Załącznik nr 1a do SWZ

**Opis przedmiotu zamówienia na część nr 1**

**Opis funkcjonalności oprogramowania** **DLP oferowanego**

**przez Wykonawcę**

 …………………………….…………………………………………..

 (producent, pełna nazwa oprogramowania oferowanego przez Wykonawcę)

|  |
| --- |
| **Opis funkcjonalności oprogramowania DLP wymaganej przez Zamawiającego**  |
|  | **TAK\*** | **NIE** |
| \*należy potwierdzić spełnianie funkcji poprzez wpisanie „TAK” lub „NIE” w przypadku niespełniania funkcji) |
| System operacyjny: Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi, Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi, MacOS 12 lub nowszy |  |  |
| Serwer administracyjny musi zostać wystawiony w wersji chmurowej. |  |  |
| System powinien zapewniać retencje danych systemu maksymalnie przez 18 miesięcy |  |  |
| System zapewnia historię kontekstu danych do klasyfikacji poprzez śledzenie zmian w danych oraz ich kontekst maksymalnie przez 18 miesięcy. |  |  |
| Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta. |  |  |
| Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych. |  |  |
| Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym. |  |  |
| Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia. |  |  |
| Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli. |  |  |
| Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, |  |  |
| Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu. |  |  |
| Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu). |  |  |
| Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory. |  |  |
| Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP |  |  |
| 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 |  |  |
| Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików |  |  |
| Administrator musi mieć możliwość filtrowania i sortowania zebranych danych. |  |  |
| Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email. |  |  |
| Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu. |  |  |
| Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania. |  |  |
| 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. |  |  |
| Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku. |  |  |
| Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach lokalnych. |  |  |
| 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. |  |  |
| 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. |  |  |
| Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym. |  |  |
| Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania. |  |  |
| System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365. |  |  |
| System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams. |  |  |
| System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach |  |  |

*(****podpis elektroniczny*** *osoby/osób upoważnionej do reprezentowania Wykonawcy)*