**Załącznik nr 2 do SWZ**

**Nr sprawy EI-4-12-2024**

1. Przedmiotem zamówienia jest dostawa oraz roczne wsparcie techniczne i serwisowe systemu DLP (Data Loss Prevention) dedykowanego do ochrony 700 użytkowników.
2. Oznaczenie przedmiotu zamówienia wg Kod CPV:

48732000-8 Pakiety oprogramowania do zabezpieczania danych

48730000-4 Pakiety oprogramowania zabezpieczającego

48731000-1 Pakiety oprogramowania zabezpieczającego pliki

1. Licencja na system DLP (Data Loss Prevention) zostanie udzielona w terminie 3 dni roboczych od dnia podpisania Umowy, na 12 miesięcy.
2. Wykonawca dostarczy dokumenty licencyjne, warunki licencjonowania oraz klucze licencyjne i instrukcje instalacji do Oprogramowania na adres e-mail: [postepowania-it@kopernik.lodz.pl](mailto:postepowania-it@kopernik.lodz.pl)
3. Udzielona na oprogramowanie licencja musi umożliwiać co najmniej:
   1. Dostęp do najnowszej wersji oprogramowania.
   2. Wsparcia technicznego producenta lub dystrybutora oprogramowania.
4. Parametry i funkcjonalności dostarczonego oprogramowania, nie mogą być gorsze niż wskazane poniżej:
   1. Konfiguracja, nadzór nad pracą poszczególnych modułów oraz instalacja/deinstalacja musi być wykonywana z Centralnej konsoli zarządzającej, która jest dostępna min. przez przeglądarkę internetową.
   2. Wsparcie techniczne musi odbywać się w języku polskim przez cały czas trwania umowy w trybie zgłoszeniowym w Dni Robocze (tj. od poniedziałku do piątku z wyłączeniem sobót, świąt i dni wolnych od pracy) na adres e-mail ……………………………………. **/PODAĆ/** w godzinach od 8.00 do 16.00.

|  |  |  |  |
| --- | --- | --- | --- |
| **Opis Przedmiotu Zamówienia** Przedmiotem zamówienia jest dostawa oraz roczne wsparcie techniczne i serwisowe systemu DLP (Data Loss Prevention) dedykowanego do ochrony 700 użytkowników . | | | |
| Lp. | Opis wymaganych funkcjonalności i parametrów | Parametry wymagane | Podać/opisać lub potwierdzić spełnienie wymogu wpisać „*Spełniam*” |
|  | Wymagania ogólne |  |  |
|  | System musi być dostarczony z dokumentacją w języku polski lub angielskim | Tak |  |
|  | System zainstalowany na zasobach zamawiającego (model on-premises) | Tak |  |
|  | Zakres dostawy obejmuje dostarczenie oprogramowania wraz licencją | Tak |  |
|  | Architektura: serwer centralny + endpoit agent | Tak |  |
|  | Roczne wsparcie techniczne | Tak |  |
|  | Wymagania systemowe i funkcjonalne |  |  |
|  | System operacyjny: | Tak |  |
|  | Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi | Tak |  |
|  | Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi | Tak |  |
|  | MacOS 12 lub nowszy | Tak |  |
|  | Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016  (64-bit) i nowszych. | Tak |  |
|  | Serwer administracyjny musi obsługiwać bazy danych: a. MS SQL Server 2016 lub nowsze, b. MS SQL Express, c. AzureSQL S3 lub nowsze. | Tak |  |
|  | Pomoc i dokumentacja programu dostępne w języku polskim lub angielskim | Tak |  |
|  | Konsola administracyjna i komunikaty klienta muszą być w języku polskim. | Tak |  |
|  | Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta. | Tak |  |
|  | Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na  stacjach roboczych. | Tak |  |
|  | Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a  serwerem zarządzającym. | Tak |  |
|  | Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia. | Tak |  |
|  | Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli. | Tak |  |
|  | System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy  danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit. | Tak |  |
|  | Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania  stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania. | Tak |  |
|  | Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli  programu. | Tak |  |
|  | Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych  modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu). | Tak |  |
|  | Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory. | Tak |  |
|  | Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a  serwerem w czasie rzeczywistym. | Tak |  |
|  | Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika | Tak |  |
|  | Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w  oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia,  odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach. | Tak |  |
|  | Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych,  aplikacji i typów plików. | Tak |  |
|  | Administrator musi mieć możliwość filtrowania i sortowania zebranych danych. | Tak |  |
|  | Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem  wiadomości email. | Tak |  |
|  | Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych,  użytkowników lub grup w określonym przedziale czasu. | Tak |  |
|  | Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez  producenta oprogramowania. | Tak |  |
|  | Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików. | Tak |  |
|  | Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie  aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku. | Tak |  |
|  | Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących  blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp. | Tak |  |
|  | Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne  kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN. | Tak |  |
|  | Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym. | Tak |  |
|  | Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM. | Tak |  |
|  | Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP. | Tak |  |
|  | Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania  klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania. | Tak |  |
|  | System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail  wysyłaną przez użytkowników Microsoft 365. | Tak |  |
|  | System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft  SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams. | Tak |  |
|  | System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać  poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach. | Tak |  |
|  | System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.). | Tak |  |
|  | System musi zapewniać możliwość zarządzanie szyfrowaniem dysków twardych oraz urządzeń wymiennych. | Tak |  |
|  | Wsparcie techniczne |  |  |
|  | Zgłoszenia przez e-mail | Tak |  |
|  | Zgłoszenia telefoniczne w godzinach 8:00-16:00 | Tak |  |
|  | Dostęp do dokumentacji technicznej | Tak |  |