Ministerstwo Rozwoju i Technologii **Warszawa, 19.01.2026 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 licencji oprogramowania wraz ze wsparciem technicznym na okres 36 miesięcy;
2. wdrożenie dostarczonego Systemu;
3. usługi asysty technicznej.

II. TERMIN REALIZACJI ZAMÓWIENIA

1) 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 Wykonawca dostarczy i wdroży System Ochrony Przed Wyciekiem Informacji DLP (Data Loss Prevention) zapewniający ochronę danych przetwarzanych w infrastrukturze teleinformatycznej Zamawiającego, obejmującej w szczególności: stacje robocze, system poczty elektronicznej oraz serwery plików.
2. W ramach realizacji przedmiotu zamówienia Wykonawca dostarczy licencje oprogramowania składające się na zaoferowany System Ochrony Przed Wyciekiem Informacji DLP (Data Loss Prevention) wraz ze wsparciem producenta na okres 36 miesięcy. Licencje oprogramowania zostaną dostarczone ze wsparciem na okres 36 miesięcy.
3. Dostarczone dla Systemu DLP oprogramowanie nie może być przeznaczone przez producenta do wycofania ze sprzedaży.
4. Licencje oprogramowania wraz ze wsparciem producenta na okres 36 miesięcy 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. W ramach wdrożenia Wykonawca przeprowadzi instruktaż dla administratorów Zamawiającego.
6. 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.
7. System musi współpracować z istniejącą infrastrukturą teleinformatyczną Zamawiającego oraz być zgodny z wymaganiami interoperacyjności systemów publicznych w Polsce.
8. 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. Wymagania w zakresie rozwiązań infrastrukturalnych

1. System DLP musi być dostarczony jako jeden spójny produkt od jednego producenta, obejmujący: konsolę zarządzania, komponenty serwerowe, repozytoria danych oraz agentów endpoint.
2. System DLP musi umożliwiać wdrożenie w całości w infrastrukturze Zamawiającego (on-premise).
3. System DLP musi umożliwiać instalację komponentów serwerowych na serwerach wirtualnych (VM) Zamawiającego.
4. System DLP musi posiadać webową konsolę zarządzania dostępną z przeglądarki, dostępną za pomocą protokołu HTTPS i umożliwiającą: konfigurację polityk, zarządzanie agentami, obsługę incydentów, raportowanie, audyt działań administracyjnych.
5. 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.
6. System DLP musi działać w architekturze serwer-klient, gdzie komunikacja serwera administracyjnego z klientem odbywa się przy pomocy agenta instalowanego na stacji końcowej.
7. System DLP 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.
8. 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.
9. System DLP musi posiadać funkcjonalność synchronizacji użytkowników oraz stacji roboczych z usługą Microsoft Active Directory.
10. Producent/Wykonawca musi dostarczyć pakiet instalacyjny agenta w formacie umożliwiającym masową dystrybucję co najmniej jako MSI lub równoważny instalator obsługujący instalację cichą tj. bez interakcji użytkownika końcowego.
11. System DLP musi umożliwiać instalację agenta ochrony DLP dla następujących systemów operacyjnych:
    a. Microsoft Windows 10 (wersja x64).
    b. Microsoft Windows 11 (wersja x64).
    c. Microsoft Windows Server 2019 i wyżej.
    d. MacOS 13.x i wyżej.

2. Wymagania zapewnianego zakresu ochrony systemu DLP

1. System DLP musi wykorzystywać szeroką gamę mechanizmów automatycznego identyfikowania treści, m.in.:
    a. słowa kluczowe, frazy, słowniki
    b. wyrażenia regularne, właściwości pliku takie jak rozmiar, nazwa, typ
    c. skrypty umożliwiające rozpoznanie identyfikatorów takich jak PESEL, REGON, NIP, czy numer karty kredytowej.
2. System DLP musi wykorzystywać algorytm identyfikacji treści tak by, chronić poszczególne informacje zawarte w pliku a nie wyłącznie dokument w całości. Dla plików niezawierających tekstu np. binarnych lub graficznych musi być możliwe zidentyfikowanie dla całego pliku, aby możliwe było wykrycie jego transmisji lub użycia w całości.

3. System DLP musi umożliwiać łączenie w politykach wielu mechanizmów identyfikacji danych wyrażeniami logicznymi pozwalając na reagowanie w przypadku wystąpienia określonej kombinacji chronionych danych.
4. System DLP musi umożliwiać wykrywanie chronionych treści w przesyłanych plikach graficznych wykorzystując technologię OCR (ang. optical character recognition)
5. 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.

3. Wymagania w zakresie zarządzania politykami oraz obsługą incydentów

1. System DLP musi umożliwiać ziarnistą delegację uprawnień do konfiguracji systemu, polityk, raportów oraz incydentów w oparciu o role własne oraz wbudowane, takie jak administrator, audytor, manager incydentów.
2. Konsola zarządzania systemu DLP musi zawierać sekcję pozwalającą administratorom na monitorowanie i ocenę poprawności działania systemu jak i obciążenia poszczególnych modułów Systemu DLP.
3. Konsola zarządzająca musi umożliwiać zarządzanie i pracę nad incydentami, m.in:
   a. zmianę statusu incydentu
   b. zmianę ważności incydentu
   c. dodanie komentarza do incydentu
   d. dodanie etykiety do incydentu
4. 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.
5. System DLP musi 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.
6. System DLP musi 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.
7. Umożliwiać następujące reakcje na działania użytkownika naruszające polityki ochrony danych:
   a. zezwolenie działania.
   b. zezwolenie działania po podaniu przyczyny
   c. blokowanie działania.
   d. wysłanie zgodnych z przygotowanymi szablonami powiadomień
8. 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 tj. Dropbox, Google Drive, OneDrive
h. blokowanie oraz zezwalanie na przesyłanie danych za pomocą komunikatorów (w szczególności MS Teams)
i. blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego

9. System DLP musi posiadać możliwość ustawienia powiadomienia widocznego dla użytkownika.

4. Wymagania w zakresie integracji zewnętrznych systemu DLP

1. System DLP musi zapewniać integrację z systemami SIEM w postaci przekazywania informacji na temat incydentów przez protokół rsyslog lub http (webhook).
2. System DLP musi zapewniać integrację z oprogramowaniem Microsoft Outlook na stacji roboczej w postaci analizy i blokowania działań na plikach i kategoriach danych zidentyfikowanych w systemie DLP.
3. System DLP musi zapewniać integrację z przeglądarkami internetowymi Chrome, Firefox, Edge w postaci analizy i blokowania działań na plikach i kategoriach danych zidentyfikowanych w systemie DLP.

V. MINIMALNE WYMAGANIA W ZAKRESIE WSPARCIA TECHNICZNEGO PRODUCENTA SYSTEMU

Wsparcie techniczne producenta dla oferowanego Systemu DLP musi spełniać niżej opisane wymagania:

1. Minimalny okres wsparcia do oprogramowania wynosi 36 miesięcy.
2. Wsparcie będzie liczone od daty odbioru przedmiotu umowy i oparta na gwarancji producenta rozwiązania zgodnie z terminami obowiązywania wymaganymi w OPZ.
3. Wsparcie techniczne producenta musi być świadczone w reżimie 8x5xNBD. Czas naprawy Awarii Systemu 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 wsparcia technicznego producenta 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 wsparcia technicznego producenta 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 wsparcia technicznego producenta 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 WDROŻENIA SYSTEMU WRAZ Z INSTRUKTAŻEM

1. Wdrożenie dostarczonego Systemu DLP nastąpi poprzez:
   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) uruchomienie mechanizmów raportowania, audytu i alarmowania o zdarzeniach bezpieczeństwa
   h) uruchomienia procesów automatycznej klasyfikacji dokumentów
   i) przeprowadzenie testów poprawności instalacji i konfiguracji.
2. Instalacja i konfiguracja Systemu DLP nastąpi według najlepszych praktyk producenta. Instalację oprogramowania na stacjach roboczych i serwerach wykona Zamawiający na podstawie informacji i dokumentacji dostarczonej przez Wykonawcę.
3. Konfiguracja autentykacji i autoryzacji do Systemu DLP włączając w to integrację z usługami zarządzania tożsamością działających u Zamawiającego.
4. Opracowanie i wdrożenie reakcji na incydenty, obejmujących zarówno działania automatyczne, jak i półautomatyczne.
5. Konfiguracja i implementacja polityk bezpieczeństwa, reguł oraz raportów, optymalizacja pod kątem wydajności oraz minimalizacji liczby fałszywych alarmów zgodnie z najlepszymi praktykami oraz wytycznymi Zamawiającego,

6. Wykonanie testów wydajności, bezpieczeństwa oraz procedur odtwarzania po awarii w celu potwierdzenia gotowości systemów do pracy w środowisku produkcyjnym.
7. Wykonaniu testów akceptacyjnych (niezawodnościowe oraz funkcjonalne) oraz opracowaniu i przedstawieniu Raportu w dokumentacji powykonawczej.
8. 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.
9. W ramach wdrożenia systemu Wykonawca zobowiązany jest do przygotowania i przekazania Zamawiającemu dokumentacji powykonawczej.
10. Dokumentacja powinna zawierać minimum poniżej opisane informacje:
    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 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 zostaną uzgodniony na etapie przedstawienia wymagań przez Zamawiającego i wyceny pracochłonności przez Wykonawcę, poprzedzających zlecenie.
3. Zlecenia będą obejmować w szczególności wsparcie administratorów Zamawiającego w użytkowaniu Systemu, zarówno techniczne jak i merytoryczne.
4. Szczegółowy zakres usługi asysty technicznej uwzględniać będzie każdorazowo zlecenie.
5. Usługi asysty technicznej muszą być realizowane przez inżyniera posiadającego Certyfikat z oficjalnej ścieżki producenta dostarczonego systemu na poziomie eksperckim.
6. Usługi asysty technicznej Wykonawca zobowiązuje się realizować w dwóch formach:
   a) w siedzibie Zamawiającego.
   b) zdalnie.
7. Wykonawca udostępni narzędzie umożliwiające zdalną komunikację, które w uzgodnieniu z Zamawiającym zostanie uruchomione na stacji roboczej pracownika Zamawiającego.
8. Po wykonaniu usług Wykonawca przedłoży Zamawiającemu protokół z wykonania usług asysty zawierający ich rodzaj, zakres oraz termin.
9. Maksymalna liczba roboczogodzin w trakcie trwania umowy wskazana jest w Formularzu Ofertowym.
10. Zamawiający zastrzega sobie prawo do nieudzielania zleceń na usługi asysty technicznej.