Załącznik nr 1 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. ***Funkcjonalność Systemu do szyfrowania danych.***
2. ***Wymagania Zamawiającego dotyczące realizacji Projektu.***
3. ***Dokumentacja i filmy instruktażowe.***
4. ***Szkolenia.***
5. ***Projekt techniczny Systemu.***
6. ***Testy Systemu.***
7. ***Wymagania dotyczące równoważności.***

I. Funkcjonalność Systemu do szyfrowania danych

1. Zabezpieczenie danych znajdujących się na dyskach twardych w stacji roboczej.
2. Szyfrowanie wybranych plików i folderów.
3. Automatyczne szyfrowanie danych znajdujących się w wybranych folderach.
4. Szyfrowanie danych na nośnikach zewnętrznych np. typu pendrive, CD, DVD
5. Centralne zarządzanie Oprogramowaniem i uprawnieniami Użytkowników w nim zdefiniowanych w sieci LAN Zamawiającego i w sieci Internet.
6. Logowanie się do systemu operacyjnego stacji roboczej z poziomu pre-boot tzw. pojedynczy punkt logowania - SSO (Single Sign-On).
7. Pobieranie danych o użytkownikach z serwera usług katalogowych Novell eDirectory w wersji 8.7.3.10 i nowszej do Centralnego serwera zarządzającego.
8. Współpracę z klientem Novell w wersji 4.91 SP5 (PL i EN) i nowszej oraz z klientem Novell ZENworks w wersji 7 i 11SP1 (PL i EN) i nowszej na stacjach roboczych z zainstalowanym systemem operacyjnym Microsoft Windows w wersji XP SP3 PL (32-bit), Microsoft Windows w wersji 7 SP1 PL (32-bit, 64-bit) i nowszej.
9. Szyfrowanie danych Użytkowników na stacjach roboczych o minimalnych parametrach:
    a. Chipset: Intel 855GME,
    b. Procesor: 1.6 GHz (Intel Pentium M Dothan (2 MB cache)),
    c. Pamięć: 512 MB (PC2700 SO-DIMM 200pin (DDR333)),
    d. Dysk twardy: 40 GB – bez RAID,
    e. Karta graficzna: Intel Extreme Graphics 2 (64 MB),
    f. Karta sieciowa: LAN 10/100 Mbit (RJ-45).

II. Wymagania Zamawiającego dotyczące realizacji Projektu

I. Etap inicjujący Projekt

Wykonawca w terminie do **20 dni** od dnia podpisania umowy opracuje i przekaże do akceptacji Zamawiającego:

a. szczegółowy Harmonogram realizacji Projektu

b. Zasady Zarządzania Projektem (ZZP)

c. Projekt techniczny systemu

Zamawiający w terminie **5 dni** od dnia przekazania ww. dokumentów wniesie do nich uwagi bądź je zaakceptuje. Wykonawca wprowadzi niezbędne poprawki i uzupełnienia w terminie **5 dni** od dnia przekazania uwag przez Zamawiającego.

Wykonanie wszelkich prac przewidzianych dla Etapu inicjującego Projekt zostanie zakończone w nieprzekraczalnym terminie **30 dni** od dnia podpisania umowy.

WYMAGANIA OGÓLNE DOTYCZĄCE SPOSOBU PRZYGOTOWANIA HARMONOGRAMU

- ODBIORY CZĘŚCIOWE - W przypadku przekazywania Zamawiającemu do odbioru dokumentów lub funkcjonalności cząstkowych Systemu do szyfrowania danych, należy przewidzieć w harmonogramie niezbędny czas na weryfikację/odbiór przez Zamawiającego (**minimum 3 dni robocze**) oraz wprowadzenie niezbędnych poprawek i uzupełnień przez Wykonawcę przed ponownym przedstawieniem do odbioru (czas na ponowny odbiór dla Zamawiającego **minimum 2 dni robocze**).
- TESTY AKCEPTACYJNE - W przypadku testów akceptacyjnych, należy przewidzieć niezbędny czas na testy i ich odbiór przez Zamawiającego (**minimum 5 dni roboczych**) oraz wprowadzenie niezbędnych poprawek i uzupełnień przed ponownym przedstawieniem ich do odbioru (czas na ponowny odbiór dla Zamawiającego **minimum 3 dni robocze**).
- INFRASTRUKTRA TECHNICZNA - W przypadku konieczności przerwania ciągłości funkcjonowania infrastruktury sieciowej Zamawiającego, niezbędne prace muszą być wykonywane po godzinach pracy Zamawiającego (po godz. 16.00) lub w dni wolne od pracy. W uzasadnionych przypadkach mogą być realizowane w godzinach pracy Zamawiającego, po uzyskaniu od niego wcześniejszej zgody. Prace instalacyjne i konfiguracyjne muszą odbywać się na miejscu, w siedzibie Zamawiającego w Warszawie. Muszą być wykonywane przez wykwalifikowanych przedstawicieli Wykonawcy, posiadających stosowane dokumenty potwierdzające posiadaną wiedzę w zakresie realizowanych prac.

II. ETAP I

Warunkiem rozpoczęcia Etapu I jest obustronne podpisanie protokołu odbioru Etapu Inicjującego Projekt bez uwag.

Wszystkie prace przewidziane do realizacji w Etapie I muszą zostać wykonane w nieprzekraczalnym terminie **90 dni** od dnia podpisania protokołu odbioru Etapu Inicjującego Projekt bez uwag.

Zamawiający wymaga, aby w Etapie I Projektu zostały wykonane poniższe prace:

1. Instalacja, konfiguracja i uruchomienie centralnego serwera zarządzającego oprogramowaniem do szyfrowania danych (Centralnego Serwera) w infrastrukturze teleinformatycznej Zamawiającego, na sprzęcie zapewnionym przez Zamawiającego.
2. Konfiguracja Centralnego Serwera zgodnie z wymaganiami Zamawiającego.
3. Integracja Centralnego Serwera ze wskazanymi systemami Zamawiającego
4. Testowe uruchomienie Centralnego Serwera.

5. Testy poszczególnych funkcjonalności Centralnego Serwera.
6. Testy akceptacyjne w zakresie: funkcjonalności, bezpieczeństwa systemu i danych oraz wydajności Centralnego Serwera.
7. Opracowanie i wykonanie integracji Centralnego Serwera z Novell eDriectory i Novell ZENWorks.
8. Instalacja Microsoft Active Directory (AD) na serwerze Microsoft Windows 2008R2.
9. Wykonanie i skonfigurowanie konektora pomiędzy Novell eDriectory a AD.
10. Opracowanie i wykonanie mechanizmów integracji z już istniejącym środowiskiem pilotażowym EEM 5.2.10 (Endpoint Encryption Manager) albo przeprowadzenie migracji użytkowników z EEM do Centralnego Serwera.
11. Weryfikacja polityk szyfrowania, opracowanych na wcześniejszym etapie prac.
12. Weryfikacja i przetestowanie mechanizmu automatycznej instalacji oprogramowania do szyfrowania danych na stacjach roboczych.
13. Weryfikacja metod awaryjnego odzyskiwania danych na stacjach roboczych tak, aby można było je wykonać w każdej siedzibie NIK na terenie kraju.
14. Wykonanie testów poprawności działania na wybranych typach stacji roboczych użytkowników – nie więcej niż 5 grup po maksimum 3 stacje robocze.
15. Dostrajanie Centralnego Serwera na podstawie wyników uzyskiwanych podczas prowadzonych testów oraz uwag i wymagań Zamawiającego.
16. Wykonanie testów Centralnego Serwera w części dotyczącej funkcjonalności po stronie stacji roboczych.
17. Wykonanie testów akceptacyjnych w zakresie: funkcjonalności, bezpieczeństwa systemu i danych oraz wydajności dla pełnej funkcjonalności Systemu do szyfrowania danych.
18. Wykonanie procedur, instrukcji i regulaminów dla Administratorów, Trenerów Zamawiającego oraz Użytkowników dotyczących Systemu do szyfrowania danych.
19. Wykonanie procedur, instrukcji i mechanizmów archiwizacji danych dla Użytkowników.
20. Wykonanie materiałów szkoleniowych dla Trenerów Zamawiającego i Użytkowników.
21. Opracowanie prezentacji dla kierownictwa.
22. Wykonanie filmów instruktażowych.
23. Przygotowanie i przeprowadzenie przez Wykonawcę szkoleń dla Trenerów Zamawiającego.
24. Wprowadzanie do Systemu uzgodnionych konfiguracji wynikających m.in. z uwag zgłoszonych w trakcie szkoleń.
25. Wprowadzanie uzgodnionych modyfikacji materiałów szkoleniowych, filmów instruktażowych, procedur i instrukcji m.in. z uwag zgłoszonych w trakcie szkoleń.
26. Weryfikacja procedur, instrukcji i regulaminów dotyczących Systemu.
27. Weryfikacja procedur i mechanizmów archiwizacji danych.
28. Przygotowanie i przeprowadzenie prezentacji dla kierownictwa w terminie uzgodnionym z Zamawiającym.
29. Produkcyjne uruchomienie Systemu.
30. Dostarczenie dokumentacji powykonawczej.

III. ETAP II

Warunkiem rozpoczęcia Etapu II jest obustronne podpisanie Protokołu odbioru Etapu I bez uwag.

Wszystkie prace przewidziane do realizacji w Etapie II muszą zostać wykonane w nieprzekraczalnym terminie **60 dni** od dnia podpisania protokołu odbioru Etapu I bez uwag.

Zamawiający wymaga, aby w Etapie II Projektu zostały wykonane poniższe prace:

1. Nadzór i pomoc nad prawidłowym przebiegiem procesu wdrażania oprogramowania do szyfrowania danych na stacjach roboczych Zamawiającego.
2. Nadzór i pomoc przy prowadzeniu szkoleń dla użytkowników końcowych, prowadzonych przez trenerów Zamawiającego.
3. Rozwiązywanie bieżących problemów z Systemem.
4. Wsparcie pracowników Zamawiającego podczas procesu wdrażania oprogramowania do szyfrowania.
5. Weryfikacja poprawności realizacji procesu instalacji oprogramowania do szyfrowania na stacjach roboczych i w razie wystąpienia problemów korygowanie ich.
6. Podsumowanie projektu w formie dokumentu zawierającego m.in. raport doświadczeń z projektu.
7. Przygotowanie prezentacji podsumowującej projekt.

IV. Wymagania ogólne dotyczące sposobu przygotowania Zasad Zarządzania Projektem

Wykonawca przygotuje Zasady Zarządzania Projektem (ZZP) w oparciu o metodykę prowadzenia i realizacji projektów - PRINCE2. ZZP obejmą swoim zakresem co najmniej następujące elementy:

1. Strukturę organizacyjną, z zakresem obowiązków dla każdej z ról (ze strony Wykonawcy i Zamawiającego), niezbędną do zarządzania projektem.
2. Plany, w tym: Plan projektu, Plan etapu, Plan pracy zespołu i Plan naprawczy.
3. Elementy sterowania projektem.
4. Sterowanie zmianami.
5. Uzasadnienie biznesowe.
6. Szczegółowy opis przyjętych punktów kontrolnych wraz z odzwierciedleniem ich w harmonogramie projektu.
7. Listę produktów wraz z odzwierciedleniem dat ich przekazania Zamawiającemu w harmonogramie projektu.
8. Analiza ryzyk w projekcie wraz z zasadami zarządzania, aktualizacji, monitorowania i raportowania.
9. Zasady i sposób raportowania postępów pracy (nie rzadziej niż 1 raz w tygodniu).
10. Zasady tworzenia i nazewnictwo dokumentów projektowych.
11. Zasady i sposoby komunikacji pomiędzy Wykonawcą a Zamawiającym.
12. Plan zapewnienia jakości projektu.
13. Zarządzanie Zgłoszeniami.
14. Zasady akceptacji/odbiorów dokumentacji związanej z realizacją przedmiotu zamówienia.
15. Opracowanie parametrów jakości produktów końcowych.

III. DOKUMENTACJA I FILMY INSTRUKTAŻOWE

1. Dokumentacja

1. Zamawiający wymaga, aby **wszystkie dokumenty** tworzone w ramach realizacji projektu charakteryzowały się wysoką jakością, w szczególności:
   a. Czytelną i zrozumiałą strukturą zarówno poszczególnych dokumentów jak i całej dokumentacji z podziałem na rozdziały, podrozdziały i sekcje.
   b. Zachowaniem standardów oraz sposobu pisania, rozumianych jako zachowanie jednolitej i spójnej struktury, formy i sposobu prezentacji treści poszczególnych dokumentów, oraz fragmentów tego samego dokumentu jak również całej dokumentacji.
   c. Zgodnością z dostarczonym przez Zamawiającego szablonem dokumentu.
2. W ramach realizacji Etapu I i Etapu II, Wykonawca opracuje i dostarczy m.in. szczegółową dokumentację dotyczącą instalacji, konfiguracji i parametryzacji Systemu do szyfrowania danych oraz konfiguracji stacji roboczych wraz z opisem procedur i instrukcji eksploatacyjnych. Wykonawca przygotuje w szczególności:
   a. Procedury i instrukcje wykonania kopii bezpieczeństwa środowiska (całego Centralnego Serwera) i ich odtworzenia.
   b. Procedury i instrukcje wykonania backupu Systemu do szyfrowania danych i odtworzenia danych z backupu (należy uwzględnić działający w NIK system backupu oparty o oprogramowanie Tivoli Storage Manager - TSM).
   c. Procedury i instrukcje bieżącego monitoringu oraz utrzymania Systemu do szyfrowania danych.
   d. Procedury i instrukcje aktualizacji i wdrażania łat.
   e. Procedury postępowania w razie wystąpienia błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów.
   f. Szczegółowe procedury tworzenia płyty CD/DVD i pendrive z oprogramowaniem do odzyskiwania danych. W przypadku konieczności użycia do tworzenia płyty CD/DVD i pendrive oprogramowania firm trzecich, Wykonawca w ramach niniejszego projektu, bez dodatkowych kosztów dla Zamawiającego, dostarczy i przekaże na jego rzecz to oprogramowanie wraz z licencjami umożliwiającymi jego użytkowanie przez okres **3 lat** dla **20 użytkowników**.
   g. Szczegółową procedurę dystrybucji aktualnych wersji dokumentacji i produktów do szyfrowania i odzyskiwania danych w NIK.
   h. Procedury i instrukcje bieżącej analizy oraz archiwizowania zapisów systemów zabezpieczeń (logów).
   i. Procedury i instrukcje archiwizacji danych dla Użytkowników stacji roboczych.
3. Każda z procedur powinna zawierać co najmniej następujące dane:
   a. nazwa,
   b. opis,
   c. częstotliwość wykonywania,
   d. kroki do zrealizowania w procedurze,
   e. informacje (o ile są znane, jeśli jest ich dużo to przykłady bądź wzorce) na jakie należy zwrócić uwagę w trakcie wykonywania procedury,
   f. omówienie zawartości komunikatów jeśli są prezentowane,
   g. kroki jakie należy podjąć w przypadku natknięcia się na nietypowe sytuacje.

4. W ramach wdrożenia, Wykonawca opracuje i dostarczy szczegółowe instrukcje obsługi Systemu do szyfrowania danych dla: Użytkowników oraz Administratorów.
5. Dokumentacja musi być zweryfikowana i w razie potrzeby zaktualizowana po każdej modyfikacji/ aktualizacji Systemu do szyfrowania danych.
6. Dokumentacja dotycząca czynności administracyjnych związanych z utrzymaniem Sytemu do szyfrowania danych musi być dostarczana niezwłocznie wraz z nową wersją Systemu. Pozostała dokumentacja może być dostarczona nie później niż w terminie **14 dni** od daty przekazania nowej wersji Systemu.
7. Zamawiający wymaga, aby cała dokumentacja, o której mowa powyżej, podlegała jego akceptacji zgodnie z przyjętymi zasadami akceptacji/odbiorów określonymi w Zasadach Zarządzania Projektem.
8. Wykonawca będzie wersjonował wszystkie tworzone produkty w projekcie, a w szczególności dokumenty, wersje płyt CD/DVD i pendrive z oprogramowaniem do odzyskiwania danych. Przyjęty sposób wersjonowania ma jednoznacznie umożliwiać określenie wersji produktu. Musi być wykonana centralna baza danych umożliwiająca zarządzanie wersjami produktów.

2. Filmy instruktażowe

Wykonawca przygotuje filmy instruktażowe wg. poniższych wymagań:

1. Filmy instruktażowe muszą zawierać materiał ilustrujący działanie wszystkich opracowanych procedur i instrukcji dla Użytkowników.
2. Filmy instruktażowe muszą być wykonane wg następujących parametrów:
   a) Format AVI kodowany za pomocą np. DivX, xvid, wmv,
   b) Materiały w wysokiej jakości i niskim stopniu kompresji (optymalizowany pod kątem jakości),
   c) Rozdzielczość minimum 500x326,
   d) Stosowane kodeki muszą być darmowe i powszechnie dostępne w Internecie.
3. Zamawiający udostępni filmy instruktażowe Użytkownikom poprzez swój portal wewnętrzny.
4. Filmy instruktażowe m.in. muszą zawierać zarówno informacje uwzględniające postępowanie w codziennej pracy z Oprogramowaniem jak i sposoby reakcji w sytuacjach nietypowych/awaryjnych, np. zapomniane hasło.
5. Filmy muszą być zwięzłe, zrozumiałe dla osób nie technicznych, jednoznacznie omawiające dany temat.

IV. Szkolenia

1. Szkolenie z oferowanego produktu do szyfrowania danych

1. Wykonawca zorganizuje szkolenie prowadzone przez certyfikowanego inżyniera oferowanego oprogramowania, z zakresu szyfrowania danych dla 1 grupy administratorów składającej się z 4 osób, w siedzibie Zamawiającego w Warszawie.
2. Program szkolenia musi obejmować całość zagadnień z zakresu szyfrowania danych oraz szczegółowo omawiać proces zdalnej pomocy użytkownikom, odzyskiwania danych i mechanizmów szyfrowania danych.
3. Program szkolenia musi obejmować omówienie najczęściej występujących awarii Systemu, oraz sposoby ich usuwania i zabezpieczania się przed nimi.
4. Szkolenie musi uwzględniać korzystanie systemu do szyfrowania danych z Novell eDirectory oraz korzystanie z pojedynczego punktu logowania (SSO) na stacjach roboczych, na których zainstalowany jest klient Novell oraz informacje dotyczące funkcjonowania konektora pomiędzy AD a Novell eDirectory.
5. Szkolenie administratorów musi trwać minimum 2 dni robocze po 6 godzin efektywnych zajęć dziennie.
6. Wykonawca zapewni uczestnikom szkolenia materiały szkoleniowe w formie papierowej i elektronicznej.

2. Szkolenie z serwera bazodanowego - Microsoft SQL Server 2008 R2

1. Wykonawca zorganizuje certyfikowane szkolenie dla 2 pracowników Zamawiającego, obejmujące administrację serwerem bazodanowym Microsoft SQL 2008R2, który przechowuje dane konsoli zarządzającej Systemu.
2. Szkolenie musi trwać 5 dni roboczych po 6 godzin efektywnych zajęć dziennie i być realizowane w języku polskim.
3. Szkolenie musi umożliwiać:
   a. Poznanie zagadnień dotyczących utrzymania i obsługi baz danych Microsoft SQL Server 2008R2.
   b. Zdobycie umiejętności pozwalających na planowanie, instalację, konfigurację, zabezpieczanie oraz konserwację serwera baz danych.
   c. Nauczenie wykonywania zadań administracyjnych obejmujących wykonywanie i odtwarzanie baz danych, monitorowanie serwera oraz importowanie i eksportowanie danych.
   d. Zapoznanie się z elementami automatyzacji zadań administracyjnych serwera Microsoft SQL Server 2008R2.

3. Szkolenie z systemu operacyjnego - Microsoft Windows Server 2008 R2

1. Wykonawca zorganizuje certyfikowane szkolenie dla 2 pracowników Zamawiającego, obejmujące sowim zakresem administrację Microsoft Windows 2008R2, na którym uruchomiona jest konsola zarządzająca Systemu do szyfrowania danych.
2. Szkolenie musi trwać 5 dni roboczych po 6 godzin efektywnych zajęć dziennie i być realizowane w języku polskim.
3. Szkolenie musi umożliwiać:
   a. Zapoznanie z podstawowymi zagadnieniami dotyczącymi wdrażania, konfiguracji i zarządzania usługą katalogową Active Directory w Windows Server 2008 R2.

b. Zdobycie umiejętności pozwalających na implementację obiektów i relacji zaufania. Nauczenie wykorzystania polityk grupowych.

c. Zapoznanie z zagadnieniami monitorowania i utrzymywania Active Directory Domain Services (AD DS).

d. Zdobycie umiejętności pozwalających na utrzymywanie usług infrastruktury.

e. Przedstawienie zasad zabezpieczania środowiska serwerowego.

4. Wykonawca zapewni uczestnikom szkoleń, o których mowa w pkt 2 i 3 materiały szkoleniowe w formie elektronicznej i papierowej.
5. Na zakończenie szkoleń, o których mowa w pkt 2 i 3, uczestnicy muszą otrzymać certyfikaty, akredytowane przez firmę Microsoft, potwierdzające jego ukończenie.
6. W ramach szkoleń, o których mowa w pkt 2 i 3, uczestnicy muszą mieć możliwość, w ciągu 6 miesięcy od jego zakończenia, zweryfikowania przyswojonej wiedzy w procesie autoryzowanym przez firmę Microsoft.
7. W razie realizacji szkolenia poza Warszawą, Wykonawca, na własny koszt, zapewni transport, pełne wyżywienie i noclegi dla jego uczestników.

4. Szkolenie dla Trenerów Zamawiającego

1. Wykonawca przygotuje i przeprowadzi szkolenia dla nie więcej niż 20 Trenerów Zamawiającego, z zakresu posługiwania się Systemem do szyfrowania danych.
2. Szkolenia Trenerów przeprowadzone zostaną w Ośrodku Szkoleniowym NIK w Goławicach, w uzgodnionych wcześniej z Zamawiającym terminach. Uczestnicy szkoleń zostaną podzieleni na 2 grupy szkoleniowe (różne terminy), w każdej grupie będzie nie więcej niż 12 osób. W pierwszym i ostatnim dniu szkolenia, jego czas trwania może wynieść nie więcej niż 5 godz. W pozostałe dni szkolenie może trwać maksymalnie 8 godz.
3. Szkolenie Trenerów musi trwać minimum 3 dni robocze i zawierać oprócz omówienia oprogramowania do szyfrowania danych przede wszystkim warsztaty, na których zostaną przedstawione w praktyce m.in. sposoby odszyfrowywania danych w razie awarii (Wykonawca musi zapewnić wszystkie wymagane elementy konieczne do przeprowadzenia wszystkich prac podczas warsztatów oprócz stacji roboczych, które dostarczy Zamawiający) z uwzględnieniem infrastruktury Zamawiającego.
4. Ze względu na to iż Trenerzy Zamawiającego będą szkolić pozostałych pracowników Zamawiającego z obsługi Systemu do szyfrowania danych oraz będą pełnić rolę Administratora z ograniczonymi uprawnieniami, i być wsparciem dla Użytkowników, Zamawiający wymaga aby:
   a. Szkolenie obejmowało zagadnienia pozwalające realizować powyższe zadania.
   b. Trenerzy otrzymali materiały szkoleniowe w języku polskim, na podstawie których będą prowadzić szkolenia dla pozostałych Użytkowników.
   c. Trenerzy zostali przeszkoleni w czasie szkolenia z korzystania z tych materiałów.
5. Przed rozpoczęciem szkoleń Wykonawca przedstawi Zamawiającemu do akceptacji plan szkoleń i materiały szkoleniowe.
6. Plan szkoleń musi zawierać:
   a. Cel szkolenia.
   b. Zakres szkolenia.
   c. Metodę i formę szkolenia.

d. Niezbędny czas przeszkolenia jednej grupy danego szkolenia (ilość godzin pojedynczego szkolenia).

e. Agendę danego szkolenia.

f. Harmonogram szkoleń.

7. Uczestnicy otrzymają od Wykonawcy zaświadczenie uczestnictwa w szkoleniu, które zawierało będzie co najmniej następujące informacje:

   a. Datę i miejsce przeprowadzenia szkolenia.

   b. Imiona i nazwiska prowadzących szkolenie.

   c. Wymiar szkolenia (ilość godzin).

   d. Zakres tematyczny szkolenia.

   e. Poziom przyswojonej wiedzy przez osobę uczestniczącą w szkoleniu.

8. Przed rozpoczęciem szkolenia Wykonawca przygotuje stacje robocze udostępnione przez Zamawiającego do przeprowadzenia szkolenia.

9. Przed rozpoczęciem szkolenia Wykonawca przygotuje środowisko szkoleniowe dla Administratorów w postaci obrazu VMware, które musi być odzwierciedleniem środowiska docelowego.

10. Na zakończenie szkolenia musi zostać przeprowadzony przez Wykonawcę test weryfikujący poziom przyswojenia wiedzy przez uczestników szkolenia.

11. Potwierdzeniem odbytego szkolenia jest przekazanie Zamawiającemu przez prowadzącego szkolenie imiennej listy uczestników potwierdzonej ich własnoręcznym podpisem.

12. Wszystkie szkolenia Wykonawca przeprowadzi w języku polskim, zapewniając na swój koszt materiały szkoleniowe w języku polskim dla uczestników szkoleń.

13. W celu weryfikacji jakości przeprowadzonych szkoleń Zamawiający zastrzega sobie możliwość przeprowadzenia ankiety wśród uczestników szkoleń dotyczy oceny jakości przeprowadzonych szkoleń (ocena w skali 1-6. W przypadku, gdy średnia ocen z danego szkolenia będzie poniżej 3 - Zamawiający ma prawo żądać powtórzenia szkolenia).

5. Prezentacja Systemu dla Kierownictwa NIK

1. Wykonawca przygotuje do akceptacji Zamawiającego i przeprowadzi prezentację Systemu dla Kierownictwa NIK w zakresie uwzględniającym całą specyfikę użytkowania Systemu przez Użytkowników, a w szczególności zawierać będzie następujące elementy:

   a. Omówienie powodów wdrażania szyfrowania danych na podstawie wymogów prawnych, ochrony danych, dobrych praktyk a także w celu uniknięcia potencjalnego uszczerbku na wizerunku NIK w przypadku kradzieży/zgubienia laptopa czy też nośnika zewnętrznego z danymi.

   b. Praktyczna prezentacja szyfrowania danych i procedur z tym związanych.

2. Szacowany czas trwania prezentacji około 1 godzin.

3. Wykonawca zapewni uczestnikom materiały z prezentacji w formie uzgodnionej z Zamawiającym (papierowej i elektronicznej).

V. PROJEKT TECHNICZNY SYSTEMU

Projekt techniczny musi zawierać co najmniej:

1. Opracowane polityki szyfrowania danych na stacjach roboczych.
2. Opracowany mechanizm automatycznej instalacji Oprogramowania na stacjach roboczych.
3. Metody odzyskiwania danych z zaszyfrowanych stacji roboczych oraz nośników zewnętrznych.
4. Opracowanie ról i ich uprawnień do Systemu.
5. W przypadku, gdy w Oprogramowaniu do szyfrowania danych występuje okno do logowania Wykonawca zmodyfikuje je w taki sposób, aby zawierało m.in. logo NIK, nazwę instytucji, oprawę graficzną i uwzględniało stosowane przez Zamawiającego rozdzielczości ekranu (**minimum 5 rozdzielczości** wskazanych przez Zamawiającego). Przygotowany projekt graficzny Wykonawca dostarczy do akceptacji Zamawiającemu.
6. Zaaprobowaną przez Zamawiającego listę instrukcji niezbędnych do bezpiecznego użytkowania Oprogramowania dla Użytkowników i Administratorów.
7. Opracowanie polityki archiwizacji danych na Centralnym serwerze zarządzającym z wykorzystaniem oprogramowania IBM Tivoli Storage Manager (TSM).
8. Opracowanie polityk konfiguracji oprogramowania antywirusowego, antyspamowego i firewall zainstalowanego na Centralnym serwerze zarządzającym w kontekście oprogramowania do szyfrowania danych.
9. Opracowanie polityki zgodnie, z którą skonfigurowany będzie klient UPS zainstalowany na Centralnym serwerze zarządzającym.
10. Opracowanie procedury konfiguracji i integracji Oprogramowania z Novell eDirectory i Novell ZENWorks.
11. Opracowanie polityki szyfrowania plików i folderów uwzględniającą posiadanego przez Zamawiającego klienta pocztowego Novell GroupWise.
12. Wykonawca opracuje procedury uwzględniające instalację Oprogramowania w trakcie tworzenia obrazów stacji roboczych z wykorzystaniem użytkowanego przez Zamawiającego oprogramowania Symantec Ghost Corporate Edition w wersji 11.5 lub nowszej oraz przy wykorzystywaniu Windows Deployment Services.
13. Opracowanie procedur współpracy Oprogramowania z infrastrukturą Zamawiającego.

VI. TESTY SYSTEMU

1. Wszystkie dostarczone w ramach umowy produkty i świadczone usługi będą podlegały procedurom w zakresie testów akceptacyjnych i odbioru jakościowego - przyjęcia do eksploatacji. Upoważnione osoby ze strony Zamawiającego będą obecne przy wszystkich przeprowadzanych testach.
2. Celem testów akceptacyjnych jest potwierdzenie spełnienia przez System kryteriów jakościowych, potwierdzenie że funkcjonalność jest zgodna z wymaganiami Zamawiającego. Wynikiem testów akceptacyjnych jest raport z testów, stanowiący podstawę sporządzenia protokołu odbioru systemu.
3. Na testy akceptacyjne składają się następujące rodzaje testów:
    a) Administracyjne - testy funkcji i procedur administracyjnych dla Systemu.
    b) Instalacji i konfiguracji - sprawdzenie kompletności instalacji i zgodności jej przebiegu z instrukcjami i dokumentacją oraz poprawności uzyskanej konfiguracji.
    c) Testy integracyjne – testy poprawności współpracy poszczególnych modułów Systemu, sprawdzają czy funkcjonalności, w których bierze udział kilka modułów Systemu są realizowane prawidłowo.
    d) Testy wydajnościowe - testowanie wydajności i czasów reakcji Systemu przy obciążaniu go zgodnie z zadanymi warunkami, przy symulowanych (zbliżonych do realnych) lub innych wymaganych warunkach pracy testowanego Systemu.
    e) Testy bezpieczeństwa – testujące zabezpieczenia przed utratą danych i nieupoważnionym dostępu do danych i funkcji Systemu, zarządzanie uprawnieniami, zakres dostępu do danych i funkcji Systemu.
4. Wykonawca odpowiedzialny jest za:
    a) Przygotowanie środowiska testowego.
    b) Dostarczenie uzgodnionych i zatwierdzonych przez Zamawiającego scenariuszy testowych wraz z danymi testowymi.

VII. Wymagania dotyczące równoważności

1. Cechy ogólne

1. System do szyfrowania danych musi realizować w szczególności następujące funkcjonalności:
   a) szyfrowanie dysków twardych w sposób transparentny dla systemu operacyjnego zainstalowanego na stacji roboczej i pracujących na nim użytkowników, z funkcjonalnością uwierzytelnienia użytkownika bezpośrednio po uruchomieniu stacji roboczej, przed wystartowaniem właściwego systemu operacyjnego (tzw. Pre-boot authentication, PBA);
   b) szyfrowanie plików i katalogów w ramach lokalnego systemu operacyjnego na stacji roboczej;
   c) umożliwiać uwierzytelnienie użytkownika chcącego skorzystać z zaszyfrowanych danych;
   d) szyfrowanie danych kopiowanych na nośniki zewnętrzne;
   e) musi umożliwiać pobranie danych o użytkownikach do Systemu z serwera usług katalogowych Novell eDirectory w wersji 8.7.3 jak i w nowszych wersjach.
2. Oprogramowanie do szyfrowania danych musi się integrować z istniejącym już w infrastrukturze NIK serwerem do zarządzania bezpieczeństwem stacji roboczych i serwerów – tj. serwerem McAfee ePO 4.6, a w przyszłości z nowymi wersjami, co najmniej w następującym zakresie (rozwiązanie to musi być zarządzane przez rozwiązanie McAfee ePO):
   a) musi być możliwe wykorzystanie infrastruktury McAfee ePO do wykonania zdalnej instalacji oprogramowania szyfrującego na wybranych stacjach roboczych;
   b) musi być możliwe raportowanie z wykorzystaniem McAfee ePO, stanu oprogramowania na stacjach roboczych;
   c) musi być możliwe uzyskanie raportu podsumowującego, które stacje robocze objęte zarządzaniem McAfee ePO nie są objęte szyfrowaniem danych – raport taki musi być generowany okresowo i na żądanie.
3. Centralny serwer zarządzania Systemu musi mieć możliwość pracy na systemie operacyjnym Microsoft Windows Server 2008 R2 i wykorzystywać bazę danych Microsoft SQL Server 2008 R2.
4. System musi bezproblemowo funkcjonować w infrastrukturze sieciowej Zamawiającego.
5. Wszelkie koszty zwłaszcza związane ze sprzętem, dostosowaniem, konfiguracją oraz pracami związanymi z wdrożeniem, migracją, dokumentacją powykonawczą, i szkoleniem służb IT oraz wszystkich pracowników Zamawiającego wraz z dostarczeniem materiałów szkoleniowych i dokumentacji powdrożeniowej, w przypadku zaoferowania rozwiązania równoważnego, ponosi Wykonawca.

2. Oprogramowanie do szyfrowania danych

1. Oprogramowanie musi zapewniać centralne zarządzanie, w oparciu o centralną bazę danych, gdzie przetrzymywane są informacje o użytkownikach, kluczach i politykach szyfrowania.
2. Oprogramowanie zainstalowane na stacjach roboczych musi komunikować się z Centralnym serwerem zarządzającym z wykorzystaniem protokołów opartych na TCP/IP (wykorzystanie SSL-a lub TLS-a).
3. Komunikacja między Oprogramowaniem zainstalowanym na stacjach roboczych a Centralnym serwerem zarządzającym powinna być możliwa poprzez sieci rutowalne, w tym sieć Internet bez dodatkowych nakładów w postaci zewnętrznego systemu VPN.
4. Komunikacja między Oprogramowaniem zainstalowanym na stacjach roboczych a Centralnym serwerem zarządzającym musi być zabezpieczona przez zastosowanie szyfrowania.

5. Komunikacja między Oprogramowaniem zainstalowanym na stacjach roboczych a Centralnym serwerem zarządzającym musi być chroniona poprzez obustronne uwierzytelnienie przed atakiem typu „man-in-the-middle" polegającym na wstawieniu do sieci nieautoryzowanego serwera zarządzania.

2.1. SZYFROWANIE DANYCH

1. Oprogramowanie musi umożliwiać obsługę szyfrowania dysku twardego w sposób transparentny dla użytkownika i systemu operacyjnego zainstalowanego na stacji roboczej włączając w to szyfrowanie wszystkich plików także tymczasowych, swap, danych użytkownika bez konieczności ręcznej ingerencji użytkownika.
2. Oprogramowanie musi mieć możliwość ręcznego wskazania partycji dysku, która ma podlegać szyfrowaniu.
3. Oprogramowanie musi obsługiwać tryb automatycznego szyfrowania wszystkich partycji dysku bez konieczności ręcznego wskazania ich przez Użytkownika lub Administratora.
4. Oprogramowanie musi mieć możliwość wyboru algorytmu szyfrowania danych – wśród opcji do wyboru musi się znaleźć AES 256 bit i minimum 2 inne korzystające z klucza o długości większej niż 128 bitów.
5. Oprogramowanie musi posiadać obsługę algorytmów szyfrowania posiadających certyfikat FIPS 140-2.
6. Oprogramowanie musi posiadać Certyfikację Common Criteria EAL4 dla oferowanych produktów do szyfrowania danych.
7. Uwierzytelnienie Użytkownika ma być możliwe z wykorzystaniem hasła i nazwy użytkownika, ale także z użyciem tokenów i smart cards.
8. Proces uwierzytelnienia Użytkownika musi umożliwiać mu wybór sposobu uwierzytelnienia (nazwa-hasło, token/smart-card) w zakresie określonym przez administratora.
9. Po poprawnym uwierzytelnieniu Użytkownika procesy szyfrowania i deszyfrowania danych na dysku i w ramach systemu operacyjnego nie mogą mieć wpływu na normalne działania aplikacji, z których korzysta Użytkownik na stacji roboczej.
10. Szyfrowanie plików i katalogów musi być realizowane z poziomu systemu operacyjnego Windows XP, Windows Vista i Windows 7.
11. Centralny serwer zarządzający musi umożliwiać wskazanie katalogów lokalnych na stacjach roboczych, które obligatoryjnie podlegają szyfrowaniu.
12. Centralny serwer zarządzający musi zapewniać nadanie uprawnienia dla wybranego użytkownika lub grup użytkowników do samodzielnego wskazania plików, które mają podlegać szyfrowaniu i wyboru klucza, którym wykonane zostanie szyfrowanie.
13. System musi umożliwiać szyfrowanie plików na udziałach sieciowych udostępnianych przez serwery plików Windows. Szyfrowanie udziałów sieciowych nie może wymagać instalowania oprogramowania szyfrującego na serwerze plików
14. Podczas przenoszenia szyfrowanych plików między stacja roboczą a sieciowym udziałem dyskowym w trakcie całej transmisji w sieci pliki muszą pozostawać zaszyfrowane.
15. Centralny serwer zarządzający musi posiadać centralne generowanie i przechowywanie kluczy używanych do szyfrowania plików i katalogów, z opcją generacji kluczy lokalnie przez wskazanych przez administratora użytkowników lub grupy użytkowników.
16. Oprogramowanie szyfrujące pliki i foldery musi umożliwiać integrację z Windows Explorer umożliwiająca użytkownikowi przez kliknięcie myszą na wybranych plikach lub katalogach:
    a) wskazanie plików, które mają być zaszyfrowane;

b) stworzenie samorozpakowującego się, zaszyfrowanego archiwum chronionego hasłem wybranym przez użytkownika;

c) wywołanie funkcji „zaszyfruj i wyślij mailem".

17. Oprogramowanie szyfrujące pliki i foldery musi umożliwiać modyfikację ikony oznaczające plik/katalog dla zaznaczenia, że jest on zaszyfrowany.

2.2. DOSTĘP I UWIERZYTELNIENIE

1. Oprogramowanie musi umożliwiać określenie co najmniej 500 użytkowników, którzy mają prawo korzystać ze stacji roboczej gdzie wykonane jest szyfrowanie dysków.
2. Musi być możliwość przypisania do stacji roboczej pojedynczych użytkowników i grup użytkowników.
3. Zmiany hasła użytkownika na jednej maszynie muszą być automatycznie powielane i synchronizowane na pozostałych stacjach roboczych, do których jest przypisany ten użytkownik w przypadku kiedy dostępny jest Centralny serwer zarządzający.
4. Oprogramowanie musi umożliwiać, w systemie Windows XP, obsługę trybu SSO „single sign-on". Użytkownik wykorzystuje podczas PBA „pre-boot authentication" te same dane (nazwa użytkownika i hasło), które stosuje logując się do klienta Novell zainstalowanego na stacji roboczej i w drugiej kolejności do Windows.
5. Po zalogowaniu się w trybie „pre-boot authentication" (PBA) użytkownik nie musi już logować się po raz kolejny korzystając z klienta Novell.
6. W trybie „single sign-on" hasło użytkownika w trybie pre-boot authentication musi się automatycznie synchronizować ze zmianami hasła wykonanymi przez użytkownika na stacji roboczej.
7. Użytkownik musi być uwierzytelniany w następujących sytuacjach:
   a) przed startem Windows;
   b) przed dostępem do Windows po uruchomieniu wygaszacza ekranu;
   c) po wylogowaniu z Windows i podczas ponownego logowania do systemu.
8. Musi być możliwa obsługa kart typu smart cards i tokenów USB w trybie „pre-boot authentication" i przez oprogramowanie szyfrujące pliki i foldery w Windows.
9. System musi umożliwiać centralne zarządzanie jakością haseł używanych przez użytkowników przy uwierzytelnianiu się w PBA „pre-boot authentication" przez określenie minimum:
   a) długości hasła;
   b) zawartość hasła (znaki numeryczne i alfanumeryczne, symbole);
   c) ograniczenie stosowania haseł, które były już wcześniej wykorzystywane (historia hasła);
   d) wymuszenie zmiany hasła przez użytkownika.
10. Musi być opcja umożliwiająca blokowanie dostępu do konta użytkownika po zdefiniowanej liczbie nieprawidłowych prób podania danych użytkownika.

2.3. ZARZĄDZANIE KLUCZAMI DO SZYFROWANIA

1. System musi zapewnić centralne przechowywanie kluczy użytych do szyfrowaniu danych na Centralnym serwerze zarządzającym i możliwość odzyskania zaszyfrowanych danych z ich wykorzystaniem w sytuacji awarii.
2. Baza zawierająca klucze musi być chroniona przez zaszyfrowanie z wykorzystaniem algorytmu symetrycznego opartego na kluczu o długości minimum 256 bitów.

3. Dostęp do bazy i zawartych w niej danych musi wymagać uwierzytelnienia.
4. Musi być możliwość centralnego zdefiniowania uprawnień poszczególnych użytkowników do operacji na kluczach użytych do szyfrowania danych.
5. System musi umożliwiać zresetowanie hasła zapomnianego przez użytkownika bez konieczności otwierania połączenia zdalnego do stacji roboczej lub ze stacji roboczej do serwera zarządzającego.
6. Użytkownik, który stracił token (klucz USB lub smart card) musi mieć możliwość, po rekonfiguracji odpowiednich ustawień, wykorzystania nazwy/hasła bez konieczności otwierania połączenia zdalnego do stacji roboczej lub ze stacji roboczej do serwera zarządzającego.
7. Każda stacja robocza musi posiadać swój unikalny klucz wykorzystywany do szyfrowania wewnętrznego dysku twardego – zaszyfrowany dysk nie może być odczytany na innej stacji roboczej nawet, jeśli jest na niej zainstalowany taki sam agent do szyfrowania.
8. Musi istnieć możliwość użycia kluczy wykorzystywanych do szyfrowania plików i katalogów także w sytuacji, kiedy stacja robocza jest odłączona od sieci (tryb off-line).
9. Musi istnieć możliwość ograniczenia dostępu do kluczy do szyfrowania/deszyfracji plików i katalogów tylko w sytuacji, kiedy stacja robocza jest podłączona do sieci i ma dostęp do serwera zarządzającego (wymuszenie pracy z danymi szyfrowanymi w trybie on-line).

2.4. ODTWARZANIE DANYCH W RAZIE AWARII

1. W sytuacji zablokowania lub usunięcia oprogramowania szyfrującego zainstalowanego na stacji roboczej użytkownika musi być dostępny mechanizm i narzędzie bezpiecznego odzyskania zaszyfrowanych danych oraz odinstalowania oprogramowania szyfrującego przez Administratora.
2. Oprogramowanie szyfrujące musi kontynuować pracę po niespodziewanym zaniku zasilania, bez wpływu na możliwość zaszyfrowania i odszyfrowania danych.
3. Operacje szyfrowania i deszyfracji muszą pozostawać bezpieczne w sytuacji nagłego zaniku zasilania.
4. Dane zaszyfrowane w szczególności na dysku twardym, oraz na nośnikach zewnętrznych muszą pozostawać nadal zaszyfrowane nawet w sytuacji niespodziewanego zaniku zasilania.

2.5. FUNKCJE ADMINISTRACYJNE

1. System musi zapewniać możliwość centralnej konfiguracji jego parametrów, w tym centralne ustalanie polityki szyfrowania dla Użytkowników i stacji roboczych.
2. Musi istnieć możliwość obsługi wielu poziomów administracji (minimum 30) – wyższy poziom administracji umożliwia zarządzanie wyłącznie niższymi poziomami.
3. Musi istnieć możliwość obsługi różnych ról administratorów, których zakres może być szczegółowo definiowany w zakresie poszczególnych zadań (w szczególności: dodanie użytkownika, dodanie/usunięcie użytkownika do/z grupy, definiowanie grup użytkowników, dodanie stacji roboczej, zmiana polityki szyfrowania dysków i nośników zewnętrznych, generowanie raportów z działania systemu, zmiana hasła użytkownika, usunięcie użytkownika, usunięcie stacji roboczej, usunięcie klucza, itp.).
4. Musi istnieć możliwość oddzielenia zarządzania kluczami do szyfrowania danych od innych ról administracyjnych.
5. Musi istnieć możliwość określenia grup użytkowników, które podlegają administracji przez danego administratora.
6. Musi istnieć możliwość ochrony przed dostępem do bazy danych serwera zarządzającego przez nieuprawnionych użytkowników i administratorów.

7. Stacje robocze muszą automatycznie synchronizować zmiany w politykach szyfrowania i parametrach systemu bez konieczności interwencji administratora.
8. Musi być zapewniona możliwość wymuszenia z poziomu serwera zarządzającego synchronizacji polityki przez stacje robocze.
9. Uaktualnienia polityk szyfrowania i parametrów konfiguracji systemu mają się odbywać poprzez protokół/protokoły oparte na TCP/IP ze zdefiniowanymi wymaganiami konfiguracji dla firewall znajdujących się na drodze między stacją roboczą a Centralnym serwerem zarządzającym.
10. Musi istnieć możliwość obsługi mechanizmu zmiany/odzyskiwania hasła i tokenu bez konieczności wykorzystywania najwyższych przywilejów administratora.
11. Wszyscy administratorzy systemu muszą mieć swoje, niezależne konta dostępu do Systemu.
12. System musi zapisywać historię czynności wykonywanych w Systemie.
13. Zmiany w konfiguracji oprogramowania systemu szyfrowania przez Użytkowników muszą być zablokowane.

2.6. WDROŻENIE SYSTEMU SZYFROWANIA

1. Instalacja oprogramowania na stacjach roboczych musi się odbywać z wykorzystaniem pojedynczego pliku zawierające niezbędne moduły i opcjonalnie parametry polityki szyfrowania.
2. Musi być jeden, ten sam plik instalacyjny niezależnie od wersji i rodzaju systemu operacyjnego zainstalowanego na stacjach roboczych.
3. Musi być zapewnione wsparcie dla różnych systemów dystrybucji oprogramowania (wymagane McAfee ePO 4.6 i nowsze oraz Novell ZenWorks).
4. Instalacja oprogramowania na stacji roboczej powinna się odbywać bez interwencji Użytkownika.
5. Aktualizacje oprogramowania zainstalowanego na stacjach roboczych powinny być wykonywane automatycznie poprzez szyfrowane połączenia, bez konieczności wdrażania dodatkowych systemów VPN.

2.7. ODTWARZANIE DANYCH I UŻYTKOWNIKÓW W RAZIE AWARII

1. Oprogramowanie musi zawierać aplikację opartą na przeglądarce internetowej służącą do zmiany przez helpdesk lub administratorów haseł użytkowników i odblokowania stacji roboczych zablokowanych po niepoprawny podaniu hasła przez użytkownika.
2. Aplikacja do odzyskiwania haseł, która korzysta z przeglądarki internetowej powinna posiadać własny serwer WWW. Zamawiający wymaga jej prawidłowego działania co najmniej w przeglądarce Internet Explorer.
3. Oprogramowanie musi umożliwiać odzyskanie danych zaszyfrowanych w sytuacji jego uszkodzenia (uszkodzona pre-boot authentication, atak wirusa, itp.).
4. Nie może być możliwe zablokowanie przez użytkownika dostępu do danych uprawnionemu administratorowi.

2.8. AUDYTY I RAPORTOWANIE

1. Rejestr wszystkich zdarzeń „logon” i „BOOT” na stacjach roboczych musi być centralnie dostępny w celach audytowych.

2. Administrator musi mieć możliwość wyeksportowania logów audytowych w celu ich późniejszej analizy w uniwersalnych formatach: csv, xml, http.
3. Możliwość oglądania i eksportu logów do audytu powinna być zarezerwowana dla określonych administratorów.
4. Powinna istnieć możliwość wyczyszczenia informacji audytowych dla wszystkich obiektów dotyczących zdarzeń przed określoną datą w przeszłości.
5. System musi umożliwiać generowanie raportów dotyczących w szczególności: stanu systemu, wersji użytych produktów, przypisania użytkowników do stacji roboczej, statusu szyfrowania dysków na poszczególnych stacjach roboczych.
6. Raporty powinny być generowane na żądanie, ale powinna istnieć możliwość określenia zakresu raportu i częstotliwości jego automatycznego generowania.
7. System musi umożliwić współpracę z wykorzystywanym przez Zamawiającego serwerem zarządzania McAfee ePO 4.6 dla opracowania raportów dotyczących co najmniej: statusu systemu szyfrowania (zainstalowany, aktywowany), listy stacji objętych szyfrowaniem i tych gdzie szyfracja nie jest wdrożona i gdzie nie jest aktywna.

2.9. WYMAGANIA TECHNICZNE

1. System szyfrowania dysków musi zapewnić obsługę następujących systemów operacyjnych (w oparciu o tego samego klienta systemu szyfrowania):
   a) Microsoft Windows XP Professional SP3 (32-bit);
   b) Microsoft Windows Vista (32-bit i 64-bit);
   c) Microsoft Windows 7 (32-bit i 64-bit).
2. System szyfrowania plików i katalogów musi zapewnić obsługę następujących systemów operacyjnych (w oparciu o tego samego klienta systemu szyfrowania):
   a) Microsoft Windows XP Professional SP3 (32-bit);
   b) Microsoft Windows Vista (32-bit i 64-bit);
   c) Microsoft Windows 7 (32-bit i 64-bit).
3. Wielkość pakietu instalacyjnego dla oprogramowania instalowanego na stacjach roboczych użytkowników nie może przekraczać 10MB.
4. Aktualizacja oprogramowania szyfrującego nie może wymagać deszyfracji danych i ponownego ich szyfrowania.

2.10. INTEGRACJA Z SERWERAMI USŁUG KATALOGOWYCH

1. Wraz z systemem szyfrowania musi być dostępny konektor/konektory umożliwiający pobranie danych o użytkownikach do systemu szyfrowania z zewnętrznego serwera usług katalogowych.
2. Wymagane jest wsparcie dla następujących rodzajów serwerów usług katalogowych:
   a) Novell eDirectory;
   b) LDAP;
   c) Active Directory.
3. Zastosowanie konektora i pobranie danych z serwera usług katalogowych nie może mieć wpływu na uprawnienia użytkowników i administratora serwera usług katalogowych ani nie może wymagać zmian w jego schemacie.

4. Zmiany użytkowników i ich parametrów dokonywane na serwerze usług katalogowych powinny być automatycznie uwzględniane przez serwer zarządzający systemem szyfrowania.
5. Usunięcie użytkownika w serwerze usług katalogowych musi skutkować automatycznym usunięciem użytkownika w serwerze zarządzającym systemem szyfrowania.

2.11. AUTOMATYZACJA Z WYKORZYSTANIEM SKRYPTÓW

1. Musi być dostępne API lub narzędzie skryptowe umożliwiające automatyzację wybranych zadań administracyjnych i obsługi systemu szyfrowania.
2. System musi posiadać obsługę skryptów z linii komend i plików wsadowych (batch files).
3. System musi posiadać obsługę plików com / xml / DCOM.

2.12. DODATKOWE WYMAGANIA

1. Razem z instalacją oprogramowania serwera zarządzającego musi być instalowany system plików pomocy dostępny dla administratorów.
2. Proces szyfrowania dysku nie może pogarszać wydajność stacji roboczej o więcej niż 20% i musi zapewniać wydajność szyfrowania na poziomie nie mniejszym niż 20GB na godzinę (stacja robocza z Pentium IV 2.5GHz, 512MB RAM, HDD SATA).
3. Baza danych serwera zarządzającego musi być dostosowana do okresowego wykonywania kopii zapasowych z wykorzystaniem użytkowanego przez Zamawiającego systemu IBM TSM lub własnego mechanizmu producenta dostępnego bez dodatkowych kosztów dla Zamawiającego.
4. Musi być możliwość pobierania i zapisywania plików np. z Internetu, innej stacji roboczej, itp. do zdefiniowanego polityką folderu automatycznie szyfrowanego, a następnie użytkownik musi mieć możliwość odszyfrowywania takich danych po wcześniejszym ich przeniesieniu do folderu nieobjętego taką polityką.
5. Dostępny w dostarczonym Systemie moduł archiwizacyjny musi umożliwiać wykonywanie kopii w trybie przyrostowym.
6. System musi umożliwiać przeprowadzenie zdalnej instalacji aktualizacji do systemu operacyjnego Windows zainstalowanego na stacji roboczej, bez obecności użytkownika, z wykorzystaniem mechanizmu WOL (Wake On LAN).

2.13. INTEGRACJA SYSTEMU Z INNYMI PRODUKTAMI

1. Oprogramowanie do szyfrowania danych musi bezproblemowo współpracować z McAfee HIPS 7 i nowszymi wersjami.
2. Oprogramowanie do szyfrowania danych musi bezproblemowo współpracować z McAfee VSE 8.7i i nowszymi wersjami.
3. Oprogramowanie do szyfrowania danych musi bezproblemowo współpracować z klientem Novell i Novell ZENWorks dla Microsoft Windows XP, Microsoft Windows Vista, Microsoft Windows 7 i nowszymi wersjami.
4. Oprogramowanie do szyfrowania danych musi bezproblemowo współpracować klienta pocztowym Novell GroupWise 8 i nowszymi wersjami.

3. Zakres produktu Maintenance producenta oprogramowania

3.1. PRODKT MAINTENANCE NA SYSTEM DO SZYFROWANIA DANYCH NA POZIOMIE GOLD SUPPORT

Elementy, które muszą być oferowane, bez dodatkowych kosztów, przez producenta proponowanego oprogramowania w ramach produktu Maintenance na poziomie Gold Support:

1. Dostęp do najnowszych wersji oprogramowania wchodzącego w skład zakupionego pakietu.
2. Dostęp do informacji o aktualizacjach i poprawkach do oprogramowania przez system automatycznych powiadomień przez email.
3. Dostęp przez Internet do bazy wiedzy o produktach i technologiach producenta oferowanego oprogramowania.
4. Dostęp do narzędzia umożliwiającego automatyczne rozwiązanie wielu popularnych problemów.
5. Możliwość otwarcia zgłoszenia serwisowego przez chat i poprzez Web portal producenta oraz możliwość monitorowania obsługi zgłoszenia.
6. Dostęp online do dokumentacji i opracowań typu FAQ na temat każdego z produktów.
7. Dostęp do poradników wideo prezentujących produkty i sposoby ich konfiguracji.
8. Powiadomienia o zmianach w otartych zgłoszeniach serwisowych.
9. Dostęp do podcastów i blogów dotyczących oferowanego oprogramowania.
10. Nielimitowana liczba otwieranych zgłoszeń i połączeń do pomocy technicznej producenta oferowanego oprogramowania.
11. Regularne aktualizacje na temat zmian w statusie otwartych zgłoszeń serwisowych realizowana przez system zgłoszeń producenta.
12. Zdalna analiza problemów oraz dostęp do narzędzi analizujących problem.
13. 24/7 pomoc telefoniczna ze strony producenta oferowanego oprogramowania.
14. Komunikacja przez chat, email i telefoniczna z pomocą techniczną producenta oferowanego oprogramowania wraz z możliwością nawiązania zdalnych sesji i zdalnego dostępu do komputera Zamawiającego.
15. Dostęp do narzędzi do wykonywania automatycznej diagnostyki i naprawiania problemów.
16. Dostęp do materiałów na temat produktów i technologii (baza wiedzy, dokumentacje).
17. Dostęp przez Internet do środowiska testowego z produktami producenta oferowanego oprogramowania.
18. Dostęp przez Internet do środowiska testowego dla testów produktów i ich konfiguracji.
19. Dostęp do wersji ewaluacyjnych produktów.
20. Możliwość zgłaszania propozycji zmian w funkcjonalności produktów.