Ministerstwo Rozwoju i Technologii **Warszawa, 17.10.2025 r.**

ul. Plac Trzech Krzyży 3/5

00-507 Warszawa

ZAPYTANIE O WYCENĘ DO OSZACOWANIA WARTOŚCI ZAMÓWIENIA

Ministerstwo Rozwoju i Technologii planuje uruchomić postępowanie przetargowe o udzielenie zamówienia publicznego na zakup i wdrożenie Systemu DLP.

Uprzejmie prosimy o wycenę, poniżej opisanych minimalnych wymagań stanowiących przedmiot planowanego zamówienia do wszczęcia postępowania przetargowego na zakup i wdrożenie Systemu Ochrony Przed Wyciekiem Informacji DLP (Data Loss Prevention) wraz z instruktażem oraz usługami wsparcia technicznego dla Ministerstwa Rozwoju i Technologii.

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem Zamówienia jest zakup i wdrożenie Systemu DLP.
Zamówienie zostanie zrealizowane poprzez wykonanie następujących zadań:

1. zakup subskrypcji oprogramowania wraz ze wsparciem technicznym na okres 36 miesięcy;
2. wdrożenie dostarczonego Systemu;
3. usługi asysty technicznej.

II. TERMIN REALIZACJI ZAMÓWIENIA

Przedmiot zamówienia zostanie zrealizowany w terminie maksymalnie **do 60 dni** od daty podpisania przez strony umowy **(termin realizacji do uzupełnienia przez Wykonawcę w Formularzu Ofertowym).**

III. MINIMALNE WYMAGANIA DOTYCZĄCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1. W ramach realizacji przedmiotu zamówienia zostanie zrealizowana dostawa Systemu Ochrony Przed Wyciekiem Informacji DLP (Data Loss Prevention) zapewniającego możliwość kompleksowej ochrony danych przetwarzanych w infrastrukturze teleinformatycznej Zamawiającego, obejmującej w szczególności: stacje robocze, urządzenia mobilne, serwery, serwery plików, systemy poczty elektronicznej oraz wybrane usługi chmurowe wraz z wdrożeniem i instruktażem oraz usługami wsparcia technicznego dla Ministerstwa Rozwoju i Technologii.
2. W ramach realizacji przedmiotu zamówienia zostaną dostarczone subskrypcje oprogramowania składającego się na zaoferowany System Ochrony Przed Wyciekiem Informacji DLP (Data Loss Prevention)
3. Zaoferowane oprogramowanie nie może być przeznaczone przez producenta do wycofania ze sprzedaży.
4. Dostarczone subskrypcje oprogramowania muszą być zarejestrowane na Zamawiającego i pochodzić z legalnego kanału dystrybucyjnego producenta na rynek UE oraz nie posiadać wad prawnych, zaś korzystanie z nich przez Zamawiającego nie powinno stanowić naruszenia majątkowych praw autorskich osób trzecich.
5. Prawo do aktualizacji przedmiotowego oprogramowania musi być zarejestrowane u producenta na użytkownika końcowego (Zamawiającego).
6. Wymagane jest zapewnienie wsparcia producenta przez okres 36 miesięcy. W ramach wsparcia należy zapewnić dostęp do aktualizacji oprogramowania. Wsparcie powinno być realizowane w języku polskim. W ramach wsparcia zgłoszenia będą realizowane za pomocą

systemu informatycznego wykonawcy (całodobowo) lub telefonicznie - w dni robocze w godzinach 8-16.
7. Wykonawca musi zagwarantować przywrócenie funkcjonalności systemu, licząc od momentu zgłoszenia przez Zamawiającego w ciągu 8 godzin roboczych.
8. System musi spełniać wymogi w zakresie ochrony poufności, integralności i dostępności informacji oraz systemów informatycznych zgodnie z polskimi normami i Krajowymi Ramami Interoperacyjności (KRI), w tym aktualizację oprogramowania oraz zarządzanie konfiguracją.
9. System musi współpracować z istniejącą infrastrukturą teleinformatyczną Zamawiającego, (Zamawiający udostępni dane w osobnym załączniku) oraz być zgodny z wymaganiami interoperacyjności systemów publicznych w Polsce.
10. System musi zapewniać szyfrowanie komunikacji pomiędzy komponentami systemu oraz posiadać mechanizmy ochrony integralności i poufności przetwarzanych danych.

IV. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE SYSTEMU DLP

1. Zarządzanie serwerem administracyjnym

Serwer administracyjny i oprogramowanie systemu DLP:

1. Musi umożliwiać instalację na systemach Windows Server 2019 lub nowszych. Zamawiający dopuszcza pracę na systemach z rodziny GNU/Linux pod warunkiem, że oferowana dystrybucja posiada wsparcie producenta i będzie to dystrybucja LTS.
2. Wszystkie moduły funkcjonalne systemu muszą być dostarczone od jednego producenta.
3. System musi realizować swoje funkcje zarówno na poziomie sieci oraz stacjach końcowych takich jak komputer, laptop, urządzenie mobilne
4. Zarządzanie, konfiguracja polityk, obsługa incydentów oraz raportowanie muszą być spójne dla ochrony na poziomie sieci i stacji końcowych i muszą być zarządzane z pojedynczej webowej konsoli zarządzającej.
5. Dostęp do konsoli zarządzającej musi odbywać się w bezpiecznym połączeniu https
6. Dostęp do konsoli zarządzającej musi wymagać uwierzytelnienia. Oprócz hasła systemu DLP oraz hasła użytkownika z usługi katalogowej, system DLP musi wspierać silne uwierzytelnianie z wykorzystaniem MFA.
7. System powinien umożliwiać ziarnistą delegację uprawnień do konfiguracji systemu, polityk, raportów oraz incydentów w oparciu o role własne oraz wbudowane, takie jak administrator, audytor, manager incydentów.
8. Konsola zarządzająca powinna zawierać ekran przedstawiający podstawowe statystki aktywności z ostatnich 24 godzin jak: ilość incydentów względem ważności, najczęściej naruszane kategorie polityk, stacje końcowe, na których wykryto najwięcej naruszeń, etc.
9. Dostęp do konsoli zarządzającej musi wymagać uwierzytelnienia. System DLP musi wspierać uwierzytelnianie cyfrowym certyfikatem użytkownika oraz integrację z systemem silnego uwierzytelniania opartego o hasło jednorazowe (ang. One Time Password) przynajmniej jednego producenta.
10. Ochrona dla danych na poziomie sieci, urządzeń mobilnych i stacji roboczych musi być realizowana z poziomu jednego zestawu polityk i reguł. Niedopuszczalne jest rozwiązanie, w którym polityki dla ochrony na poziomie sieci i stacji roboczych są osobnymi zestawami polityk.
11. System musi umożliwiać monitorowanie i ochronę danych przesyłanych w kanałach komunikacyjnych, w szczególności:
    a) ruch webowy z wykorzystaniem protokołów HTTP oraz HTTPS;
    b) poczta elektroniczna – protokół SMTP.
12. System musi umożliwiać definiowanie własnych kanałów transmisji, które mają być

monitorowane.

13. Architektura systemu DLP musi być modularna i umożliwiać wdrażanie kolejnych instancji jego modułów, w szczególności kolejnych serwerów systemu DLP, z możliwością delegowania ich do poszczególnych zadań zdefiniowanych w systemie DLP, w szczególności zadań tworzenia cyfrowych odcisków palców (ang. fingerprint) dla chronionych danych oraz wyszukiwania określonych danych na zasobach w sieci.
14. W przypadku jeśli System DLP wymaga do pracy zewnętrznego silnika bazodanowego Wykonawca musi dostarczyć kompletne rozwiązanie tj. oprogramowanie Systemu DLP oraz silnik bazodanowy wraz z ewentualnymi licencjami wymaganymi do rekomendowanej przez producenta oprogramowania pracy. Zamawiający dopuszcza wykorzystanie zewnętrznych silników bazodanowych pod warunkiem, że posiadają one wsparcie producenta co najmniej do końca roku 2027. Zamawiający nie dopuszcza rozwiązań bazodanowych nie posiadających komercyjnego wsparcia technicznego producenta silnika bazodanowego (np. Microsoft SQL Server Express Edition);
15. Zamawiający posiada licencję silnika bazodanowego Microsoft SQL Server Standard dla 20 CPU oraz licencje Microsoft Windows Server 2019 Datacenter.
16. Musi działać w architekturze serwer-klient, gdzie komunikacja serwera administracyjnego z klientem odbywa się przy pomocy agenta instalowanego na stacji końcowej.
17. Musi umożliwiać zarządzanie za pośrednictwem konsoli (webowej lub lokalnie instalowanej);
18. Musi posiadać funkcję automatycznej kopii bazy danych w określonym przez administratora harmonogramie;
19. Musi umożliwiać wykonanie instalacji/deinstalacji zdalnej klienta Systemu DLP na stacjach roboczych;
20. Musi komunikować się ze stacjami roboczymi za pomocą instalowanego na nich agenta i/lub klienta. W przypadku braku połączenia agenta/klienta z serwerem administracyjnym, agent/klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym;
21. Musi umożliwiać przygotowanie pliku instalacyjnego agenta za pośrednictwem konsoli zarządzającej. Zamawiający dopuszcza sytuację gdy producent oprogramowania Systemu DLP będzie oferować pliki instalacyjne do dystrybucji przez Zamawiającego.
22. Musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą co najmniej do raportowania i zarządzania stacjami roboczymi;
23. Musi posiadać funkcjonalność synchronizacji użytkowników oraz stacji roboczych z usługą Microsoft Active Directory;
24. Musi zapewniać administratorowi możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym;
25. Musi umożliwiać ustawianie powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP
26. System musi umożliwiać integracje z systemami ticketowymi.
27. Serwer administracyjny musi umożliwiać integrację w stopniu umożliwiającym przesyłanie logów i incydentów z Systemu DLP do oprogramowania klasy SIEM i SOAR (Zamawiający udostępni dane w osobnym załączniku).
28. Musi umożliwiać integrację z Office365, pakietem biurowym MS Office oraz MS Exchange Online oraz On-Premise. Integracja musi pozwalać na:
    a) wprowadzanie polityk zabezpieczeń do wiadomości e-mail oraz plików.
    b) tagowanie i klasyfikowanie dokumentów
29. Musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość w czasie rzeczywistym, co najmniej o:
    a) numery kart kredytowych,
    b) numer PESEL,
    c) numer polskiego dowodu osobistego,
    d) polski numer paszportu,
    e) wyrażenia regularne (możliwość definiowania swoich własnych wzorców opartych na

wyrażeniach regularnych),
   f) określone ciągi znaków,
   g) numer IBAN.
30. Musi umożliwiać określenie list zawierających urządzenia pamięci masowej, drukarek fizycznych i sieciowych, lokalizacji sieciowych, adresów email, domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu;
31. Musi posiadać możliwość wysłania alertów co najmniej za pośrednictwem wiadomości email.
32. System DLP musi posiadać możliwość wykrywania, monitorowania i blokowania przesyłania danych firmowych do publicznych i prywatnych platform sztucznej inteligencji (m.in. ChatGPT, Copilot, Perplexity, Bard) poprzez inspekcję treści w polach tekstowych przeglądarek.
33. Ochrona wdrożona w postaci agenta systemu DLP na komputerze użytkownika musi umożliwiać detekcję z użyciem wszystkich zdefiniowanych w systemie mechanizmów identyfikacji danych wliczając w to fingerprinty dla danych ustrukturyzowanych z baz danych.
34. Analiza danych przeprowadzana przez agenta systemu DLP na komputerze użytkownika musi być pełna i nie może wymagać przesyłania danych do bardziej szczegółowej analizy na serwerze systemu DLP. Agent systemu DLP musi zapewniać tak samo dobrą ochronę danych niezależnie od tego czy ma komunikację z serwerem systemu DLP czy nie.
35. System musi umożliwiać wykrywanie danych w następujących zasobach w sieci Zamawiającego:
   a) Serwery plików
   b) Sharepoint On-Premise oraz Sharepoint Online
   c) Serwery MS Exchange
   d) Lokalne archiwa poczty w formacie PST

2. Ochrona danych i bezpieczeństwo

System DLP musi:

1. Posiadać możliwość importu własnych słowników do wyszukiwania danych;
2. Umożliwiać przypisywanie i odbieranie uprawnień do wybranych modułów programu przez administratora Systemu DLP.
3. Umożliwiać tworzenie własnych kategorii dla stron internetowych, aplikacji oraz typów plików przez administratora Systemu DLP;
4. Umożliwiać filtrowanie oraz sortowanie zebranych danych przez administratora Systemu DLP. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF lub XLS lub CSV;
5. Umożliwiać wyszukiwanie danych osobowych na zasobach zarówno lokalnych jak i sieciowych przez administratora Systemu DLP.
6. Umożliwiać monitorowanie i blokowanie treści naruszających zasady polityki w kanale WWW (http i https);
7. Zawierać wbudowane zestawy reguł i polityk oraz kreator ułatwiający ich wybór, które znacznie przyspieszają proces wdrożenia rozwiązania dostarczając ochrony dla popularnych typów danych, np. w celu uzyskania zgodności z różnymi regulacjami.
8. W szczególności System powinien zawierać predefiniowane reguły ochrony oraz mechanizmy identyfikacji danych takich jak numery kart kredytowych, IBAN, oraz identyfikatorów jak PESEL, REGON, NIP, oraz numer dowodu osobistego.
9. Dla wyżej wymienionych identyfikatorów System, oprócz sprawdzenia ich zgodności z wzorcem, musi walidować ich poprawność przez weryfikację zawartej w nich sumy kontrolnej.
10. Umożliwiać tworzenie własnych mechanizmów identyfikacji danych opartych o własne wzorce i konfigurowalne mechanizmy walidacji.
11. Ochrona informacji musi odbywać się w oparciu o reguły bezpieczeństwa informacji odzwierciedlające procesy biznesowe.
12. Umożliwiać budowanie polityk ochrony informacji uwzględniając kontekst w jaki informacja jest używana, czyli uwzględnia okoliczności jak:

a) Kto wysyła informacje,
b) Dokąd informacje są wysyłane,
c) W jaki sposób informacje są wysyłane,
d) Co jest wysyłane, czyli właściwa identyfikacja treści.

13. Umożliwiać następujące reakcje na działania użytkownika naruszające polityki ochrony danych:
    a) zezwolenie działania,
    b) blokowanie działania,
    c) kwarantannę wiadomości email,
    d) szyfrowanie wiadomości email oraz plików kopiowanych na zewnętrzne nośniki danych,
    e) umożliwienie użytkownikowi kontynuowania operacji po podaniu uzasadnienia i zatwierdzeniu komunikatu wyświetlonego przez agenta ochrony informacji na komputerze użytkownika,
    f) wysłanie zgodnych z przygotowanymi szablonami powiadomień, przy czym jest możliwość selektywnego wysyłania powiadomień do:
        - nadawcy, czyli osoby, która naruszyła politykę ochrony danych,
        - przełożonego (menadżera, kierownika) nadawcy,
        - właściciela danych zdefiniowanego w polityce chroniącej określone dane, np. dział HR w przypadku danych osobowych pracowników,
        - administratora systemu DLP,
        - dowolnego zdefiniowanego adresata.
14. Umożliwiać zwalnianie maili zatrzymanych w kwarantannie systemu DLP przynajmniej na następujące sposoby:
    a) Uprzywilejowana osoba (administrator systemu DLP, analityk incydentów) loguje się do konsoli zarządzania systemu DLP, odnajduje odpowiedni incydent i zwalnia mail z kwarantanny.
    b) Przełożony pracownika otrzymuje automatyczne powiadomienie o naruszeniu polityki DLP przez swojego podwładnego, zapoznaje się z szczegółami zdarzenia zawartymi w powiadomieniu i odpowiada na nie. To powoduje zwolnienie maila z kwarantanny bez konieczności logowania się przez kogokolwiek do konsoli zarządzania systemu DLP.
    c) Za pośrednictwem REST API oferowanego przez System.
15. Umożliwiać łączenie polityk w grupy.
16. Wykorzystywać szeroką gamę mechanizmów identyfikowania treści, m.in.:
    a) słowa kluczowe, frazy, słowniki,
    b) wyrażenia regularne, właściwości pliku takie jak rozmiar, nazwa, typ,
    c) tworzenie odcisku palca – fingerprint, polegającej na tworzeniu cyfrowej reprezentacji danych zawartych w dokumencie lub w bazie danych z wykorzystaniem jednokierunkowej funkcji skrótu – hash,
    d) skrypty umożliwiające rozpoznanie identyfikatorów takich jak PESEL, REGON, NIP, czy numer karty kredytowej wraz z zweryfikowaniem poprawności tego identyfikatora poprzez np. sprawdzenie zaszytej w nim sumy kontrolnej,
    e) możliwość wytrenowania systemu DLP tak, aby odróżniał dokumenty określonego rodzaju tworzone w ramach organizacji od innych dokumentów tego samego typu poprzez zaprezentowanie odpowiednich zestawów dokumentów treningowych.
17. W przypadku, gdy System będzie działać w integracji z wspieranymi systemami klasyfikacji informacji, musi rozpoznać etykiety klasyfikacji nadane plikom oraz wiadomościom email i na tej podstawie powinien egzekwować zdefiniowane polityki ochrony danych.
18. Umożliwiać łączenie w politykach wielu mechanizmów identyfikacji danych wyrażeniami logicznymi pozwalając na reagowanie w przypadku wystąpienia określonej kombinacji chronionych danych.
19. Umożliwiać tworzenie fingerprint zarówno dla danych ustrukturyzowanych takich jak bazy danych oraz pliki csv jak i dla danych nieustrukturyzowanych.

20. Tworzenie fingerprintów dla danych ustrukturyzowanych powinno być możliwe w odniesieniu do:
    a) Baz danych
    b) Plików CSV
21. Tworzenie fingerprintów dla danych nieustrukturyzowanych powinno być możliwie dla:
    a) Serwerów plików
    b) SharePoint
22. Algorytm tworzenia fingerprint dla pliku musi tworzyć wiele odcisków palca dla pojedynczego pliku, tak aby chronić informacje zawarte w pliku a nie wyłącznie dokument w całości.
23. Dla plików niezawierających tekstu np. binarnych lub graficznych musi być możliwe tworzenie odcisku palca dla całego dokumentu, aby możliwe było wykrycie jego transmisji lub użycia w całości.
24. System musi umożliwiać wykrywanie chronionych treści w przesyłanych plikach graficznych wykorzystując technologię OCR (ang. optical character recognition). Wspomniana analiza powinna odbywać się na dedykowanym serwerze, aby nie obciążać agenta na stacji roboczej.
25. Rozpoznawanie danych w plikach graficznych musi być możliwe także dla procesu przeszukiwania repozytoriów sieciowych takich jak serwery plików oraz Sharepoint.
26. System w zakresie ochrony danych na stacji końcowej musi umożliwiać monitorowanie takich czynności jak:
    a) kopiowanie informacji na zewnętrzne nośniki danych, np. pendrive,
    b) nagrywanie płyt,
    c) drukowanie zarówno na drukarki lokalne jak i sieciowe,
    d) kontrola aplikacji w zakresie operacji kopiuj/wytnij, wklej oraz dostęp aplikacji do pliku,
    e) kontrola treści przesyłanych za pomocą przeglądarki internetowej oraz klienta poczty,
    f) lokalne wykrywanie chronionych informacji w plikach na dysku stacji końcowej.
27. W zakresie wysyłania danych przez przeglądarkę internetową agent systemu DLP na komputerze użytkownika musi umożliwiać analizę i wykrywanie chronionych danych również do portali, w przypadku których dane wysyłane są dzielone na fragmenty, co normalnie uniemożliwia ich właściwą analizę.
28. Umożliwiać blokowanie wykonywania zrzutów ekranu (print screen) na stacji końcowej, co
29. W połączeniu z funkcją OCR dla danych przesyłanych w sieci powinno znacznie utrudnić możliwość wykonania zrzutu ekranu i przesłania chronionych treści w postaci grafiki.
30. Ochrona wdrożona w postaci agenta systemu DLP na komputerze użytkownika musi umożliwiać detekcję z użyciem wszystkich zdefiniowanych w systemie mechanizmów identyfikacji danych wliczając w to fingerprinty dla danych ustrukturyzowanych z baz danych.
31. Analiza danych przeprowadzana przez agenta systemu DLP na komputerze użytkownika musi być pełna i nie powinna wymagać przesyłania danych do bardziej szczegółowej analizy na serwerze systemu DLP. Agent systemu DLP musi zapewniać tak samo dobrą ochronę danych niezależnie od tego czy ma komunikację z serwerem systemu DLP czy nie.
32. Wykrywać próby wysyłania danych nie tylko w dużych paczkach, ale również w mniejszych partiach, np. po kilka rekordów z bazy danych. W tym celu system umożliwia kumulowanie informacji o transmisjach chronionych informacji, nawet gdy poszczególne transmisje nie spełniają zdefiniowanego w regułach progu, ale sumarycznie go przekraczają. Po spełnieniu określonego w regule warunku w systemie powstaje incydent naruszenia polityk DLP ze wskazaniem szczegółów incydentu oraz dodatkowo informacji, kiedy miał miejsce pierwszy i ostatni incydent związany z sumarycznym spełnieniem warunku reguły DLP.
33. Maksymalny czas agregacji informacji o odnotowanych transmisjach chronionych treści powinien wynosić 7 dni.
34. Umożliwiać integrację z usługami katalogowymi w celu m.in.:
    a) przypisania użytkowników i grup jako autoryzowanych nadawców i odbiorców chronionych informacji,
    b) przypisania użytkowników do ról zarządzających takich jak administrator, audytor, manager incydentów,

c) wyświetlenia szczegółów dotyczących użytkownika w ramach incydentu związanego z jego aktywnością, np. powinno być możliwe wyświetlenie informacji o przełożonym oraz departamencie użytkownika.
d) automatycznego wysłania powiadomienia do przełożonego (menadżera) osoby będącej źródłem incydentu w przypadku jego wystąpienia.

35. Umożliwiać zautomatyzowane wykrywanie informacji objętych politykami ochrony na serwerach i stacjach końcowych w sieci Zamawiającego.
36. Proces wykrywania danych musi być dostępny zarówno jako zadanie wykonywane z poziomu serwera systemu DLP, wobec zasobów na serwerach w sieci Zamawiającego jak i jako zadanie wykonywane przez agentów instalowanych na komputerach użytkowników wobec zasobów lokalnych każdego z komputerów.
37. W przypadku wykrycia plików, których nie powinno być w danym miejscu oprócz stworzenia incydentu System musi umożliwiać automatyczną reakcję np. usunięcie pliku i stworzenie w nim innego pliku z informacją dla użytkownika.
38. W przypadku, gdy System działa w integracji z wspieranymi systemami klasyfikacji informacji, musi umożliwiać nadanie etykiety klasyfikacji dla pliku spełniającego kryteria zdefiniowane w zadaniu wykrywania danych na komputerach użytkowników.
39. W ramach odnotowanych incydentów udostępniać informacje dotyczące reguły, która została naruszona, jak również kopię informacji, która była przesyłana (dane forensic). Wgląd w tak szczegółowe informacje powinien być kontrolowany.
40. Konsola zarządzająca musi umożliwiać zarządzanie i pracę nad incydentami, m.in.
    a) zmianę statusu incydentu (nowy, przetwarzany, zamknięty), przy czym musi istnieć możliwość tworzenia własnych statusów,
    b) zmianę ważności incydentu (niska, średnia, wysoka),
    c) dodanie komentarza do incydentu,
    d) dodanie etykiety (Tag) do incydentu,
    e) oznaczenie incydentu jako ignorowany,
    f) przypisanie incydentu do administratora systemu DLP,
    g) przekazywanie incydentu do innego administratora systemu DLP (eskalacja),
    h) usunięcie incydentu, przy czym usunięciu incydentu musi towarzyszyć automatyczne odnotowanie tej operacji w logu audytowym oraz opcjonalne wysłanie powiadomienia do administratora systemu DLP.
41. Zarządzanie incydentami musi być możliwie na co najmniej dwa sposoby:
    a) Uprzywilejowana osoba (administrator systemu DLP, analityk incydentów) loguje się do konsoli zarządzania systemu DLP, odnajduje odpowiedni incydent i wykonuje na nim odpowiednie akcje.
    b) System DLP wysyła automatyczne powiadomienie dotyczące naruszenia polityki DLP do wyznaczonej osoby (administrator systemu DLP, analityk incydentów). Powiadomienie zawiera szczegóły incydentu oraz odnośniki pozwalające na zarządzanie nim, dzięki czemu podejmowanie działań względem incydentu nie wymaga od tej osoby logowania się do konsoli zarządzania systemu DLP.
42. Udostępniać REST API umożliwiające dostęp do incydentów oraz zarządzanie nimi z poziomu aplikacji i systemów firm trzecich.
43. Wspomniane API musi wykorzystywać mechanizmy bezpieczeństwa w oparciu o JSON Web Token (JWT).
44. Konsola zarządzania zawiera sekcję pozwalającą administratorom na monitorowanie i ocenę poprawności działania systemu jak i obciążenia poszczególnych modułów systemu DLP
45. Dostarczać mechanizmy wspomagające pracę administratorów poprzez wykorzystanie cyklicznej automatycznej analizy incydentów pod kątem ryzyka stanowionego dla organizacji i prezentowania tak rozpoznanych zagrożeń w sposób pogrupowany i uporządkowany począwszy od zagrożeń najbardziej istotnych.
46. W odniesieniu do poprzedniego punktu System DLP musi klasyfikować rozpoznane zagrożenia do kilku kategorii np. potencjalna kradzież danych, czy nieprawidłowy proces biznesowy.

47. Ze względu na różne role pełnione przez pracowników Zamawiającego system musi umożliwiać nadawanie odpowiednich kategorii pracownikom np. pracownik wysokiego ryzyka, czy pracownik uprzywilejowany, które to kategorie będą odpowiednio uwzględniane przez mechanizm opisany w dwóch wcześniejszych punktach.
48. Umożliwiać identyfikację oznaczonych plików w wiadomościach mailowych wysyłanych za pośrednictwem poczty mailowej;
49. Dla plików, musi być możliwe utworzenie następujących reguł:
    a) blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń,
    b) blokowanie oraz zezwalanie na drukowanie na określonych drukarkach,
    c) blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej,
    d) blokowanie oraz zezwalanie na przekazywanie danych do publicznych platform sztucznej inteligencji
    e) blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen,
    f) blokowanie oraz zezwalanie na wysyłanie do poczty webowej za pomocą przeglądarki (np. gmail, onet)
    g) blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:
        - Dropbox,
        - Google Drive,
        - OneDrive
    h) blokowanie oraz zezwalanie na przesyłanie danych za pomocą komunikatorów (w szczególności MS Teams, Skype, Webex),
    i) blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego,
    j) blokowanie oraz zezwalanie na przesyłanie za pomocą protokołów sieciowych takich jak http, ftp, smtp, pop3, imap, p2p oraz ich szyfrowanych odpowiedników,
50. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia widocznego dla użytkownika;
51. Umożliwiać monitorowanie ruchu przesyłanych plików np. poprzez FTP oraz p2p;
52. Umożliwiać monitoring usług na niestandardowych portach oraz zakresach portów.
53. Umożliwiać monitoring sklasyfikowanych i oznaczonych plików w sieci Zamawiającego oraz powiadamiać o próbach przesyłania tak oznaczonych plików dowolnym kanałem na zewnątrz organizacji Zamawiającego;
54. Umożliwiać inspekcję zawartości plików i załączników,
55. Umożliwiać inspekcję plików skompresowanych (w tym spakowanych wielokrotnie),
56. Umożliwiać wykrywanie zdefiniowanych informacji na podstawie zawartości plików (np. dokumentacja finansowa, kod źródłowy, oprogramowanie), z uwzględnieniem możliwości tworzenia wzorców takich dokumentów;
57. Umożliwiać ochronę wzorcowych dokumentów zawierających wrażliwe dane, bez konieczności używania słów kluczowych;
58. Umożliwiać wykrywanie, przy użyciu ww. mechanizmu, nieustrukturyzowanych danych rozmieszczonych w wielu miejscach organizacji (dane w ruchu), a także nowych i nigdy niewidzianych plików, spoza organizacji;
59. Umożliwiać tworzenie reguł opartych co najmniej o: słowa kluczowe i zdania kluczowe,
60. Umożliwiać wykorzystanie predefiniowanych lub umożliwienie tworzenia wzorców opisowych dla poszukiwanych informacji;
61. Umożliwiać walidację wykrytych informacji (np. wyliczanie sum kontrolnych dla numeru PESEL) oraz definiowania walidacji;
62. Umożliwiać edycję dostarczonych wzorców opisowych, walidatorów oraz możliwość tworzenia nowych, także na ich podstawie;

3. Klasyfikacja dokumentów

System DLP musi

1. Umożliwiać oznaczanie dokumentów w formie tagów lub metadanych,
2. Umożliwiać definiowanie własnych kategorii oraz polityk klasyfikacji wraz z możliwością tworzenia różnych klas i polityk klasyfikacji z możliwością ich przypisania do grup użytkowników, jednostkowych użytkowników i ról w systemie, także wynikających z repozytorium użytkowników (np. Active Directory);
3. Umożliwiać ustalanie zasad automatycznych zmian w klasyfikacji dokumentów;
4. Posiadać mechanizm automatycznego rozwiązywania konfliktów klasyfikacji i wykonywania definiowalnych akcji;
5. Zapewniać interaktywność mechanizmu klasyfikacji z użytkownikiem (np. notyfikacja lub żądanie świadomego potwierdzenia wykonania określonej czynności);
6. Umożliwiać definiowanie własnego nazewnictwa dla poszczególnych kategorii dokumentów (np. dane poufne, dane tajne);
7. Umożliwiać integrację z oprogramowaniem MS Office oraz MS Office 365, które posłuży między innymi do wybrania kategorii dokumentu, w szczególności integrować się z oknem tworzenia/odczytu oraz oknem "Zapisz/Zapisz jako";
8. Zapewniać możliwości klasyfikacji plików z menu kontekstowego dla plików i katalogów
9. Zapewnić wymuszenie klasyfikacji dokumentu przed jego wydrukowaniem lub inną formą udostępnienia;
10. Umożliwiać klasyfikację plików PDF (skany), archiwów, plików tekstowych, obrazów oraz dodawanie do dokumentów metadanych w postaci np. tagu;

4. Agent stacji końcowych

System DLP musi umożliwiać:

1. Instalację klienta na następujących systemach operacyjnych:
   a) Microsoft Windows 10 (wersja x64),
   b) Microsoft Windows 11 (wersja x64),
   c) Microsoft Windows Server 2016 i wyżej
   d) Mac OSX 13.x i wyżej oraz MacOS.
2. Wspierać instalację agenta ochrony stacji końcowej Windows w następujących środowiskach VD (Virtual Desktop Infrastructure)
   a) Citrix XenApp
   b) Citrix XenDesktop
   c) Citrix Virtual Apps
   d) VMWare Horizon
3. Egzekwowanie reguł DLP również w przypadku braku połączenia między klientem, a serwerem administracyjnym;
4. Instalację na stacjach końcowych za pośrednictwem GPO lub innych systemów dystrybucji oprogramowania
5. Zabezpieczenie klienta DLP przed wyłączeniem/zawieszeniem lub dezinstalacją przez nieuprawnionego użytkownika;
6. Lokalne przechowywanie informacji w przypadku zerwania połączenia z serwerem administracyjnym, do czasu ponownego połączenia;
7. Wyświetlanie powiadomień (np. okno pop-up) dla użytkowników w języku polskim.

5. Raportowanie, analityka oraz obsługa zdarzeń

System DLP musi:

1. Zapewniać generowanie raportów w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu. Raporty muszą być generowane do pliku PDF i/lub XLS, CSV po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail.
2. Zapewnić wizualizację zdarzeń/incydentów, która musi być realizowana w sposób zrozumiały, przejrzysty i czytelny dla operatorów, a każdy element zdarzenia powinien być jasno opisany, ze szczególnym uwidocznieniem: kanału transmisji, powodu wygenerowania oraz elementów naruszających politykę;
3. Opis incydentu musi zawierać informacje podstawowe, co najmniej: imię i nazwisko, datę i czas wystąpienia incydentu, podjętą czynność, rodzaj incydentu;
4. Umożliwić filtrowanie przy użyciu różnych warunków, w tym zmiennych, atrybutów oraz możliwość ich wykorzystywania dla różnych filtrów;
5. Umożliwić raportowanie: reguł bezpieczeństwa w oparciu o incydenty na plikach chronionych, ogółu wykonanych operacji na plikach, podsumowania wszystkich incydentów bezpieczeństwa, akcji użytkowników na zabezpieczonych plikach, podsumowania korzystania z urządzeń oraz ich typów;

V. MINIMALNE WYMAGANIA W ZAKRESIE GWARANCJI SYSTEMU

Gwarancja dla oferowanego systemu musi spełniać niżej opisane wymagania:

1. Minimalny okres gwarancji na oprogramowanie wynosie 36 miesięcy.
2. Gwarancja będzie liczona od daty odbioru przedmiotu umowy i oparta na gwarancji producenta rozwiązania zgodnie z terminami obowiązywania wymaganymi w OPZ.
3. Gwarancja ma być świadczona w reżimie 8x5xNBD. Czas naprawy Awarii liczony jest od czasu przesłania zgłoszenia o awarii do Wykonawcy zgodnie z procedurą przyjmowania zgłoszeń serwisowych.
4. Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub www) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją w godzinach pracy Zamawiającego.
5. W okresie gwarancji Wykonawca w ramach otrzymanego wynagrodzenia udostępni Zamawiającemu możliwość wielokrotnego uaktualniania całego dostarczonego Oprogramowania do najnowszych wersji oferowanych przez producenta oraz patche i programy korekcji błędów.
6. Na okres przedłużającej się naprawy Wykonawca może stosować procedury zastępcze. Czas trwania procedur zastępczych nie może być dłuższy niż 45 dni kalendarzowe od chwili zgłoszenia awarii.
7. Przez usunięcie Awarii należy rozumieć przywrócenie pierwotnej funkcjonalności Systemu we wszystkich modułach i zaprzestanie stosowania w bieżącej pracy procedur zastępczych.
8. Po usunięciu każdej Awarii, Wykonawca zobowiązuje się do doprowadzenia całego systemu do stanu integralnej całości w rozumieniu poprawnego działania wszystkich zainstalowanych komponentów.
9. W ramach gwarancji Zamawiający będzie miał prawo przez okres wskazany w formularzu ofertowym do:
    a) pobierania i instalowania nowych wersji oprogramowania dla każdego elementu Systemu;
    b) dostępu do bazy wiedzy oraz dokumentacji dostarczonych elementów;
    c) dostępu do powiadomień/ogłoszeń/alarmów w zakresie dostarczonych elementów;
    d) zgłaszania nieograniczonej liczby awarii systemu w trybie 24x365x7 za pomocą dedykowanego portalu i/lub zgłoszenia telefonicznego.
10. Czasy reakcji/naprawy na zgłoszenie będą na poziomie:
    a) 1 godzina/8 godzin - błąd krytyczny – tj. przerwa w działaniu usług w środowisku produkcyjnym, brak dostępnego obejścia problemu,

b) 2 godziny/2 dni - błędy wysokie – tj. problem z poprawnym działaniem usługi znacząco utrudniający realizację procesów biznesowych, brak dostępnego obejścia problemu,
c) 4 godziny/7 dni - błędy średnie - tj. problem z poprawnym działaniem usługi, utrudnienie realizacji procesów biznesowych, dostępne obejście problemu,
d) 8 godzin/14 dni - błędy niskie – tj. problem z poprawnym działaniem usługi, brak wpływu na realizację procesów biznesowych.

11. Wykonawca w terminie 7 dni od zawarcia Umowy dostarczy Zamawiającemu procedury zgłaszania i obsługi Awarii wraz z listą osób upoważnionych do kontaktów, wykazem adresów poczty elektronicznej i nr telefonów.
12. W okresie gwarancji Wykonawca ponosi odpowiedzialność za poprawne funkcjonowanie oprogramowania stanowiącego przedmiot zamówienia, z zastrzeżeniem, że Wykonawca nie ponosi odpowiedzialności za uszkodzenia oprogramowania powstałe z wyłącznej winy Zamawiającego lub osób trzecich działających w jego imieniu.
13. Wymagany tryb zgłaszania wszelkich awarii, wad i błędów. Zgłoszenie następuje w drodze pisemnej mailem na adres podany przez Wykonawcę lub za pośrednictwem telefonicznego zgłaszania awarii, wad i błędów dotyczących sprzętu i oprogramowania w dni robocze w godzinach 8:00-16:00.
14. Zamawiający wymaga obsługi zgłoszeń w języku polskim.

VI. MINIMALNE WYMAGANIA W ZAKRESIE DOKUMENTACJI POWYKONAWCZEJ

1. Informacje ogólne
    - Tytuł projektu/systemu
    - Zamawiający i wykonawca
    - Zakres wdrożenia
    - Daty realizacji (rozpoczęcia i zakończenia)
    - Osoby kontaktowe/odpowiedzialne
2. Opis systemu
    - Cel i funkcjonalność systemu
    - Zakres objęty wdrożeniem
    - Architektura systemu (np. model warstwowy, serwer-klient, chmura)
    - Schematy lub diagramy (np. diagramy UML, sieciowe, architektury logicznej i fizycznej)
    - Licencje
3. Wykonane prace
    - Opis wykonanych etapów wdrożenia
    - Zastosowane technologie i narzędzia
    - Zainstalowane oprogramowanie i ich wersje
    - Dostarczone komponenty ich specyfikacja
4. Konfiguracja systemu
    - Parametry konfiguracyjne
    - Zastosowane ustawienia (system operacyjny, bazy danych, serwery, aplikacje)
    - Dane dostępowe (jeśli to możliwe) lub procedura ich uzyskania
    - Schematy połączeń (np. sieciowych, zasilania, logiki sterowania)
5. Testy i odbiory
    - Protokoły testów funkcjonalnych i integracyjnych
    - Wyniki testów
    - Protokół odbioru końcowego
    - Wykryte i rozwiązane problemy (jeśli były)
6. Instrukcje i procedury
    - Instrukcja użytkownika systemu
    - Instrukcja administratora

- Procedury awaryjne i odzyskiwania danych (Disaster Recovery)
- Szczegóły dotyczące kopii zapasowych i przywracania systemu
- Procedury utrzymaniowe

7. Załączniki
    - Licencje na oprogramowanie
    - Certyfikaty zgodności
    - Rysunki techniczne
    - Zrzuty ekranów lub dokumentacja fotograficzna
    - Raporty z testów

VII. MINIMALNE WYMAGANIA W ZAKRESIE WDROŻENIA SYSTEMU WRAZ Z PRZEPROWADZENIEM INSTRUKTAŻU

1. Wdrożenie dostarczonego systemu DLP, w tym:
    a) Instalację subskrypcji oprogramowania,
    b) analizę przedwdrożeniową obejmującą rozpoznanie potrzeb i przygotowanie architektury rozwiązania, która zostanie ujętą w projekcie technicznym
    c) konfigurację i uruchomienie systemu DLP
    d) wykonanie dokumentacji technicznej i eksploatacyjnej,
    e) przeprowadzenie instruktażu dla administratorów Systemu,
    f) opracowanie oraz wdrożenie polityk bezpieczeństwa i reguł kontrolnych adekwatnych do potrzeb Zamawiającego, umożliwiających monitorowanie, blokowanie oraz raportowanie incydentów związanych z nieuprawnionym przetwarzaniem lub przesyłaniem informacji.
    g) zapewnienie funkcjonalności kontroli danych w spoczynku, w użyciu oraz w ruchu (data-at-rest, data-in-use, data-in-motion), realizowanej w ramach wdrożonego systemu.
    h) uruchomienie mechanizmów raportowania, audytu i alertowania o zdarzeniach bezpieczeństwa, z możliwością ich eksportu i integracji z posiadanymi systemami bezpieczeństwa Zamawiającego
    i) zapewnienie ochrony i monitoringu danych przesyłanych za pośrednictwem sieci LAN i WAN
    j) zapewnienie ochrony danych przesyłanych za pośrednictwem kanału komunikacyjnego poczty email Zamawiającego
    k) zapewnienie monitoringu i ochrony zasobów plikowych Zamawiającego np. baz danych, plików współdzielonych, archiwów cyfrowych i elektronicznego obiegu dokumentów
    l) uruchomienia wielopoziomowej klasyfikacji dokumentów (tj. dodawanie dynamicznych nagłówków plików, dodawanie informacji o ważności pliku) Klasyfikacja jest widoczna dla użytkowników i systemów i podąża razem z plikiem;
    m) przeprowadzenie testów poprawności instalacji i konfiguracji

2. Instalacja i konfiguracja Systemu DLP według najlepszych praktyk producenta. Instalację oprogramowania na stacjach roboczych i serwerach wykona Zamawiający na podstawie informacji i dokumentacji dostarczonej przez Wykonawcę.
3. Konfigurację autentykacji i autoryzacji do systemu DLP włączając w to integrację z usługami zarządzania tożsamością działających u Zamawiającego
4. Przeprowadzenie integracji z istniejącymi narzędziami SIEM, SOAR, XDR IAM, systemami pocztowymi Zamawiającego.
5. Skonfigurowanie procesów normalizacji i parsowania danych, aby wszystkie informacje były ujednolicone i gotowe do skutecznej analizy.
6. Utworzenie reguł korelacyjnych pozwalających na wykrywanie zaawansowanych scenariuszy i nietypowych aktywności w środowisku.
7. Przygotowanie spersonalizowanych dashboardów i raportów, które umożliwią zespołowi SOC szybkie monitorowanie stanu bezpieczeństwa.

8. Zrealizowanie integracji DLP z narzędziami zabezpieczeń, systemami ticketowymi, platformami skanowania i urządzeniami sieciowymi w celu umożliwienia automatycznych reakcji.
9. Opracowanie i wdrożenie reakcji na incydenty, obejmujących zarówno działania automatyczne, jak i półautomatyczne.
10. Konfiguracja i implementacja polityk bezpieczeństwa, reguł oraz raportów, optymalizacja pod kątem wydajności oraz minimalizacji liczby fałszywych alarmów zgodnie z najlepszymi praktykami oraz wytycznymi Zamawiającego,
11. Wykonanie testów wydajności, bezpieczeństwa oraz procedur odtwarzania po awarii w celu potwierdzenia gotowości systemów do pracy w środowisku produkcyjnym
12. Wykonaniu testów akceptacyjnych (niezawodnościowe oraz funkcjonalne) oraz opracowaniu i przedstawieniu Raportu w dokumentacji powykonawczej
13. Wykonawca przeprowadzi instruktaż dla administratorów wskazanych przez Zamawiającego:
    a) Instruktaż zostanie przeprowadzony w terminie uzgodnionym z Zamawiającym (jednak nie później niż 10 dni od daty wdrożenia), w jego siedzibie, tj. Plac Trzech Krzyży 3/5, 00-507 Warszawa lub w formie zdalnej.
    b) Instruktaż powinien obejmować:
        - omówienie dostarczonego systemu (parametry, funkcjonalności),
        - omówienie przeprowadzonych prac instalacyjno-konfiguracyjnych,
        - omówienie i weryfikację przygotowanych i dostarczonych procedur,
        - omówienie scenariuszy w przypadku wystąpienia błędów/awarii

VIII. MINIMALNE WYMAGANIA W ZAKRESIE ASYSTY TECHNICZNEJ

1. Wykonawca przez cały okres trwania umowy zobowiązany będzie do świadczenia usługi asysty technicznej na każde żądanie Zamawiającego, tj. każdorazowo na podstawie pisemnego zlecenia asysty technicznej, wystawianego przez Zamawiającego.
2. Zakres, sposób oraz termin realizacji zostanie uzgodniony na etapie przedstawienia wymagań przez Zamawiającego i wyceny pracochłonności przez Wykonawcę, poprzedzających zlecenie.
3. Zlecenia będą obejmować w szczególności:
    a) Zapewnieniu Zamawiającemu pomocy w rozwiązaniu problemów i incydentów wynikłych w trakcie obsługi dostarczonego systemu DLP tj.:
        - analiza problemów zgłaszanych przez Zamawiającego,
        - asysta przy określaniu i usuwaniu przyczyn oraz skutków zgłaszanych incydentów,
        - dostarczanie, instalacja (po uzyskaniu zgody Zamawiającego) i konfiguracja uaktualnień i nowych wersji oprogramowania lub jego komponentów, oraz związana z tym aktualizacja dostarczonej dokumentacji,
        - przeprowadzanie analiz oraz udzielanie konsultacji Zamawiającemu,
        - dokonywanie zmian konfiguracji oprogramowania,
        - opracowywanie i dostarczanie dokumentacji, w tym aktualizacji dokumentacji oraz dostarczanie dokumentacji wprowadzanych zmian.
        - implementację nowych funkcjonalności lub modyfikację już skonfigurowanych.
    b) Wsparcie w przypadku wystąpienia incydentu bezpieczeństwa.
        - Wsparcie w zakresie wykonania analizy wykorzystanych podatności.
        - Kontaktu z ekspertem w zakresie bezpieczeństwa dostarczonego systemu.
        - Analizy zakresu kompromitacji systemu.
        - Wsparcia w konfiguracji/rekomendacji w celu zabezpieczenia systemu,
        - Wsparcia w zakresie usunięcia skutków oraz rozwiązania incydentu bezpieczeństwa,
    c) Wsparcie w planowanych pracach serwisowych,

- Przeprowadzenia standardowych prac serwisowych,
- Przeprowadzania aktualizacji komponentów systemu,
- Weryfikacji poprawności konfiguracji,
- Wsparcia w okresie podwyższonej czujności (np. Monitoring środowiska w czasie biznesowo krytycznych wydarzeń),

d) Dokonywanie okresowych (nie rzadziej niż co 6 m-cy) przeglądów gwarancyjnych dostarczonego oprogramowania. W ramach przeprowadzanych okresowych przeglądów gwarancyjnych muszą być wykonane co najmniej następujące czynności:
   - weryfikacja poprawności działania oraz optymalizacja konfiguracji wszystkich komponentów wchodzących w skład dostarczonego rozwiązania,
   - analiza logów i podjęcie działań naprawczych w razie potrzeby,
   - aktualizacja (w razie potrzeby i po uzyskaniu uprzedniej zgody Zamawiającego) wersji poszczególnych komponentów wchodzących w skład dostarczonego rozwiązania.

e) Wsparcie on-site w przypadku braku możliwości rozwiązania problemu zdalnie.

f) usługi asysty technicznej muszą być realizowane przez inżyniera posiadającego Certyfikat z oficjalnej ścieżki producenta dostarczonego systemu na poziomie eksperckim.

4. Usługi asysty technicznej Wykonawca zobowiązuje się realizować w dwóch formach:
   a) w siedzibie Zamawiającego przez pracowników Wykonawcy na podstawie pisemnego zlecenia Zamawiającego określającego zakres oraz termin wykonania tych usług, uzgodnionych wcześniej z Wykonawcą. Usługi te będą świadczone, przez liczbę godzin wskazanych w zleceniu,
   b) zdalnie przez pracowników Wykonawcy na podstawie pisemnego zlecenia Zamawiającego określającego zakres oraz termin wykonania tych usług, uzgodnionych wcześniej z Wykonawcą. Usługi te będą świadczone, przez określoną liczbę godzin w danym dniu. Wykonawca udostępni narzędzie umożliwiające zdalną komunikację, które w uzgodnieniu z Zamawiającym zostanie uruchomione na stacji roboczej pracownika Zamawiającego.
5. Po wykonaniu usług Wykonawca przedłoży Zamawiającemu protokół z wykonania usług asysty zawierający ich rodzaj, zakres oraz termin.
6. Maksymalna liczba roboczogodzin w trakcie trwania umowy wskazana jest w Formularzu Ofertowym.
7. Zamawiający zastrzega sobie prawo do nie udzielania zleceń na usługi asysty technicznej.
8. Proces realizacji asysty technicznej będzie przebiegał następująco:
   a) Zamawiający przekaże Wykonawcy drogą mailową zlecenie wykonania asysty technicznej. Zgłoszenie zawierać będzie co najmniej:
      - zakres prac do wykonania lub opis problemu do rozwiązania,
      - określenie proponowanego terminu realizacji (opcjonalnie).
      - W terminie nie dłuższym niż 3 dni robocze od dnia otrzymania zgłoszenia o asystę techniczną Wykonawca skontaktuje się z Zamawiającym w celu ustalenia szczegółowego zakresu prac, terminu realizacji i szacowanego wymiaru godzin realizacji asysty technicznej.