

OPIS PRZEDMIOTU ZAMÓWIENIA

„DOSTAWA OPROGRAMOWANIA INFORMATYCZNEGO - SYSTEMU DLP WRAZ Z WDROŻENIEM ROZWIĄZANIA”
Część 4 zamówienia na „Dostawę oprogramowania informatycznego” będącego częścią projektu pn. „Cyberbezpieczna Gmina Porąbka”

WYMAGANE MINIMALNE PARAMETRY JAKOŚCIOWE

I.	System DLP
1	INFORMACJE OGÓLNE
	PRODUCENT / NAZWA ROZWIĄZANIA
2	WYMAGANIA OGÓLNE
1)	Wsparcie instalacji w oparciu o bazę MS SQL.
2)	Praca w architekturze serwer, agent, klienta gdzie komunikacja serwera zarządzającego z klientem odbywa się tylko przy pomocy agenta.
3)	Serwer administracyjny musi umożliwiać wykonanie instalacji/deinstalacji zdalnej klienta na stacjach roboczych.
4)	Rozwiązanie musi być dostępne minimum w polskiej wersji językowej.
5)	Możliwość aktualizacji komponentów własnych.
6)	Automatyczne pobieranie aktualizacji definicji kategorizowania stron internetowych oraz aplikacji. Musi być możliwość wyłączenia automatycznego pobierania.
7)	Wymuszenie komunikacji w czasie rzeczywistym dla wybranej stacji komputerowej w celu sprawdzania konfiguracji.
8)	Możliwość zablokowania/uruchomienia trybu awaryjnego na stacji końcowej
9)	Możliwość zdefiniowania portów dla ruchu pocztowego które mają być monitorowane przez oprogramowania zainstalowane na stacji końcowej.
10)	Możliwość ustawień powiadomień dla użytkownika końcowego w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP.
11)	Możliwość audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, dokumenty drukowane, ruch sieciowy, wysyłane oraz odbierane wiadomości e-mail oraz wykonywane czynności na plikach.
12)	Filtrowanie poprzez podanie zakresu czasu.

13)	<p>Analiza lub tagowanie nowo powstałych plików wrażliwych w oparciu o minimum:</p> <ul style="list-style-type: none"> – aplikację z której zostały utworzone – lokalizację lokalną oraz sieciową – adres URL, z którego został pobrany plik – format pliku – zawartość pliku
14)	Analiza lub tagowania posiadanych plików wrażliwych w oparciu o minimum : lokalizację lokalną oraz sieciową, format pliku oraz zawartość pliku.
15)	<p>Możliwość powiadamiania użytkownika jeśli zidentyfikuje w wiadomości e-mail m.in.:</p> <ul style="list-style-type: none"> – numery Kart kredytowych – numer PESEL – numer polskiego dowodu osobistego – wyrażenia regularne – określone ciągi znaków – numer IBAN
16)	<p>Dla tagowanych plików możliwość utworzenia reguł w oparciu o czynności:</p> <ol style="list-style-type: none"> a) blokowania oraz zezwalania na zapisywanie, przenoszenie plików do lokalizacji na dyskach lokalnych lub konfiguracji określonych lokalizacji, do której będzie możliwość bądź nie będzie możliwości zapisu. b) blokowania oraz zezwalania na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń. c) zabezpieczenia możliwości drukowania, utworzenia białej oraz czarnej listy drukarek. d) blokowania oraz zezwalania na zapisywanie, przenoszenie do lokalizacji sieciowej oraz określenie białej oraz czarnej listy lokalizacji sieciowych. e) blokowania oraz zezwalania wysyłki plików za pośrednictwem klientów pocztowych oraz określenia białej oraz czarnej listy adresów e-mail oraz domen. f) blokowania oraz zezwalania na zapisywanie, przenoszenie plików na dyski zaszyfrowane w oparciu o lokalnie zaszyfrowane dyski oraz zewnętrzne zaszyfrowane dyski. g) blokowania oraz zezwalania na zapisywanie, przenoszenie plików do folderów synchronizacji z usługami chmury (Google Drive, OneDrive Business, One Drive Personal, Dropbox, Box Sync, SharePoint). h) blokowania oraz zezwalania na zapisywanie, przenoszenie plików poprzez usługę pulpitu zdalnego i) blokowania oraz zezwalania na wykonywanie zrzutów ekranowych, skopiowania zawartości, nagrywania na płyty CD/DVD oraz wirtualnego drukowania plików. j) uruchomienia wybranego formatu pliku przez wskazaną przez administratora aplikację.
17)	Możliwość określenia stref urządzeń pamięci masowej,
18)	Możliwość globalnego zablokowania oraz zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury (Google Drive, OneDrive Business, One Drive Personal, Dropbox, Box Sync, SharePoint).
19)	Szyfrowanie dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzowanie do zaszyfrowanych nośników wymiennych musi być w pełni niezauważalne dla użytkownika.



20)	Możliwość tworzenia kluczy szyfrujących które będą kompatybilne z funkcjonalnością BitLocker dla zapewnienia transparentności współdzielenia zaszyfrowanych nośników wymiennych.
21)	Możliwość globalnego zablokowania, zezwolenia, dostępu tylko do odczytu z korzystania z określonych urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.
22)	Możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
23)	Możliwość wygenerowania hasła ratunkowego do odblokowania dostępu do zaszyfrowanych dysków oraz dysków wymiennych, w sytuacji jeżeli użytkownik zapomni hasła.
24)	Blokowanie stron internetowych w oparciu o kategorię stron oraz po podaniu adresu URL. Musi istnieć możliwość konfiguracji przekierowania z dowolnej strony która została zablokowana.
25)	Możliwość określenia stref urządzeń pamięci masowej,
3	RAPORTOWANIE
1)	Możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, dokumenty drukowane, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.
2)	Możliwość raportowania reguł bezpieczeństwa w oparciu o incydenty na plikach chronionych, ogółu wykonanych operacji na plikach, podsumowania wszystkich incydentów bezpieczeństwa, akcji użytkowników na zabezpieczonych plikach, zablokowanych operacji na dyskach lokalnych, zewnętrznych, podsumowanie korzystania z urządzeń oraz ich typów.
3)	Możliwość utworzenia raportu w oparciu o użycie aplikacji, zablokowanych aplikacji, zablokowanych drukarek, podsumowanie drukowania, zablokowane strony internetowe, zablokowanych użytkowników, aktywność użytkowników na serwerze, alarmy, ustawień klienta, kopii bezpieczeństwa, zarządzania stacjami końcowymi, dezaktywacją licencji oraz zaawansowanego debugowania.
4)	Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
5)	Raporty muszą być generowane do pliku PDF, XLS po podaniu lokalizacji zapisywanego pliku, na wskazane adresy e-mail.
4	ADMINISTRACJA
1)	Synchronizacja użytkowników oraz stacji roboczych z usługą Active Directory.
2)	Możliwość zarządzania bazą danych poprzez określone zadania – kopii bazy danych, kopii oraz usunięcia bazy danych, usunięcia bazy danych, ustawieniach kopii bazy danych - dostępne z poziomu konsoli wraz z określeniem automatycznego powtarzania zadań: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.
3)	Możliwość zdefiniowania przedziału czasowego dla kopii zapasowej bazy programu.
4)	Funkcje automatycznej kopii bazy danych programu DLP co 7, 14, 30 dni
5)	Tworzenie nowych/usuwanie/klonowanie kont administratorów w konsoli programu.
6)	Możliwość zmiany hasła oraz loginu innego administratora.
7)	Przypisywanie / odbieranie uprawnień do wybranych modułów programu.



8)	Możliwość logowania za pośrednictwem grup domenowych administratorów.
9)	Możliwość ustawienia godzin w których nie będą obowiązywały użytkownicy reguły kontroli aplikacji oraz stron internetowych. Godziny pracy muszą być ustalane dla poszczególnych dni tygodnia.
10)	Możliwość określenia czy dokumenty zawierające dane wrażliwe takie jak numery Kart kredytowych, numer PESEL, numer polskiego dowodu osobistego, wyrażenia regularne, określone ciągi znaków, numer IBAN, mogą zostać przesłane do chmur lub innych źródeł WWW.
11)	Określanie bezpiecznych stref oraz domen do których pliki mogą zostać przesłane.
12)	Możliwość określenia czy dokumenty zawierające dane wrażliwe takie jak numery Kart kredytowych, numer PESEL, numer polskiego dowodu osobistego, wyrażenia regularne, określone ciągi znaków, numer IBAN, mogą zostać przesłane na urządzenia zewnętrzne.
13)	Możliwość przygotowania pliku instalacyjnego agenta.
14)	Możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
15)	Możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
5	KONSOLA ZDALNA
1)	Możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
2)	Możliwość współdziałania z bazą danych MS SQL Server.
3)	Logowanie do konsoli webowej musi opierać się na wcześniej utworzonych kontach użytkowników w konsoli aplikacyjnej.
4)	Uprawnienia dostępu wybranych użytkowników do poszczególnych informacji na temat grup komputerów lub grupy użytkowników w konsoli webowej, muszą być ustalane z poziomu konsoli aplikacyjnej.
5)	<p>Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz użycia sprzętu które są podzielone na:</p> <p>a) Bezpieczeństwo danych:</p> <ul style="list-style-type: none"> – przegląd informacji o incydentach bezpieczeństwa. – przegląd danych przychodzących. – przegląd danych wychodzących. – przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików. – podłączane/odłączane urządzenia przenośne. <p>b) Produktywność:</p> <ul style="list-style-type: none"> – przegląd informacji na temat produktywności użytkowników.



	<ul style="list-style-type: none"> – aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji. – trendy <p>c) Eksploatacja sprzętu:</p> <ul style="list-style-type: none"> – przegląd informacji na temat eksploatacji sprzętu komputerowego. – eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery. – eksploatacja drukarek. – eksploatacji sieci.
6)	Możliwość dodania klucza licencji.
7)	Możliwość konfiguracji/zmiany domyślnego serwera SMTP.
8)	Weryfikacja wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.
9)	Generowanie raportów z danymi na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu. Raporty muszą być generowane dla wybranych grup komputerów/użytkowników w interwałach tygodniowych lub miesięcznych. Raporty będą przesyłane drogą e-mailową.
II.	<i>Wymagania dodatkowe</i>
1	INSTALACJA I KONFIGURACJA
1)	Instalacja i konfiguracja rozwiązania w środowisku Zamawiającego. Instalacja musi obejmować również minimum 105 stacji komputerowych (łącznie przewidywana wstępnie ilość stacji w jednostkach organizacyjnych Zamawiającego tj. Urząd Gminy Porąbka, GOPS w Porąbce oraz Gminny Zespół Obsługi Szkół i Przedszkoli w Porąbce.
2)	<p>W ramach konfiguracji Zamawiający wymaga:</p> <ul style="list-style-type: none"> a) włączenie funkcji audytora, b) ustawienie tagowania minimum jednej przykładowej ścieżki lokalnej w oparciu o minimum 10 plików tekstowych, c) ustawienie kategorii danych w oparciu o wskazane przez klienta dane wrażliwe, d) ustawienie reguł DLP,
2	DOKUMENTACJA POWYKONAWCZA
1)	<p>Po zakończeniu realizacji, Zamawiający wymaga dostarczenia pełnej dokumentacji powykonawczej oraz procedur eksploatacji rozwiązań. Dokumentacja powykonawcza musi zawierać minimum:</p> <ul style="list-style-type: none"> a) opis ogólnych informacji o rozwiązaniach; b) zestawienie loginów i haseł; c) zestawienie ustawień rozwiązania; d) instrukcje instalacji, konfiguracji, uruchomienia; e) zestawienie licencji; f) listę autoryzowanych kontaktów serwisowych.



