

Załącznik nr 1 do ogłoszenia: Opis potrzeb Zamawiającego

## **1. Cel:**

Zamawiający planuje przedłużenie licencji dla 3500 użytkowników oprogramowania antywirusowego ESET PROTECT Advanced z zarządzaniem lokalnym i chmurowym na okres 46 miesięcy od dnia 1.07.2026 r. albo dostawę oprogramowania równoważnego do oprogramowania ESET PROTECT Advanced, ze wsparciem producenta, na okres 46 miesięcy od dnia 1.07.2026 r. W przypadku zaoferowania oprogramowania równoważnego do ESET PROTECT Advanced, Wykonawca będzie zobowiązany do przeprowadzenia szkoleń.

Środowisko Zamawiającego:

Zamawiający obecnie posiada licencję dla 4700 użytkowników oprogramowania ESET PROTECT Advanced z zarządzaniem lokalnym i chmurowym ważną do dnia 31.06.2026 r.

Powyższe oprogramowanie przeznaczone jest dla komputerów i urządzeń mobilnych pracowników Państwowej Inspekcji Pracy, na których zainstalowany jest Windows 11 Pro 64-bit lub Android/IOS, dlatego zaoferowane oprogramowanie musi być w pełni kompatybilne z wymienionymi systemami.

## **2. Wymagania dotyczące oprogramowania ESET PROTECT Advanced**

ESET PROTECT Advanced z zarządzaniem lokalnym i chmurowym – licencja dla 3500 użytkowników ważna 46 miesięcy od dnia 1.07.2026 r. wraz ze wsparciem producenta. Jedna licencja na użytkownika pozwalająca na jednoczesne używanie oprogramowania antywirusowego na komputerze i urządzeniu mobilnym.

Przez wsparcie producenta należy rozumieć:

- 1) dedykowany adres mailowy, na który są wysyłane zgłoszenia;
- 2) priorytetowa obsługa zgłoszeń serwisowych;
- 3) podejmowanie nowych zgłoszeń serwisowych tego samego dnia (wysłanych do godz. 15.00);
- 4) wsparcie producenta przez okres 46 miesięcy od dnia 1.07.2026 r

## **3. Wymagania dotyczące oprogramowania równoważnego**

Oprogramowanie równoważne do oprogramowania ESET PROTECT Advanced z zarządzaniem lokalnym i chmurowym – licencja dla 3500 użytkowników ważna 46 miesięcy od dnia 1.07.2026 r. wraz ze wsparciem producenta. Jedna licencja na użytkownika pozwalająca na jednoczesne używanie oprogramowania antywirusowego na komputerze i urządzeniu mobilnym. Dopuszcza się zaoferowanie oddzielnej licencji dla urządzeń komputerowych i mobilnych przy założeniu ochrony dla 3500 urządzeń komputerowych i serwerów oraz dla 3000 urządzeń mobilnych.

Przez wsparcie producenta należy rozumieć:

- 1) dedykowany adres mailowy, na który są wysyłane zgłoszenia;
- 2) priorytetowa obsługa zgłoszeń serwisowych;
- 3) podejmowanie nowych zgłoszeń serwisowych tego samego dnia (wysłanych do godz. 15.00).
- 4) Wsparcie producenta przez okres 46 miesięcy od dnia 1.07.2026 r.

Oprogramowanie równoważne do oprogramowania ESET PROTECT Advanced, musi spełniać następujące minimalne wymagania (oprogramowanie równoważne musi spełniać niżej wymienione minimalne wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji):

#### I. Wymagania ogólne:

1. Pełne wsparcie dla systemu Windows 11, Android/iOS.
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows 11.
3. Wersja systemu dla stacji roboczych Windows 11 dostępna zarówno w języku polskim jak i angielskim.
4. Instalator musi umożliwiać wybór wersji językowej systemu Windows 11, przed rozpoczęciem procesu instalacji.
5. Pomoc w systemie (help) i dokumentacja do systemu Windows 11, dostępna w języku polskim.

#### II. Administracja zdalna:

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2019,2022,2025 oraz systemach Linux.
2. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.
3. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
4. Konsola administracyjna musi umożliwiać podgląd szczegółów dotyczących bazy danych, takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.
5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
6. 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.

7. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
8. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy.
9. Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.
10. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.
11. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.
12. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
13. Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym.
14. Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
15. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
16. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
17. Serwer administracyjny musi posiadać wsparcie dla „VDI” oraz „Golden Master Image”.
18. Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów.
19. Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy.
20. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
21. Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
22. Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS.
23. Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP.
24. Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń, takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11.
25. Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap.
26. Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych.
27. Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów.

28. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
29. 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.
30. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.
31. Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS.
32. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zaporą osobistą, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
33. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
34. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
35. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, 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 dla systemów Windows oraz MacOS z możliwością jego odinstalowania.
36. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
37. Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.
38. W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play.
39. Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
40. Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzeniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS.

41. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
42. Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.
43. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
44. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
45. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
46. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.
47. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.
48. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
49. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
50. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.
51. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
52. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
53. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

54. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
55. 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.
56. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.
57. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
58. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.
59. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.
60. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
61. Z poziomu konsoli musi istnieć możliwość skalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.
62. Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta.
63. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
64. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
65. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
66. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.
67. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
68. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostęp do najbardziej interesujących danych. Panel ten musi być edytowalny.
69. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może
70. zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF lub CSV.

71. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
72. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.
73. Powiadomienia mailowe mają być wysyłane w formacie HTML.
74. Powiadomienia muszą być wywoływane po zmianie liczby członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.
75. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
76. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
77. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
78. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.
79. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.
80. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania, musi być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
81. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
82. Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.
83. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
84. Serwer musi posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.
85. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.
86. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.
87. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.

88. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.
89. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.
90. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.
91. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych.
92. Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault).
93. Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk.
94. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal).
95. Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.

### III. 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, co tygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

#### IV. Ochrona stacji roboczych

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 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 integrować się z Intel Threat Detection Technology.

11. 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).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. 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.
14. 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.
15. 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.
16. 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.
17. Rozwiązanie musi być wyposażone w 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.

18. 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.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. 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.
24. Rozwiązanie musi być wyposażone w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.

29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. 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.

## V. Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon 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.
9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

13. Rozwiązanie musi zapewniać 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.
14. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikację, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
21. 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 zawieszonoego mikro-serwisu.

## VI. Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykację 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 tylko 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 urządzenia 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. Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam,

dokumenty oraz inne pliki typu .jar, .reg, .msi.

4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzewać jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
  - a) czysty,
  - b) podejrzany,
  - c) bardzo podejrzany,
  - d) szkodliwy.
13. 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.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

#### IX. Szyfrowanie:

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10/11 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.
5. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.
6. Aplikacja musi mieć możliwość korzystania z technologii TCG OPAL - dyski sprzętowo szyfrowane.
7. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
8. W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania.
9. Aplikacja do szyfrowania musi być zarządzana z poziomu konsoli webowej, wykorzystywanej do zarządzania produktem do ochrony antywirusowej.
10. Konsola centralnego zarządzania musi pozwalać na wygenerowanie, dla każdej zaszyfrowanej stacji, dysku ratunkowego.
11. 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.
12. Aplikacja musi posiadać możliwość ograniczenia wyświetlania interfejsu graficznego użytkownikom.
13. Administrator musi posiadać możliwość zablokowania dostępu do zaszyfrowanego dysku.

#### X. Pozostałe wymagania:



W przypadku zaoferowania oprogramowania równoważnego do oprogramowania ESET PROTECT Advanced, Wykonawca musi, w terminie 4 dni roboczych od zawarcia umowy, wykonać następujące działania:

1. Dostarczenie wszystkich niezbędnych licencji (ze wsparciem producenta na 46 miesięcy na oprogramowanie) wymaganych do wdrożenia i uruchomienia systemu.
2. Przeprowadzenie procesu deinstalacji obecnie używanego przez Zamawiającego oprogramowania antywirusowego ESET oraz zainstalowanie i skonfigurowanie oprogramowania równoważnego na wskazanych przez Zamawiającego urządzeniach:
  - a) stacjach roboczych, laptopach (Microsoft Windows 11),
  - b) serwerach (Microsoft Windows Server 2016/2019/2022/2025),
  - c) urządzeniach mobilnych z systemem Android/IOS.
3. Wykonanie analizy przedwdrożeniowej środowiska Zamawiającego oraz dostarczenie projektu technicznego systemu równoważonego, obejmującego specyfikację techniczną określającą wymogi na infrastrukturę teleinformatyczną / środowisko wirtualne dla systemu, m.in.:
  - a) szczegółową specyfikację sprzętową serwerów/urządzeń sieciowych,
  - b) ilość maszyn wirtualnych, procesorów wirtualnych, pamięci RAM, przestrzeni dyskowej,
  - c) wymagane parametry łącza,
  - d) wymagane parametry systemu operacyjnego,
  - e) wymagania wirtualizacji.oraz szczegółowy opis zakresu prac, ich sekwencji oraz wskazania, kto ma je realizować (Zamawiający, Wykonawca) niezbędnych do wdrożenia i konfiguracji systemu równoważnego.
4. Wykonanie dokumentacji powykonawczej systemu równoważnego zgodnie z wymogami Zamawiającego, zawierającej m. in. informacje o szczegółach wykonanych prac wdrożeniowych, instrukcje instalacji, konfiguracji i użytkowania wdrożonego oprogramowania równoważnego.
5. Przeprowadzenie szkoleń z instalacji, konfiguracji i zarządzania wdrożonym systemem równoważnym zgodnie z wymogami Zamawiającego zawartymi w rozdziale XI.

#### XI. Opis wymagań dotyczących realizacji szkolenia

1. Wykonawca zaplanuje, zorganizuje i przeprowadzi szkolenie dla maksymalnie 38 pracowników Państwowej Inspekcji Pracy, zwanych dalej: „uczestnikami”.
2. Celem szkolenia jest zapoznanie uczestników z wymaganiami w zakresie administracji i obsługi dostarczonego oprogramowania równoważnego.
3. Szkolenia odbędą się w podziale na dwie grupy, które będą liczyły po 19 uczestników.

4. Szkolenie dla każdej grupy trwać będzie 2 dni. Szkolenie w każdym dniu rozpocznie się najwcześniej o godz. 10.00 i zakończy się najpóźniej o godz. 16.00. Dzień szkoleniowy trwać będzie 8 godzin (godzina szkoleniowa = 45 min.). Łączna liczba godzin szkoleniowych dla każdego dnia szkolenia wynosi 16.
5. Budynek oraz sale szkoleniowe, nie mogą posiadać barier architektonicznych dla osób z niepełnosprawnością ruchową.
6. Szkolenia zostaną zorganizowane w Warszawie.
7. Szkolenia zostaną przeprowadzone w uzgodnionych terminach, przed terminem dostawy zaoferowanego oprogramowania równoważnego, w kolejno po sobie następujących dniach od poniedziałku do piątku.
8. Szkolenia mają mieć charakter warsztatów (każdy z uczestników szkolenia samodzielnie wykonuje ćwiczenia pod nadzorem trenerów). Sale muszą mieć powierzchnię dostosowaną do wielkości grup szkoleniowych. Wykonawca zapewni niezbędne oprzyrządowanie do przeprowadzenia szkoleń, w tym w szczególności specjalistyczny sprzęt komputerowy odpowiedni do rodzaju zajęć, m.in. indywidualne stanowisko dla każdego uczestnika szkolenia, infrastrukturę sieciową, zainstalowane i skonfigurowane do zajęć odpowiednie oprogramowanie. Sale szkoleniowe muszą być wyposażone w sprzęt prezentacyjny (m.in. projektor, flipchart, tablica). Sale muszą mieć powierzchnię dostosowaną do wielkości grup szkoleniowych.
9. Wykonawca ma obowiązek zapewnić minimum dwóch trenerów posiadających odpowiednie kwalifikacje zawodowe do przeprowadzenia zajęć danej grupy, w każdym dniu szkoleniowym. Zamawiający wymaga, by ww. osoby przeprowadziły w okresie ostatnich dwóch lat (licząc wstecz od upływu terminu wyznaczonego na składanie ofert) co najmniej dwa szkolenia z zakresu szkoleń objętych przedmiotem zamówienia. W przypadku gdyby wykładowca, wskazany w wykazie, o którym mowa w pkt 13 ppkt 3, nie mógł przeprowadzić szkolenia, Wykonawca zobowiązany jest zapewnić innego wykładowcę, posiadającego wymagane kwalifikacje. Informację o zmianie wykładowcy Wykonawca przekaże Zamawiającemu w formie pisemnej, przed rozpoczęciem szkolenia, wraz z opisem jego kwalifikacji. Powyższa zmiana wymaga pisemnej akceptacji Zamawiającego.
10. Wykonawca zapewni każdemu uczestnikowi materiały szkoleniowe, które przekaże uczestnikom poszczególnych szkoleń pocztą elektroniczną oraz w wersji papierowej przed rozpoczęciem każdego szkolenia, a także materiały piśmiennicze (notatnik, długopis) dla każdego uczestnika.
11. Zamawiający przekaże Wykonawcy listy uczestników szkoleń wraz z adresami poczty elektronicznej oraz informacją o korzystaniu z noclegów, najpóźniej 7 dni roboczych po

uzyskaniu informacji, o której mowa w pkt 12. Zamawiający zastrzega, że w przypadku choroby lub wyniknięcia innej szczególnej okoliczności może zmienić uczestnika szkolenia lub zmniejszyć/zwiększyć liczbę uczestników danego szkolenia, w tym liczbę osób korzystających z noclegów. Zamawiający informuje, że uisći zapłatę tylko za faktyczną liczbę uczestników szkolenia oraz za faktycznie wykorzystane noclegi. O zmianie osób w poszczególnych grupach Zamawiający poinformuje Wykonawcę przed rozpoczęciem szkolenia dla danej grupy. Zamawiający może zmniejszyć wskazaną w pkt. 1 liczbę uczestników szkoleń, łącznie ze wszystkich grup, o maksymalnie 2.

12. Wykonawca opracuje i przedstawi Zamawiającemu do akceptacji, na co najmniej 10 dni roboczych przed rozpoczęciem pierwszego szkolenia, na adres wskazany w Umowie, dokumentację szkoleniową zawierającą:

- 1) harmonogram szkoleń, obejmujący terminy i miejsca realizacji każdego szkolenia (co najmniej nazwa i adres budynku) oraz miejsce zakwaterowania (nazwa i adres hotelu), ze wskazaniem grupy, której szkolenie dotyczy. Do harmonogramu należy dołączyć informacje o możliwości przemieszczania się komunikacją publiczną: z dworca PKP do miejsca noclegu, z miejsca prowadzenia szkolenia na dworzec PKP oraz z miejsca noclegu do miejsca prowadzenia szkolenia,
- 2) program szkolenia, który musi uwzględniać pełny zakres tematyczny szkolenia z podziałem na dni i godziny prowadzenia zajęć i przerw, z podziałem na bloki tematyczne, a w blokach zagadnienia do omówienia,
- 3) wykaz wykładowców, o których mowa w pkt 9, wraz z opisem ich kwalifikacji do przeprowadzenia zajęć,
- 4) materiały szkoleniowe, które zostaną opracowane w języku polskim,
- 5) opis metody badania satysfakcji uczestnictwa w szkoleniu oraz projekt karty oceny zawierającej co najmniej punkty dotyczące stopnia omówienia zagadnień ujętych w programie, oceny wiedzy merytorycznej wykładowcy oraz oceny umiejętności dydaktycznych wykładowcy,
- 6) wzór protokołu odbioru szkolenia.

Zamawiający uprawniony jest do wniesienia uwag do przekazanej dokumentacji szkoleniowej w terminie 3 dni roboczych od jej otrzymania. Uwagi przekazywane będą pocztą elektroniczną (e-mail). Wykonawca zobowiązany jest uwzględnić uwagi Zamawiającego i przekazać dokumentację do ponownej akceptacji Zamawiającego w terminie do 2 dni roboczych od otrzymania ww. uwag.

13. Wykonawca przygotowuje formularze badania satysfakcji uczestnictwa w szkoleniu i przeprowadzi badanie, odrębnie dla każdego szkolenia.
14. Wykonawca zobowiązany jest przygotować i wręczyć uczestnikom, w drugim dniu szkolenia, dokument potwierdzający udział w szkoleniu (zaświadczenie/certyfikat).
15. W terminie 3 dni roboczych od daty zakończenia szkolenia dla każdej grupy szkoleniowej, Wykonawca sporządzi (zgodnie z zaakceptowanym wzorem, o którym mowa w pkt 12 ppkt 6), podpisze i złoży protokół odbioru szkolenia. Protokoły mają zawierać co najmniej następujące informacje: datę i miejsce przeprowadzenia szkolenia, imię i nazwisko wykładowcy, informację, że uczestnicy szkolenia otrzymali materiały szkoleniowe oraz stwierdzenie, że szkolenie zostało przeprowadzone zgodnie z zakresem obowiązków określonym przez Zamawiającego, miejsce zakwaterowania i liczbę wykorzystanych noclegów oraz kolacji. Oryginały list uczestników szkolenia (podpisane każdego dnia, przez każdego uczestnika szkolenia), wynik badania satysfakcji wraz z wypełnionymi kartami oceny szkolenia oraz kopie wydanych zaświadczeń/certyfikatów stanowić będą załączniki do protokołów. Wymagane załączniki do protokołów dostarczone będą do siedziby PIP GIP. Protokoły będą podpisywane przez upoważnionego przedstawiciela Zamawiającego; osobami uprawnionymi do podpisania protokołów odbioru szkolenia są osoby upoważnione do składania oświadczeń woli w imieniu Wykonawcy – zgodnie z zasadami reprezentacji, określonej w KRS, ewidencji działalności gospodarczej lub zgodnie z pełnomocnictwem, zaś po stronie Zamawiającego przez Dyrektora lub Wicedyrektora Departamentu Kadr i Szkoleń PIP GIP.
16. W ramach szkolenia Wykonawca zapewni każdemu uczestnikowi szkolenia, w każdym dniu szkolenia, dwie przerwy kawowe (serwis kawowy musi zawierać: kawę z ekspresu oraz rozpuszczalną, herbatę, dodatki: mleko, cukier, cytryna, napoje: butelkowana woda mineralna gazowana i niegazowana, kruche ciasteczka – 2 rodzaje, owoce) oraz obiad dwudaniowy (pierwsze danie zupa, drugie danie – do wyboru 2 rodzaje dań z surówką, w tym jedno wegetariańskie), napoje.
17. Wykonawca zobowiązany jest zapewnić jeden nocleg. Zakwaterowanie w hotelu o standardzie co najmniej trzygwiazdkowym, usytuowanym w tej samej miejscowości (w Warszawie), w której prowadzone będą szkolenia (obiekt zlokalizowany w odległości od miejsca gdzie będą prowadzone szkolenia, umożliwiający dojazd komunikacją miejską w czasie 30 minut; czas dojazdu liczony będzie razem z dojściem do i od przystanku komunikacji miejskiej). Zamawiający dopuszcza, zapewnienie noclegów w motelach, pensjonatach, domach studenckich itp. – pod warunkiem, że będą one spełniały wymagania hotelu trzygwiazdkowego. Pokoje nie mogą posiadać barier architektonicznych dla osób z niepełnosprawnością ruchową. Zamawiający dopuszcza by nocleg odbywał się w pokojach maksymalnie dwuosobowych – z zastrzeżeniem, że

niedopuszczalne jest kwaterowanie osób różnej płci w tych samych pokojach. Zamawiający informuje, że uczestnicy szkolenia z miasta, w którym odbywać się będzie szkolenie, nie będą korzystać z noclegu (natomiast w przypadku oddelegowania na szkolenie osoby zatrudnionej w oddziale danej jednostki organizacyjnej Państwowej Inspekcji Pracy może wystąpić konieczność zapewnienia dla ww. osoby noclegu).

18. Wykonawca zapewni uczestnikom szkolenia korzystającym z noclegów, śniadania w miejscu zakwaterowania, w każdym dniu szkolenia oraz kolację, w pierwszym dniu szkolenia.
19. Wykonawca zobowiązany jest ponieść (i uwzględnić w maksymalnej cenie oferty) wszystkie koszty związane z realizacją szkoleń, w tym w szczególności koszty noclegów i wyżywienia, wykładowców, materiałów szkoleniowych, wynajmu pomieszczeń, cateringu, oprzyrządowania itp. Zamawiający pokrywał będzie jedynie koszt dojazdu uczestników na szkolenie oraz diet z tytułu podróży służbowej.
20. W przypadku niemożności przeprowadzenia szkolenia, w którymkolwiek z terminów, wskazanych w zaakceptowanym przez Zamawiającego harmonogramie szkoleń, Wykonawca zobowiązuje się niezwłocznie poinformować o powyższym Zamawiającego. W takiej sytuacji Zamawiający ma prawo wskazać termin, w którym ma być przeprowadzone dane szkolenie. Termin wskazany przez Zamawiającego jest wiążący dla Wykonawcy.
21. Zamawiający zastrzega sobie możliwość zmiany terminu szkolenia, w sytuacji losowej związanej z organizacją pracy. Zamawiający niezwłocznie poinformuje o powyższym Wykonawcę oraz przedstawi propozycję nowego terminu szkolenia. Wykonawca będzie zobowiązany, w terminie 3 dni roboczych od dnia otrzymania powyższej informacji, do poinformowania Zamawiającego o możliwości realizacji szkolenia w nowym terminie.
22. Zamawiający zapłaci Wykonawcy wynagrodzenie za szkolenie dla danej grupy, gdy jego ocena merytoryczna, obejmująca stopień omówienia zagadnień ujętych w programie oraz ocenę wiedzy merytorycznej i umiejętności dydaktycznych wykładowcy, obliczona na podstawie kart oceny wyników badania satysfakcji, będzie równa lub wyższa niż 3,8 w skali 1-5. W przypadku, gdy ocena merytoryczna szkolenia, obejmująca stopień omówienia zagadnień ujętych w programie oraz ocenę wiedzy merytorycznej i umiejętności dydaktycznych wykładowcy, obliczona na podstawie kart oceny wyników badania satysfakcji, będzie niższa niż 3,8 pkt w skali 1-5, Strony uznają, że szkolenie dla tej grupy nie zostało wykonane należycie i Wykonawcy, nie przysługuje wynagrodzenie. W przypadku nie załączenia przez Wykonawcę do protokołu odbioru szkolenia danej grupy wyników badania satysfakcji (wraz z wypełnionymi kartami oceny satysfakcji), Zamawiający uzna, że ocena merytoryczna szkolenia na podstawie kart oceny wyników badania satysfakcji była niższa niż 3,8 pkt w skali 1-5 dla danej grupy i Wykonawcy nie przysługuje wynagrodzenie. W przypadkach wskazanych powyżej, Wykonawca zobowiązany będzie

przeprowadzić ponownie szkolenie na własny koszt, na warunkach określonych w umowie, w terminie uzgodnionym z Zamawiającym. W takim przypadku, koszt wyjazdu służbowego uczestników szkolenia pokrywa Wykonawca (refundacja kosztu zakupu biletów, ryczałtu za dojazdy samochodem prywatnym, diety i itp.). Podstawą obliczenia ww. kosztów będą rozliczenia kosztów podróży służbowej (rozliczenia delegacji) uczestników szkolenia przedłożone przez Zamawiającego. W przypadkach wskazanych powyżej, Wykonawcy przysługuje wynagrodzenie po ponownym przeprowadzeniu szkolenia z zastrzeżeniem, że jego ocena merytoryczna, obejmująca stopień omówienia zagadnień ujętych w programie oraz ocenę wiedzy merytorycznej i umiejętności dydaktycznych wykładowcy, obliczona na podstawie kart oceny wyników badania satysfakcji, będzie równa lub wyższa niż 3,8 w skali 1-5.

23. Po przeprowadzeniu wszystkich szkoleń, Wykonawca zobowiązany jest do złożenia podpisanego przez Wykonawcę raportu z przeprowadzonych szkoleń. Raport będzie zawierał co najmniej wykaz szkoleń wraz z terminami, liczbą uczestników szkolenia w danym szkoleniu, średnią oceną merytoryczną z każdego szkolenia, liczbę wykorzystanych noclegów. Raport ma być przedstawiony Zamawiającemu w terminie 10 dni od dnia zakończenia ostatniego szkolenia..
24. Zamawiający oświadcza, że udział pracowników Państwowej Inspekcji Pracy w szkoleniu będzie całkowicie finansowany ze środków publicznych.