SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa systemu ochrony przed wyciekiem informacji DLP (Data Loss Prevention) oraz ochrony urządzeń mobilnych MDM (Mobile Device Management), wraz z kompletem niezbędnych licencji, przeszkoleniem pracowników oraz zapewnieniem wsparcia technicznego i serwisu dla zaoferowanego systemu.

SŁOWNIK POJĘĆ

Tag – Oznaczenie stosowane na plikach i dokumentach elektronicznych, wiadomościach mailowych umożliwiające identyfikację. Tag może istnieć: w treści dodanej w metadanych, w postaci nagłówka, stopki lub dodatkowego elementu np. pliku JPEG dodanego do pliku;

Klasyfikacja dokumentów / plików – Nadawanie odpowiedniej kategorii. Kategorie są możliwe do zdefiniowania i edycji np. poufne, tajne. Możliwość nadawania poprzez odpowiedni system lub funkcję np. menu kontekstowe w systemie Windows;

Polityka – inaczej zasada DLP to pakiet stanowiący zbiór reguł, które zawierają określone warunki, akcje i wyjątki, które mogą np. monitorować pliki na podstawie ich zawartości i generować incydenty.

1. **W ramach realizacji przedmiotu zamówienia mieści się:**
   - 1.1 Dostawa niezbędnych licencji i oprogramowania oferowanego systemu DLP dla 800 stanowisk w ramach zamówienia podstawowego;
   - 1.2 Zamawiający zastrzega sobie możliwość zakupu w ramach prawa opcji 20% dodatkowych licencji, ujętych w zamówieniu podstawowym pkt 1.1., w razie zaistnienia potrzeby;
   - 1.3 Dostawa niezbędnych licencji i oprogramowania oferowanego systemu MDM dla 800 urządzeń
   - 1.4 Zamawiający zastrzega sobie możliwość zakupu w ramach prawa opcji 20% dodatkowych licencji, ujętych w zamówieniu podstawowym pkt 1.3., w razie zaistnienia potrzeby;
   - 1.5 Instalacja oprogramowania na serwerze wskazanym przez Zamawiającego;
   - 1.6 Świadczenie serwisu i wsparcia technicznego producenta elementów oprogramowania (punkt 3) przez okres 24 miesięcy, licząc od daty podpisania bez uwag protokołu odbioru;
   - 1.7 Gwarancja Producenta elementów oprogramowania (punkt 3) świadczona przez okres 24, licząc od daty podpisania bez uwag protokołu odbioru;

1.8 Przeprowadzenie szkolenia z zakresu administracji zamawianego oprogramowania, dla min. 4 osób zrealizowane najpóźniej w terminie 90 dni kalendarzowych od dnia podpisania protokołu odbioru;

1.9 Zamawiający preferuje zastosowanie oprogramowania MDM zintegrowanego z DLP i zarządzanego jedną konsolą administracyjną.

2. Wymagania dotyczące dostawy oprogramowania oraz licencji:

2.1 Dostawa musi zostać zrealizowana zgodnie z terminem wskazanym w ofercie Wykonawcy, ale nie później niż 10 dni roboczych od dnia podpisania umowy;

2.2 Wykonawca zobowiązuje się dostarczyć wymagane, oprogramowanie oraz licencje pochodzące z legalnego źródła, zakupione w autoryzowanym kanale sprzedaży producenta i objęte standardowym pakietem usług gwarancyjnych świadczonych przez sieć serwisową producenta na terenie Polski;

2.3 Dostawa oprogramowania, aplikacji, modułów, wymaganych do prawidłowego funkcjonowania zaoferowanego systemu DLP, zgodnie z wymaganymi funkcjonalnościami oraz specyfikacją Zamawiającego;

2.4 Dostawa licencji wymaganych do poprawnej pracy systemu DLP, zgodnie z wymaganymi funkcjonalnościami opisanymi w specyfikacji;

2.5 Dostarczone do Zamawiającego licencje muszą być w postaci wygenerowanych na stronie producenta plików licencyjnych lub w formie wygenerowanych i przesłanych emailem przez Wykonawcę plików.

3. Wymagania dot. oprogramowania DLP

3.1. Zamawiający wymaga dostarczenia oprogramowania, zapewniającego ochronę przed wyciekiem poufnych danych (ang. Data Loss Prevention - DLP) obejmującego:

3.1.1. Ochronę stacji końcowych użytkowników Zamawiającego;

3.1.2. Ochronę i monitoring danych przesyłanych za pośrednictwem sieci LAN i/lub WAN;

3.1.3. Ochronę danych przesyłanych za pośrednictwem kanału drukowania (np. protokół LPD, IPP);

3.1.4. Ochronę danych przesyłanych za pośrednictwem kanału komunikacyjnego poczty email Zamawiającego (np. protokół SMTP, SMPTS);

3.1.5. Monitorowanie bezpieczeństwa plików aktualnie używanych np. zapisanych tymczasowo w pamięci podręcznej, otwartych w edytorze tekstu;

3.1.6. Monitorowanie i ochronę zasobów plikowych Zamawiającego np. baz danych, plików współdzielonych, archiwów cyfrowych i elektronicznego obiegu dokumentów;

3.1.7. Wielopoziomową klasyfikację dokumentów (tj. dodawanie dynamicznych nagłówków plików, dodawanie informacji o ważności pliku) Klasyfikacja jest widoczna dla użytkowników i systemów i podąża razem z plikiem;

3.1.8. Monitorować przepływ danych usług zdalnego pulpitu, zdalnego dostępu i udostępniania ekranu (np. RDP, VNC, SSH) wraz z wywoływaniem określonych akcji, zgodnie z przyjętymi politykami, w zależności od rodzaju przesyłanych treści;

3.2. **Podstawowe funkcje oprogramowania DLP**

Zamawiane oprogramowanie musi:

3.2.1. Być typu „End-Point" (serwer zarządzający/konsola zarządzająca + końcówki klienckie);

3.2.2. Umożliwiać przeglądanie zaistniałych zgłoszeń poprzez konsolę zarządzającą;

3.2.3. Umożliwiać definiowanie polityki ochrony przed wyciekiem np. na stacjach końcowych, poprzez pojedynczy punkt konfiguracji (konsola zarządzająca);

3.2.4. Umożliwiać definiowanie określonych akcji (przynajmniej blokowanie, monitorowanie, wysłanie komunikatu do użytkownika i/lub administratora Systemu DLP) następujących w przypadku wykrycia zagrożenia wycieku danych, w zależności od kanału komunikacyjnego, którego zagrożenie dotyczy;

3.2.5. Zapewniać, aby zasady tworzenia polityk bezpieczeństwa umożliwiały budowę polityki w oparciu o co najmniej następujące dane wprowadzane do tej polityki: zdefiniowaną zawartość podlegająca wykryciu, odbiorcę, nadawcę, rodzaje plików, rodzaje kanałów komunikacyjnych (np. protokoły HTTPS, SMPT), dane użytkownika końcowego jak: nazwy stacji końcowej użytkownika;

3.2.6. Umożliwiać nadawanie określonych poziomów ważności zdarzeń dotyczących wycieku danych;

3.2.7. Wspierać co najmniej uwierzytelnianie użytkowników w modelu użytkownik, grupa, rola (ang. model RBAC) oraz integrację z repozytorium danych Microsoft Active Directory, z uwzględnieniem możliwości wykorzystania struktury danych w nim zawartych (np. działy, grupy, lokalizacje);

3.2.8. Umożliwiać przeprowadzenie audytu stacji końcowych w oparciu o: uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, pliki wysłane do drukowania, ruch sieciowy, wysłane oraz odbierane wiadomości e-mail oraz wykonywane czynności na plikach;

3.2.9. Umożliwiać stosowanie gotowych algorytmów detekcji, wykrywających pojawienie się ustalonego wzorca (np. PESEL) (działających tam gdzie to możliwe o mechanizm sum kontrolnych w celu walidacji danych);

3.2.10. Umożliwiać zarządzanie ilością i retencją przechowywanych danych, obejmując dane całego systemu jak i dane dotyczące pojedynczych zdarzeń (w tym incydentów);

3.2.11. Zapewniać konsolę zarządczą oprogramowania, która jest dostępna przez przeglądarkę internetową (Web) z możliwością użycia przeglądarek wiodących dostawców, takich jak co najmniej dwie z podanych: Microsoft (egde), Google (Chrome), Mozilla (Firefox);

3.2.12. Umożliwiać integrację z innymi rozwiązaniami bezpieczeństwa używanymi u Zamawiającego tj.: system SIEM (Splunk), poprzez automatyczne raportowanie incydentów, NGFW (Fortigate) oraz system antyspam (Fortimail), celem zachowania automatyzacji środowiska Zamawiającego;

3.2.13. Musi posiadać własny klasyfikator, umożliwiający klasyfikację informacji, którą może prowadzić zarówno administrator i użytkownik systemu na stacji końcowej;

3.2.14. Umożliwiać integrację z systemami wspierającymi zarządzanie stacjami roboczymi (w szczególności Microsoft SCCM wykorzystywanym u Zamawiającego) w zakresie dystrybucji i zarządzania konfiguracją oprogramowania na końcówkach klienckich, a także posiadać instalatory w formatach msi lub exe (dmg/pkg); Zamawiający planuje dystrybucję oferowanego oprogramowania za pomocą oprogramowania Microsoft SCCM.

3.2.15. Stanowić jednolity produkt, najlepiej zarządzany pojedynczą konsolą zarządczą z dodatkową konsolą webową, działający bez konieczności używania zewnętrznych modułów administracyjnych firm trzecich, z wykorzystaniem oprogramowania zainstalowanego na serwerze;

3.2.16. Posiadać konsolę webową, która umożliwia przeglądanie informacji dotyczących bezpieczeństwa w oparciu o próby wycieku danych, operacji na plikach posiadających tag, plików pobieranych i wysyłanych za pośrednictwem protokołów sieciowych (TCP oraz UDP), zarówno w obrębie sieci LAN, jak i sieci WAN, plików wysyłanych drogą mailową, plików kopiowanych na dyski zewnętrzne, plików drukowanych. Konsola webowa

musi umożliwiać obserwację produktywności pracy użytkowników w oparciu o zdefiniowane przez administratora aplikacje oraz strony internetowe;

3.3. **Zarządzanie serwerem administracyjnym**

Serwer administracyjny musi:

3.3.1. Umożliwiać instalację na systemach Windows Server 2016 lub nowszych; Zamawiający dopuszcza pracę na systemach z rodziny GNU/Linux pod warunkiem, że oferowana dystrybucja posiada wsparcie producenta co najmniej do końca roku 2024 (dystrybucje LTS).

3.3.2. Współpracować z bazą danych MS SQL Server 2016 i nowszymi; Zamawiający dopuszcza wykorzystanie innych silników bazodanowych pod warunkiem, że posiadają one wsparcie producenta co najmniej do końca roku 2024.

3.3.3. Umożliwiać zarządzanie za pośrednictwem interfejsu graficznego (konsola);

3.3.4. Umożliwiać zarządzanie bazą danych poprzez określone zadania np.: wykonanie kopii bazy danych; usunięcie kopii bazy danych, usunięcie bazy danych, wprowadzenie ustawień dla kopii bazy danych. Zadania te powinny być dostępne z poziomu konsoli wraz z możliwością określenia automatycznego powtarzania zadań;

3.3.5. Posiadać funkcje automatycznej kopii bazy danych programu DLP w określonym przez administratora harmonogramie;

3.3.6. Posiadać możliwość zdefiniowania w programie przedziału czasowego dla kopii zapasowej bazy programu;

3.3.7. Komunikować się ze stacjami roboczymi wyłącznie za pomocą instalowanego na nich agenta;

3.3.8. Umożliwiać wykonanie instalacji/deinstalacji zdalnej klienta na stacjach roboczych;

3.3.9. Umożliwiać przygotowanie pliku instalacyjnego agenta za pośrednictwem konsoli zarządzającej.
Zamawiający dopuszcza sytuacje gdy producent oprogramowania będzie oferować pliki instalacyjne do dystrybucji poprzez SCCM;

3.3.10. Posiadać funkcjonalność aktualizacji własnych komponentów;

3.3.11. Mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych oraz aplikacji, z możliwością wyłączenia automatycznego pobierania;

3.3.12. Umożliwiać tworzenie nowych kont administratorów w konsoli programu, jak i ich usuwanie oraz klonowanie;

3.3.13. Posiadać możliwość automatycznej synchronizacji użytkowników oraz stacji roboczych z usługą Microsoft Active Directory;

3.3.14. Umożliwiać oznaczanie plików, które już znajdują się na stacjach roboczych i zasobach sieciowych;

3.3.15. Umożliwiać analizę lub oznaczanie nowo powstałych plików w oparciu o:

a) Aplikację, z której zostały utworzone.
b) Lokalizację lokalną oraz sieciową.
c) Adres URL, z którego został pobrany plik.
d) Format pliku,
e) Zawartość pliku,
f) Autora pliku opcjonalnie,
g) Datę utworzenia pliku opcjonalnie.

3.3.16. Serwer administracyjny musi mieć możliwość analizy lub oznaczania posiadanych plików wrażliwych w oparciu o:

a) Lokalizację lokalną oraz sieciową.
b) Format pliku.
h) Zawartość pliku,
i) Autora pliku opcjonalnie,
j) Datę utworzenia pliku opcjonalnie.

3.3.17. Oznaczanie plików, musi być dostępne dla wszystkich formatów plików oraz w oparciu o dowolną aplikacje;

3.3.18. Posiadać wbudowany serwer SMTP udostępniony przez producenta oprogramowania;

3.3.19. Umożliwiać określenie stref urządzeń pamięci masowej, drukarek fizycznych, sieciowych, lokalizacji sieciowych, adresów mailowych oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu. Strefy muszą posiadać możliwość dodania elementów ręcznie oraz elementów, które były podłączane do stacji roboczych;

3.3.20. Posiadać funkcjonalność konsoli webowej, która umożliwia przeglądanie informacji dotyczących bezpieczeństwa w oparciu o próby wycieku danych, operacji na plikach posiadających tag, plików wysyłanych do sieci, plików pobieranych z sieci, plików wysyłanych drogą mailową, plików kopiowanych na nośniki zewnętrzne;

3.4. **Zarządzanie konsolą webową**

Konsola webowa musi:

3.4.1. Umożliwiać obserwację produktywności pracy użytkowników w oparciu o zdefiniowane przez administratora aplikacje oraz strony internetowe;
3.4.2. Umożliwiać dodanie klucza licencji;
3.4.3. Umożliwiać konfigurację/zmianę domyślnego serwera SMTP;
3.4.4. Umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością deaktywacji tego oprogramowania oraz pobrania pakietu najnowszej wersji;
3.4.5. Umożliwiać generowanie raportów z danymi na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu;
3.4.6. Udostępniać konfigurowalny system paneli (ang. dashboard), operujący na różnych poziomach szczegółowości, z możliwością uwzględnienia różnych kanałów komunikacyjnych oraz możliwością wersjonowania (dostępu do danych historycznych panelu);

3.5. **Ochrona danych przesyłanych za pośrednictwem WWW**

Zamawiane oprogramowanie musi:

3.5.1. Umożliwiać monitorowanie i blokowanie treści naruszających zasady polityki w kanale WWW (http i https);
3.5.2. Umożliwiać, aby polityki chroniące informacje posiadały co najmniej możliwość konfiguracji:
   a) Poprzez użycie centralnych polityk zdefiniowanych dla innych kanałów komunikacji;
   b) W zależności od rodzaju użytkownika, także w oparciu o dane pochodzące ze zintegrowanego repozytorium użytkowników (np. jednostka organizacyjna, dział, grupa);
   c) W zależności od docelowych adresów IP, na których odbywa się komunikacja;
   d) W zależności od rodzaju przesyłanych plików i posiadanych przez pliki metadanych (np. tagów);
3.5.3. Umożliwiać przeglądanie aktywności użytkowników przeglądanych stron WWW i aplikacji internetowych;

3.6. **Agent stacji końcowych**

Zamawiane oprogramowanie musi:

3.6.1. Wspierać następujące systemy operacyjne:
   a) Microsoft Windows 8.1 (wersja x64)
   b) Microsoft Windows 10 (wersja x64)

c) Mac OS X 10.15.x i wyżej

3.6.2. Zapewniać ochronę i monitoring urządzenia końcowego bez względu na to, czy komputer jest podłączony do sieci czy nie;

3.6.3. Posiadać możliwość instalacji agenta na stacjach końcowych za pośrednictwem systemu SCCM;

3.6.4. Umożliwiać zabezpieczenie przed wyłączeniem/zawieszeniem lub dezinstalacją przez nieuprawnionego użytkownika.

3.6.5. Umożliwiać lokalne przechowywanie informacji w przypadku zerwania połączenia z serwerem zarządzającym, do czasu ponownego połączenia;

3.6.6. Umożliwiać wyświetlanie powiadomień (np. okno pop-up) dla użytkowników w języku polskim;

3.7. **Ochrona danych przesyłanych za pośrednictwem poczty e-mail**

Zamawiane oprogramowanie musi:

3.7.1. Umożliwiać identyfikację treści i załączników wiadomości mailowych m.in.: numery kart kredytowych, PESEL, określone ciągi znaków zdefiniowane przez administratora oraz umożliwiać powiadomienie o tym użytkownika;

3.7.2. Nadzorować wysyłane informacje kanałem poczty email (SMTP, POP3, IMAP oraz ich szyfrowane odpowiedniki)

3.7.3. Umożliwiać identyfikację oznaczonych plików w wiadomościach mailowych wysyłanych za pośrednictwem poczty mailowej;

3.7.4. Współpracować z klientem pocztowym MS Outlook;

3.7.5. Umożliwiać skanowanie plików poczty Microsoft zapisanych w formacie PST,

3.7.6. Umożliwiać dodawanie własnych nagłówków (X-HEADER) do wysyłanej poprzez klienta pocztowego wiadomości pocztowej.

3.8. **Monitorowanie bezpieczeństwa sieci Zamawiającego**

Zamawiane oprogramowanie musi:

3.8.1. Umożliwiać wykonywanie monitoringu sieciowego bez wywoływania dodatkowych opóźnień w transmisji danych, ani powodowania dodatkowych pojedynczych punktów awarii;

3.8.2. Analizować sieć co najmniej na poziomie rozróżniania protokołów sieciowych transmisji wraz z numerami portów TCP/IP, a ponadto ruch (z możliwością deszyfracji), odbywający się w kanale pocztowym email i kanale WWW, powinien być wykrywany za pomocą sygnatur (w tym monitorować załączniki poczty email oraz web-mail i inne usługi wykorzystujące np. protokół web - HTTP);

3.8.3. Umożliwiać monitorowanie ruchu przesyłanych plików np. poprzez FTP oraz p2p;

3.8.4. Umożliwiać monitoring usług na niestandardowych portach oraz zakresach portów.

3.8.5. Umożliwiać monitoring sklasyfikowanych i oznaczonych plików w sieci Zamawiającego oraz powiadamiać o próbach przesyłania tak oznaczonych plików dowolnym kanałem na zewnątrz firmy Zamawiającego;

3.9. **Wykrywanie wycieków danych**

Zamawiane oprogramowanie musi zapewniać:

3.9.1. Inspekcję zawartości plików i załączników,

3.9.2. Inspekcję plików skompresowanych (w tym spakowanych wielokrotnie),

3.9.3. Mechanizm wykrywania wycieku danych uwzględniający brak konieczności umieszczania wzorca danych na urządzeniu końcowym (stacji roboczej),

3.9.4. Możliwość konstrukcji polityk (tworzenia reguł wewnątrz polityk, ich edycji i przenoszenia pomiędzy politykami);

3.9.5. Możliwość wprowadzania szczególnych wyjątków w politykach, w których na podstawie dodatkowych kryteriów wykluczających dane podlegające zakazowi mogą być dystrybuowane;

3.9.6. Możliwość identyfikacji i wysyłania alarmów dla zdarzeń:

a) odmowy dostępu dla użytkownika do:
   I. lokalizacji sieciowych,
   II. stron internetowych,
   III. aplikacji,
   IV. pliku,
   V. folderu;
b) zablokowanie możliwości przenoszenia oraz kopiowania danych;
c) podłączenie nieznanych urządzeń;
d) zablokowanie podłączonego urządzenia;
e) podłączenie nowej drukarki;
f) przekroczenie dopuszczalnego limitu drukowanej liczby stron;
g) zablokowanie drukowania;
h) kopiowanie oznaczonego pliku na nośnik zewnętrzny (np. pamięć USB);

3.9.7. Możliwość wykrywania zdefiniowanych informacji na podstawie zawartości plików (np. dokumentacja finansowa, kod źródłowy, oprogramowanie), z uwzględnieniem możliwości tworzenia wzorców takich dokumentów;

3.9.8. Możliwość ochrony wzorcowych dokumentów zawierających wrażliwe dane, bez konieczności używania słów kluczowych;

3.9.9. Możliwość wykrywania, przy użyciu ww. mechanizmu, nieustrukturyzowanych danych rozmieszczonych w wielu miejscach organizacji (dane w ruchu), a także nowych i nigdy niewidzianych plików, spoza organizacji;

3.9.10. Możliwość tworzenia reguł opartych co najmniej o: słowa kluczowe i zdania kluczowe,

3.9.11. Możliwość tworzenia reguł na podstawie wyrażeń regularnych, także zgodnych z REGEXP,

3.9.12. Możliwość wykorzystania predefiniowanych lub umożliwienie tworzenia wzorców opisowych dla poszukiwanych informacji;

3.9.13. Możliwość walidacji wykrytych informacji (np. wyliczanie sum kontrolnych dla numeru PESEL) oraz definiowania walidacji;

3.9.14. Możliwość edycji dostarczonych wzorców opisowych, walidatorów oraz możliwość tworzenia nowych, także na ich podstawie;

3.9.15. Możliwość analizy zewnętrznych, zabezpieczonych szyfrowaniem lub hasłem plików (w tym po zmianie rozszerzenia pliku), w celu ich weryfikacji i ewentualnego wykonania akcji (np. blokady) jeśli zostaną ujęte w polityce DLP;

3.9.16. Umożliwiać integrację z systemami klasy SIEM w zakresie przesyłania definiowalnej informacji o zdarzeniach lub incydentach dotyczących wycieku informacji; Zamawiający posiada i wykorzystuje oprogramowanie Splunk ES.

3.10. **Reakcja na wyciek danych**

Zamawiane oprogramowanie musi zapewniać:

3.10.1. Możliwość wysyłania powiadomienia w formie wiadomości mailowych, których treść musi być modyfikowalna przez administratora i obsługiwać co najmniej język polski i angielski (z uwzględnieniem mechanizmu tworzenia szablonów treści tych maili);

3.10.2. Możliwość automatycznego poinformowania o wykrytym naruszeniu polityk, co najmniej nadawcy, jak i innych określonych osób (np. administratora),

3.10.3. Możliwość wyświetlenia komunikatu dla użytkownika naruszającego politykę (na jego stacji roboczej) oraz umożliwienie temu użytkownikowi podjęcia określonych akcji (np. dalszej wysyłki informacji lub tylko wyświetlenia zdefiniowanego komunikatu i wygenerowaniu alertu widocznego dla administratora);

3.10.4. Możliwość podejmowania automatycznych oraz semi-automatycznych (wymagających udziału uprawnionej osoby) akcji naprawczych w przypadku wykrycia naruszenia polityki – reakcje te muszą być uzależnione od typu polityki, kategorii i wagi incydentu, liczby podobnych zdarzeń, kanału komunikacji (protokołu komunikacji);

3.10.5. Możliwość zdefiniowania akcji (np. blokowania) w przypadku naruszenia więcej niż jednej polityki.

3.10.6. Możliwość zabezpieczenia kopii plików, naruszających politykę bezpieczeństwa w momencie wykrycia naruszenia, w celu zabezpieczenia i ochrony zgromadzonego materiału dowodowego incydentów;

3.11. **Obsługa zdarzeń wycieku danych**

Oprogramowanie musi zapewniać następujące funkcje:

3.11.1. Wizualizacja zdarzeń/incydentów musi być realizowana w sposób zrozumiały, przejrzysty i czytelny dla operatorów spoza działów IT i bezpieczeństwa informatycznego, a każdy element zdarzenia powinien być jasno opisany, ze szczególnym uwidocznieniem: kanału transmisji, powodu wygenerowania oraz elementów naruszających politykę;

3.11.2. Opis incydentu powinien zawierać informacje podstawowe, co najmniej: imię i nazwisko, datę i czas wystąpienia incydentu, podjętą czynność, rodzaj incydentu;

3.11.3. Grupy incydentów muszą być możliwe do wyeksportowania z poziomu konsoli operatora, w formie czytelnej i przejrzystej dla użytkowników spoza IT oraz zapisane w formacie pliku łatwym do obsługi dla tych użytkowników (np. PDF, HTML lub CSV)

3.11.4. Mechanizm manualnego wywoływania akcji dotyczącej danego zdarzenia/incydentu (np. zablokowania oznaczonych plików przed wysyłaniem);

3.11.5. Blokowanie oraz zezwalanie na zapisywanie, przenoszenie do innej lokalizacji w tym na dyski zaszyfrowane, zewnętrzne i sieciowe plików ujętych w polityce (również pliki oznaczonych);

3.11.6. Możliwość utworzenia białej oraz czarnej listy urządzeń przeznaczonych do zapisu (np. dyski, pamięci USB) i drukarek;

3.11.7. Blokowanie oraz zezwalanie na wysyłanie plików (w tym oznaczonych) za pośrednictwem klienta pocztowego, folderów synchronizacji z usługami chmury (np. Google Drive, One Drive, SharePoint);

3.11.8. Możliwość utworzenia białej oraz czarnej listy domen pocztowych i adresów mailowych;

3.11.9. Blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików (w tym oznaczonych) poprzez usługę pulpitu zdalnego;

3.11.10. Blokowanie oraz zezwalanie na wykonywanie zrzutów ekranów, kopiowania treści plików do schowka, nagrywania na płyty CD/DVD, SD/CF oraz drukowania wirtualnego plików;

3.11.11. Globalne zablokowanie oraz zezwolenie na korzystanie z określonych folderów lokalnych, dysków sieciowych, dysków o określonej literze oraz folderów synchronizacji z usługami chmury;

3.12. **Raportowanie i analityka**

Zamawiane oprogramowanie musi zapewniać:

3.12.1. Możliwość filtrowania przy użyciu różnych warunków, w tym zmiennych, atrybutów oraz możliwość ich wykorzystywania dla różnych filtrów;

3.12.2. Możliwość łatwego przechodzenia z raportu ogólnego do szczegółowych danych,

3.12.3. Możliwość wygenerowania raportu podsumowującego incydenty i trendy w rozbiciu na różne atrybuty, (także pobierane z repozytorium użytkowników), z możliwością ograniczenia zakresów czasowych;

3.12.4. Możliwość uproszczonego i zaawansowanego wyszukiwania incydentów z określonych grupy, w tym także przy użyciu określonych atrybutów;

3.12.5. Możliwość uzyskania raportów w czytelnych formatach, takich jak PDF oraz formatach do dalszego użytku,np. CSV lub XLS;

3.12.6. 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, podsumowania korzystania z urządzeń oraz ich typów;

3.12.7. Możliwość, generowania raportów w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu;

3.12.8. Automatyczne generowanie raportów, wysyłanych za pośrednictwem poczty mailowej;

3.12.9. Generowanie raportu z wykorzystaniem różnych opcji językowych (np. polski, angielski);

3.13. **Szczegółowe funkcjonalności w zakresie klasyfikacji dokumentów**

Zamawiane oprogramowanie musi:

3.13.1. Umożliwiać oznaczanie dokumentów w formie tagów lub metadanych, rozpoznawanych przez systemy informatyczne;

3.13.2. Umożliwiać definiowane własnych kategorii oraz polityk klasyfikacji wraz z możliwością tworzenia różnych klas i polityk klasyfikacji z możliwością ich przypisania do grup użytkowników, jednostkowych użytkowników i ról w systemie, także wynikających z repozytorium użytkowników (np. Active Directory);

3.13.3. Umożliwiać ustalanie zasad automatycznych zmian w klasyfikacji dokumentów;

3.13.4. Posiadać mechanizm automatycznego rozwiązywania konfliktów klasyfikacji i wykonywania definiowalnych akcji;

3.13.5. Zapewniać interaktywność mechanizmu klasyfikacji z użytkownikiem (np. notyfikacja lub żądanie świadomego potwierdzenia wykonania określonej czynności);

3.13.6. Posiadać scentralizowaną bazę logów, w tym logów audytowych, zawierających dane dotyczące czynności administratorów i operatorów oprogramowania, a także użytkowników, obejmujące dane o klasyfikacji informacji oraz o ewentualnych niezgodnościach;

3.13.7. Umożliwiać definiowanie własnego nazewnictwa dla poszczególnych kategorii dokumentów (np. dane poufne, dane tajne);

3.13.8. Umożliwiać integrację z oprogramowaniem MS Office oraz MS Office 365, które posłuży między innymi do wybrania kategorii dokumentu, w szczególności integrować się z oknem tworzenia/odczytu oraz oknem "Zapisz/Zapisz jako";

3.13.9. Zapewniać możliwości klasyfikacji plików z menu kontekstowego dla plików i katalogów (Domyślnie w systemie Windows: kliknięcie prawym przyciskiem myszki skutkuje wywołaniem menu kontekstowego);

3.13.10. Zapewnić wymuszenie klasyfikacji dokumentu przed jego wydrukowaniem lub inną formą udostępnienia;

3.13.11. Umożliwiać klasyfikację plików PDF (skany), archiwów, plików tekstowych, obrazów oraz dodawanie do dokumentów metadanych w postaci np. tagu;

3.13.12. Zapewniać automatyczną klasyfikację informacji bazującą na zawartości danych zgodnie z polityką firmy (np. poprzez użyte słowa kluczowe, wyrażenia regularne, format).

3.13.13. Zapewniać automatyczną klasyfikację informacji w oparciu o kontekst informacji (np. wybrany właściciel informacji lub autor, określony odbiorca

lub grupa użytkowników);

3.14. **Szczegółowe funkcjonalności w zakresie usługi szyfrowania plików i danych**

Zamawiane oprogramowanie musi:

3.14.1. Realizować szyfrowanie całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM;

3.14.2. Realizować szyfrowanie dysków zewnętrznych w oparciu o funkcjonalność BitLocker, szyfrowanie oraz autoryzowanie do zaszyfrowanych nośników wymiennych musi być w pełni niezauważalne dla użytkownika;

3.14.3. Umożliwiać szyfrowanie dokumentów w oparciu o polityki związane z klasyfikacją użytkownika lub automatyczną analizą treści, realizowane w sposób automatyczny,

3.14.4. Zapewniać możliwość przechowywania kluczy szyfrujących w infrastrukturze zamawiającego;

3.14.5. Posiadać możliwość wygenerowania hasła ratunkowego do odblokowania dostępu do zaszyfrowanych dysków oraz dysków wymiennych, w sytuacji jeżeli użytkownik zapomni hasła;

3.14.6. Zapewnić, aby szyfrowanie dokumentów działało poprawnie w systemach MS Windows 8.1, 10 oraz Mac OS X 10.15;

4. Szczegółowe funkcjonalności Mobile Device Management (MDM)

Oprogramowanie musi:

4.1. Zapewniać monitorowanie oraz blokowanie zagrożeń występujących na urządzeniach mobilnych (tablety, telefony z systemem IOS I Android);

4.2. Umożliwiać pełną kontrolę nad urządzeniem przenośnym oraz zdalne zablokowanie i wyczyszczenie urządzenia ze wszystkich danych;

4.3. Umożliwiać zdalny podgląd statusu urządzenia oraz sprawdzenie jego lokalizacji;

4.4. Automatycznie pobierać, kolekcjonować następujące dane identyfikacyjne urządzeń przenośnych:

4.4.1. Nazwa urządzenia

4.4.2. Model urządzenia

4.4.3. Producent urządzenia

4.4.4. Numer seryjny urządzenia

4.4.5. Numery ID (co najmniej):

4.4.6. Numer Telefonu, IMEI, IMSI (ICCID) numer wydrukowany na karcie SIM;

4.5. Automatycznie pobierać, kolekcjonować następujące dane eksploatacyjne urządzeń przenośnych:
   4.5.1. Numer wersji oprogramowania OS urządzenia
   4.5.2. Aktualna lista zainstalowanych na urządzeniu przenośnym aplikacji z uwzględnieniem wersji oraz rozmiaru.
   4.5.3. Wyświetlanie listy zainstalowanych profilów na urządzeniu przenośnym.
   4.5.4. Aktualne informacje na temat zajętości pamięci (wbudowanej, kart pamięci) oraz pojemności baterii urządzenia przenośnego;
   4.5.5. Informacje dotyczące przeprowadzanych napraw i usług serwisowych urządzeń (do wprowadzenia przez operatora w systemie);
4.6. Zapewniać pełną separację danych prywatnych od danych służbowych;
4.7. Umożliwiać zdalne instalowanie, jak i odinstalowywanie aplikacji na urządzeniach przenośnych;
4.8. Zapewniać wprowadzanie polityk poprzez konsolę zarządzającą lub web panel;

5. Zakres wsparcia technicznego i serwisu dla zakupionego oprogramowania:

5.1. Zakres wsparcia producenta, w terminie obowiązywania umowy, obejmuje:
   5.1.1. Dostęp do pomocy technicznej w dni robocze w godzinach 8.00-16.00, przez okres trwania umowy;
   5.1.2. Usługę konsultacji w zakresie konfiguracji, optymalizacji i innych czynności dotyczących zamawianego oprogramowania w ilości 120 roboczogodzin (ang. man-day), zgodnie z zapotrzebowaniem Zamawiającego, możliwych do wykorzystania w terminie obowiązywania umowy.
   5.1.3. Dostęp do poprawek i nowych wersji oprogramowania i/lub systemu;
   5.1.4. Dostęp do dokumentacji technicznej;
   5.1.5. Dostęp do konta wsparcia oprogramowania, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta.