Załącznik nr 5a do SWZ

Opis przedmiotu zamówienia - Część I

Zamawiający zastrzega sobie prawo sprawdzenia zgodności oferowanego oprogramowania w oparciu o informacje zamieszczone na stronie internetowej producenta, w przypadku braku takiej możliwości, Zamawiający będzie wymagał przedstawienia dokumentacji producenta potwierdzającej wymagania minimalne.

Przedmiotem zamówienia jest zakup i dostawa wraz z wdrożeniem **oprogramowania klasy DLP (Data Loss Prevention)** ze wsparciem serwisowym i aktualizacjami do 17.04.2026.

Oprogramowanie ma zabezpieczać dane przed wyciekiem i utratą na potrzeby Starostwa Powiatowego w Radomsku, o parametrach nie gorszych niż wskazane poniżej:

Parametr	**Wymagania minimalne**
Licencja	Bezterminowa
Liczba stanowisk	170
Serwis/wsparcie techniczne	Oferowane oprogramowanie musi posiadać aktywne wsparcie producenta do 17.04.2026 r., umożliwiające bezpłatne aktualizacje w tym do najnowszych wersji oraz wsparcie w zakresie zgłaszania ewentualnych problemów drogą mailową lub przez portal online, a w dni robocze również telefonicznie, w godzinach 9:00 – 15:00. W ramach wsparcia technicznego producent lub oficjalny dystrybutor zapewni bezpłatną dostępność w języku polskim inżyniera w zakresie rozwiązywania problemów dotyczących przedmiotu zamówienia.
Wdrożenie	W ramach wdrożenia wymagane jest aby Wykonawca wykonał następujące czynności: a) instalację i konfigurację wszystkich komponentów oprogramowania na infrastrukturze Zamawiającego, b) ustawienie kategorii danych w oparciu o wskazane przez klienta dane wrażliwe, ustawienie reguły (jednej) DLP, d) szkolenie z funkcjonalności oprogramowania dla 2 osób wskazanych przez Zamawiającego.

	Usługa może być wykonana zdalnie lub na miejscu przez pracownika posiadającego wiedzę potwierdzoną aktualnym certyfikatem/dokumentem producenta – wymagane przedstawienie przed przystąpieniem do wdrożenia aktualnego certyfikatu/dokumentu osoby potwierdzającego jej kwalifikacje do wdrożenia wydanego przez producenta oprogramowania lub oficjalnego przedstawiciela w Polsce. Koszty wdrożenia należy ująć w cenie oprogramowania.
Stacje robocze	Pełne wsparcie dla posiadanych przez Zamawiającego stacji roboczych z systemami Windows 10/11.
Ogólne	System musi umożliwiać ochronę przed wyciekiem informacji z systemów informatycznych Zamawiającego.
	Ochrona informacji powinna odbywać się w oparciu o reguły DLP oraz predefiniowane lub zdefiniowane przez administratora polityki bezpieczeństwa.
	System musi umożliwiać monitorowanie i ochronę wielu kanałów komunikacyjnych, w szczególności: • http oraz https, • email (w tym załączniki), • komunikatory internetowe, • pliki udostępniane w chmurze.
Baza danych	Jeżeli system DLP wymaga do swego działania bazy danych, musi ona być wkalkulowana w cenę oprogramowania lub posiadać bezpłatną licencję.
Serwer Administracyjny	System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows Server (minimum Server 2022) lub Redhat/Oracle Linux (minimum 7.x).
	Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem a serwerem zarządzającym.
	Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość - co najmniej o:

	a) numer PESEL, b) numer polskiego dowodu osobistego, c) określone ciągi znaków, d) numer IBAN.
	Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
	Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition).
	W przypadku braku połączenia klienta z serwerem zarządzającym klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.
	Serwer musi zapewnić możliwość synchronizacji użytkowników oraz stacji roboczych z wykorzystywaną przez Zamawiającego usługą Active Directory.
	System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej logowanie oraz wylogowanie użytkownika.
	Serwer administracyjny musi umożliwiać kategoryzację (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku.
	Serwer musi posiadać możliwość wysłania alertów, co najmniej za pośrednictwem wiadomości email.
Interfejs użytkownika	W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim.
Konsola administratora	Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych oraz typów plików.
	Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane administrator może zapisać w postaci plików PDF bądź XLS.

	Administrator musi posiadać możliwość 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.
	Możliwość tworzenia raportów, które muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
	Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
	Administrator musi mieć możliwość tworzenia i usuwania nowych kont administratorów w konsoli programu.
	Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.
Polityki bezpieczeństwa	System musi umożliwiać budowanie polityk ochrony informacji uwzględniając kontekst w jakim informacja jest używana, czyli musi uwzględniać okoliczności jak: • co jest wysyłane, • kto wysyła informacje, • gdzie (do kogo) są wysyłane informacje.
	Polityki bezpieczeństwa muszą umożliwiać zezwalanie/blokowanie takich czynności jak: - kopiowanie na zewnętrzne nośniki danych, dyski chmurowe, wysyłanie przez pocztę elektroniczną, - używanie schowka systemowego, - drukowanie.
	System musi mieć możliwość wysyłania powiadomień do każdej z polityk.

Funkcjonalność	a) pobranie pliku instalacyjnego agenta za pomocą konsoli zarządzającej, b) instalacja/dezinstalacja zdalnego klienta na stacjach roboczych za pomocą serwera administracyjnego, c) reguły DLP egzekwowane przy braku połączenia między klientem a serwerem zarządzającym, d) brak połączenia klienta z serwerem zarządzającym umożliwia lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia, e) zarządzanie za pośrednictwem konsoli, f) konfiguracja automatycznej konserwacji dla bazy danych, usuwająca najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit, g) automatyczne pobieranie aktualizacji definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją jej wyłączenia, h) tworzenie i usuwanie i kont administratorów w konsoli programu, i) rejestrowanie zdarzenia aktywności stacji roboczej, jak logowanie, wylogowanie, włączenie, wyłączenie, blokada, odblokowanie i przejście w stan bezczynności. j) wymuszenie synchronizacji ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym, k) ustawianie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa, l) audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości e-mail oraz czynności na plikach,

	m) tworzenie własnych kategorii dla stron internetowych, aplikacji i typów plików, n) filtrowanie i sortowanie zebranych danych, o) wysyłanie alertów, za pośrednictwem wiadomości email, p) dashboardy generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu, q) kategoryzacja plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku, r) wyszukiwanie danych osobowych na zasobach zarówno lokalnych, jak i sieciowych, s) dla plików skategoryzowanych, tworzenie reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp., t) wyszukiwanie i ochrona 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, u) weryfikacja zawartości pliku w czasie rzeczywistym, v) eksport logów do rozwiązań klasy SIEM, w) konfiguracja/zmiana domyślnego serwera SMTP, x) konsola webowa pozwala na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
Wymagania sprzętowe	Oprogramowanie musi poprawnie funkcjonować i nie może mieć wymagań większych niż posiadany przez Zamawiającego serwer o parametrach: - dwa procesory 8-rdzeniowe, klasy serwerowej x86, - pamięć 64 GB, - macierz dyskowa 4 TB, - system operacyjny Windows Server Standard 2022 x64.

Gwarancja	1. Wykonawca zapewni prawidłowe i sprawne działanie oferowanego oprogramowania - systemu jako całości, jak również każdego z elementów tego systemu oddzielnie i udzieli gwarancji do 17.04.2026 roku na system i wszystkie jego elementy. 2. Wykonawca zapewni również wsparcie serwisowe dla dostarczonego rozwiązania, które będzie świadczone przez Producenta oprogramowania w ramach wynagrodzenia przysługującego Wykonawcy na podstawie umowy. 3. Zgłoszenia dotyczące wystąpienia wad, awarii mogą być przyjmowane drogą mailową lub przez portal online, a w dni robocze również telefonicznie, w godzinach 9:00 – 15:00. W ramach wsparcia technicznego Producent lub oficjalny dystrybutor zapewni bezpłatną dostępność w języku polskim inżyniera w zakresie rozwiązywania problemów dotyczących przedmiotu zamówienia. 4. Bieg terminu gwarancji rozpoczyna się od daty odbioru przedmiotu umowy. 5. W okresie gwarancji Wykonawca zobowiązuje się do bezpłatnego usunięcia stwierdzonych wad. 6. Gwarancja obejmuje wszelkie wady z wyjątkiem wad spowodowanych niewłaściwym lub niezgodnym z instrukcją obsługi użytkowaniem produktu oraz wad spowodowanych zdarzeniami losowymi. 7. Jeżeli usunięcie ujawnionej wady wdrożonego systemu jest możliwe wyłącznie w drodze dokonania zakupu jakichkolwiek udoskonaleń (w tym: unowocześnień, aktualizacji, dodatków sprzętowych, wszelkiego rodzaju usług, serwisów, licencji i uprawnień), Wykonawca jest zobowiązany dokonać tego zakupu na własny koszt i zainstalować przedmiot zakupu we wdrożonym systemie.

	8. Wykonawca pokrywa w ramach gwarancji wszelkie koszty napraw i wymiany elementów systemu, w tym koszty dojazdu, transportu, demontażu, montażu, odinstalowania lub zainstalowania. 9. Udzielona przez Wykonawcę gwarancja nie wyłącza uprawnień Zamawiającego wynikających z rękojmi za wady oraz uprawnień Zamawiającego z tytułu gwarancji udzielonych przez producenta oprogramowania. 10. Wykonawca do oprogramowania dostarczonego Zamawiającemu na podstawie umowy dołącza Licencje oraz wszelkie inne dokumenty konieczne do prawidłowego korzystania z Systemu. 11. Dla oprogramowania wymaga się dostarczenia wsparcia technicznego producenta tego oprogramowania do 17.04.2026 roku z możliwością jego odnawiania po tym czasie.