Toruń, dn. 26.11.2019

Urząd Miasta Torunia
Biuro Projektów Informatycznych
Ul. Wały gen. Sikorskiego 8
e-mail: zp_bpi@um.torun.pl

--- Wg. rozdzielnika ---

Zapytanie ofertowe poniżej 30 000 Euro
nr BPI/3400/66/2019

postępowanie o udzielenie zamówienia publicznego o wartości nieprzekraczającej 30 000 euro prowadzone jest poza przepisami ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych, (tekst jednolity Dz.U. z 2017r., poz. 1579) zgodnie z zarządzeniem nr 9 PMT z dnia 09.01.2018 r w sprawie zasad udzielania zamówień publicznych w Urzędzie Miasta Torunia

Biuro Projektów Informatycznych
Urząd Miasta Torunia
87-100 Toruń
ul. Wały gen. Sikorskiego 8

zwraca się z prośbą o przygotowanie oferty na: Zakup pakietu licencji ESET Endpoint Encryption lub równoważnego -50 licencji stanowiskowych z możliwością rozszerzenia do 100, bezterminowa, z serwisem 1-rocznym;

(Treść opisu przedmiotu zamówienia stanowi załącznik nr 2 do Zapytania ofertowego).

1. Proszę podać jako kryterium 1: ryczałtową cenę **netto i brutto w złotych**
2. Wraz z ofertą Oferent złoży wypełniony formularz oferty – załącznik nr 1.
3. Wraz z ofertą Oferent złoży aktualny pełny odpis z KRS bądź z CEiDG.
4. Termin realizacji: Zamawiający oczekuje realizacji zadania w terminie do 15.12.2019r
5. Kryterium wyboru ofert: Dla porównania ofert zostaną zastosowane kryteria:
   a) Kryterium 1: Cena – 100%
   Za korzystniejszą ofertę zostanie uznana oferta, która otrzyma największą liczbę punktów stanowiących sumę punktów za kryterium a)
   Każda oferta może uzyskać za dane kryterium określoną liczbę punktów przy zastosowaniu wzorów:
   a) Kryterium 1:

$$\text{cena oferty} = \frac{\textit{najniższa oferowana cena spośród złożonych ofert}}{\textit{cena oferty badanej}} \times \text{znaczenie kryterium tj. 100 \%}$$

6. Miejsce składania ofert: Ofertę proszę dostarczyć do Biura Projektów Informatycznych UMT ul. Wały gen. Sikorskiego 8 pok. 62, osobiście lub na adres e-mail (np. w formacie PDF): zp_bpi@um.torun.pl
7. Warunki płatności: przelew, **21 dni od dnia dostarczenia faktury**.
8. Termin składania ofert: do 03.12.**2019r. do godz. 12:00 (decyduje godzina otrzymania oferty przez Zamawiającego)**
9. Wykonawca, który prowadzi jednoosobową działalność gospodarczą zobowiązany jest dołączyć do oferty oświadczenie czy w swojej jednoosobowej działalności:
   - zatrudnia / nie zatrudnia pracowników
   - zawiera / nie zawiera umowy ze zleceniobiorcami
10. Wymagania i warunki Zamawiającego:
    a) Zamawiający nie dopuszcza składania ofert wariantowych, chyba, że zostało wskazane inaczej.
    b) Zamawiający nie dopuszcza składania ofert częściowych, chyba, że zostało wskazane inaczej.
    c) W celu zapewnienia porównywalności wszystkich ofert, Zamawiający zastrzega sobie prawo do skontaktowania się z Oferentami w celu uzupełnienia lub doprecyzowania ofert.
    d) Z wyłonionym Wykonawcą zostanie zawarta pisemna umowa zgodnie z procedurami obowiązującymi w UMT. Umowa do podpisania zostanie wysłana do Wykonawcy w formie elektronicznej i papierowej.
    e) Zamawiający zastrzega sobie prawo odstąpienia bądź unieważnienia zapytania ofertowego bez podania przyczyny w przypadku zaistnienia okoliczności nieznanych Zamawiającemu w dniu sporządzania niniejszego zapytania Ofertowego.
    f) Zamawiający zastrzega sobie prawo odstąpienia bądź unieważnienia zapytania ofertowego bez podania przyczyny na każdym etapie postępowania do zawarcia umowy.
    g) Ze względu na założenia budżetowe i ograniczenia finansowe, w przypadku, gdy kwoty przedstawione w ofertach na zapytanie będą wyższe od zaplanowanych w budżecie na ww. zadanie Zamawiający zastrzega sobie prawo odstąpienia bądź unieważnienia zapytania ofertowego bez negocjacji z Oferentami.
    h) Oferent może złożyć wyłącznie jedną ofertę.
    i) Oferent może wprowadzić zmiany w złożonej ofercie lub ją wycofać, pod warunkiem, że uczyni to przed upływem terminu składania ofert. Zarówno zmiana jak i wycofanie oferty wymagają zachowania formy pisemnej.
    j) Oferty złożone po terminie nie zostaną rozpatrzone.
    k) Oferenci uczestniczą w postępowaniu ofertowym na własne ryzyko i koszt, nie przysługują im żadne roszczenia z tytułu odstąpienia przez Zamawiającego od postępowania ofertowego.
    l) Oferenci biorący udział w postępowaniu zostaną poinformowani o wynikach postępowania pisemnie (drogą elektroniczną).
    m) Zamawiający zastrzega sobie możliwość wyboru kolejnej wśród najkorzystniejszych ofert, jeżeli oferent, którego oferta zostanie wybrana jako najkorzystniejsza, uchyli się od zawarcia umowy w przedmiocie realizacji niniejszego zamówienia.
    n) Oferenci mogą zwrócić się do Zamawiającego o wyjaśnienie treści zapytania ofertowego drogą elektroniczną na adres e-mail: zp_bpi@um.torun.pl
    o) Ewentualne pytania dotyczące postępowania wraz z odpowiedziami Zamawiającego będą publikowane na BIP Zamawiającego.
11. Niniejsza oferta nie stanowi oferty w myśl art. 66 Kodeksu Cywilnego, jak również nie jest ogłoszeniem w rozumieniu ustawy Prawo zamówień publicznych.

12. Zaproszenie nie jest postępowaniem o udzielenie zamówienia publicznego w rozumieniu przepisów Prawa zamówień publicznych oraz nie kształtuje zobowiązania Zamawiającego do przyjęcia którejkolwiek z ofert. Zamawiający zastrzega sobie prąwo do rezygnacji z zamówienia bez wyboru którejkolwiek ze złożonych ofert.
13. Zamawiający, w przypadku wpłynięcia jednej oferty, zastrzega sobie prawo do negocjacji warunków zamówienia oraz ceny za jego wykonanie, a także do rezygnacji z zamówienia bez podania przyczyny.

DYREKTOR
Biura Projektów Informatycznych
Mariusz Szefera

Załącznik 1

PRZEDMIOT ZAMÓWIENIA	Zakup pakietu licencji ESET Endpoint Encryption lub równoważnego - 50 licencji stanowiskowych z możliwością rozszerzenia do 100, bezterminowa, z serwisem 1-rocznym; .....
ZAMAWIAJĄCY	Gmina Miasta Toruń - wydział prowadzący – Biuro Projektów Informatycznych UMT .....
WYKONAWCA **Adres** **Numer telefonu / fax** **Internet http: //** **e-mail**	
Kryterium 1. CENA OFERTY NETTO / BRUTTO * (z obowiązującym podatkiem VAT)	Cyfrowo netto: ..... Cyfrowo brutto: ..... Słownie brutto: .....
Osoba uprawniona do podpisania umowy	.....
Osoba uprawniona do podpisania protokołu odbioru	.....
Adres e-mail służący do zgłaszania reklamacji	.....
Data **Podpis**	

1. Zakup pakietu licencji ESET Endpoint Encryption lub równoważnego - 50 licencji stanowiskowych z możliwością rozszerzenia do 100,bezterminowa, z serwisem 1-rocznym;
2. Dostawca przeprowadzi wdrożenie systemu w siedzibie Zamawiającego w terminie do 15.12.2019r
3. W ramach wdrożenia Wykonawca zapewni jednodniowe, nie krótsze niż 8 godzin, autoryzowane szkolenie z obsługi systemu dla 6 administratorów, przeprowadzone przez producenta oprogramowania w siedzibie Zamawiającego. Szkolenie zostanie przeprowadzone w terminie 2 tygodni od chwili podpisania umowy.

WYMAGANIA FUNKCJONALNE

Wymagania ogólne.

- Wymagana jest praca całego środowiska szyfrowania w architekturze klient – serwer
- Wymagane jest dostarczenie oprogramowania do instalacji serwera i konsoli centralnego zarządzania
- Wymagane jest dostarczenie oprogramowania szyfrującego do instalacji na stacjach klienckich
- Wymagana jest obsługa systemów operacyjnych z rodziny Microsoft Windows MS Windows 7/8/10 32-bit i 64-bit oraz w serwerowych systemach operacyjnych z rodziny MS Windows Server 2008 32-bit i 64-bit, MS Windows Server 2012-2019 64-bit
- Wymagane jest zarządzanie serwerem i konsolą poprzez przeglądarkę internetową
- Wymagane jest zdalne zarządzanie użytkownikami na stacjach klienckich oraz stacjami klienckimi, w tym współdzielenie kluczy szyfrujących, za pomocą połączeń internetowych i intranetowych
- Wymagana jest możliwość zdalnego zarządzania stacjami klienckimi będącymi poza siedzibą firmy
- Wymagane są bezpieczne połączenia ze stacjami klienckimi w oparciu o protokół HTTPS
- Wymagana jest możliwość tworzenia grup użytkowników w celu współużytkowania zdalnych zaszyfrowanych zasobów współdzielonych
- Wymagana jest możliwość tworzenia polityk bezpieczeństwa pozwalających zdalnie wdrażać reguły na wszystkich stacjach klienckich
- Wymagana jest możliwość tworzenia paczek MSI z poziomu serwera – dla celów przygotowania wersji preinstalacyjnej na stacje klienckie oraz wdrażania za pomocą GPO
- Wymagana jest możliwość zdalnego uruchomienia procesu szyfrowania
- Wymagane jest bezpieczne zdalne zarządzanie kluczami szyfrującymi użytkowników (dodawanie/usuwanie) z poziomu serwera, a także zmiany polityk w sposób niewidoczny dla użytkownika
- Do komunikacji stacji klienckich z serwerem centralnym wymagane jest zastosowania bezpiecznego serwera proxy, a samo połączenie szyfrowane ma być za pomocą algorytmów RSA lub AES przy użyciu bezpiecznego połączenia SSL
- Wymagany jest brak konieczności posiadania własnego certyfikatu SSL, wprowadzania zmian w sieci firmowej oraz specjalnej dodatkowej konfiguracji firewall'a
- Konsola administracyjna serwera zarządzającego powinna także udostępniać informacje o licencjach, poszczególnych politykach, kluczach szyfrujących, stacjach roboczych, użytkownikach
- Wymagana jest możliwość zdalnego odzyskania zapomnianego przez użytkownika hasła
- Wymagana jest możliwość wykorzystania struktury Active Directory
- Wymagane jest szyfrowanie całych powierzchni dysków twardych stacji klienckich (Full Disk Encryption)
- Wymagany jest mechanizm pre-boot authentication, umożliwiający autoryzację użytkownika jeszcze przed uruchomieniem systemu operacyjnego wykorzystujący 256-bitowy algorytm AES, zgodny ze standardami FIPS
- Wymagane jest szyfrowanie wybranych nośników wymiennych (całej powierzchni lub tylko jej części) podłączanych do stacji klienckich z zachowaniem dostępności całej pojemności nośnika dla użytkownika, realizowane w oparciu o mechanizm szyfrowania nośników wymiennych niewymagający rezerwowania dodatkowej przestrzeni dla zaszyfrowanych danych znajdujących się na nośniku
- Wymagane jest szyfrowanie nośników wymiennych w sposób umożliwiający dostęp do zaszyfrowanych danych na stacjach klienckich bez zainstalowanego oprogramowania szyfrującego np.: za pomocą specjalnej aplikacji dostarczanej na nośniku wymiennym umożliwiającej odczytanie zawartości bez instalacji programu
- Wymagana jest współpraca oprogramowania z każdym rodzajem nośników wymiennych – USB, CD, DVD
- Wymagane jest szyfrowanie plików i katalogów w lokalizacjach lokalnych i zdalnych
- Wymagane jest automatyczne szyfrowanie plików umieszczanych w zaszyfrowanych folderach
- Wymagana jest możliwość szyfrowania wybranych fragmentów tekstów w dokumentach lub całości tekstu i korespondencji email
- Wymagana jest możliwość szyfrowania poczty elektronicznej i jej zawartości (w tle)
- Wymagane jest automatyczne odszyfrowywanie poczty elektronicznej tylko przez adresata posiadającego taki sam klucz szyfrujący jak nadawca lub (na stacjach bez oprogramowania szyfrującego) odszyfrowanie za pomocą

hasła udostępnionego przez nadawcę oddzielnym i bezpiecznym kanałem komunikacji przy wykorzystaniu dostarczonego przez producenta oprogramowania deszyfrującego nie podlegającego licencjonowaniu
- Wymagana jest możliwość szyfrowania schowka
- Wymagane są zaawansowane algorytmy oraz standardy używane do generowania silnych kluczy szyfrujących
- Wymagana jest minimalna interakcja ze strony użytkownika
- Wymagana jest integracja oprogramowania z programem MS Outlook pozwalająca na szyfrowanie poczty elektronicznej oraz jej załączników bezpośrednio z poziomu programu pocztowego
- Wymagana jest możliwość tworzenia dysków wirtualnych (dodatkowo zaszyfrowane woluminy) i skompresowanych archiwów samorozpakowujących
- Wymagana jest możliwość nieodwracalnego usuwania plików
- Wymagana jest funkcja współdzielenia zaszyfrowanych zasobów pomiędzy wieloma użytkownikami
- Wymagana jest funkcja konta serwisowego administratora
- Wymagana jest funkcja procedury samodzielnego odzyskiwania hasła
- Wymagana jest funkcja jednorazowego tokenu do odzyskania hasła
- Wymagana jest funkcja wsparcia dla hibernacji komputera
- Wymagana jest funkcja ukrytego kontenera (folderu)
- Wymagana jest funkcja synchronizacji z AD
- Wymagane jest, aby oprogramowanie spełniało wymagania certyfikatu FIPS 140-2 level 1 i otrzymało tenże certyfikat
- Wymagane są dostępne w oprogramowaniu algorytmy i standardy: AES 256 bit; AES 128 bit; SHA 256 bit; SHA1 160 bit; RSA 1024 bit; Triple DES 112 bit; Blowfish 128 bit
- Wymagana jest całkowicie bezkonfliktowa współpraca oprogramowania szyfrującego z oprogramowaniem antywirusowym ESET Endpoint Antivirus i ESET Endpoint Security, które użytkuje Zamawiający

Wymagania funkcjonalne dotyczące konsoli centralnego zarządzania.

- Konsola centralnego zarządzania musi wspierać systemy operacyjne MS Windows 7/8/10 32-bit i 64-bit oraz w serwerowych systemów operacyjnych z rodziny MS Windows Server 2008 32-bit i 64-bit, MS Windows Server 2012-2019 64-bit
- Serwer konsoli centralnego zarządzania musi bezkonfliktowo funkcjonować wraz z oprogramowaniem antywirusowym ESET
- Konsola centralnego zarządzania musi umożliwiać centralne administrowanie klientami systemu szyfrowania danych dla systemów Microsoft Windows
- Konsola centralnego zarządzania dzięki wykorzystaniu bazy danych SQL ma stanowić centralną bazę informacji o klientach systemu szyfrowania danych, kluczach szyfrujących oraz użytkownikach
- Konsola centralnego zarządzania musi współpracować z bazą danych Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012 zarówno w wersji 32-bit i 64-bit oraz z Microsoft SQL Server 2005 Express Edition, Microsoft SQL 2008 Express Edition, Microsoft SQL Server 2012 Express Edition zarówno w wersji 32-bit i 64-bit
- Środowisko wymaga instalacji następujących składników: MS SQL w wersjach pełnych i Express; Apache od wersji 2 lub IIS od wersji 6; PHP od wersji 5.3
- Pakiet instalacyjny konsoli administracyjnej musi być wyposażony we wbudowane instalatory składników SQL Express, Apache oraz PHP
- Konsola centralnego zarządzania musi pozwalać na generowanie paczek instalacyjnych dla stacji końcowych na dwa różne sposoby: instalacja ręczna na kliencie; instalacja wypychana
- Komunikacja pomiędzy konsolą centralną zarządzania, a serwerem proxy musi odbywać się na bezpiecznym porcie 443 z użyciem SSL
- Administrator może w konsoli do zarządzania tworzyć wiele kluczy szyfrujących opartych o kilka algorytmów szyfrujących, co najmniej AES, DES, Blowfish
- Administrator powinien mieć możliwość tworzenia różnych użytkowników mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisywania im różnych ról
- Administrator powinien mieć możliwość tworzenia dodatkowych ról na podstawie opcji dostępnych w konsoli centralnego zarządzania
- Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła
- Powinna istnieć możliwość konfiguracji złożoności hasła do konsoli centralnego zarządzania, w tym: ilości znaków, czy hasło ma zawierać wielkie litery, czy hasło ma zawierać małe litery, czy hasło ma zawierać cyfry, czy hasło ma zawierać znaki specjalne, okres ważności hasła, ilość nieudanych logowań
- Administrator powinien mieć możliwość konfiguracji złożoności haseł dla użytkowników na stacjach roboczych

- Powinna istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w tym: ilości znaków, czy hasło ma zawierać wielkie litery, czy hasło ma zawierać małe litery, czy hasło ma zawierać cyfry, czy hasło ma zawierać znaki specjalne, okres ważności hasła, ilość nieudanych logowań, możliwość zmiany hasła
- Konsola centralnego zarządzania powinna gromadzić informacje o:
    - nazwach stacji roboczych, na których jest zainstalowany klient systemu szyfrowania danych
    - dacie ostatniej modyfikacji ustawień klienta systemu szyfrowania danych
    - dacie instalacji klienta systemu szyfrowania danych
    - statusu szyfrowania zastosowanego na stacji roboczej
    - typie urządzenia, na którym jest zainstalowany klient systemu szyfrowania danych
    - informacjach czy profil ustawień został zaktualizowany na stacjach roboczych
    - wersji klienta systemu szyfrowania danych
    - wersji systemu operacyjnego stacji roboczej
    - liczbie użytkowników uprawnionych do logowania do klienta systemu szyfrowania danych na stacji roboczej
- Konsola centralnego zarządzania powinna pozwalać na generowanie dla każdej ze stacji płyty ratunkowej
- Konsola musi być dostępna z poziomu przeglądarki internetowej
- Administrator powinien mieć możliwość zarządzania stacjami klienckimi, które mają dostęp do sieci Internet, niezależnie od tego, gdzie komputery w danym momencie się znajdują
- Administrator musi mieć możliwość konfiguracji automatycznego szyfrowania pełnej powierzchni dysku po wykonanej instalacji oprogramowania
- Serwer administracyjny musi posiadać możliwość automatycznej aktywacji licencji w ramach kont domenowych
- Administrator musi mieć możliwość wykonania poniższych czynności w sposób zdalny:
    - instalacji klienta na stacji
    - zaszyfrowania/odszyfrowania stacji
    - wygenerowania klucza aktywacyjnego dla użytkownika
    - zablokowania stacji
    - zablokowania użytkownika
    - administrowania kluczami szyfrującymi
    - administrowania użytkownikami, którzy mają dostęp do stacji
    - administrowania profilem ustawień dla użytkowników
    - administrowania profilem ustawień dla stacji roboczych
    - wymuszenia zmiany hasła
    - zarządzania wieloma organizacjami z poziomu jednej konsoli
- Wymagane jest, aby konsola zdalnego zarządzania była oferowana przez producenta oprogramowania do szyfrowania bez dodatkowych opłat licencyjnych, a ewentualna licencja na korzystanie z niej (jeśli jest wymagana) była zawarta w licencjach na oprogramowanie stacji klienckich

Wymagania systemowe aplikacji klienckiej.

- System szyfrowania danych musi wspierać instalacje aplikacji klienckiej w środowisku MS Windows 7/8/10 32-bit i 64-bit oraz w serwerowych systemach operacyjnych z rodziny MS Windows Server 2008 32-bit i 64-bit, MS Windows Server 2012-2019 64-bit
- System szyfrowania i aplikacja kliencka muszą bezkonfliktowo funkcjonować wraz z oprogramowaniem antywirusowym ESET
- Wymagana jest aplikacja kliencka z graficznym interfejsem użytkownika (GUI)
- Administrator musi mieć możliwość zainstalowania systemu szyfrowania danych w środowisku wirtualnym (VMware)
- System szyfrowania musi posiadać certyfikat FIPS 140-2 Level 1

Wymagania dotyczące uwierzytelniania.

- Wymagana jest autentykacja typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny
- System powinien umożliwiać określenie co najmniej 127 unikalnych użytkowników, którzy będą mieć dostęp do chronionej stacji roboczej na poziomie Pre-Boot
- System powinien umożliwiać przetrzymywanie co najmniej 64 kluczy szyfrujących w jednym pęku kluczy (key file)
- Dostęp do klucza powinien być chroniony przy pomocy hasła

- Administrator musi posiadać możliwość graficznej modyfikacji ekranu logowania (Pre-boot)

Wymagania dotyczące ustawień aplikacji klienckiej.

- Wymagana jest polska lokalizacja językowa aplikacji klienckiej, powinien też być oferowany język angielski
- System szyfrowania danych powinien umożliwiać zarządzanie z poziomu konsoli centralnego zarządzania
- Hasło dla użytkowników na stacjach roboczych powinno zawierać co najmniej poniższe założenia (w przypadku wersji centralnie zarządzanej): ilości znaków, czy hasło ma zawierać wielkie litery, czy hasło ma zawierać małe litery, czy hasło ma zawierać cyfry, czy hasło ma zawierać znaki specjalne, okres ważności hasła, ilość nieudanych logowań, możliwość zmiany hasła
- Defragmentacja dysku nie może mieć negatywnego wpływu na system szyfrowania
- System szyfrowania danych musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób: sektor po sektorze; kontener
- Wymagane jest, aby zaszyfrowany nośnik wymienny USB oraz nośnik CD/DVD mógł być odczytany także na dowolnej stacji, na której nie ma zainstalowanego klienta systemu szyfrowania - dostęp do takiego nośnika musi być udzielony po podaniu hasła
- Dostęp do zaszyfrowanych nośników wymiennych lub zaszyfrowanych nośników CD/DVD może być zabezpieczony hasłem
- System szyfrowania danych musi pozwalać na szyfrowanie wiadomości e-mail wraz z załącznikami
- System szyfrowania danych musi umożliwiać automatyczną deszyfrację otrzymywanych wiadomości e-mail
- System szyfrowania danych musi pozwalać na szyfrowanie całego tekstu aktywnego dokumentu, jego części a także zawartości schowka systemowego
- Zaszyfrowany tekst oraz zawartość schowka systemowego powinny mieć możliwość odczytania w wbudowanej w aplikację kliencką przeglądarkę
- Wymagane jest, aby zaszyfrowany tekst mógł być odczytany za pomocą darmowego narzędzia dostarczanego przez producenta oprogramowania na stacji bez zainstalowanego klienta systemu szyfrowania
- System szyfrowania danych powinien umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania
- System szyfrowania danych powinien umożliwiać wybór domyślnego klucza szyfrowania
- System szyfrowania danych powinien umożliwiać zaszyfrowanie obiektu z poziomu menu kontekstowego
- System szyfrowania danych powinien umożliwiać zaszyfrowanie obiektu z poziomu menu kontekstowego a następnie wysłanie go przy pomocy dedykowanego klienta pocztowego jako załącznik
- Wymagana jest funkcjonalność utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/odszyfrowanie całego tekstu aktywnego dokumentu, jego części a także zawartości schowka systemowego
- System szyfrowania danych powinien umożliwiać tworzenie wirtualnych partycji - dostęp do takich partycji ma być możliwy przy użyciu klucza szyfrującego lub hasła
- System szyfrowania danych powinien umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB
- System szyfrowania danych musi umożliwiać tworzenie zaszyfrowanego archiwum - dostęp do takiego archiwum ma być możliwy przy użyciu klucza szyfrującego lub hasła
- System szyfrowania danych powinien umożliwiać trwałe usuwanie danych za pomocą poniższych algorytmów: Guttman; US Department of Defence 5220.22-M (8-306. /E); US Department of Defence 5220.22-M (8-306. /E, CiE); Cryptographic Random Number Data
- Wymagane jest, aby dedykowana wtyczka wspierała co najmniej klientów pocztowych MS Outlook 2003 i nowszych, również dostępnych z poziomu Office 365
- System szyfrowania danych powinien umożliwiać automatyczne zalogowanie użytkownika do konsoli klienta systemu szyfrowania danych po uruchomieniu systemu operacyjnego
- System szyfrowania danych powinien umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności użytkownika w systemie
- System szyfrowania danych powinien posiadać opcję automatycznego odpytywania serwerów producenta o dostępność nowszych wersji
- Użytkownik powinien posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI

Wymagania dotyczące szyfrowania.

- System szyfrowania danych powinien umożliwiać szyfrowanie powierzchni dysku sektor po sektorze
- Szyfrowanie całej powierzchni dysku nie wymaga wykorzystania modułu TPM, w przypadku jego braku w urządzeniu

- System szyfrowania danych powinien umożliwiać wstrzymanie procesu szyfrowania powierzchni dysku i jego wznowienie. Po wznowieniu proces szyfrowania danych powinien rozpocząć się od momentu, w którym został przerwany
- System szyfrowania danych powinien umożliwiać wstrzymanie procesu szyfrowania w sytuacji, gdy laptop nie jest podłączony do zasilania. Proces szyfrowania powinien zostać wznowiony automatycznie po podłączeniu zasilacza
- System szyfrowania danych, oprócz szyfrowania całej powierzchni dysku, powinien posiadać możliwość szyfrowania pojedynczych plików, zawartości katalogów, pamięci przenośnych, wiadomości e-mail wraz z załącznikami, tekstu oraz schowka systemowego
- Wymagane jest wykorzystanie do szyfrowania poniższych algorytmów szyfrowania: AES (Rijndael); Blowfish; Triple DES (3DES)
- System szyfrowania danych powinien umożliwiać współpracę z dyskami SSD
- System szyfrowania danych powinien umożliwiać szyfrowanie danych na komputerach z UEFI
- Administrator ma mieć możliwość sprawdzenia przed zaszyfrowaniem całej powierzchni dysku, czy nie pojawią się problemy po ponownym uruchomieniu komputera
- Administrator ma mieć możliwość wybrania szyfrowania dodatkowych partycji dysku (niesystemowych)

Wymagania dotyczące sytuacji krytycznych.

- W przypadku utraty hasła, system szyfrowania danych powinien umożliwiać Administratorowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie zdefiniowanego wcześniej hasła administratora
- System szyfrowania danych powinien umożliwiać wygenerowanie płyty ratunkowej (dostępnej na nośniku wymiennym USB lub CD/DVD) z poziomu konsoli centralnego zarządzania
- W przypadku utraty hasła, system szyfrowania danych powinien umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie otrzymanego od administratora unikalnego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania

Wymagania dotyczące licencji na oprogramowanie, pakietów oprogramowania oraz wsparcia.

- Oprogramowanie powinno zawierać pakiet/pakiety instalatora stacji klienckiej oraz pakiet/pakiety instalatora serwera i konsoli centralnego zarządzania
- Instalator powinien zawierać wbudowane wszelkie niezbędne komponenty umożliwiające w pełni funkcjonalne uruchomienie środowiska szyfrowania danych i centralnego zarządzania nim
- Pakiety oprogramowania w trakcie dostawy, należy dostarczyć w najnowszej aktualnie oferowanej przez producenta wersji
- Wymagane jest dostarczenie bezterminowych licencji na oprogramowanie
- Wymagane jest, aby wraz z licencjami został dostarczony pakiet wsparcia serwisowego i aktualizacyjnego na okres 1 roku
- Wymagane jest wsparcie techniczne dostępne w języku polskim