**Załącznik nr 1a do SWZ**

**Opis Przedmiotu Zamówienia**

Przedmiotem zamówienia jest przedłużenie licencji na oprogramowanie antywirusowe ESET Protect Enterprise lub równoważne, odnowienie 118 posiadanych licencji oprogramowania antywirusowego dla Starostwa Powiatowego w Golubiu-Dobrzyniu na minimalny okres do 16.02.2026 r. z możliwością używania zakupionych i wdrożonych licencji w 11 podległych jednostkach organizacyjnych wg podziału:

1. Powiatowe Centrum Pomocy Rodzinie w Golubiu-Dobrzyniu -10 licencji
2. Poradnia Psychologiczno-Pedagogiczna w Golubiu-Dobrzyniu - 12 licencji
3. Dom Pomocy Społecznej w Golubiu-Dobrzyniu - 5 licencji
4. Specjalny Ośrodek Szkolno-Wychowawczy w Wielgiem - 35 licencji
5. Powiatowa Placówka Opiekuńczo-Wychowawcza w Wielgiem - 10 licencji
6. Powiatowa Placówka Opiekuńczo-Wychowawcza typu specjalistyczno-terapeutycznego w Golubiu-Dobrzyniu -10 licencji
7. Powiatowe Centrum Opiekuńczo-Mieszkalne w Golubiu-Dobrzyniu - 5 licencji
8. Powiatowy Środowiskowy Dom Samopomocy w Golubiu-Dobrzyniu - 5 licencji
9. Zarząd Dróg Powiatowych w Golubiu-Dobrzyniu - 6 licencji
10. Publiczna Szkoła Muzyczna I stopnia w Golubiu-Dobrzyniu - 10 licencji
11. Publiczna Szkoła Muzyczna I stopnia w Kowalewie Pomorskim - 10 licencji

Nr użytkownika: EAV-0415365019, odnowienie na minimalny okres do 16.02.2026 r. Wydłużenie okresu licencjonowania stanowi jedno z kryteriów oceny ofert. Aktualna licencja ważna jest do dnia 18.05.2025 r.

2. Okres na jaki będzie nabywane przedłużenie licencji nie może być krótszy niż do 16.02.2026 r.

3. Zawarte w Opisie przedmiotu zamówienia wymagania i zobowiązania Wykonawcy - o ile nie zastosowano wyłączenia - dotyczą zarówno Wykonawcy, który dostarczy oprogramowanie wymagane, jak i Oprogramowanie równoważne.

4. Oprogramowanie wymienione w Opisie przedmiotu zamówienia musi pochodzić bezpośrednio od producenta lub z oficjalnych i autoryzowanych przez producenta kanałów dystrybucyjnych.

5. Zamawiający wymaga, aby Wykonawca dostarczył najnowsze wersje Oprogramowania i umożliwił jego aktualizację w każdym momencie użytkowania.

6. Wykonawca dostarczy Zamawiającemu wszelkie dane niezbędne do prawidłowego uruchomienia i korzystania z Oprogramowania.

7. Zamawiający wymaga świadczenia usługi wsparcia technicznego przez cały okres używania Oprogramowania lub Oprogramowania równoważnego. Usługa wsparcia technicznego świadczona będzie przez producenta lub autoryzowany przez niego podmiot (w przypadku, gdy wsparcie techniczne będzie świadczone przez autoryzowany podmiot Wykonawca załączy do oferty oświadczenie producenta w tym zakresie).

8. Zakres usługi wsparcia to:

1) zapewnienie świadczenia obsługi zgłoszeń serwisowych we wszystkie dni tygodnia w formie elektronicznej - poprzez internetowy serwis asysty technicznej lub dedykowaną skrzynkę mailową, a także obsługę telefoniczną.

2) elektroniczny dostęp do informacji na temat posiadanego Oprogramowania, biuletynów technicznych, poprawek programistycznych oraz bazy danych zgłoszonych problemów technicznych przez 24 godziny na dobę, 7 dni w tygodniu przez internetowy serwis asysty technicznej,

3) publikowanie i udostępnianie aktualizacji dokumentacji do Oprogramowania w postaci elektronicznej przez internetowy serwis asysty technicznej producenta, takich jak np.: techniczna dokumentacja, internetowa baza wiedzy lub forum internetowe producenta Oprogramowania oraz informowanie o dostępnych aktualizacjach, np. poprzez newsletter lub dedykowaną stronę WWW udostępnioną Jednostkom.

4) publikowanie i udostępnianie wersji instalacyjnych Oprogramowania (w tym dostęp do aktualizacji wersji, poprawek programistycznych, wydań uzupełniających Oprogramowania objętego usługą wsparcia) do pobrania poprzez internetowy serwis asysty technicznej producenta (nowe wersje Oprogramowania mają być dostępne dla Jednostek, od momentu publikacji w internetowym serwisie asysty technicznej producenta, przez cały okres obowiązywania wsparcia technicznego dla Oprogramowania)

5) przyjmowanie, rejestrowanie, monitorowanie i obsługiwanie zgłoszeń serwisowych przez Wykonawcę (w tym także telefonicznych).

9. Sposób dostawy Oprogramowania:

1) Wykonawca w terminie do 14 dni kalendarzowych od dnia podpisania Umowy zapewnia Jednostce możliwość pobierania zamówionego Oprogramowania i kluczy licencyjnych za pośrednictwem witryny producenta - strony internetowej wskazanej przez Wykonawcę.

2) Możliwość pobierania wersji instalacyjnych Oprogramowania producenta, o których mowa w ust. 1) będzie zapewniona w trybie 24 godziny na dobę, 7 dni w tygodniu.

3) Na potwierdzenie prawidłowej realizacji dostawy Strony podpiszą Protokół odbioru Oprogramowania.

**Parametry minimalne lub równoważne dla oprogramowania równoważnego:**

**I. Administracja zdalna w chmurze**

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.

2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.

3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.

4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.

5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.

6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.

7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.

8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.

9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.

10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.

11. 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.

12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

**II. Ochrona stacji roboczych**

1. Rozwiązanie musi wspierać posiadane przez Zamawiającego systemy operacyjne Microsoft Windows 10 / 11.

2. Rozwiązanie musi wspierać architekturę ARM64.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.

5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.

9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.

10. Rozwiązanie musi zapewniać 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).

11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

12. Rozwiązanie musi posiadać 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.

13. Rozwiązanie musi zapewniać 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.

14. Rozwiązanie musi posiadać funkcję 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.

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

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

b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

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

d. tryb uczenia się, w którym rozwiązanie 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,

e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, 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.

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

18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

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

21. Rozwiązanie musi posiadać ochronę antyspamową dla posiadanego przez Zamawiającego programu pocztowego MS Outlook.

22. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

a. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,

b. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

c. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,

d. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

23. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.

24. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

25. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.

27. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.

28. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

29. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

**III. Ochrona serwera**

1. Rozwiązanie musi wspierać posiadane przez Zamawiającego systemy operacyjne Microsoft Windows Server 2012 i nowsze oraz Linux.

2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.

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

6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

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

**IV. Dodatkowe wymagania dla ochrony posiadanych przez Zamawiającego serwerów Windows:**

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej Microsoft OneDrive.

2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).

3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.

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

5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych oraz urządzeń przenośnych.

6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.

7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.*

8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

**V. Dodatkowe wymagania dla ochrony posiadanych przez Zamawiającego serwerów Linux:**

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.

2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.

3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN.

4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

**VI. Szyfrowanie**

1. System szyfrowania danych musi wspierać instalację posiadanych przez Zamawiającego aplikacji klienckich w środowisku minimum Microsoft Windows.

2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).

3. 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.

4. Aplikacja musi umożliwiać szyfrowanie danych na komputerach z UEFI.

**VII. Ochrona urządzeń mobilnych opartych o system Android**

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.

2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.

3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.

5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

a. usunięcie zawartości urządzenia,

b. przywrócenie urządzenie do ustawień fabrycznych,

c. zablokowania urządzenia,

d. uruchomienie sygnału dźwiękowego,

e. lokalizację GPS.

6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.

7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:

a. nazwę aplikacji,

b. nazwę pakietu,

c. kategorię sklepu Google Play,

d. uprawnienia aplikacji,

e. pochodzenie aplikacji z nieznanego źródła.

**VIII. Moduł XDR**

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.

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

3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.

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

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

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

7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.

8. Serwer musi posiadać zestaw wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.

9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.

10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.

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

12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.

13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.

14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.

15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: 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) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.

16. Konsola administracyjna musi mieć możliwość tagowania obiektów.

17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.