Szczegółowy opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa wraz z wdrożeniem oprogramowania i rocznym wsparciem serwisowym klasy DLP (Data Loss Prevention) do zabezpieczania danych przed wyciekiem i utratą na potrzeby Ministerstwa Rodziny i Polityki Społecznej (MRiPS) dla 800 zasobów sprzętowych Ministerstwa.

1. Wymaganie minimalne dla oprogramowania klasy DLP

Typ wymagania	**Wymaganie minimalne**
Ogólne	licencja bezterminowa
	pełne wsparcie dla stacji roboczych z systemami Windows 7/8/8.1/10 w wersjach 32 i 64 bitowej
	konsola zarządzająca i komunikaty generowane przez oprogramowanie muszą być w języku polskim
	musi zapewnić możliwość synchronizacji użytkowników oraz stacji roboczych z usługą Active Directory przez administratora
	musi zapewnić możliwość synchronizacji grup administratorów konsoli DLP z grupami zabezpieczeń Active Directory przez administratora
	musi zapewnić możliwość zarządzania bazą danych przez administratora poprzez określone zadania: 1. kopia bazy danych; 2. kopia oraz wyczyszczenie bazy danych; 3. wyczyszczenie bazy danych; 4. kopia ustawień serwera.
	musi zapewnić możliwość określenia przez administratora czasu związanego z wykonywaniem zadań na bazie danych; zadania powinny być wykonywane co najmniej w interwałach: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące
	musi zapewnić możliwość przypisywania jak i odbierania uprawnień do wybranych modułów przez administratora; uprawnienia muszą być podzielone na moduły: 1. **monitorowania:** wykorzystywanych aplikacji, odwiedzanych stron internetowych, wykorzystywanych plików, podłączonych urządzeń zewnętrznych oraz przesłanych i odebranych wiadomości e-mail; 2. **DLP:** służące do oznaczania plików, tworzenia reguł wykorzystania plików wrażliwych, białych i czarnych list urządzeń; 3. **Nadzorcy:** kontroli dostępu do stron internetowych, kontroli dostępu do aplikacji oraz kontroli dostępu do druku.
	musi zapewniać możliwości audytu stacji roboczych oraz konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach
	musi zapewni możliwość filtrowania oraz sortowania zebranych danych oraz zapisania ich w postaci plików: PDF, XLS i/lub CSV przez administratora
Serwer Administracyjny	musi zapewnić możliwość instalacji na systemach Windows Server w wersjach: 2012, 2012 R2, 2016, 2019

	musi działać w architekturze klient-serwer, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta
	musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych
	reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem a serwerem administracyjnym
	w przypadku braku połączenia klienta z serwerem administracyjnym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem
	musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików
	musi mieć możliwość ustawienia powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanych z ochroną DLP
	musi posiadać wbudowany serwer SMTP udostępniony przez producenta oprogramowania
	musi umożliwiać tagowanie plików na poziomie systemu plików lub na poziomie metadanych pliku
	musi umożliwiać wykonanie zadania tagowania plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie istniejących plików z tagami
	musi mieć możliwość tagowania plików wrażliwych w oparciu o: 1. aplikację, w której zostały utworzone; 2. lokalizację; 3. adres URL; 4. format pliku; 5. zawartość pliku
	dla plików, które zostały otagowane, musi być możliwe utworzenie reguł blokowania oraz zezwalania na: 1. zapisywanie, przenoszenie plików do lokalizacji na określonych dyskach lokalnych; 2. przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń; 3. drukowanie na określonych drukarkach; 4. zapisywanie i przenoszenie do lokalizacji sieciowej; 5. wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen; 6. zapisywanie, przenoszenie plików do folderów synchronizacji z usługami chmury; 7. zapisywanie i przenoszenie poprzez usługę pulpitu zdalnego; 8. wykonywanie zrzutów ekranowych, nagrywanie na płyty oraz wirtualne drukowanie
	musi umożliwiać określenie białych i czarnych list zawierających urządzenia pamięci masowej, drukarki, lokalizacje sieciowe, adresy e-mail oraz domeny, urządzenia przenośne, które mogą być wykorzystywane do określenia reguł dostępu
	musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych oraz dysków o określonych literach

	musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych oraz nośników optycznych (CD/DVD)
	musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM (Trusted Platform Module)
	musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych
	musi posiadać możliwość blokowania aplikacji w oparciu o jej kategorię, lokalizację oraz źródło pochodzenia
	musi posiadać możliwość blokowania drukowania na wszystkich lub określonych drukarkach fizycznych, sieciowych oraz wirtualnych
	musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych od jakich zostanie uruchomione zadanie tagowania
	musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi
Konsola zarządzająca (webowa)	musi umożliwiać pobranie pliku instalacyjnego agenta
	musi zapewnić administratorowi możliwość tworzenia nowych kont administratorów, ich usuwania oraz klonowania
	musi posiadać możliwość wysyłania alarmów dotyczących incydentów bezpieczeństwa
	musi wyświetlać informacje na temat produktywności pracowników i bezpieczeństwa danych, które są podzielone na: 1. przegląd informacji o incydentach bezpieczeństwa; 2. przegląd danych przychodzących; 3. przegląd danych wychodzących; 4. podłączane/odłączane urządzenia przenośne; 5. aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji
	musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP
	musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania
	musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje nt.: 1. plików przenoszonych na nośniki USB i inne urządzenia przenośne; 2. plików przesłanych za pomocą wiadomości e-mail; 3. plików przesłanych za pomocą poczty webowej; 4. plików przesłanych do Internetu; 5. plików wysłanych za pomocą komunikatorów; 6. plików przesłanych na dyski chmurowe; 7. analiza sposobu korzystania z aplikacji; 8. analiza korzystania z Internetu; 9. analiza wykorzystania portali do poszukiwania pracy

2. **Wdrożenie**

Zakres wdrożenia będzie obejmować w szczególności:

a) instalację i konfigurację wszystkich komponentów oprogramowania na infrastrukturze Zamawiającego;
b) instalację klientów na maksymalnie 10 stacjach roboczych;
c) włączenie funkcji audytora oraz ustawienie tagowania jednej przykładowej ścieżki lokalnej (tagowanie w oparciu o maksymalnie 10 plików tekstowych);
d) ustawienie kategorii danych w oparciu o wskazane przez klienta dane wrażliwe, ustawienie reguły (jednej) DLP, instruktaż do funkcjonalności konsoli;

3. Wykonawca zobowiązany jest przeprowadzić instruktaż dla maksymalnie 3 osób wskazanych przez Zamawiającego.
4. Zakres instruktażu musi odnosić się bezpośrednio do przedmiotowego wdrożenia.
5. Instruktaż może odbywać się w formie zdalnej. W takim przypadku Wykonawca musi zapewnić dostęp do zdalnego środowiska, tak by zakres instruktażu nie uległ zmianie w porównaniu z instruktażem prowadzonym w sposób tradycyjny.
6. Instruktaż musi być prowadzony przez minimum 1 inżyniera biorącego bezpośredni udział we wdrożeniu oferowanego oprogramowania w siedzibie Zamawiającego.

7. **Wsparcie serwisowe**

a) Oferowane oprogramowanie musi posiadać aktywne wsparcie producenta w okresie 12 miesięcy od daty zakupu, umożliwiające aktualizację do najnowszych wersji oraz wsparcie Wykonawcy w zakresie zgłaszania ewentualnych problemów w trybie 24x7 drogą mailową, lub przez portal online, a w dni robocze również telefonicznie, w godzinach 8:15 – 16:15.
b) W ramach wsparcia technicznego Wykonawca przez okres 12 miesięcy po wdrożeniu zapewni bezpłatną dostępność w języku polskim inżyniera w zakresie rozwiązywania problemów dotyczących przedmiotu zamówienia.