dziennie, 5 dni w tygodniu) z opcją **Next Business Day (NBD)**, czyli naprawą sprzętu następnego dnia roboczego.
	* Dla urządzeń **IBM TS4300** wsparcie producenta w trybie **9x5** (9 godzin dziennie, 5 dni w tygodniu) z opcją **Next Business Day (NBD)**, czyli naprawą sprzętu następnego dnia roboczego.
	* Dla urządzeń **IBM z serii SN: 781G5T3, 781G9B8, 781G6A0, 781G9B9** wsparcie w trybie **24x7 fix24**, które zapewnia dostępność technika serwisowego 24 godziny na dobę, 7 dni w tygodniu, oraz gwarancję naprawy w ciągu 24 godzin od zgłoszenia.
2. **Pozostawienie uszkodzonych części**:
	* Dla urządzeń **IBM z serii SN: 781G5T3, 781G9B8, 781G6A0, 781G9B9** wymóg **pozostawienia uszkodzonych dysków twardych** u zamawiającego, w celu zapewnienia bezpieczeństwa danych.
3. **Okres wsparcia**:
	* **Okres wsparcia** musi być zapewniony do odpowiednich dat dla każdego urządzenia, tj. do 30.09.2025 lub 02.10.2025, w zależności od sprzętu.
4. **Zakres wsparcia**:
	* **Wsparcie techniczne producenta** obejmujące zarówno pomoc zdalną, jak i wsparcie serwisowe na miejscu (on-site).
	* Dla urządzeń IBM TS4300 oraz Lenovo ThinkSystem SR650 wsparcie musi obejmować zarówno naprawę sprzętu, jak i dostarczenie niezbędnych części zamiennych.
5. **Równoważne wsparcie producenta**:
	* Wsparcie powinno być oferowane bezpośrednio przez **producenta sprzętu** lub autoryzowanego partnera serwisowego producenta, który posiada stosowne certyfikaty.
6. **Zakres dostępności części zamiennych**:
	* Gwarancja **dostępności części zamiennych** przez cały okres trwania wsparcia.
7. **Dodatkowe wymagania**:
	* Wsparcie musi być świadczone przez personel posiadający odpowiednie **certyfikaty producenta** na obsługę serwisową sprzętu IBM/LENOVO.
	* Możliwość **rejestracji zgłoszeń serwisowych** w systemie producenta oraz śledzenia ich statusu.
8. **Czas naprawy**:
	* W przypadku opcji **fix24** - naprawa musi być zakończona w ciągu maksymalnie **24 godzin** od zgłoszenia awarii.
9. **Zgłaszanie awarii**:
	* Możliwość zgłaszania awarii zarówno telefonicznie, jak i online, z możliwością śledzenia statusu zgłoszenia w czasie rzeczywistym.
10. **Umowa SLA**:
	* Określenie **poziomu usług (SLA)**, które obejmują czas reakcji na zgłoszenie, czas naprawy oraz dostępność wsparcia technicznego.
11. Wykaz urządzeń i licencji posiadanych przez Zamawiającego, których dotyczy odnowienie:

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa** | **Ilość szt.** |
| 1. | FortiGate-100F 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) SN: FG100FTK2200544 | 1 |
| 2. | FortiGate-100F 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) SN: FG100FTK2200591 | 1 |

Kryteria równoważności dla urządzeń FortiGate-100F na subskrypcję i wsparcie techniczne:

1. **Urządzenie**:
	* FortiGate-100F lub równoważne pod względem funkcjonalności, wydajności oraz przepustowości sieciowej.
2. **Ochrona zagrożeń (UTP)**:
	* Zintegrowana ochrona przed zagrożeniami obejmująca IPS (Intrusion Prevention System), zaawansowaną ochronę przed złośliwym oprogramowaniem, kontrolę aplikacji, filtrowanie URL, filtrowanie DNS oraz filtrowanie wideo.
	* Antyspam - usługa zapewniająca skuteczną ochronę przed niechcianą pocztą.
3. **FortiCare Premium lub Równoważne wsparcie techniczne**:
	* Wsparcie techniczne 24/7 z dostępem do centrum wsparcia i baz wiedzy.
	* Czas reakcji: zapewnienie szybkiego wsparcia dla zgłoszonych incydentów, czas reakcji nie gorszy niż w FortiCare Premium.
	* Możliwość wymiany sprzętu w przypadku awarii.
	* Aktualizacje oprogramowania i subskrypcji zabezpieczeń.
4. **Przepustowość i Wydajność**:
	* Urządzenie o przepustowości porównywalnej do FortiGate-100F, z minimalną przepustowością zapory wynoszącą 20 Gbps.
	* Wydajność IPS na poziomie co najmniej 1,6 Gbps.
5. **Subskrypcja**:
	* Subskrypcja zapewniająca dostęp do aktualizacji zabezpieczeń, sygnatur zagrożeń oraz wsparcia technicznego przez okres minimum jednego roku.
6. **Funkcjonalności dodatkowe**:
	* Obsługa VPN (IPsec oraz SSL VPN) z możliwością jednoczesnej obsługi użytkowników VPN na poziomie FortiGate-100F.
	* Możliwość zarządzania urządzeniem za pomocą interfejsu GUI oraz CLI.
	* Obsługa segmentacji sieci i VLAN.
7. **Zgodność i Licencje**:
	* Licencje muszą obejmować wszystkie wymienione moduły i funkcje przez okres minimum jednego roku, zapewniając równoważną ochronę i wsparcie jak Unified Threat Protection (UTP) oferowany przez Fortinet.
8. Wykaz subskrypcji do odnowienia dla posiadanych przez Zamawiającego systemów operacyjnych:

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa** | **Ilość szt.** |
| 1. | RedHat Subs – 1 Year | 3 |

**Kryteria równoważności dla subskrypcji RedHat – 1 rok:**

1. **Zakres wsparcia technicznego:**
	* Wsparcie 24/7 z gwarantowanym czasem odpowiedzi.
	* Dostęp do aktualizacji, poprawek bezpieczeństwa oraz nowych wersji oprogramowania.
	* Możliwość korzystania z portalu wsparcia technicznego z bazą wiedzy, dokumentacją i systemem zgłoszeń.
2. **Gwarancja kompatybilności:**
	* Subskrypcja musi zapewniać pełną kompatybilność z oprogramowaniem RedHat Enterprise Linux (RHEL) lub jego odpowiednikiem.
	* Obsługa architektury sprzętowej i wersji oprogramowania równoważnej do RHEL.
3. **Oprogramowanie klasy Enterprise:**
	* Produkt musi być przeznaczony do wdrożeń klasy enterprise z naciskiem na wysoką niezawodność i stabilność działania.
	* Dostępność dodatkowych modułów i rozszerzeń równoważnych z rozwiązaniami oferowanymi przez RedHat.
4. **Bezpieczeństwo:**
	* Oprogramowanie musi posiadać podobne mechanizmy bezpieczeństwa oraz częstotliwość aktualizacji poprawek zabezpieczeń jak RedHat.
	* Musi spełniać wymogi zgodności z normami bezpieczeństwa, jakie wymagane są dla systemów używanych w organizacji (np. FIPS, CIS).
5. **Zgodność z otwartymi standardami:**
	* Produkt musi być oparty na otwartym kodzie źródłowym, co zapewnia możliwość weryfikacji i dostosowywania oprogramowania do specyficznych potrzeb.
	* Wsparcie dla narzędzi i technologii zgodnych z RHEL, takich jak Ansible, OpenShift itp.
6. **Certyfikacja:**
	* Produkt musi posiadać certyfikację równoważną do RedHat, która jest uznawana przez kluczowych dostawców sprzętu i oprogramowania (np. VMware, SAP, Oracle).
7. **Warunki licencyjne:**
	* Subskrypcja musi obejmować taki sam lub równoważny zakres licencyjny – dostęp dla określonej liczby instancji systemowych (np. licencja na serwery fizyczne lub wirtualne).
8. **Wsparcie społeczności:**
	* Dostęp do wsparcia społecznościowego oraz baz wiedzy o porównywalnym zakresie, jak dla RedHat.
9. Wykaz posiadanego przez Zamawiającego oprogramowania INFOSCALE, którego dotyczy dostarczenie dodatkowych licencji wraz ze wsparciem technicznym producenta:

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa** | **Ilość szt.** |
| 1. | INFOSCALE ENTERPRISE LNX 1 CORE ONPREMISE STANDARD PERPETUAL LICENSE GOV | 4 |

Kryteria równoważności dla zakupu licencji INFOSCALE ENTERPRISE LNX 1 CORE ONPREMISE STANDARD PERPETUAL LICENSE GOV

 **Typ licencji**: Licencja powinna być **perpetualna** (wieczysta) i dedykowana dla środowisk on-premise, aby zapewnić stały dostęp do oprogramowania bez ograniczeń czasowych.

 **System operacyjny**: Oprogramowanie musi być kompatybilne z systemem operacyjnym **Linux** w środowisku serwerowym.

 **Wersja licencji**: Oprogramowanie powinno być dostępne w wersji odpowiadającej **licencji standardowej** dla 1 rdzenia procesora, umożliwiającej jego elastyczne wykorzystanie w środowisku wirtualnym lub fizycznym.

 **Wymagania funkcjonalne**:

* **Zarządzanie danymi**: Oprogramowanie musi zapewniać **wysoką dostępność i ochronę danych**, umożliwiając szybkie przywracanie danych w razie awarii.
* **Replikacja danych**: Musi wspierać **replikację danych** pomiędzy różnymi lokalizacjami, aby minimalizować ryzyko utraty danych.
* **Konsolidacja pamięci masowej**: Oprogramowanie powinno umożliwiać **konsolidację pamięci masowej**, obsługując różne typy macierzy dyskowych.

 **Wydajność i skalowalność**: Oprogramowanie musi wspierać **skalowanie** zgodnie z rosnącymi wymaganiami infrastruktury, zarówno pod kątem mocy obliczeniowej, jak i przestrzeni dyskowej.

 **Wsparcie dla środowisk wirtualnych**: Powinno zapewniać pełną kompatybilność z wiodącymi platformami wirtualizacyjnymi, takimi jak **VMware, Hyper-V** czy **KVM**.

 **Bezpieczeństwo**: Oprogramowanie powinno zapewniać zaawansowane mechanizmy **szyfrowania danych** oraz ochronę przed nieautoryzowanym dostępem.

 **Wsparcie techniczne**: Dostawca powinien oferować **wsparcie techniczne** na poziomie odpowiadającym licencji dla instytucji rządowych (GOV), w tym dostęp do aktualizacji i poprawek bezpieczeństwa.

 **Certyfikaty i zgodność**: Oprogramowanie musi spełniać standardy i posiadać certyfikaty odpowiednie dla zastosowań w sektorze publicznym, takie jak **FIPS, ISO/IEC 27001**, oraz być zgodne z wymogami **RODO** (GDPR).

 **Model licencjonowania**: Licencja powinna być oferowana na **poziomie rdzenia procesora**, co pozwala na elastyczne dopasowanie do wymagań sprzętowych.

Kryteria równoważności dla InfoScale:

**InfoScale – Kryteria równoważności:**

1. **Wysoka dostępność**: Rozwiązanie musi oferować mechanizm automatycznego przełączania awaryjnego (failover) w przypadku awarii serwera, który zapewnia przełączenie w czasie nie dłuższym niż 60 sekund.
2. **Zarządzanie pamięcią masową**: System musi umożliwiać dynamiczne zarządzanie przestrzenią dyskową z możliwością rozbudowy w czasie rzeczywistym bez przerw w działaniu aplikacji.
3. **Replikacja danych**: Oprogramowanie musi oferować replikację danych między różnymi lokalizacjami z maksymalnym opóźnieniem do 5 minut. Replikacja musi być możliwa w trybie synchronicznym lub asynchronicznym.
4. **Integracja z różnymi środowiskami**: Wymagana jest kompatybilność z przynajmniej trzema systemami operacyjnymi (np. Windows Server, Red Hat Linux, SUSE Linux) oraz wsparcie dla platform wirtualizacyjnych, takich jak VMware i Hyper-V.
5. **Monitorowanie i raportowanie**: Rozwiązanie musi posiadać wbudowane mechanizmy monitorowania w czasie rzeczywistym oraz generowania raportów dostępności, wydajności i wykorzystania zasobów z możliwością ich eksportu do formatów CSV oraz PDF.

**Dodatkowy warunek**:

Wykonawca zobowiązuje się, na swój własny koszt, przeprowadzić migrację oprogramowania posiadanego przez zamawiającego do nowego, oferowanego rozwiązania równoważnego. Migracja obejmuje pełne przeniesienie danych, konfiguracji oraz testowanie działania w celu zapewnienia ciągłości funkcjonowania usług. Migracja musi zostać wykonana w ciągu 3 dni kalendarzowych.

**Pakiet 2 –** dostawa licencji na oprogramowanie antywirusowe ESET PROTECT

1. **W ramach realizacji zamówienia Wykonawca:**

 dostarczy licencje na oprogramowanie antywirusowe ESET PROTECT (przedłużenie 500 licencji na okres jednego roku).

1) nazwa programu i opis: ESET PROTECT ENTERPRISE:

– wznowienie 500 rocznych licencji,

– kontynuacja z licencją na okres 12 miesięcy,

– nazwa użytkownika pozostaje bez zmian,

– hasło pozostaje bez zmian;

2) ilość licencji: 500, każda na 1 rok,

3) rodzaj licencji: CLIENT (do pobrania ze strony WWW producenta),

4) identyfikator publiczny licencji: 3AH-86R-DP4.

Zamawiający dopuszcza możliwość dostawy rozwiązania równoważnego.

Wymagania dotyczące sposobu realizacji zamówienia:

1) Wykonawca gwarantuje, że dostarczone oprogramowanie komputerowe w ramach realizacji umowy pochodzi z legalnego źródła (dystrybucji) i nie jest częścią żadnego projektu oferowanego dla innych podmiotów na terenie Unii Europejskiej.

2) Wykonawca gwarantuje, że dostarczone oprogramowanie komputerowe w ramach realizacji umowy będzie fabrycznie nowe z bieżącej produkcji i będzie posiadało gwarancję.

3) Wykonawca dostarczy przedmiot umowy w wersji elektronicznej, do pobrania przez Zamawiającego z serwisu internetowego producenta oprogramowania.

4) Wykonawca zapewni dostęp do pomocy technicznej, umożliwiając zgłaszanie wad i usterek drogą internetową lub telefoniczną.

5) Wykonawca dostarczy licencje potwierdzającą wznowienie licencji w terminie nie dłuższym niż 14 dni od daty zawarcia Umowy (kryterium oceny oferty)

Zamawiający dopuszcza zapewnienie rozwiązania równoważnego do licencji na oprogramowanie antywirusowe, z którego obecnie korzysta Zamawiający. Licencje na rozwiązanie równoważne obowiązujące przez okres 12 miesięcy od momentu dostarczenia licencji. Szczegółowy opis równoważności znajduje się w pkt 2.

1. **Opis równoważności** (kryteria równoważności)

Za rozwiązanie równoważne Zamawiający uzna rozwiązanie spełniające wymagania opisane w pkt. 1 (za wyjątkiem nazwy oprogramowania, niezmienności hasła i nazwy użytkownika i identyfikatora) oraz poniższe wymagania:

1. Dostawę oprogramowania nie gorszego od posiadanych przez Zamawiającego.

2. Spełniających szczegółowe wymagania opisane w pkt. 3 OPZ.

3. Zapewnienie usługi kompletnej nieinwazyjnej deinstalacji dotychczasowego oprogramowania antywirusowego z całej infrastruktury informatycznej (komputerów i serwerów) Zamawiającego w ciągu 1 dnia roboczego.

4. Zapewnienie usługi kompletnej nieinwazyjnej instalacji i konfiguracji nowego rozwiązania
w infrastrukturze informatycznej Zamawiającego.

5. Zapewnienia dodatkowego wsparcia technicznego (zdalnego oraz, w razie potrzeby bezpośredniego – realizowanego w siedzibie Zamawiającego) przez Wykonawcę przez okres miesiąca od daty wdrożenia produkcyjnego rozwiązania równoważnego.

6. Przeszkolenie do 6 pracowników Zamawiającego z zakresu obsługi, konfiguracji i administracji całości rozwiązania równoważnego.

7. Wdrożenie, szkolenie, asysta techniczna i dodatkowe wsparcie techniczne Wykonawcy –
w języku polskim.

8. Usługi wdrożeniowe równoważnego oprogramowania antywirusowego zostaną zrealizowane w terminie do 5 dni od daty zawarcia umowy.

8. Usługi wdrożeniowe obejmują:

a) Instalacje, konfiguracje i uruchomienie produkcyjne oprogramowania antywirusowego
i systemu, zgodnie z zaleceniami Zamawiającego.

b) Świadczenie bezpośredniej, w siedzibie Zamawiającego, asysty technicznej przez cały okres wdrożenia.

c) Szkolenia.

3. Wymagania w stosunku do wdrożenia równoważnego oprogramowania antywirusowego:

Wymagania odnośnie wspieranych systemów operacyjnych:

1. Microsoft Windows: 10 Professional, 11 Professional

2. Windows Server: 2008, 2012, 2022 (Zamawiający wymaga rozwiązanie wspierające
w najnowszej wersji systemy Windows Server 2012 i nowsze oraz dopuszcza rozwiązane
w starszej wersji systemy Windows Server 2008)

3. Debian Linux

4. Oracle Linux

5. Ubuntu LTS

6. Fedora Linux

Moduły:

***CENTRALNE ZARZĄDZANIE***

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Microsoft Windows Server (od wersji 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego
w formacie VHD.

2. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.

3. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.

4. Dostęp do konsoli centralnego zarządzania musi odbywać się w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.

5. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.

6. Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.

7. Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS i Android (Zamawiający dopuszcza rozwiązanie polegające na obsłudze urządzeń Android i iOS w konsoli chmurowej)

8. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.

9. Serwer administracyjny musi pozwalać na weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).

10. Serwer administracyjny musi pozwalać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.

11. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania
do konsoli administracyjnej.

12. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.

13. Serwer administracyjny musi posiadać minimum 100 szablonów raportów, przygotowanych przez producenta oraz możliwość tworzenia własnych raportów przez administratora.

14. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.

15. Serwer administracyjny musi posiadać możliwość podziału uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

***OCHRONA STACJI ROBOCZYCH***

1. Pełne wsparcie dla systemu Microsoft Windows Professional 10, 11.

2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

4. Wbudowana technologia do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.

5. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

8. Możliwość skanowania plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.

9. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (min. SHA2) oraz lokalizacji pliku.

10. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.

11. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

12. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.

13. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

14. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

15. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

16. Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.

17. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.

18. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.

19. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz
z możliwością wykorzystania reguł utworzonych przez użytkownika,

• tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

• tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

• tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

20. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

21. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.

22. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.

23. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

24. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

25. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.

***OCHRONA SERWERA PLIKÓW***

1. Wsparcie dla systemów Microsoft Windows Server 2012 i nowszych,

2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

4. Wbudowana technologia do ochrony przed rootkitami i exploitami.

5. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.

6. Aplikacja musi wspierać mechanizm klastrowania.

7. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).

8. Program musi oferować możliwość skanowania dysków sieciowych typu NAS.

9. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

10. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.

11. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony i nie wymaga restartu serwera.

12. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.

13. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).

14. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

15. System antywirusowy musi wspierać automatyczną, inkrementacyjną aktualizację silnika

detekcji.

16. System antywirusowy musi wspierać skanowanie magazynu Hyper-V.

17. System antywirusowy musi posiadać możliwość wykluczania ze skanowania procesów.

18. System antywirusowy musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

19. System antywirusowy musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.

20. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

21. System antywirusowy musi posiadać ochronę przed przyłączeniem komputera do sieci botnet.

22. System antywirusowy musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

23. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

24. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.

25. Program musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

***PEŁNE SZYFROWANIE DYSKÓW***

1. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.

2. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.

3. Aplikacja musi mieć możliwość korzystania z technologii TCG OPAL - dyski sprzętowo szyfrowane.

4. Aplikacja do szyfrowania musi być zarządzana z poziomu konsoli webowej, wykorzystywanej do zarządzania produktem do ochrony antywirusowej.

5. Konsola centralnego zarządzania musi pozwalać na wygenerowanie, dla każdej zaszyfrowanej stacji, dysku ratunkowego.

6. Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach

roboczych, w oparciu o przynajmniej:

a) ilość znaków,

b) czy hasło ma zawierać wielkie litery,

c) czy hasło ma zawierać małe litery,

d) czy hasło ma zawierać cyfry,

e) czy hasło ma zawierać znaki specjalne,

f ) okres ważności,

g) ilość nieudanych logowań,

h) możliwość zmiany hasła.

7. Aplikacja musi posiadać możliwość ograniczenia wyświetlania interfejsu graficznego użytkownikom.

8. Administrator musi posiadać możliwość zablokowania dostępu do zaszyfrowanego dysku.

***ROZWIĄZANIE KLASY ENDPOINT DETECTION AND RESPONSE***

1. System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.

2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.

3. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

4. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.

5. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.

6. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-2, nazwę komputera, grupę, użytkownika.

7. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-2, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.

8. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.

9. Konsola administracyjna musi mieć możliwość tagowania obiektów.

10. Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli.

11. Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci.

12. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością

wykonywania poleceń powershell.