Załącznik nr 2 do SIWZ

# SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja oprogramowania służącego do ochrony przed wyciekiem danych wskutek ich kradzieży lub niezamierzonych (nieświadomych) działań użytkowników. Dane te mogą zawierać informacje, które podlegają ochronie z powodów biznesowych (tajemnica przedsiębiorstwa) lub prawnych (osobowe, dane wrażliwe, finansowe, itp.).
W skład oprogramowania będącego przedmiotem zamówienia muszą wchodzić następujące moduły:

- Moduł Data Loss Prevention (zwany dalej DLP).
- Moduł Kontroli Urządzeń (zwany dalej KU).
- Moduł szyfrowania dysków dla systemu Windows (zwany dalej SD).
- Moduł Szyfrowania Plików i Folderów (zwany dalej SP).
- Centralna Konsola Zarządzania (zwana dalej CKZ).

**Wymagania ogólne:**

1. Dostarczone rozwiązanie powinno być skalowalne i musi być w stanie zarządzać infrastrukturą złożoną z minimum 350 stacji końcowych.
2. Wszystkie komponenty instalowane na stacji roboczej powinny pochodzić od jednego producenta i być zarządzane przez pojedynczą Centralną Konsolę Zarządzania. Centralna Konsola Zarządzania powinna być dostępna jako oprogramowanie instalowane w środowisku wirtualnym Zamawiającego zbudowanym w oparciu o VMware vSphere 6.5.
3. Wszystkimi komponentami po stronie stacji roboczej powinien zarządzać jeden agent, którego zadaniem będzie przekazywanie polityk z CKZ do stacji roboczych oraz przekazywanie zdarzeń z komponentów zarządzanych do CKZ.

**Wymagania szczegółowe dla systemu będącego przedmiotem zamówienia:**

1. Wszystkie moduły powinny pracować na stacjach klienckich z następującymi systemami operacyjnymi:
   a. Windows 10 (wersja x32 i x64).
   b. Mac OS X 10.10.x, 10.11.x, 10.12.x oraz 10.13.x.
2. Moduł KU oraz moduł DLP powinien pracować na następujących systemach serwerowych:
   a. Windows 2012 / 2012 R2 oraz nowszych.
3. W przypadku systemów Mac OS oraz Windows Server - Zamawiający dopuszcza pewne różnice we wspieranych funkcjonalnościach w stosunku do systemów Windows.
4. Instalacja systemu będącego przedmiotem zamówienia (co najmniej agenta zarządzającego) powinna być możliwa poprzez instalację ręczną oraz instalację automatyczną z użyciem CKZ lub zewnętrznego oprogramowania do zdalnej instalacji wymagającego plików MSI.
5. Oprogramowanie powinno umożliwić prace w środowiskach całkowicie izolowanych, gdzie nie ma dostępu do Internetu. Powinna istnieć możliwość ręcznej aktualizacji wszystkich komponentów z użyciem CKZ.
6. Graficzny interfejs wszystkich komponentów powinien być dostępny co najmniej w języku angielskim oraz polskim. Powinna istnieć możliwość automatycznego wyboru języka, wyświetlana w zależności od języka klienckiego systemu operacyjnego.
7. W ramach modułów systemu będącego przedmiotem zamówienia powinny być obecne mechanizmy samoobrony przed próbami zatrzymania lub wyłączenia ochrony poprzez te moduły. Powinny być

zaimplementowane mechanizmy zapobiegające modyfikacjom zarówno struktury plików, procesów jak i rejestrów niezbędnych do pracy ww. systemu.

**Wymagania dotyczące modułu ochrony przed wyciekiem danych (DLP)**

**KLASYFIKACJA**

1. Moduł powinien być odpowiedzialny za odpowiednią klasyfikację plików oraz wymuszanie ochrony zaklasyfikowanych plików poprzez wspierane kanały wycieku danych.
2. Moduł DLP powinien przeprowadzać klasyfikację plików na następujące sposoby:
   a. Klasyfikacja w oparciu o etykiety.
   b. Klasyfikacja w oparciu o typ/zawartość pliku.
   c. Klasyfikacja ręczna dokonana przez użytkownika.

3. Klasyfikacja w oparciu o etykiety powinna być nadawana ręcznie lub automatycznie. Powinny być dostępne co najmniej następujące mechanizmy nadawania etykiet:
   a. Automatyczne nadawanie etykiet w zależności od udziału sieciowego, z którego dany plik został skopiowany na stację roboczą.
   b. Automatyczne nadawanie etykiet w zależności od aplikacji, która wytworzyła dany plik na danej stacji roboczej.
   c. Automatyczne nadawanie etykiet w oparciu o aplikację webową z której został wygenerowany (ściągnięty) dany plik.
   d. Ręczne nadawanie etykiet przed administratora systemu lub udziału sieciowego.

4. Klasyfikacja w oparciu o etykiety powinna mieć mechanizm chroniący przed zgubieniem etykiet w wyniku wykonania manipulacji związanych z plikiem.
   a. Klasyfikacja takiego pliku nie może się zmieniać (w szczególności być gubiona) w przypadku, co najmniej zmiany nazwy pliku, zmiany formatu/typu pliku.
   b. W przypadku skopiowania fragmentu tak sklasyfikowanego pliku do innego dokumentu, nowy dokument musi dziedziczyć taką samą klasyfikację jak plik oryginalny. W przypadku późniejszego usunięcia tego fragmentu, który przyczynił się do nadania klasyfikacji – klasyfikacja powinna być też usunięta.
   c. W przypadku manualnego przepisania odpowiednio długiego fragmentu pliku do innego dokumentu (bez użycia schowka).

5. Nadanie etykiety w ramach klasyfikacji opartej o etykiety nie może modyfikować zawartości pliku. Uruchomienie funkcji skrótu (jak MD5, SHA1, SHA-256) na pliku przed klasyfikacją i po klasyfikacji powinna dać taki sam wynik.

6. Klasyfikacja w oparciu o typ/zawartość pliku powinna być nadawana w oparciu o następujące parametry:
   a. Słowa kluczowe występujące w pliku. Powinna być możliwość zdefiniowania ile słów kluczowych musi wystąpić by uznać plik za sklasyfikowany. Powinny być dostępne słowniki predefiniowane oraz możliwość tworzenia własnych.
   b. Wykrycie fraz w pliku zgodnie ze zdefiniowanym wyrażeniem regularnym. Powinny być predefiniowane wyrażenia wyszukujące co najmniej PESEL, NIP, REGON oraz powinna istnieć możliwość definicji własnych wyrażeń regularnych.
   c. Podobieństwo do innych, wcześniej zeskanowanych dokumentów. Jeśli dokument zawiera część tekstu zbieżną z wcześniej zeskanowanym repozytorium - dokument powinien być automatycznie klasyfikowany (tzw. fingerprinting).

d. Rodzaj pliku poprzez zbadanie faktycznej zawartości pliku niezależnie od rozszerzenia, jakim opatrzony jest dany plik.
e. Rozszerzenie pliku niezależnie od zawartości pliku.
f. Atrybuty pliku jeśli jest to dokument pakietu Microsoft Office lub PDF jak co najmniej Autor, Firma, Słowa Kluczowe czy Komentarz.

7. Klasyfikacja danych w oparciu o typ/zawartość powinna być wykonywana dynamicznie przez moduł DLP na stacjach w momencie dostępu do pliku, bez konieczności wykonywania okresowego, masowego znakowania danych.

8. Klasyfikacja ręczna powinna być nadawana przez użytkownika systemu na pliki pakietu Microsoft Office, pliki PDF oraz wysyłaną pocztę w następujących sytuacjach:

   a. Użytkownik zapisuje plik na dysku.
   b. Użytkownik próbuje wysłać email poza organizację.
   c. Użytkownik wybierze odpowiednią opcję w programach pakietu Microsoft Office.

9. Klasyfikacja ręczna dokonana przez użytkownika powinna w momencie wysyłania email dodać stosowny nagłówek i stopkę w treści maila informujące o poziomie klasyfikacji danego emaila.
10. Nazwy etykiet klasyfikacji danych, zarówno dotyczących klasyfikacji w oparciu o typ/zawartość jak i klasyfikacji w oparciu o etykiety powinny być konfigurowalne przez administratora.

**OCHRONA PRZED WYCIEKIEM**

1. System powinien chronić dane przed wyciekiem za pomocą następujących kanałów danych:
   a. Ochrona przed wyciekiem przez wydruk.
      i. Definiowanie ograniczeń w drukowaniu wskazanych dokumentów sklasyfikowanych, w tym możliwość wskazania, który dokument może być drukowany na której drukarce lokalnej lub sieciowej.
      ii. Monitorowanie, blokowanie drukowania danych na wskazanych drukarkach lokalnych i sieciowych oraz raportowanie takiego zdarzenia obejmujące minimum: nazwę drukarki, nazwę użytkownika, proces, który wysłał dokument do drukowania, IP adres komputera użytkownika, czas zdarzenia oraz zawartość drukowanego pliku.
   b. Ochrona przed wyciekiem do sieci WEB.
      i. Definiowanie ograniczeń przy wysyłaniu plików sklasyfikowanych z użyciem przeglądarek webowych do Internetu, w tym możliwość wskazania, na jakie adresy powinna być możliwa wysyłka a na jakie nie.
      ii. Monitorowanie, blokowanie wysyłania plików oraz raportowanie takiego zdarzenia obejmującego minimum adres URL, nazwę procesu przeglądarki internetowej oraz zawartość wysyłanego pliku.
      iii. Powinny być wspierane co najmniej przeglądarki: Internet Explorer, Edge, Firefox oraz Chrome.
      iv. Blokowanie powinno być również wspierane dla połączeń szyfrowanych przy czym nie dopuszcza się deszyfracji ruchu pomiędzy przeglądarką internetową a serwerem docelowym.
   c. Ochrona przed wyciekiem przez EMAIL.
      i. Definiowanie ograniczeń przy wysyłaniu plików sklasyfikowanych z użyciem klientów pocztowych Microsoft Outlook. Możliwość uzależnienia ochrony od domen adresów email lub konkretnych adresów email.

ii. Monitorowanie, blokowanie wysyłania plików oraz raportowanie takiego zdarzenia obejmującego minimum docelowy adres email, proces klienta pocztowego oraz zawartość plików sklasyfikowanych załączonych do wiadomości.
iii. Etykiety klasyfikacji plików dołączanych do email powinny być przekazywane przez email poprzez nadawanie nagłówków do wiadomości lub w inny, podobny sposób tak, by w momencie zapisywania plików na innej stacji roboczej odpowiednia klasyfikacja była automatycznie nadawana.
iv. Klasyfikacja powinna odbywać się po naciśnięciu przycisku „wyślij", jednak przed faktyczną próbą wysłania wiadomości. Po blokadzie wysyłki edytowana wiadomość powinna pozostać otwarta.

d. Ochrona przed generowaniem zrzutów ekranów.
i. Definiowanie ograniczeń przy generowaniu zrzutów ekranu, jeśli wyświetlony na nim jest plik sklasyfikowany.
ii. Monitorowanie, blokowanie realizacji funkcji zrzutu ekranu oraz raportowanie takiego zdarzenia obejmującego minimum aplikację wyświetlającą sklasyfikowaną treść podczas próby zrealizowania zrzutu ekranu oraz sam zrzut ekranu w postaci pliku graficznego.
iii. Powinny istnieć wbudowane definicje programów używanych do zrzutów ekranu i powinna istnieć możliwość dodania własnych definicji. W momencie uruchomienia programu z listy możliwość robienia zrzutów ekranu nie powinna być możliwa.

e. Ochrona przed skopiowaniem plików na zewnętrzne nośniki danych.
i. Definiowanie ograniczeń przy kopiowaniu sklasyfikowanych plików na zewnętrzne dyski oraz kopiowania danych z nośników wymiennych na stacje roboczą.
ii. Monitorowanie, blokowanie kopiowania oraz raportowanie takiego zdarzenia obejmującego minimum nazwę pliku kopiowanego, numer seryjny nośnika zewnętrznego oraz zawartość kopiowanych plików.

f. Ochrona przed użyciem schowka systemowego.
i. Definiowanie ograniczeń przy kopiowaniu fragmentów dokumentu poprzez schowek systemowy do innych dokumentów.
ii. Funkcja schowka powinna działać w obrębie tego samego dokumentu bez żadnych przeszkód.
iii. Monitorowanie, blokowanie kopiowania treści oraz raportowanie takiego zdarzenia obejmującego minimum nazwę aplikacji źródłowej i docelowej oraz treść schowka.

g. Ochrona przed wysyłką danych poprzez sieć.
i. Definiowanie ograniczeń przy dostępnie do sieci dla aplikacji, która wykonuje operacje plikowe na sklasyfikowanych plikach.
ii. W momencie wykrycia operacji na plikach sklasyfikowanych aplikacja powinna zostać pozbawiona dostępu do sieci, działanie powinno zostać monitorowane oraz zaraportowane w zakresie minimum nazwy procesu, źródłowego adresu IP, docelowego adresu IP, portu źródłowego, portu docelowego oraz kierunku ruchu.

2. Dostępność różnych rodzajów reakcji modułu DLP na wykryte naruszenia polityki ochrony:
a. Blokowanie akcji (np. blokada wysyłki email ze sklasyfikowanymi załącznikami).
b. Monitorowania akcji (wysłanie incydentu do CKZ).
c. Powiadomienie użytkownika (wyświetlenie użytkownikowi informacji, że podjęta akcja została zablokowana/jest monitorowana przez moduł DLP).
d. Zapytanie użytkownika o podanie powodów wykonywania akcji – powód wpisany przez użytkownika musi być zachowany w CKZ.

e. Automatyczne szyfrowanie chronionych plików podczas ich przesyłania do katalogów sieciowych lub na dysk zewnętrzny USB - przy czym administrator systemu ma możliwość wskazania jaki klucz zostanie użyty do szyfrowania i jakie osoby/grupy użytkowników mają prawo dostępu do klucza i zaszyfrowanych danych.
f. Zachowanie dowodów w postaci skopiowania danych, które spowodowały podjęcie akcji przez moduł DLP we wskazanym udziale sieciowym (w tym też obrazy wykonanych zrzutów z ekranu). Dane kopiowane na udział muszą być szyfrowane, a dostęp do nich możliwy tylko z konsoli systemu zarządzania.

3. System powinien dawać możliwość aplikowania różnych reakcji w zależności od tego, czy system znajduje się w sieci korporacyjnej czy poza nią (w szczególności stanowiska mobilne). Badanie obecności w sieci korporacyjnej powinno odbywać się poprzez badanie otwartości dowolnie wybranego portu na dowolnie wybranym serwerze.
4. Moduł DLP musi umożliwiać natywne, okresowe przeszukiwanie dysków twardych na stacjach roboczych pod kątem występowania tam plików niesklasyfikowanych, a spełniających wymogi do sklasyfikowania. W razie wykrycia takiego pliku powinno być możliwe wykonanie akcji:
   a. Przesłanie powiadomienia do serwera zarządzającego.
   b. Przydzielenie do pliku polityki RM (Rights Management).
   c. Przydzielenie do pliku etykiety klasyfikacji.
   d. Przeniesienie pliku do lokalnej kwarantanny.
      i. Plik w kwarantannie musi być chroniony przed niepowołanym dostępem przez jego zaszyfrowanie.
      ii. Musi być możliwe odzyskanie pliku z kwarantanny przez użytkownika po potwierdzeniu tego przez administratora systemu DLP (proces challenge – response). Przy czym wykonanie odzyskania pliku z kwarantanny nie może wymagać podłączenia stacji do sieci firmowej.
   e. Automatyczne szyfrowanie plików przy czym administrator systemu ma możliwość wskazania jaki klucz zostanie użyty do szyfrowania i jakie osoby/grupy użytkowników mają prawo dostępu do klucza i zaszyfrowanych danych.

5. Musi istnieć możliwość definiowania harmonogramu skanowania okresowego w celu przeszukiwania dysków twardych.

**ZADZĄDZANIE INCYDENTAMI**

1. System musi znakować czasowo wszystkie zdarzenia napływające do serwera CKZ.
2. Wszystkie incydenty związane z naruszeniem danych powinny mieć nadany priorytet w co najmniej pięciostopniowej skali tak, by możliwe było odróżnienie incydentów bardziej istotnych od mniej istotnych.
3. Powinna istnieć możliwość automatycznego przydzielania incydentów do konkretnego właściciela lub grupy właścicieli oraz informowania przez email nowych właścicieli incydentów.
4. Każdy incydent powinien posiadać odpowiedni status – co najmniej „nowy”, „przejrzany”, „eskalowany”, „rozwiązany” oraz „fałszywy alarm”. System powinien dawać możliwość tworzenia nowych statusów o własnych nazwach.
5. Powinna istnieć możliwość anonimizacji niektórych danych, które jednoznacznie identyfikują użytkownika dla wybranych grup użytkowników. W szczególności powinno być możliwe stworzenie sposobu zarządzania incydentami, gdzie pierwsza linia wsparcia nie ma dostępu do szczegółowych danych incydentu oraz załączonych dowodów a druga linia wsparcia już taki dostęp posiada.

6. Moduł DLP musi współpracować z systemami RM (rights management), co najmniej Microsoft RMS oraz Seclore FileSecure (IRM).
   a. Moduł DLP musi umożliwiać sprawdzenie, czy plik posiada przydzieloną politykę RM, a jeśli nie, zablokować jego wysłanie na zewnątrz.
   b. Moduł DLP musi umożliwiać automatyczne przydzielenie określonej polityki RM do plików podlegających ochronie znajdujących się na dysku stacji użytkownika

**INNE WYMAGANIA**

**1.** System DLP po stronie klienta powinien posiadać polski interfejs użytkownika. Cała komunikacja z użytkownikiem powinna być prowadzona w języku polskim.
**2.** System powinien wymuszać politykę DLP nawet w sytuacji, gdy zostanie uruchomiony w trybie awaryjnym (tzw. Safe Mode).
**3.** System DLP powinien umożliwiać czasowe wyłączenie ochrony na stacji klienckiej poprzez mechanizm challange-response. Wyłączenie funkcjonalności powinno być terminowe – na zadany okres czasu od 5 min do 30 dni.
**4.** System powinien współpracować z sieciowym DLP tego samego producenta. Powinien istnieć pojedynczy punkt konfiguracji hostowego oraz sieciowego systemu DLP.

**Wymagania dotyczące modułu Kontroli Urządzeń (KU)**

**1.** Moduł KU musi zapewnić ochronę przed podłączaniem niepożądanych urządzeń do stacji klienckich i powinien być zarządzany przez CKZ.
**2.** Musi istnieć możliwość skonfigurowania modułu tak, aby jego praca była niewidoczna dla użytkownika (tryb ukryty).
**3.** Musi istnieć możliwość podania w języku polskim treści informacji o powodzie podjęcia akcji przez moduł KU, która jest wyświetlana użytkownikowi.
**4.** Moduł musi mieć możliwość: logowania zdarzenia, powiadomienia użytkownika poprzez monit w języku polskim, zablokowania zdarzenia oraz kopiowania przedmiotu akcji (jeśli istnieje) w celach dowodowych na wskazany udział sieciowy (CIFS).
**5.** Moduł KU musi wykrywać i blokować urządzenia podłączane przez porty zewnętrzne komputera (wliczając w to: USB, Serial, Fire-Wire, Bluetooth), takie jak pendrive, PDA, kamera cyfrowa, odtwarzacze MP3, drukarki i inne typy urządzeń oraz umożliwiać zmianę sposobu dostępu do urządzeń posiadających system plików (pendrive USB, CD/DVD) na tryb „tylko do odczytu”.
**6.** Rozwiązanie musi przechowywać informacje o nazwie urządzenia, czasie przyłączenia, typie urządzania, kodzie producenta i urządzenia, nr seryjnym i typie systemu plików (zależnie od typu urządzenia i jego zestawu parametrów).
**7.** System powinien umożliwić blokowanie dowolnego urządzenia oraz tworzyć definicje, gdzie blokowane będą wszystkie urządzenia danego typu oprócz wyjątków dodanych przez administratora (na przykład: blokuj wszystkie lokalne drukarki oprócz drukarek o podanych numerach seryjnych)
**8.** Konfiguracja polityki działania modułu musi umożliwiać zdefiniowanie dopuszczonych do użytkowania nośników danych USB na podstawie ich numeru seryjnego, ID producenta i ID produktu.
**9.** Polityka działania modułu może być różna (np. bardziej restrykcyjna), jeśli stacja działa poza wewnętrzną, firmową siecią Zamawiającego. Badanie obecności w sieci korporacyjnej powinno odbywać się poprzez badanie otwartości dowolnie wybranego portu na dowolnie wybranym serwerze.
**10.** Polityka działania modułu musi umożliwiać przypisanie różnych polityk zależnie od przynależności użytkownika do grup użytkowników synchronizowanych z Active Directory.

11. Polityka działania modułu ma umożliwiać zdefiniowanie zawartości plików (na podstawie słów kluczowych oraz wyrażeń regularnych), której wykrycie spowodowuje zablokowanie zapisu pliku na nośnik zewnętrzny, nawet, jeśli został on dopuszczony do użytkowania. W ramach reakcji na incydent powinna istnieć możliwość zapisania pliku wraz z incydentem, którego dotyczyło zablokowane, kopiowanie.
12. System powinien pozwalać nadać każdemu z incydentów właściciela, a każdy administrator powinien mieć ściśle zdefiniowane uprawnienia w ramach separacji obowiązków.
13. System KU powinien umożliwiać czasowe wyłączenie ochrony na stacji klienckiej poprzez mechanizm challange-response. Wyłączenie funkcjonalności powinno być terminowe - na zadany okres czasu od 5 min do 30 dni.

**Wymagania dotyczące modułu szyfrowania dysków dla systemu Windows (moduł SD)**

1. Rozwiązanie musi zapewnić szyfrowanie danych na poziomie dysku w sposób transparentny dla systemu operacyjnego i użytkownika, z funkcjonalnością uwierzytelniania użytkownika bezpośrednio po uruchomieniu komputera (przed wystartowaniem właściwego systemu operacyjnego - tzw. pre-boot authentication, zwany dalej PBA).
2. System szyfrowania musi zapewniać centralne zarządzanie poprzez CKZ, w oparciu o centralną bazę danych, gdzie przetrzymywane są informacje o użytkownikach, kluczach i politykach szyfrowania niezbędne do uzyskania dostępu do danych zaszyfrowanych na stacji w sytuacji awaryjnej.
3. Oprogramowanie szyfrujące na stacjach użytkowników musi komunikować się z CKZ w bezpieczny sposób (transmisja szyfrowana z obustronną autentykacją) z wykorzystaniem protokołów opartych na TCP/IP, które umożliwiają połączenie przez sieci routowane.
4. Musi istnieć możliwość określenia czy szyfrowaniu mają podlegać wszystkie partycje dysku, czy tylko partycja bootowalna (z której startuje właściwy system operacyjny) czy tylko partycje „niebootowalne". Musi też istnieć możliwość określenie dowolnej konfiguracji partycji do zaszyfrowania.
5. Rozwiązanie musi obsługiwać co najmniej algorytm AES 256 jako algorytm szyfrowania danych. Rozwiązanie musi samodzielnie wykrywać czy procesor chronionego komputera obsługuje sprzętowe wsparcie szyfrowania (Intel AES-NI) i automatycznie wykorzystywać tę funkcjonalność podczas szyfrowania/deszyfrowania danych.
6. Uwierzytelnianie użytkownika w PBA ma być możliwa z wykorzystaniem hasła i nazwy użytkownika, ale także z użyciem kart inteligentnych różnych producentów oraz biometrii.
7. System powinien pozwalać na użycie modułu TPM 2.0 w celu uniknięcia potrzeby ręcznego wpisywania hasła przez użytkowników.
8. Musi być zapewniona obsługa uwierzytelniania użytkowników w trybie PBA z wykorzystaniem systemu PKI (kart inteligentnych przechowujących certyfikaty użytkowników). Wymagana jest obsługa co najmniej Microsoft PKI.
9. System powinien pobierać użytkowników z AD oraz dać możliwość ręcznej definicji użytkowników niezależnie od AD. System musi umożliwiać wskazanie, który użytkownik i grupa mają prawo używać komputer i uzyskać dostęp do zaszyfrowanych danych.
   a. System musi umożliwiać przypisanie co najmniej 2000 użytkowników (użytkowników lub grup z AD obejmujących w sumie 2000 użytkowników) do jednego komputera.
   b. Użytkownicy i grupy użytkowników przypisywani do komputerów muszą być synchronizowani z domeny Microsoft AD.
   c. Usunięcie użytkownika w serwerze usług katalogowych AD powinno skutkować automatycznym usunięciem lub zablokowaniem użytkownika w serwerze zarządzającym systemem szyfrowania.

**d.** System musi umożliwiać automatyczne dodanie do listy uprawnionych użytkowników, użytkowników z domeny AD, którzy wcześniej korzystali z komputera (logowali się do niego).

**10.** Zmiany hasła użytkownika na jednej maszynie muszą być automatycznie powielane i synchronizowane na pozostałych komputerach, do których jest przypisany ten użytkownik.

**11.** Zmiana hasła z poziomu systemu Windows powinna być automatycznie replikowana do systemu szyfrującego tak, by nie było potrzeby dwukrotnej zmiany hasła.

**12.** Rozwiązanie musi umożliwiać pracę w trybie single sign-on - po zalogowaniu się w trybie PBA użytkownik nie musi już logować się po raz kolejny do systemu Windows, jego dane są automatycznie przekazywane przez moduł PBA do procesu logowania Windows.

**13.** System szyfrowania musi umożliwiać centralną kontrolę jakości haseł używanych przez użytkowników przez określenie minimum: długości hasła, zawartości hasła (znaki numeryczne i alfanumeryczne, symbole, itp.), historię stosowanych haseł, wymuszenie zmiany hasła przez użytkownika.

**14.** System musi zapewnić centralne przechowywanie kluczy użytych do szyfrowania danych i możliwość odzyskania zaszyfrowanych danych z ich wykorzystaniem w sytuacji awarii.

**15.** Każdy komputer musi posiadać swój unikalny klucz wykorzystywany do szyfrowania danych na dysku oraz powinien być obecny w bazie CKZ.

**16.** Oprogramowanie szyfrujące musi kontynuować pracę po niespodziewanym zaniku zasilania, bez wpływu na możliwość zaszyfrowania i odszyfrowania danych.

**17.** System musi zapewniać możliwość centralnej konfiguracji parametrów szyfrowania, w tym centralne ustalanie polityk dla użytkowników i komputerów.

**18.** Rozwiązanie powinno umożliwiać definiowanie uprawnień i ról dla kont administratorów.

**19.** Stacje i użytkownicy mają synchronizować zmiany w politykach szyfrowania i parametrach systemu bez konieczności interwencji administratora.

**20.** Instalacja oprogramowania szyfrującego na stacjach użytkowników powinna się odbywać z wykorzystaniem paczki instalacyjnej, niezależnej od wersji i rodzaju systemu operacyjnego, zawierającego niezbędne moduły systemu szyfrowania.

**21.** Instalacja oprogramowania na stacji powinna się odbywać bez interwencji użytkownika.

**22.** System przed rozpoczęciem szyfrowania powinien sprawdzić, czy na komputerze nie znajduje się oprogramowanie niekompatybilne.

**23.** System musi umożliwiać zalogowanie się do głównego systemu operacyjnego z pominięciem PBA pod warunkiem wyrażenia na to zgody przez administratora systemu (np. celem zdalnej instalacji oprogramowania na stacji, bez obecności ich użytkownika) bez obecności modułu TPM. Pominięcie PBA musi być możliwe w z góry określonym przedziale czasu i na żądanie z poziomu stacji pod warunkiem, że używane jest do tego konto administratora domeny i pod warunkiem, że taki tryb pominięcia PBA jest zgodny z centralnie określoną polityką.

**24.** System powinien umożliwiać generowanie raportów dotyczących co najmniej: stanu zaszyfrowania systemu (stacja nie zaszyfrowana, stacja zaszyfrowana, stacja w trakcie szyfrowania), wersji działającego oprogramowania szyfrowania, przypisanych do stacji użytkowników.

**25.** Musi istnieć dobrze zdefiniowany proces odzyskiwania danych w sytuacjach awaryjnych: zagubienie hasła i nazwy użytkownika, po uszkodzeniu systemu operacyjnego, po uszkodzeniu systemu szyfrowania.

- **a.** Obsługa mechanizmu resetowania/odzyskiwania hasła użytkownika w rozwiązaniu do szyfrowania danych nie może wymagać podłączenia stacji do sieci firmowej.
- **b.** Musi istnieć możliwość samodzielnego zresetowania hasła przez użytkownika w trybie PBA w oparciu o udzielenie odpowiedzi na wcześniej zdefiniowane pytania, bez konieczności podłączenia stacji do sieci firmowej.

**c.** Musi istnieć możliwość odzyskiwania dostępu do danych przy pomocy aplikacji dla smartfona użytkownika. Aplikacja do obsługi tego odzyskiwania powinna być dostępna bezpłatnie minimum dla systemu Android.

**d.** W sytuacji zablokowania lub usunięcia oprogramowania szyfrującego zainstalowanego na stacji użytkownika musi być dostępny mechanizm i narzędzie do odzyskania zaszyfrowanych danych oraz odinstalowania oprogramowania szyfrującego opartego na narzędziu typu liveCD.

**26.** System szyfrowania dysków musi obsługiwać dyski twarde z wbudowanym mechanizmem szyfrowania sprzętowej w standardzie OPAL.

**a.** Po automatycznym wykryciu takiego dysku, oferowane rozwiązanie musi przekazać obsługę szyfrowania do wbudowanego mechanizmu w dysku.

**b.** Rozwiązanie musi być przetestowane przez producenta z minimum czteroma różnymi dyskami OPAL. Producent powinien zapewnić dostęp do listy kompatybilności dysków z OPAL.

**27.** System musi oferować możliwość wykorzystania wbudowanego mechanizmu szyfrowania w system operacyjny zamiast własnego mechanizmu szyfrującego. Wtedy system będzie odpowiedzialny za konfigurację funkcjonalności Bitlocker w przypadku systemów Microsoft Windows oraz FileVault w przypadku systemów Mac OS.

**Wymagania dotyczące modułu szyfrowania plików i folderów (moduł SP)**

**1.** Rozwiązanie musi zapewnić:

**a.** szyfrowanie plików i katalogów w ramach systemu operacyjnego i udziałów sieciowych udostępnianych przez serwery sieciowe.

**b.** szyfrowanie danych kopiowanych na urządzenia zewnętrzne USB oraz CD/DVD.

**c.** zabezpieczenie danych przenoszonych na USB między komputerami poprzez utworzony na dysku USB szyfrowany kontener.

**d.** integrację z podsystemem ochrony przed wyciekiem danych DLP opisanym powyżej, co najmniej poprzez wymuszenie sterowania szyfrowania plików kopiowanych na nośniki USB z poziomu polityki DLP.

**2.** System szyfrowania plików i folderów musi być możliwy do wdrożenia niezależnie od modułu szyfrowania danych (SD).

**3.** Moduł SP powinien mieć w pełni spolonizowany interfejs użytkownika.

**4.** Instalacja oprogramowania na stacjach użytkowników powinna się odbywać z wykorzystaniem paczki instalacyjnej, niezależnej od wersji i rodzaju systemu operacyjnego, zawierającej niezbędne moduły i opcjonalnie parametry polityki szyfrowania.

**5.** Instalacja oprogramowania na stacji powinna się odbywać bez interwencji użytkownika.

**6.** System szyfrowania SP musi zapewniać centralne zarządzanie, w oparciu o CKZ.

**7.** Oprogramowanie szyfrujące na stacjach użytkowników musi komunikować się z serwerem zarządzającym w bezpieczny (transmisja szyfrowana z obustronną autentykacją) sposób z wykorzystaniem protokołów opartych na TCP/IP.

**8.** Rozwiązanie musi wykorzystywać algorytm AES 256 do szyfrowania danych.

**9.** Szyfrowanie plików nie powinno wpływać na datę ostatniego dostępu do pliku zapisanej w atrybutach pliku.

**10.** Powinien istnieć mechanizm ograniczający utylizację dysku twardego do zadanej wartości procentowej przy szyfrowaniu plików tak, by samo szyfrowanie nie wpływało na komfort pracy użytkownika.

**11.** Oprogramowanie SP powinno umożliwić stworzenie listy wyjątków przy dostępie do plików zaszyfrowanych tak, by ich praca nie była wstrzymywana w przypadku próby dostępu do pliku zaszyfrowanego kluczem, do którego użytkownik nie ma dostępu (np. dla systemu antywirusowego lub backupowego).

12. System powinien wspierać wymazywanie zawartości pliku z dysku przy kasowaniu pliku tak, by niemożliwe było jego odzyskanie.
13. System powinien umożliwić tworzenie kluczy synchronizowanych z CKZ oraz takich generowanych lokalnie - nie podlegających synchronizacji z CKZ. Klucze lokalne powinny być tworzone bezpośrednio przez użytkowników.
14. Możliwość tworzenia kluczy nie podlegających synchronizacji z CKZ powinna być możliwa do zablokowania.
15. Tworzenie i przechowywanie kluczy powinno odbywać się na CKZ. Wszystkie klucze za wyjątkiem kluczy zdefiniowanych lokalnie powinny być przechowywane w bazie CKZ powinno być możliwe ich odzyskanie w sytuacji awaryjnej.
16. System musi zapewniać centralne przydzielenie tych samych kluczy używanych do szyfrowania do wielu użytkowników i grup użytkowników z Active Directory (AD).
17. Niezależnie od centralnie przydzielonych wspólnych kluczy dla grupy użytkowników, każdy użytkownik musi posiadać także unikalny klucz, przypisany do niego automatycznie, wykorzystywany do szyfrowania plików i katalogów.
18. Musi istnieć możliwość użycia kluczy wykorzystywanych do szyfrowania plików i katalogów oraz USB/CD/DVD także w trybie off-line (kiedy stacja nie jest podłączona do sieci Zamawiającego i jeśli nie ma połączenia z centralnym serwerem zarządzającym).
19. Decyzja o zaszyfrowaniu pliku może zostać podjęta w oparciu o:
    a. Centralnie zdefiniowaną politykę wskazująca foldery/pliki obligatoryjnie szyfrowane ze wskazaniem konkretnego klucza szyfrującego.
    b. Lokalnie przez użytkownika z użyciem kluczy, do których użycia użytkownik jest uprawniony.
20. W przypadku centralnie definiowanej polityki powinno być możliwe, co najmniej:
    a. Wskazanie plików/folderów, które powinny być obligatoryjnie szyfrowane.
    b. Wskazanie udziałów sieciowych, których pliki powinny być zaszyfrowane. Szyfrowanie udziałów sieciowych nie może wymagać instalowania oprogramowania na serwerach plików. Komunikacja między stacją użytkownika a udziałem sieciowym z zaszyfrowanymi plikami nie może powodować, że pliki lub ich części są przesyłane niezaszyfrowane.
    c. Wskazanie usług chmurowych (co najmniej: Box, Dropbox, Googe Drive, Microsoft Onedrive), których pliki będą szyfrowane przed synchronizacją.
    d. Przy wskazywaniu plików/folderów powinna istnieć możliwość użycia typowych, predefiniowanych lokalizacji jak pulpit systemowy, katalog profilu użytkownika, itp.
    e. Określenie typów plików, jakie mają być szyfrowane przez wskazanie procesu jakie je tworzy i rozszerzeń plików.
21. W przypadku ręcznego szyfrowania przez użytkownika powinno być możliwe co najmniej:
    a. Ręczne zaszyfrowanie pliku/katalogu wybranego przez użytkownika wybranym kluczem do którego użytkownik ma dostęp.
    b. Stworzenia samo-rozpakowującego się, zaszyfrowanego archiwum chronionego hasłem wybranym przez użytkownik
    c. Użycia funkcji „zaszyfruj i wyślij mailem”, która tworzy nową wiadomość z załączonym zaszyfrowanym plikiem.
22. Pliki zaszyfrowane modułem SP powinny być wizualnie oznaczane zmianą ikony tak, by użytkownik wiedział o stanie zaszyfrowania pliku bez podejmowania dodatkowych akcji.
23. Użytkownik powinien mieć możliwość łatwego sprawdzenia którym kluczem dany plik pozostał zaszyfrowany.
24. Plik zaszyfrowany konkretnym kluczem powinien być automatycznie możliwy do odczytania przez wszystkich użytkowników, którzy mają dostęp do klucza użytego do zaszyfrowania pliku na wszystkich stacjach roboczych.

25. Uwierzytelnianie użytkownika na potrzeby systemu SP musi wykorzystywać uwierzytelnianie Microsoft Windows i umożliwiać przezroczystą pracę dla użytkowników bez potrzeby dodatkowego uwierzytelniania się.
26. W przypadku, gdy zamawiający zrezygnuje z mechanizmów uwierzytelniania wbudowanych w Microsoft Windows powinna istnieć możliwość wykorzystania wbudowanego systemu uwierzytelniania do modułu SP.
27. Uwierzytelnianie użytkownika na potrzeby modułu SP musi umożliwiać użycie tokenów sprzętowych, kart inteligentnych i certyfikatów PKI, które są obsługiwane przez Microsoft Windows.
28. System musi umożliwiać dostęp do danych zaszyfrowanych przez wielu użytkowników (min. 100) zarówno w przypadku szyfrowania plików i katalogów jak również plików szyfrowanych przy kopiowaniu na USB/CD/DVD.
29. System musi zapewniać automatyczne szyfrowanie tzw. pliku wymiany Windows (*pagefile*).
30. System SP musi obsługiwać dowolne nośniki wymienne USB i umożliwiać szyfrowanie na nich plików. Powinny istnieć następujące możliwości szyfrowania nośników wymiennych:
    a. Szyfrowanie proste, poprzez wymuszenie szyfrowania kopiowanych plików wprost na dysk USB. Pliki nie mogłyby być odczytane na zewnętrznej stacji roboczej nienależącej do organizacji.
    b. Szyfrowanie poprzez kontener. Odczytanie plików jest możliwe zarówno na stacjach korporacyjnych jak i zewnętrznych po podaniu hasła ustawionego przy inicjalizacji takiego nośnika.
31. Szyfrowanie poprzez kontener musi spełnić następujące wymagania:
    a. Założony katalog musi być dostępny, po podaniu hasła, na innych komputerach bez konieczności instalowania na nich jakiegokolwiek dodatkowego oprogramowania na zewnętrznych stacjach.
    b. Kontener musi być gotowy do pracy zaraz po wpięciu pamięci USB do komputera w przypadku stacji korporacyjnej bez konieczności wpisywania hasła.
    c. Użytkownik może wybrać podczas inicjalizacji jak duży obszar dysku może zostać zajęty przez kontener. Powinna być możliwość wymuszenia zajęcia całego obszaru dysku przez kontener.
    d. Powinna istnieć procedura odzyskiwania dostępu do kontenera poprzez mechanizm challenge/response polegający na wymianie kodów pomiędzy użytkownikiem a operatorem helpdesk.

## Wymagania dotyczące Centralnej Konsoli Zarządzająca(CKZ)

Centralna konsola zarządzająca (zwana dalej CKZ) ma za zadanie zarządzanie wszystkimi produktami bezpieczeństwa wchodzącymi w skład rozwiązania będącego przedmiotem niniejszego zamówienia. Powinna się składać z oprogramowania serwerowego oraz agenta instalowanego na stacjach końcowych, którego zadaniem jest konfigurowanie produktów zarządzanych oraz zbieranie zdarzeń i przekazywanie ich do CKZ.

1. Zarządzanie wszystkimi modułami i pełnym zakresem funkcji dostarczonego systemu ochrony musi następować z jednej i tej samej aplikacji (konsoli) działającej na serwerze Microsoft Windows (wymagane wsparcie dla wersji Windows 2012 R2 oraz Windows 2016) i korzystającej z bazy danych Microsoft SQL (wymagane wsparcie dla wersji SQL 2008, SQL 2008R2, SQL 2012, SQL 2016 – wszystkie w wersji Express i wersjach komercyjnych).
    a. Platforma sprzętowa dla wdrożenia systemu zarządzania, system operacyjny Microsoft Windows oraz serwer Microsoft SQL zostaną zapewnione przez Zamawiającego.

**b.** Aplikacja musi być skalowalna i umożliwiać zarządzanie co najmniej 2 tys. komputerów i zainstalowanych na nich produktów.
**c.** Wdrożenie dowolnej ilości dodatkowych serwerów zarządzających zarówno pracujących niezależnie od siebie jak również w układzie hierarchicznym nie może wymagać zakupu dodatkowych licencji lub oprogramowania.
**d.** System musi umożliwiać migrację zarządzanych komputerów między serwerami zarządzającymi (zmiana przypisania komputera do konkretnego serwera zarządzającego).
**e.** System musi umożliwiać odzyskiwanie w przypadku awarii (Disaster Recovery) a konfiguracja potrzebna do odtworzenia serwera powinna być przechowywana w bazie danych.

**2.** System zarządzający musi mieć możliwość działania w klastrze HA zbudowanym na bazie klastra Microsoft Windows.

**3.** Centralna konsola zarządzająca ma umożliwić zdalną instalację produktów na komputerach z domeny Microsoft Active Directory objętych ochroną, bez konieczności stosowania dodatkowych narzędzi i oprogramowania, z możliwością zaplanowania z wyprzedzeniem momentu wykonania instalacji dla poszczególnych komputerów i grup komputerów.
**a.** Oferowane rozwiązanie powinno umożliwiać metodę dystrybucji oprogramowania poprzez wygenerowanie specjalnego adresu URL, którego dystrybucja dla użytkowników końcowych przez inny kanał komunikacji (np. Email) pozwoli na ściągnięcie i instalacji produktów.
**b.** Oferowane rozwiązanie ma umożliwiać selektywne wskazanie, który z produktów ochronnych wchodzących w skład systemu zostanie wdrożony i na którym z komputerów. Nie jest dopuszczalne wdrożenie pakietu w postaci jednej paczki instalacyjnej obejmującej kilka produktów na raz.
**c.** Definiowanie komputerów, które mają być objęte wdrożeniem poszczególnych produktów musi być możliwe na bazie zdefiniowanych grup maszyn oraz na bazie dynamicznie przydzielanych znaczników, niezależnie od podziału na grupy maszyn, uzależnionych od parametrów komputera - co najmniej takich jak: rodzaj CPU, ilość RAM, wielkość dysku, rodzaj systemu operacyjnego, ilość dostępnego miejsca na dysku.

**4.** Zarządzanie powinno odbywać się poprzez standardową przeglądarkę WWW i połączenie https. Nie jest dopuszczalne wykorzystanie do zarządzania dedykowanych aplikacji (tzw. thick client / gruby klient) instalowanych na stacjach administratorów. Powinny być wspierane przeglądarki minimum Internet Explorer 9, Firefox 10 lub Google Chrome 17 oraz Safari 6.

**5.** Komunikacja wszystkich produktów wdrożonych na danym komputerze musi odbywać się okresowo, w jednolity sposób, poprzez jeden kanał komunikacji inicjowany ze strony chronionych komputerów.
**a.** Musi być możliwe wymuszenie połączenia komputera z serwerem zarządzającym na żądanie, ze strony konsoli zarządzania.
**b.** Muszą istnieć mechanizmy, gdzie jeden z komputerów może być węzłem pośredniczącym dla innych komputerów znajdujących się w tej samej domenie rozgłoszeniowej w przypadku wywołania na żądanie ze strony konsoli zarządzania oraz w przypadku, gdy komputer nie ma bezpośredniego połączenia z serwerem zarządzającym.
**c.** Komunikacja musi być obustronnie uwierzytelniania z pomocą certyfikatów cyfrowych wygenerowanych dla poszczególnych komponentów komunikujących się poprzez sieć.

**6.** Centralna aplikacja zarządzająca CKZ musi umożliwiać tworzenie szczegółowych konfiguracji pracy poszczególnych produktów i dystrybucję polityk oraz wymuszanie ich zastosowania.
**a.** System musi umożliwiać definiowanie dedykowanych wersji polityki działania poszczególnych produktów.
**b.** System musi umożliwiać przydzielenie różnych polityk działania do poszczególnych komputerów, grup maszyn oraz dynamicznie (niezależnie od przydziału do grupy maszyn)

na podstawie filtrów bazujących na parametrach komputerów (co najmniej rodzaj CPU, wielkość RAM, wielkość dysku, ilość wolnego miejsca na dysku, rodzaj systemu operacyjnego).

**c.** Musi być dostępna funkcjonalność wymuszania, co zdefiniowany przedział czasowy, konfiguracji w przypadku, gdy użytkownik zmieni w niej cokolwiek (pod warunkiem, że zmiana przez użytkownika jest dozwolona w polityce).

**d.** W przypadku modyfikacji polityki system musi wskazać, ile systemów zostanie dotkniętych zmianą edytowanej polityki.

**7.** W ramach konsoli powinno być dostępne wersjonowanie polityk produktów zarządzanych. Powinna też być możliwość przywrócenia dowolnej wersji polityki używanej w przeszłości oraz porównania jej z bieżącą polityką.

**8.** CKZ musi posiadać możliwość powiadamiania o wszystkich zdarzeniach za pomocą poczty elektronicznej, wiadomości SNMP i syslog lub wywołania komendy/skryptu.

**9.** CKZ musi mieć możliwość integracji z Active Directory zarówno w rozumieniu powielenia struktury komputerów jak i uwierzytelnienia administratorów i dynamicznego przypisywania uprawnień w serwerze zarządzającym w zależności od przynależności do odpowiedniej grupy w Active Directory.

**10.** System zarządzania CKZ musi być przygotowany do pracy w strefie DMZ (dostępnej z sieci publicznych) tak, aby było możliwe zarządzanie komputerami znajdującymi się poza siecią korporacyjną, bez zestawiania połączeń VPN lub SSL VPN i aby jednocześnie podstawowy serwer zarządzający z aplikacją zarządzającą nie był narażony na potencjalne ataki z zewnątrz.

**11.** System zarządzania CKZ ma zapewnić centralne repozytorium (oparte na relacyjnej bazie danych MS SQL) dla logów i zdarzeń logowanych przez wszystkie moduły systemu ochrony.

**a.** Zbieranie zdarzeń logowanych we wszystkich modułach dostarczanego systemu ochrony na wszystkich chronionych węzłach (komputerach i serwerach) i składowanie ich w centralnym repozytorium będącym integralną częścią systemu.

**b.** Zbieranie zdarzeń musi obejmować wszystkie zdarzenia logowane przez moduły dostarczonego oprogramowania.

**c.** Mechanizm zbierania zdarzeń musi umożliwiać ograniczenie zbieranych zdarzeń na podstawie wybieranego przez administratora kryterium.

**d.** Podsystem zbierający zdarzenia musi zapewniać centralnie zarządzanie z pojedynczej konsoli dla wszystkich komponentów oprogramowania.

**12.** Aplikacja zarządzająca CKZ ma umożliwiać centralne opracowanie raportów na podstawie zgromadzonych danych i prezentację ich w różnych formatach (co najmniej PDF, XML, HTML).

**a.** Raporty powinny być generowane na żądanie, ale powinna istnieć możliwość określenia zakresu raportu i częstotliwości jego automatycznego generowania.

**b.** Raporty powinny bazować na predefiniowanych przez producenta szablonach dla poszczególnych zarządzanych produktów, a także powinna być możliwość tworzenia własnych raportów przez administratorów.

**13.** CKZ musi umożliwiać zdefiniowanie wielu kont administratorów i przydzielenie im szczegółowych ról umożliwiających co najmniej: ograniczenie dostępu do wskazanych grup maszyn, ograniczenie administracji do poszczególnych produktów i ich specyficznych funkcji.

**14.** CKZ musi mieć wbudowane mechanizmy integracji z serwisami zarządzania helpdesk i zgłoszeniami serwisowymi (co najmniej BMC Remedy i HP Service Desk).

**15.** System powinien posiadać możliwość skanowania w poszukiwaniu niezarządzanych hostów w sieci poprzez instalowanie odpowiedniego oprogramowania na systemy zarządzane. Skanowanie powinno odbywać się przez pasywne nasłuchiwanie ruchu rozgłoszeniowego (np.: ARP, DHCP). Wyniki skanowania powinny być przesyłane do centralnej konsoli w celu dalszej analizy.

16. CKZ musi posiadać dostępny bez dodatkowych opłat interfejs API umożliwiający Zamawiającemu automatyzację podstawowych czynności administracyjnych, w tym co najmniej: dodawanie i usuwanie kont administratorów systemu, usuwanie logów, uruchamianie i zatrzymywanie zadań do wykonania przez serwer zarządzający (np. ściągaj aktualizację produktów), przypisywanie określonych polityk produktów do grup komputerów, dodawanie komputerów do listy zarządzanych maszyn wraz z automatycznym uruchomieniem dla nich zadań instalacji oprogramowania ochronnego, usuwanie komputerów z listy zarządzanych maszyn.
17. Pliki instalacyjne i inne elementy, których dostępność jest wymagana do poprawnej pracy środowiska powinny być zlokalizowane w centralnym repozytorium na konsoli zarządzającej.
    a. Powinien istnieć mechanizm dystrybucji plików instalacyjnych na zdalne repozytoria danych zapewnione przez zamawiającego obsługujące co najmniej protokoły FTP, HTTP i UNC.
    b. Replikacja centralnego repozytorium na repozytoria dodatkowe powinna być możliwa na żądanie oraz powinno być możliwe zdefiniowanie harmonogramu.
    c. Powinna istnieć możliwość definicji listy repozytoriów, z których chronione komputery będą korzystały osobno dla różnych grup komputerów. Wybór repozytorium powinien się odbywać zgodnie z kolejnością na liście lub czasów odpowiedzi na ping.
    d. W przypadku lokalizacji, gdzie nie ma możliwości skorzystania z serwerów dla zdalnych repozytoriów - taką rolę powinien przejąć dowolny z systemów. System ten powinien mieć możliwość buforowania plików instalacyjnych. Powinna istnieć możliwość tworzenia hierarchii ze wspomnianych wyżej systemów.

**Wymagania dotyczące usługi wdrożenia rozwiązania.**

1. Wykonanie projektu technicznego, zwanego dalej Projektem Technicznym, oraz przeniesienie autorskich praw majątkowych do Projektu Technicznego, oraz praw zależnych.
2. Dostawa oprogramowania wraz z koniecznymi licencjami na korzystanie z oprogramowania w ilości niezbędnej do budowy i uruchomienia Systemu wraz z 36-miesięcznym wsparciem technicznym producenta oprogramowania (maintenance), zwanego dalej Oprogramowaniem.
3. Wykonanie usług instalacyjno-wdrożeniowych, zgodnie z Projektem Technicznym, w ramach którego zostanie zaimplementowane wdrożenie minimum 5 scenariuszy zapobiegania wyciekowi danych.
4. Prace wdrożeniowe muszą odbywać się w godzinach pracy Zamawiającego, od poniedziałku do piątku w godzinach 8:00 - 16:00.
5. Wykonanie dokumentacji powykonawczej wykonanych usług instalacyjno-wdrożeniowych, zwanej dalej Dokumentacją Powykonawczą, oraz przeniesie autorskich praw majątkowych do Dokumentacji Powykonawczej, oraz praw zależnych.
6. Przeprowadzenie warsztatów instruktażowo-szkoleniowych dla pracowników Zamawiającego z zakresu obsługi wdrożonego Systemu.
7. Świadczenie usługi wsparcia serwisowego Wykonawcy dla Systemu, zwanej dalej Usługą Serwisową.
8. Świadczenie usług konsultacyjnych, w minimalnej ilości 150 godzin w okresie obowiązywania Umowy.