Załącznik nr 3 do Zapytania ofertowego

System ochrony przeciw wyciekom poufnych danych

(ang. DLP – Data Loss Protection)

Opis Przedmiotu Zamówienia

I. Przedmiot zamówienia

Przedmiotem zamówienia jest:

A) Dostawa 100 licencji oprogramowania, z co najmniej 24-miesięcznym wsparciem technicznym producenta, zapewniającego ochronę przed wyciekiem poufnych danych (ang. Data Leak Prevention - DLP) obejmujących:
   a. ochronę stacji końcowych użytkowników Zamawiającego,
   b. ochronę danych przesyłanych za pośrednictwem kanału komunikacyjnego WWW,
   c. ochronę danych przesyłanych za pośrednictwem kanału komunikacyjnego poczty email Zamawiającego,
   d. monitorowanie bezpieczeństwa sieci Zamawiającego,
   e. monitorowanie i ochronę zasobów plikowych Zamawiającego,
   f. wielopoziomową klasyfikację dokumentów,
   g. usługę szyfrowania plików i danych.

   Dostawa licencji, suportu i oprogramowania, może nastąpić nie później niż 3 dni robocze od dnia zawarcia umowy.

   Wsparcie zamawianego oprogramowania musi być świadczone bezpośrednio przez producenta i umożliwiać dostęp do:

   a. bazy wiedzy dot. zamawianego oprogramowania,
   b. najnowszych wersji oraz update („łatek") zamawianego oprogramowania,
   c. informacji o błędach i zagrożeniach dot. zamawianego oprogramowania,
   d. pełnej dokumentacji zamawianego oprogramowania

B) Wdrożenie zamawianego oprogramowania, wykonane w ciągu 20 dni roboczych, zrealizowane do 30 dnia roboczego po dniu zawarciu umowy

C) Szkolenie z zakresu administracji zamawianego oprogramowania oraz obsługi biznesowej, trwające 2 dni robocze, zrealizowane nie wcześniej niż po zakończeniu wdrożenia oprogramowania i nie później niż do 40 dnia roboczego od dnia zawarcia umowy.

D) Świadczenie konsultacji z zakresu konfiguracji, optymalizacji i innych czynności dotyczących zamawianego oprogramowania w ilości 8 roboczo-dni (ang. man-day), zgodnie

z zapotrzebowaniem Zamawiającego, realizowanych po skutecznym wdrożeniu nie później niż 6 miesięcy od daty zawarcia umowy.

II. Szczegółowy opis przedmiotu zamówienia

Oprogramowanie, będące przedmiotem zamówienie musi spełniać wszystkie poniższe wymagania.

A) Ogólne wymagania dotyczące ochrony przed wyciekiem danych, dotyczące wszystkich kanałów komunikacji i wszystkich mechanizmów wykrywania wycieku informacji.

Zamawiane oprogramowanie musi:

A.1. umożliwiać definiowanie polityki ochrony przed wyciekiem, która może być realizowana jednocześnie we wszystkich podlegających ochronie kanałach komunikacyjnych (np. ta sama polityka może obsługiwać stację końcową, pocztę e-mail, kanał WWW oraz sieć Zamawiającego), poprzez pojedynczy punkt konfiguracji (centralny dashboard),

A.2. umożliwiać definiowanie określonych akcji następujących w przypadku wykrycia zagrożenia wycieku danych, w zależności od kanału komunikacyjnego, którego zagrożenie dotyczy,

A.3. zapewniać, aby zasady tworzenie 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 sieciowe), dane użytkownika końcowego jak, lokalizacji stacji końcowej oraz stacji roboczej użytkownika,

A.4. umożliwiać nadawanie określonych poziomów ważności zdarzeń dotyczących wycieku danych, w oparciu o:

a. ilość powtarzających się zdarzeń dotyczących wycieku danych
b. określone grupy nadawców i/lub odbiorców (z uwzględnieniem struktury danych zawartych w repozytorium użytkowników np. dział , departament)
c. zdefiniowane kanały komunikacyjne (protokoły sieciowe)
d. wybranych rodzajach dokumentów (meta danych)
e. rodzaju zawartości

(Rozwiązanie musi wspierać możliwość uwzględnienia wystąpienia co najmniej kilku powyższych zasad jednocześnie),

A.5. wspierać co najmniej uwierzytelnianie użytkowników w modelu użytkownik, grupa, rola (ang. model RBAC) oraz integracje z repozytorium danych Microsoft Active Directory, z uwzględnieniem możliwości wykorzystania struktury danych w nim zawartych (np. departamenty, działy, grupy, lokalizacje),

A.6. umożliwiać wykorzystanie informacji zawartych w zintegrowanym repozytorium użytkowników (np. departament, działy, grupy użytkowników, lokalizacja) do uwzględniania lub wykluczania w politykach, w klasyfikacji ważności zdarzeń,

A.7. wspierać mechanizmy pojedynczego źródła tożsamości (ang. SSO) oraz uwierzytelnienia za pomocą certyfikatów X.509 oraz zaimportowanie użytkowników wraz z atrybutami z plików CSV oraz usług katalogowych (ang. LDAP),

A.8. umożliwiać stosowanie gotowych algorytmów detekcji (działających tam gdzie to możliwe o mechanizm sum kontrolnych), co najmniej takich informacji jak numery identyfikacyjne PESEL, REGON i NIP, numer rachunku bankowego, numer karty kredytowej,

A.9. pozwalać na łatwe przenoszenia ustawień pomiędzy środowiskami testowymi i produkcyjnymi, na przykład poprzez zastosowanie mechanizmu importowania i eksportowania z zamawianego rozwiązania, plików zawierających dane,

A.10. wspierać rozwiązania zapewniające wysoką dostępność (ang. HA), poprzez zastosowanie zasad rozkładania ruchu (ang. Load balancing) oraz możliwość tworzenia klastrów niezawodnościowych obejmujące wszystkie elementy systemu,

A.11. współpracować z takimi bazami danych(posiadający i przy wykorzystaniu mechanizmów relacyjności tych baz), które przechowują wszystkie dane niezbędne do działania oprogramowania, z uwzględnieniem dodatkowych zabezpieczeń dla danych dotyczących incydentów (określone uprawnienia dostępu oraz szyfrowanie informacji), a licencja tej bazy danych musi być dostarczona razem z systemem.

A.12. umożliwiać zarządzanie ilością i retencją przechowywanych danych, obejmując dane całego systemu jak i dane dotyczące pojedynczych zdarzeń (w tym incydentów),

A.13. zapewniać, w przypadku konieczności użycia do prawidłowego działania zamawianego oprogramowania, oprogramowania firm trzecich (np. serwery Windows, Linux), wówczas wymagane oprogramowanie oraz licencje muszą zostać dostarczone razem z zamawianym oprogramowaniem.

A.14. zapewniać taką 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),

A.15. umożliwiać integrację z innymi rozwiązaniami bezpieczeństwa takimi jak wiodące: systemy zarządzania urządzeniami mobilnymi (and. MDM), systemy SIEM oraz systemy obsługi zgłoszeń (ang. Ticket Tracker),

A.16. umożliwiać, aby wszystkie komponenty systemu mogły być zainstalowane w komercyjnych chmurach IT, w co najmniej takich jak AZURE i GOOGLE w modelu IaaS i PaaS oraz wspierały możliwość instalacji w środowiskach wirtualnych takich jak co najmniej VMWARE i HYPER-V, a także w środowisku serwerów fizycznych,

A.17. wspierać integrację z zewnętrznymi mechanizmami klasyfikacji informacji, takimi jak co najmniej zintegrowane mechanizmy ochrony Microsoft, z uwzględnieniem mechanizmów klasyfikacji i ochrony danych chmury IT: AZURE i GOOGLE lub posiadać alternatywny własny klasyfikator dający możliwość integracji z produktami Microsoft takimi jak produkty MS Office,

A.18. umożliwiać wykrywanie zdarzeń dotyczących wycieku danych co najmniej w chmurze AZURE i GOOGLE poprzez własny mechanizm bezpieczeństwa (np. sondę lub brokera)

B) Ochrona danych przesyłanych za pośrednictwem WWW

Zamawiane oprogramowanie musi:

B.1. umożliwiać blokowanie treść naruszającą zasady polityki w kanale WWW (http i https),
B.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 który odbywa się komunikacja,
B.3. zapewniać możliwość integracji zamawianego oprogramowania z dowolnym rodzajem Web-Proxy obsługującego protokół ICAP,
B.4. umożliwiać, aby w przypadku wykrycia naruszenia polityki w kanale WWW, istniała możliwość usunięcia tej treści z wiadomości albo akcji HTTP POST (np. wysłanie niedozwolonego załącznika przez niezaufaną pocztę web),
B.5. umożliwiać analizę danych przesyłanych w kanale HTTPS przy wykorzystaniu mechanizmu integracji z Web-Proxy,
B.6. umożliwiać usunięcia wrażliwej treść w przypadku aplikacji Web2.0

C) Ochrona stacji końcowych

Zamawiane programowanie musi:

C.1. wspierać następujące systemy operacyjne:
  a. Windows 7 (wersja x32 i x64)
  b. Windows 8 i 8.1 (wersja x64)

c. Windows 10 (wersja x64)
d. Mac OS X 10.10.x oraz 10.11.x

(Zamawiający dopuszcza różnice w realizacji zamawianych funkcjonalności pomiędzy systemami wyprodukowanymi przez Apple lub Microsoft),

C.2. zapewniać ochronę urządzenia końcowego bez względu na to, czy komputer jest podłączony do sieci czy nie,
C.3. zapewniać aby zainstalowane mechanizmy ochrony nie utrudniały pracy użytkownikom z wolniejszym łączem , ani nie powodowały przeciążenia urządzenia n, na którym użytkownicy pracują,
C.4. reagować na wszelkie próby wysyłania niedozwolonych danych z i na stacje roboczą, także w przypadku gdy urządzenie to nie jest podłączone do sieci korporacyjnej.
C.5. nadzorować wysyłane informacje kanałem: poczty email, WWW (HTTP/HTTPS), kanałem (S)FTP, a także informacje pochodzące z operacji kopiowania danych z komputera na udział sieciowy i odwrotnie, przy wykorzystaniu wbudowanych mechanizmów MS Windows, jak i oprogramowania firm trzecich (np. Bluetooth, ssh, (s)FTP, komunikatorami – Skype, Webex, LiveMeeting),
C.6. umożliwiać blokowanie użycia i wysyłki danych podlegających ochronie przez dowolną aplikację,
C.7. monitorować i uniemożliwiać kopiowanie danych na przenośne urządzenia, w tym nośniki danych podłączane do interfejsu USB, napędy optyczne CD/DVD, SD/CF, urządzenia podłączone do portów eSATA, umożliwiając jednocześnie kopiowanie informacji tylko na zaakceptowane ww. urządzenia przenośne i tylko w postaci zaszyfrowanej przy użyciu mechanizmów zamawianego oprogramowania, zaszyfrowane informacje mogą być odszyfrowane tylko przez osobę szyfrującą oraz inne upoważnione osoby,
C.8. zapewniać monitoring i ewentualne blokowanie prób drukowania bądź faksowania zabezpieczonych danych,
C.9. nadzorować i ewentualne blokować próby wykonywania zrzutów ekranowych (ang. print-screen) oraz zapisywania do pamięci podręcznej (ang. copy-paste) ochranianych informacji,
C.10. dopuszczać stosowanie różnych polityk dla różnych urządzeń końcowych i różnych użytkowników orz grup użytkowników, w tym działać wg. zasady per użytkownik czyli móc obsługiwać w inny sposób, różnych użytkowników zalogowanych na tej samej stacji roboczej,
C.11. .informować użytkownika zalogowanego na stacji roboczej, poprzez mechanizm notyfikacji, obejmując dane o wykrytym nadużyciu wraz możliwość interaktywnego z użytkownikiem wycofania akcji blokującej (np. rezygnacji z określonego działania) przy jednoczesnym odnotowaniu tego faktu w dzienniku zdarzeń wraz z odpowiednią akcją (np. wygenerowanie incydentu),
C.12. umożliwiać implementację automatycznej akcji w przypadku wykrycia naruszenia polityki ze szczególnym uwzględnieniem możliwości wymuszenia szyfrowania przy kopiowaniu danych poufnych na zewnętrzne nośniki danych (np. ang. pendrive),
C.13. monitorować przepływ danych w kanale RDP wraz z wywoływaniem określonych akcji, zgodnie z przyjętymi politykami, w zależności od rodzaju przesyłanych treści,

C.14. posiadać lokalne (agenty) mechanizmy skanowania systemów plików urządzeń końcowych, z możliwością wykorzystania zmiennych systemowych wykorzystywanych do ustalania warunków skanowania i wykluczeń, a wszystkie operacje wykonywane w ramach zamawianego systemu w części dotyczącej stacji roboczej muszą być wykonywane przez pojedynczego agenta,

C.15. umożliwiać współpracę z oprogramowaniem antywirusowym/antymalware firm trzecich, w tym co najmniej z oprogramowaniem BitDefender

C.16. umożliwiać aby lokalne oprogramowanie instalowane na stacji roboczej posiadało możliwość ograniczenia obciążenia procesora, zapewniało zajętość na poziomie nie większym niż 500MB przestrzeni dyskowej i nie powodowało zbytniego obciążenia pamięci operacyjnej stacji roboczej oraz być dostosowane do działania zarówno w środowisku fizycznym jak i środowisku zdalnym (ang. VDI), komunikacja lokalnego oprogramowania z urządzeniami centralnymi muszą być szyfrowana,

C.17. umożliwiać wykrywanie zdarzeń/incydentów lokalnie na stacji roboczej użytkownika przy jednoczesnym braku konieczności lokalnego przechowywania wzorców do wykrywania naruszeń na tej stacji, a rozpoczęte procesy skanowania muszą być wykonywane nawet po odłączeniu komputera od sieci korporacyjnej,

C.18. zapewniać, aby zdefiniowane centralnie polityki bezpieczeństwa mogły poza stacją roboczą obejmować inne kanały komunikacji,

C.19. zapewniać w systemie centralne raportowanie postępów skanowania,

C.20. zapewniać tymczasową blokadę plików (tzw. kwarantannę), które wywołały naruszenie polityki podczas procesu lokalnego skanowania.

C.21. umożliwiać instalację agenta na stacji roboczej użytkownika za pomocą rozwiązania GPO w sposób nie wymagający interakcji z użytkownikiem.

C.22. umożliwiać zarządzania oprogramowaniem zainstalowanym na stacji roboczej użytkownika, w sposób bezpośredni z konsoli zarządczej rozwiązania, w tym posiadać możliwość co najmniej restartu, zatrzymania, pobrania logów, przegląd zdarzeń oraz podgląd statusu oraz zmianę konfiguracji tego oprogramowania(agenta),

C.23. umożliwiać automatyczne wykrywanie nowych stacji roboczych i automatycznej instalacji oprogramowania (agenta), w uzależnieniu od rodzaju urządzeń końcowych i zainstalowanego oprogramowania oraz z uwzględnieniem parametrów urządzenia i użytkownika w repozytorium użytkowników, a oprogramowanie musi wspierać co najmniej język polski i angielski,

C.24. umożliwiać podłączenia agenta do serwera w środowiskach otwartych, w tym poprzez sieć Internet, w takim wypadku komunikacja musi być zabezpieczona TLS z użyciem dwukierunkowego uwierzytelnienia klient-serwer,

C.25. umożliwiać zabezpieczenie oprogramowania lokalnego (agenta) przed wyłączeniem i restartem przez użytkownika oraz hasłem przed jego odinstalowaniem, a wykorzystywane przez niego zasoby musza być prze niego chronione.

D) Ochrona danych przesyłanych za pośrednictwem poczty e-mail

Zamawiane oprogramowanie musi:

D.1. umożliwiać blokowanie wiadomości, po wykryciu naruszenia polityki,

D.2. zapewniać tymczasową blokadę wiadomości zawierającej informacje (tzw. kwarantannę), które wywołały naruszenie polityki podczas procesu lokalnego skanowania,
D.3. umożliwiać automatyczne przesyłanie wiadomości do kwarantanny,
D.4. wspierać środowiska używające do komunikacji mechanizmy szyfrowania kanału komunikacji (np. TLS, SSL),
D.5. umożliwiać analizę wiadomości pocztowych email przesyłanych w formie zaszyfrowanej oraz załączników przesłanych w formie spakowanej (w tym wielokrotnie),
D.6. obsługiwać balansowanie ruchu serwera pocztowego, odpowiedzialnego za dystrybucje poczty (ang. MTA) zarówno dla ruchu wchodzącego jak i wychodzącego oraz zapewnienie działania w trybie wysokiej dostępności,
D.7. wspierać mechanizmy klasyfikacji poziomu poufności wiadomości
D.8. umożliwiać integrację z każdą infrastrukturą pocztową Zamawiającego w co najmniej następujących trybach:
   a. jako dodatkowy serwer pocztowy, który bierze udział w komunikacji jako kolejny host pośredniczący w stosunku do serwera pocztowego Zamawiającego,
   b. jako moduł pośredniczący, gdzie serwer pocztowy Zamawiającego przekazuje wiadomość do analizy zamawianemu oprogramowaniu, a następnie odbiera tę wiadomość zweryfikowaną w celu docelowej dystrybucji,

E) Monitorowanie bezpieczeństwa sieci Zamawiającego

Zamawiane oprogramowanie musi:

E.1. umożliwiać wykonywanie monitoringu sieciowego bez wywoływania dodatkowych opóźnień w transmisji danych, ani powodować dodatkowych pojedynczych punktów awarii.
E.2. analizować sieć co najmniej na poziomie rozróżniania protokołów sieciowych transmisji wraz z numerami portów TCP, a ponadto ruch (z możliwością deszyfracji), odbywający się w kanałach pocztowym email i kanale WWW, powinien być wykrywany za pomocą sygnatur (w tym monitorować załączniki poczty email oraz web-mail i inne usługi wykorzystujące protokół web - HTTP)
E.3. umożliwiać analizę ruchu sieciowego odbywającego się z prędkością 1 gigabit per urządzenie monitorujące a w przypadku przekroczenia swojej wydajności, powinien notyfikować o ilości ruchu nieprzetworzonego,
E.4. umożliwiać monitorowanie ruchu FTP, także poprzez porównanie transferu danych z transferem kontrolnym,
E.5. umożliwiać, w przypadku wiadomości email ich kolejkowanie, do czasu weryfikacji,
E.6. umożliwiać monitoring usług na niestandardowych portach oraz zakresach portów.

F) Posiada następujące, szczegółowe funkcjonalności:

F.1. **Wykrywanie wycieków danych**

Zamawiane oprogramowanie musi zapewniać:

a. inspekcję zawartości plików i załączników,
b. inspekcję plików skompresowanych (w tym spakowanych wielokrotnie),
c. mechanizm wykrywania wrażliwych informacji na podstawie zawartości tabeli w bazie danych w ramach utworzonych wcześniej w tej bazie wzorców danych,
d. mechanizm wykrywania wycieku danych uwzględniający brak konieczności umieszczania wzorca danych na urządzeniu końcowym (stacji roboczej),
e. możliwość wyszukiwania poufnych informacji na podstawie bazy danych o wielkości co najmniej kilku mln rekordów, na podstawie analizy porównawczej treść badanej informacji z zawartością bazy danych, uwzględniając przy tym co najmniej informacje zapisane w języku polskim.
f. możliwość wyboru kolumn w bazie danych, stanowiących wzorzec do poszukiwań, a zmiana zestawu kolumn nie może wymagać reindeksacji tej bazy danych,
g. możliwość tworzenie wzorców i wykrywanie informacji dla kolumn bazy danych zawierających dane zagregowane np. „<Imię> + <Drugie Imię> + <Nazwisko>",
h. możliwość elastycznej konstrukcji polityk dla skomplikowanych wzorców tworzonych z wielu kolumn bazy danych z uwzględnieniem kwantyfikatorów (np. każdy z , którykolwiek, żaden),
i. możliwość wprowadzania szczególnych wyjątków w politykach, w których na podstawie dodatkowych kryteriów wykluczających dane podlegające zakazowi mogą być dystrybuowane, dotyczy także wykluczeń na podstawie wzorców dokumentów,
j. możliwość, aby wszystkie dane wprowadzane do bazy wzorców muszą podlegać procesowi normalizacji danych (np. identyfikator NIP powinien być przechowany w jednakowej formie bez znaków ‘minus’),
k. możliwość definiowania „odległości” (np. ilości znaków) pomiędzy wystąpieniami poszczególnych elementów wzorca,
l. możliwość tworzenia zanonimizowanego wzorca na podstawie bazy danych zamawianego systemu przy jednoczesnym zachowaniu struktury i rodzaju danych wzorcowych, w celu prowadzenia prac testowych i konfiguracyjnych bez konieczności użycia danych realnych,
m. możliwość wykrywania wrażliwych informacji na podstawie zawartości plików (np. dokumentacja finansowa, kod źródłowy, oprogramowanie), z uwzględnieniem możliwości tworzenia wzorców takich dokumentów,
n. możliwość ochrony co najmniej kilku tysięcy wzorcowych dokumentów zawierających wrażliwe dane (takie jak kod źródłowy, dokumenty finansowe, informacje patentowe) bez konieczności używania słów kluczowych czy wzorców,
o. możliwość wykrywania zawartości lub fragmentu zawartości wzorcowych dokumentów w sposób rekurencyjny (np. dokument pdf w dokumencie doc), także wykonywane na urządzeniu końcowym,
p. możliwość, co najmniej na potrzeby „strojenia” zamawianego systemu informacje, dotyczące nawet pojedynczej polityki, w zakresie procentowego podobieństwa analizowanej informacji do wzorcowego dokumentu (np.

poprzez określenie, jaki procent analizowanego dokumentu pasuje do dokumentu wzorcowego),

q. możliwe do zaprezentowania, mechanizmy uczenia maszynowego w celu wykrywania podobnych do małej próbki dokumentów wzorcowych,
r. możliwość wykrywania, przy użyciu ww. mechanizmu uczenia maszynowego poufne, nieustrukturyzowane szybkozmienne dane rozmieszczone w wielu miejscach organizacji, a także nowe i nigdy niewidziane dokumenty,
s. możliwość tworzenia reguł opartych co najmniej o: słowa kluczowe i zdania kluczowe,
t. możliwość tworzenia reguł na podstawie wyrażeń regularnych, także zgodnych z REGEX,
u. możliwość wykorzystania predefiniowanych lub umożliwiać tworzenie wzorców opisowych dla poszukiwanych informacji np. opisujących numer karty kredytowej, nr konta bankowego,
v. możliwość walidacji wykrytych informacji (np. wyliczanie sum kontrolnych - PESEL).
w. wzorce oraz walidatory co najmniej dla nr PESEL, Nr Dowodu Osobistego, REGON, NIP, numeru bankowego, numeru konta.
x. możliwość edycji dostarczonych wzorców opisowych, walidatorów oraz możliwość tworzenia nowych, także na ich podstawie,
y. możliwość analizy zaszyfrowanych plików (w tym po zmianie rozszerzenia).
z. możliwość rozpoznawania typu pliku po przeanalizowaniu próbki plików tego samego typu,
aa. możliwość weryfikacji treści plików graficznych (np. formularze) przy użyciu metody optycznego rozpoznawania znaków (ang. OCR), którego moment uruchamiania jest konfigurowalny lub uruchamianie następuje po sprawdzeniu innymi mechanizmami weryfikacji.
bb. możliwość rozpoznawania obrazu w taki sposób, aby rozpoznawać cechy charakterystyczne dokumentów (rozróżnić dokument wypełniony od niewypełnionego)

F.2. **Reakcja na wyciek danych:**

Zamawiane oprogramowanie musi zapewniać:

a. możliwość wysyłania powiadomienia w formie wiadomości Email, których treść musi być modyfikowalna i obsługiwać wiele języków (z uwzględnieniem mechanizmu tworzenia szablonów treści tych email),
b. możliwość automatycznego poinformowania o wykrytym naruszeniu polityk, co najmniej nadawcy jak i innych określonych osób (np. przełożonego nadawcy),
c. na stacjach roboczych mechanizm interakcji z użytkownikiem zapewniający także możliwość wyświetlenia komunikatu dla użytkownika naruszającego politykę oraz dawać możliwość temu użytkownikowi podjęcia określonych akcji (np. dalszej wysyłki informacji, tylko wyświetlenia zdefiniowanego komunikatu) oraz dawać możliwość wprowadzenia komentarza przez użytkownika, które następnie będzie zarejestrowane dla osoby przeglądającej rejestr zdarzeń/incydentów,

d. możliwość wyświetlanie notyfikacji co najmniej w języku polskim i angielskim oraz umożliwiać ich modyfikowanie,
e. możliwość podejmowania automatycznych oraz semi-automatycznych (wymagających udziału uprawnionej osoby) akcji naprawczych w przypadku wykrycia naruszenia polityki, a reakcje te muszą być uzależniona od typu polityki, kategorii i wagi incydentu, ilości wystąpienia podobnych zdarzeń, kanału komunikacji (protokołu komunikacji), lokalizacji urządzenia końcowego oraz od określonego punktu kontroli.
f. możliwość zdefiniowania akcji w przypadku naruszenia w tym wielu wykluczających się polityk.

F.3. **Obsługa zdarzeń wycieku danych**

Oprogramowanie musi zapewniać następujące funkcje:

a. wizualizacja zdarzeń/incydentów musi być realizowana s w sposób zrozumiały, przejrzysty i czytelny dla operatorów spoza działów IT, a każdy element zdarzenia powinien być jasno opisany, powinien być szczególnie uwidoczniony: kanał transmisji oraz powód wygenerowania, a także elementy, które naruszają politykę,
b. opis incydentu powinien zawierać informacje podstawowe takie jak co najmniej: Imię i Nazwisko, Kierownik/przełożony, Zespół/Dział i Lokalizacja.
c. interfejs obsługi zdarzeń/incydentów musi umożliwiać także podgląd treści oryginalnego źródła informacji (np. pliku załącznika, zawartość email), bezpośrednio z miejsca obsługi danego incydentu,
d. zapewnienie mechanizmu dającego możliwość definiowania wielu właścicieli informacji oraz umożliwiać powiązanie danego właściciela z incydentem lub grupą incydentów oraz możliwość grupowania na podstawie dodatkowych atrybutów w tym także pobieranych z repozytorium użytkowników,
e. zapewnienie, aby grupy incydentów muszą być eksportowane 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)
f. zapewnienie mechanizm manualnego wywoływania akcji dotyczącej danego zdarzenia/incydentu (np. akcje zapobiegające wyciekowi danych, akcje naprawcze)
g. zapewnienie dostępu do incydentów i/lub grup incydentów z uwzględnieniem uprawnień wynikających z repozytorium użytkowników oraz uprawnień przypisanych do poszczególnych polityk bezpieczeństwa, z uwzględnieniem możliwości nadania takich uprawnień, które wykluczają możliwość podglądu oryginalnej treści/informacji, które spowodowała naruszenie polityki
h. zapewnienie możliwość takiego dostępu do danych incydentu, aby nie były widoczne danych osobowe.
i. spełnienie zasady rozdzielności ról, polegającej zapewnieniu możliwość rozdziału ról uprzywilejowanych takich jak np. administrator systemu, administrator użytkowników, operator incydentów

j. umożliwienie wycofanie prawa dostępu do dokumentu w dowolnym momencie – nawet jeżeli dokument znajdzie się poza infrastrukturą IT Zamawiającego oraz zapewniać możliwość wymazywanie kopii danych, które próbowali odczytać nieautoryzowani użytkownicy.

F.4. **Raportowanie i analityka**

Zamawiane oprogramowanie musi zapewniać:

a. możliwość filtrowania przy użyciu różnych warunków, w tym zmiennych oraz atrybutów oraz możliwość ich wykorzystywania dla różnych ról,
b. możliwość zagnieżdżania raportów w raportach, polegająca na łatwym przechodzeniu z raportu ogólnego do szczegółowych danych,
c. możliwość wygenerowania raportu podsumowującego incydenty i trendy w rozbiciu na różne atrybuty, także pobierane z repozytorium użytkowników (np. departament, jednostkę organizacyjną, grupę), z możliwością ograniczenia zakresów czasowych.
d. możliwość uproszczonego i zaawansowanego wyszukiwania incydentów z określonych grupy, w tym także przy użyciu określonych atrybutów.
e. możliwość uzyskania raportów w czytelnych formatach takich jak HTML czy PDF jak i formatach do dalszego użytku takich jak na przykład plik Excel, XML,
f. możliwość integracji oprogramowania z systemami raportowymi (udostępniania danych) za pośrednictwem własnego API ,
g. możliwość automatycznej dystrybucji określonych raportów do zdefiniowanych użytkowników i operatorów oraz manualnego wysłania raportu z interfejsu zarządczego systemu,
h. konfigurowalny system paneli (ang. dashboard), operujący na różnych poziomach szczegółowości, z możliwością uwzględnienia różnych kanałów komunikacyjnych oraz możliwością wersjonowania (dostępu do danych historycznych panelu),
i. możliwość przypisanie właściwego właściciela danych do incydentu lub grupy incydentów oraz dystrybucja tego raportu do tego właściciela.

G) Szczegółowe funkcjonalności w zakresie monitorowania i ochrony zasobów plikowych Zamawiającego

Zamawiane oprogramowanie musi:

G.1. umożliwiać skanowanie
a. udziałów sieciowych, w tym co najmniej systemów Linux i Windows,
b. systemów plików Windows i Linux bez konieczności używania udziałów sieciowych,
c. zawartości bazy danych za pomocą ODBC/JDBC,
d. zasobów sharepoint oraz standardowych serwerów HTTP (ang. HTTP crawling),

e. pliki poczty Microsoft zapisane w formacie PST,
f. plików zabezpieczone poprzez RMS lun AZURE RMS i inne metody zabezpieczenia/szyfrowania przy założeniu dostępności klucza deszyfrującego.

G.2. pozwalać na integrację oprogramowaniem firm trzecich przez API zamawianego oprogramowania ,
G.3. umożliwiać zabezpieczenie kopii plików, naruszających politykę bezpieczeństwa w momencie wykrycia naruszenia.
G.4. zapewniać automatyczną lub ręczną, tymczasową blokadę plików zawierających informacje (tzw. kwarantannę), które wywołały naruszenie polityki już w momencie wykrycia tego naruszenia, wraz z powiadomieniem użytkownika – właściciela tego pliku, a mechanizm ten powinien także obejmować zasoby sharepoint,
G.5. umożliwiać automatyczne zaszyfrowanie oraz ustawienie reguł DRM dla pliku naruszającego politykę,
G.6. zapewniać automatycznego lub manualne ręcznego wykonania dowolnej akcji implementującej szyfrowanie, tymczasową blokadę (kwarantannę), bądź inną czynność dla pliku zawierającego dane chronione,
G.7. gromadzić informacje o oryginalnej lokalizacji pliku, włączając dodatkowo co najmniej informacje o prawach dostępu, właściwościach, właścicielu tego pliku, w tym zawsze posiadać możliwość identyfikacji właściciela tego pliku,
G.8. gromadzić informacje o użytkownikach, którzy korzystali z pliku, wraz z informacjami historycznymi, w tym uwzględniać możliwość wykonywania określonych akcji w przypadku znacznych odchyleń statystyk używania tych plików,
G.9. udostępniać raport, uwzgledniający listę, zasobów w kolejności ryzyka wycieku informacji,
G.10. umożliwiać szybkie uzyskanie informacji, czy plik dokonujący naruszenia, nie został wykryty wcześniej i wypadku takiego zdarzenia – udostępnić poprzednie incydenty,
G.11. zapewniać, że atrybut „ostatniego odczytu" skanowanego pliku nie zostanie zmieniony,
G.12. zapewniać możliwość ręcznego uruchomienia skanowania oraz uruchomienie skanowania zgodnie z zaplanowanym cyklem,
G.13. umożliwiać automatyczne zatrzymanie procesów skanowania w określonych przedziałach czasowych oraz zarządzać zajmowana przepustowością sieci w przypadku zasobów sieciowych, a także umożliwiać uruchomienie wielu procesów skanowania równolegle,
G.14. umożliwiać uaktualnianie informacji o wcześniejszych incydentach w przypadku zmiany w zakresie których te incydenty dotyczą (np. usunięcie pliku chronionego naruszającego politykę),
G.15. umożliwiać skanowanie zasobów w oddalonych lokalizacjach, dysponujących wolniejszymi łączami teleinformatycznymi,

H) Szczegółowe funkcjonalności w zakresie klasyfikacji dokumentów

Zamawiane oprogramowanie musi:

H.1. umożliwiać oznaczanie dokumentów zarówno w formie wizualnej (widoczne dla użytkownika np. nagłówki, stopki, znaki wodne), a także w formie tagów lub metadanych, rozpoznawanych przez systemy informatyczne,

H.2. umożliwiać, aby komunikaty oprogramowania w stosunku do użytkownika mogły być wydawane co najmniej w języku polskim i angielskim (w zależności od wersji językowej systemu użytkownika),

H.3. stanowić jednolity produkt, najlepiej zarządzane pojedynczą konsolą zarządczą, działającym bez konieczności używania zewnętrznych modułów administracyjnych firm trzecich (np. Konsoli administracyjnej rozwiązań DLP, Konsol administracyjnych RMS, Azure RMS), jednak mechanizm klasyfikacji powinien współdziałać z mechanizmem klasyfikacji informacji RMS/Azure RMS.

H.4. umożliwiać definiowane własnych kategorii oraz polityk klasyfikacji wraz z możliwością tworzenia różnych klas i polityk klasyfikacji z możliwością ich przypisania do grup użytkowników, użytkowników i ról w systemie, także wynikających z repozytorium użytkowników (np. Active Directory), nazwy klas muszą być definiowalne przez użytkowników,

H.5. umożliwiać ustalanie zasad automatycznych zmian w klasyfikacji dokumentów,

H.6. posiadać mechanizm automatycznego rozwiązywania konfliktów klasyfikacji i wykonywania definiowalnych akcji (np. blokowanie wysyłki wiadomości poczty e-mail, w przypadku, gdy załącznik został sklasyfikowany wyższą lub niższą klauzulą, niż sama wiadomość).

H.7. zapewniać interaktywność mechanizmu klasyfikacji z użytkownikiem (np. dezaktywacja przycisku „wyślij” w programie pocztowym w przypadku próby wysyłki plików niedozwolonych do wysyłki lub poprzez stosowne notyfikacje lub żądanie świadomego potwierdzenia wysłania)

H.8. 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,

H.9. umożliwiać definiowanie własnej kolorystyki dla poszczególnych kategorii dokumentów (kolorystyka oznaczeń wizualnych) oraz dla wiadomości e-mail.

H.10. umożliwiać integrację z oprogramowaniem MS Office oraz MS Outlook, które posłuży między innymi do wybrania kategorii dokumentu lub wiadomości e-mail, w szczególności integrować się z oknem tworzenia/odczytu wiadomości oraz oknem "Zapisz/Zapisz jako" oraz w zakresie dotyczącym (A)RMS,

H.11. zapewniać możliwości klasyfikacji plików z menu kontekstowego dla plików i katalogów, dostępną po kliknięciu prawym przyciskiem manipulatora (myszki),

H.12. zapewnić wymuszenie klasyfikację dokumentu przed jego wydrukowaniem lub inną formą udostępnienia,

H.13. wspierać oprogramowanie MS Office, od wersji 2010 wzwyż, w tym wersji Outlook 2016, z uwzględnieniem oprogramowania pracującego w trybie Office 365.

H.14. umożliwiać klasyfikację plików PDF (skany), archiwów, plików tekstowych, obrazów oraz dodawanie znaku wodnego lub logo do dokumentów,

H.15. zapewniać automatyczną klasyfikację informacji bazującą na zawartości danych zgodnie z polityką firmy (np. poprzez użyte słowa kluczowe, wyrażenia, wyrażenia regularne, format).

H.16. zapewniać automatyczną klasyfikację informacji w oparciu o kontekst informacji (np. wybrany właściciel informacji lub autor, określony odbiorca lub grupa użytkowników).
H.17. umożliwiać integrację z systemami klasy SIEM w zakresie przesyłania definiowalnej informacji o zdarzeniach lub incydentach dotyczących wycieku informacji,
H.18. umożliwiać integrację z systemami wspierającymi zarządzanie końcówkami klienckimi (w szczególności Microsoft SCCM) w zakresie dystrybucji i zarządzania konfiguracją oprogramowania na końcówkach klienckich, a także posiadać instalatory w formatach msi lub exe,
H.19. umożliwiać integrację z systemem Microsoft RMS oraz Azure RMS, a integracja musi obejmować zarówno zarządzanie szablonami uprawnień RMS jak również dostępami do nich powiązanymi z określonymi kategoriami klasyfikacji.

I) Szczegółowe funkcjonalności w zakresie usługi szyfrowania plików i danych

Zamawiane oprogramowanie musi:

I.1. szyfrowanie realizowane w oprogramowaniu musi być wykonywane algorytmami nie gorszymi niż AES 256 oraz RSA 4096 lub innym o nie gorszym poziomie bezpieczeństwa,
I.2. umożliwiać szyfrowanie dokumentów w oparciu o polityki związane z klasyfikacją użytkownika lub automatyczną analizą treści realizowane w sposób automatyczny,
I.3. umożliwiać szyfrowanie wiadomości e-mail poprzez plug-in w MS Outlook,
I.4. zapewnić możliwość przechowywania kluczy szyfrujący w infrastrukturze zamawiającego,
I.5. zapewnić, aby szyfrowanie dokumentów działało poprawnie w systemach MS Windows 7, 8, 8.1, 10, Mac OS X 10.10, 10.11, 10.12 oraz Mac OS X iOS 9.x oraz 10.x.

J) Dostawa i uruchomienie dostarczanego oprogramowania w środowisku Zamawiającego

Dostawa zamawianego oprogramowania obejmuje:

J.1. Dostarczenie w ciągu 3 dni roboczych od daty zawarcia umowy, kompletu licencji oraz oprogramowania umożliwiających użytkowanie rozwiązania, zgodnie z wymogami funkcjonalnymi. Przez dostarczenie oprogramowania Zamawiający uznaje także przekazanie linków do oprogramowania dających możliwość jego pobrania ze strony producenta przez czas nie krótszy niż okres wsparcia.

J.2. Wdrożenie trwające 20 dni roboczych, zakończone podpisaniem protokołu odbioru, nie później, niż do 30 dnia roboczego po zawarciu umowy, zamawianego oprogramowania obejmującego co najmniej instalację następujących elementów oprogramowania:

a. zapewniającego ochronę kanału EMAIL,
b. zapewniającego ochronę systemów plików,
c. zapewniającego ochronę kanału WWW,
d. zapewniającego klasyfikację, szyfrowanie i ochronę informacji,

e. zapewniającego monitorowanie bezpieczeństwa sieci,
f. zapewniającego ochronę stacji roboczej użytkownika,
g. zapewniającego ochronę nośników przenośnych,
h. zapewniającego obsługę (zgłaszanie i reakcje) incydentów dotyczących DLP,

oraz

i. dostarczenie dokumentacji powdrożeniowej.

wraz ze szkoleniem trwającym 2 dni robocze, z zakresu administracji zamawianego oprogramowania oraz obsługi, zakończone otrzymaniem przez uczestników certyfikatu uczestnictwa. Szkolenia musi być wykonane nie wcześniej niż po zakończeniu wdrożenia oprogramowania i nie później niż do 40 dnia od zawarcia umowy. Szkolenie powinno:

a. obejmować zakres niezbędny do skutecznego administrowania zamawianym systemem (szkolenie dla administratorów),
b. obejmować zakres niezbędny do obsługi biznesowej zamawianego systemu np. obsługi zdarzeń (zgłaszanie i reakcja), obsługi systemu raportowego,
c. być przeprowadzone w czasie nie dłuższym niż 2 dni robocze

J.3. Świadczenie konsultacji z zakresu konfiguracji, optymalizacji i innych czynności dotyczących zamawianego oprogramowania w ilości 8 roboczo-dni (ang. man-day), zgodnie z rzeczywistym zapotrzebowaniem Zamawiającego, realizowanych po skutecznym wdrożeniu nie później niż do 6 miesięcy od daty zawarcia umowy.

Dostawca zapewni przydzielenie następujących osób do realizacji przedmiotu zamówienia:

a. przynajmniej jednego certyfikowanego inżyniera posiadającego certyfikaty producenta oferowanego rozwiązania potwierdzające jego wiedzę z zakresu wdrażania i administracji oferowanymi rozwiązaniami.

b. opcjonalnie, przynajmniej jedną osobę, która ma wiedzę i doświadczenie w obszarze zarządzania bezpieczeństwem informacji potwierdzoną certyfikatami: certyfikatem znajomości normy ISO 27001 oraz certyfikatami: Certified Information Systems Security Professional (CISSP) lub Cerified Information Security Auditor (CISA) oraz opcjonalnie, dodatkowo punktowany: Cerified Information Security Manager (CISM).