Załącznik nr 1

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa i wdrożenie systemu DLP wraz z asystą dla Narodowego Funduszu Zdrowia Podkarpackiego Oddziału Wojewódzkiego z siedzibą w Rzeszowie

Lp.	Zakres wymagań	Wymagania minimalne
1	Podstawowe wymagania techniczne i technologiczne dla rozwiązania	1. System musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.
		2. Komponenty oprogramowania instalowane na stacjach użytkowników muszą być zgodne z systemem operacyjnym Windows 10 i zapewniać wsparcie dla 32 i 64-bitowej wersji systemu Windows.
		3. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server, 2016, 2019.
		4. Administrator musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z usługą Active Directory.
		5. System musi zapewniać ochronę urządzenia końcowego bez względu na to, czy komputer jest podłączony do sieci czy nie.
		6. System musi umożliwiać zarządzanie za pośrednictwem konsoli webowej
		7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta, a serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych. Agent musi być zabezpieczony przed wyłączeniem i restartem przez użytkownika.
		8. Rozwiązanie musi reagować na próby wysyłania poufnych danych z i na urządzenia końcowe, musi zapewniać ochronę nawet, gdy urządzenie nie jest podłączone do sieci korporacyjnej. Rozwiązanie musi monitorować co najmniej wysyłane wiadomości email, HTTP/HTTPS, FTP, kopiowanie danych z komputera na udział sieciowy, kopiowanie danych z udziału sieciowego do komputera przez Windows Explorer, SFTP, SSH, Bluetooth, Skype, WebEx, LiveMeeting i inne. Musi blokować użycie i wysyłkę poufnych danych przez dowolną aplikację. Musi monitorować i blokować kopiowanie danych na przenośne urządzenia (USB, CD/DVD, SD/CF, eSATA itp) pozwalając jednocześnie na kopiowanie informacji na zaakceptowane urządzenia przenośne. Rozwiązanie musi monitorować i blokować próby drukowania bądź faksowania zabezpieczonych danych.

		9. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu , a rozwiązanie musi pozwalać na stosowanie różnych polityk dla różnych urządzeń końcowych i użytkowników. Rozwiązanie musi rozróżniać polityki dla dwóch różnych użytkowników zalogowanych na tym samym komputerze.
		10. Rozwiązanie musi umożliwiać tagowanie plików na poziomie systemu plików lub na poziomie metadanych pliku - zarówno plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, jak i nowych plików, które powstaną na bazie istniejących plików z tagami.
		11. System musi posiadać możliwość zaszyfrowania całej powierzchni dysku i dysków zewnętrznych. Musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych. Dla zaszyfrowanych dysków zewnętrznych czy pamięci typu pendrive, musi być możliwość uruchomienia i dostępu do danych poza strukturą Zamawiającego, np. poprzez podanie hasła.
		12. Rozwiązanie musi mieć możliwość ustawień powiadomień do użytkowania końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ustawieniami DLP. Jednocześnie musi istnieć możliwość wycofania funkcji blokującej przez administratora lub osobę wyznaczoną.
		13. System 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.
		14. Dostarczony system musi umożliwić objęcie ochroną min. 300 urządzeń (lub 250 użytkowników – w zależności od zasad licencjonowania). Dostarczona licencja musi być bezterminowa.
2.	Dodatkowe wymagania	Wymaganie dodatkowe (dodatkowo punktowane) - Konsola administracyjna oraz komunikaty klienta w języku polskim.
3.	Wymagania dotyczące wdrożenia	Część I – wykonanie w siedzibie Zamawiającego w terminie 30 dni od daty podpisania umowy. Wskazanie Zamawiającemu wymagań w zakresie przygotowania platformy do instalacji systemu (system operacyjny, poprawki, itp.). 1. Instalacja i wstępna konfiguracja systemu (nadanie IP, założenie kont użytkowników, konfiguracja dostępu do graficznego interfejsu użytkownika). 2. Integracja dostarczanego systemu z Active Directory. 3. Wstępna konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami Zamawiającego. 4. Propozycja scenariusza i wykonanie testów technologicznych wykazujących poprawność wdrożenia systemu (sprawdzenie poprawności działania polityk). 5. Przygotowanie podstawowych procedur obsługi dot. eksploatacji, postępowania na wypadek awarii, wykonania kopii zapasowych oraz ich odtworzenia.

		Część II – wykonanie po realizacji Części I w terminie do 20.12.2020 1. Warsztaty dla administratorów: a. Wykonawca przeprowadzi co najmniej trzydniowe warsztaty powdrożeniowe dla łącznie do 4 pracowników Zamawiającego w zakresie podstawowej i zaawansowanej obsługi i utrzymania systemu. b. Warsztaty szkoleniowe będą prowadzone w języku polskim przez osoby będące trenerami (pracownikami) producenta lub Wykonawcy i posiadające kwalifikacje i umiejętności, potwierdzone certyfikatem producenta dostarczonego systemu. c. W ramach warsztatów szkoleniowych Wykonawca zapewni materiały szkoleniowe dla każdego uczestnika, adekwatnie do zakresu szkolenia d. Warsztaty szkoleniowe będą prowadzone w siedzibie i w środowisku Zamawiającego lub w innym miejscu uzgodnionym z Zamawiającym. Zakres tematyczny warsztatów szkoleniowych Strony uzgodnią w trybie roboczym. 2. Aktywne wsparcie w dostrajaniu systemu, tworzenia nowych polityk bezpieczeństwa, ich testowania w wymiarze min. 30 godzin, realizowanych wg potrzeb Zamawiającego. Zamawiający zapewni wskazanym pracownikom Wykonawcy warunki pracy zdalnie poprzez łącza VPN niezbędne dla realizacji usług serwisowych. Zamawiający udostępni dane do ustanowienia bezpiecznego połączenia VPN, sesje VPN realizowane będą przez dedykowany serwer Zamawiającego podlegają monitorowaniu i nagrywaniu Warsztaty oraz aktywne wsparcie realizowane będą po zakończeniu Części I
4.	Gwarancja i usługi - serwisowe	Wykonawca zapewni gwarancję na dostarczony system na okres min. 24 miesięcy, w zakresie: 1. Wykonawca zapewni Zamawiającemu zdalne wsparcie oraz kontakt z działem serwisowym Wykonawcy telefonicznie oraz za pomocą poczty elektronicznej email. 2. Możliwość zakładania zgłoszeń serwisowych w dni robocze w godzinach 8:00 – 16:00. 3. Wykonawca w ramach reakcji na informację o awarii rozwiązania jest zobowiązany ją potwierdzić w dni robocze w godz. 8:00 – 16:00 z maksymalnym czasem reakcji 4 godz. Czas reakcji liczony jest od momentu zgłoszenia awarii (telefon, email) i określony jest jak przekazanie do Zamawiającego informacji zwrotnej i przyjęciu zgłoszenia i podjęciu kroków w celu jego realizacji. 4. Zamawiający dopuszcza wsparcie w formie bezpośredniej wizyty w siedzibie Zamawiającego, telefonicznej, e-mail, oraz kontrolowanego zdalnego dostępu. O wyborze formy świadczenia wsparcia decyduje Zamawiający po konsultacji z Wykonawcą. 5. Maksymalny czas usunięcia awarii lub przywrócenia funkcjonalności systemu wynosi dwa dni robocze od zgłoszenia. 6. W okresie trwania gwarancji Zamawiający musi mieć prawo do pobierania nowych wersji oprogramowania oraz niezbędnych składników systemu (np. sygnatur), niezbędnych do jego prawidłowego działania.