Załącznik nr 1

Dotyczy zamówienia pn.:

„Dostawa zasilacza awaryjnego wraz z oprogramowaniem do ochrony danych osobowych, na potrzeby Urzędu Miejskiego w Trzebiatowie"

1. **Zasilacz awaryjny – 1 szt.**
   1) Oferowane urządzenie do bezprzerwowego zasilania, zwane dalej „urządzeniem", ma być fabrycznie nowe i ma pochodzić z seryjnej produkcji. Data jego wyprodukowania nie może być wcześniejsza niż 6 miesięcy przed terminem złożenia ofert.
   2) Producent oferowanego urządzenia powinien spełniać wymagania międzynarodowego standardu jakości ISO 9001, co powinno być potwierdzone ważnym certyfikatem.
   3) Dostawca urządzenia ma zapewnić dostawę części zamiennych przez okres co najmniej 7 lat od daty zakończenia produkcji oferowanego modelu urządzenia.
   4) Urządzenie powinno być wyprodukowane w kraju należącym do Unii Europejskiej.
   5) **Dane techniczne urządzenia:**
      a) Moc wyjściowa UPS-a **20 kVA / 20 kW,** w obszarze pracy współczynnika mocy obciążenia od 0,8 indukcyjny do 0,8 pojemnościowy.
      b) Konstrukcja UPS powinna być modułowa – moduł mocy 20kVA/20kW, z możliwością dołożenia drugiego modułu 20kVA/20kW w ramach tej samej szafy.
      c) Moduły mocy wymieniane „na gorąco" (Hot Swap) – w przypadku wymiany jednego z modułów, drugi pracuje bezprzerwowo w trybie podwójnej konwersji (online).
      d) Urządzenie ma być przystosowane do przyszłej rozbudowy w układzie pracy równoległej. Układ połączeń logicznych pomiędzy poszczególnymi UPSami nie może stanowić pojedynczego punktu awarii, to znaczy przerwanie połączenia logicznego między UPSami pracującymi równolegle nie może spowodować utraty funkcjonalności systemu zasilania gwarantowanego. Nawet w przypadku braku komunikacji logicznej, urządzenia zapewnią podtrzymanie zasilania przy zaniku napięcia z sieci (praca z falownika) z równomiernym obciążeniem wszystkich jednostek układu. *Opis powinien być materiałem firmowym producenta.*
      e) Ilość faz 3/3 trzy fazy wejściowe i trzy fazy wyjściowe
      f) Napięcie wejściowe – wyjściowe 3x400 V zgodne z wartościami zapisanymi w Polskiej Normie PN-IEC 60038, z tolerancją minimum 325V do 475V przy 100% obciążeniu bez korzystania z energii z baterii.
      g) Urządzenie powinno posiadać:
         - Wejście trójfazowe 5-cio przewodowe (TN-S)
         - Wyjście trójfazowe 5-cio przewodowe (TN-S)
      h) Częstotliwość wejściowa 50 Hz zgodna z wartościami zapisanymi w Polskiej Normie PN-IEC 60038 z tolerancją min. 40Hz do 72Hz.
      i) Urządzenie powinno zapewnić ciągłe bezprzerwowe zasilanie w trybie TRUE ON-LINE z podwójną konwersją przy zupełnych lub chwilowych zanikach napięcia i

wahaniach częstotliwości w sieci elektrycznej przez cały czas pracy urządzenia. Zgodnie z normą PN-EN 62040-3, urządzenie **klasy VFI-SS-111.**

j) Czas pracy autonomicznej urządzenia przy obciążeniu 20 kW musi wynosić co najmniej 20 minut. **Baterie muszą być umieszczone wewnątrz zasilacza UPS**.

k) Urządzenie powinno być wyposażone w dotykowy, graficzny wyświetlacz LCD, z komunikatami w języku polskim.

l) Wymiary urządzenia wraz z bateriami nie powinny przekraczać następujących wymiarów:

szer. max. 500 mm
gł. max. 770 mm
wys. max. 1800 mm

m) Poziom hałasu urządzenia nie może przekraczać 60dBA z odl. 1m.

n) Ciężar zasilacza UPS wraz z bateriami nie może być większy niż 520 kg.

o) Urządzenie powinno być wyposażone w system nieciągłego ładowania baterii. Do oferty należy dołączyć opis sposobu zarządzania pracą baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. *Opis powinien być materiałem firmowym producenta.*

p) Zasilacz musi być wyposażony w wewnętrzny elektroniczny układ obejściowy o mocy nie mniejszej niż 40kW oraz zewnętrzny mechaniczny (serwisowy) układ obejściowy, umożliwiający całkowite odstawienie jednostki UPS.

q) UPS powinien być wyposażony w układ zabezpieczający przed zwrotnym podaniem energii do sieci (backfeed protection, zgodnie z normą IEC 62040), w torze bypassu statycznego.

r) Urządzenie musi posiadać możliwość przełączenia pracy w tryb oszczędzający energię charakteryzujący się zapewnieniem zasilania odbiorników z tolerancją parametrów napięcia i częstotliwości ustawioną w torze obejściowym, z czasem przełączenia nie większym niż 2 ms w tryb pracy normalnej pozwalając na osiągniecie sprawności długookresowej na poziomie min. 98,4% przy obciążeniu liniowym w zakresie 50-100% mocy znamionowej.

s) Stabilizacja napięcia wyjściowego < 1% U_n przy obciążeniu statycznym, Stabilizacja napięcia wyjściowego < 4% U_n przy obciążeniu dynamicznym zmieniającym się od 0% do 100% i odwrotnie w czasie odbudowy maks. 100 ms.

t) Sprawność >= 95,8% w trybie TRUE ONLINE w przedziale 50%-100% obciążenia znamionowego.

u) Wejściowy współczynnik mocy cos φ min. 0,99, THDi nie wyższe niż 3%.

v) Wyjściowy współczynnik mocy cos φ = 1, TDHu wyjściowe dla obciążenia liniowego nie wyższe niż 1,5%.

w) Możliwość pracy z niesymetrycznym obciążeniem poszczególnych faz, w zakresie 0-100% obciążenia każdej fazy.

x) Urządzenie musi posiadać panel komunikacyjny, w którym powinny być zainstalowane:

- Gniazdo komunikacji RS-232,

- Gniazdo wyłącznika awaryjnego p.poż.
- Karta sieciowa Gigabit Ethernet/SNMP, obsługiwane protokoły MQTT/RNDIS/LDAP/NVD/SSH/PKI, szyfrowanie TLS 1.2/SHA 256, zgodność z normą cyberbezpieczeństwa UL 2900-2-2.

y) Wymagana deklaracja producenta zgodności produktu z normami: EN 62040-1: 2008, EN 62040-2: 2006 oraz spełnienia dyrektyw: 2006/95/EC i 2004/108/EC wraz z rokiem przyznania znaku CE

z) Gwarancja producenta: minimum 24 miesiące.

aa) Zamawiający po dostawie wykona pomiary i testy funkcjonalne potwierdzające spełnianie przez urządzenie zadeklarowanych parametrów układu zasilania. Jeżeli którykolwiek parametr nie zostanie spełniony Zamawiający rozwiąże umowę z Dostawcą zaś Dostawca zobowiązany będzie do wykonania demontażu i odebrania urządzenia na własny koszt.

bb) Usługa podłączenia zasilacza do przygotowanej, zgodnie z zaleceniami producenta, instalacji.

2. Licencje do oprogramowania do ochrony danych - szyfrowanie – 60 szt.

1) Konsola centralnego zarządzania musi wspierać systemy operacyjne Microsoft Windows Server 2008 32-bit i 64-bit, 2012 64-bit, 2016 64-bit oraz Microsoft Windows 7/8/10 32-bit i 64-bit.
2) Serwer centralnego zarządzania musi współpracować co najmniej z silnikami baz danych takimi jak Microsoft SQL Server 2005, 2008, 2012.
3) Konsola centralnego zarządzania musi pozwalać na generowanie pakietów instalacyjnych dla stacji końcowych w formacie MSI.
4) Komunikacja pomiędzy serwerem centralnego zarządzania, a serwerem proxy musi odbywać się na bezpiecznym porcie 443.
5) Administrator musi mieć możliwość tworzenia i zarządzania wieloma kluczami szyfrującymi, opartymi o kilka algorytmów szyfrujących, co najmniej AES, 3DES, Blowfish.
6) Administrator musi mieć możliwość tworzenia różnych użytkowników, mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisywania im różnych ról.
7) Administrator musi mieć możliwość tworzenia dodatkowych ról, na podstawie opcji dostępnych w konsoli centralnego zarządzania.
8) Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła.
9) Musi istnieć możliwość konfiguracji złożoności hasła do konsoli centralnego zarządzania, w oparciu o przynajmniej:
    a) ilość znaków,
    b) czy hasło ma zawierać wielkie litery,
    c) czy hasło ma zawierać małe litery,

d) czy hasło ma zawierać cyfry,
e) czy hasło ma zawierać znaki specjalne,
f) okres ważności,
g) ilość nieudanych logowań.

10) Administrator musi mieć możliwość konfiguracji złożoności haseł dla użytkowników na stacjach roboczych.
11) Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:
    a) ilość znaków,
    b) czy hasło ma zawierać wielkie litery,
    c) czy hasło ma zawierać małe litery,
    d) czy hasło ma zawierać cyfry,
    e) czy hasło ma zawierać znaki specjalne,
    f) f) okres ważności,
    g) ilość nieudanych logowań,
    h) możliwość zmiany hasła.
12) Konsola centralnego zarządzania musi gromadzić informacje o:
    a) nazwach stacji roboczych, na których jest zainstalowany klient systemu szyfrowania danych,
    b) dacie ostatniej modyfikacji ustawień klienta systemu szyfrowania danych,
    c) dacie aktywacji klienta systemu szyfrowania danych,
    d) statusu szyfrowania,
    e) typie urządzenia na którym jest zainstalowany klient systemu szyfrowania danych,
    f) stanie polityki,
    g) wersji klienta systemu szyfrowania danych,
    h) wersji systemu operacyjnego stacji roboczej,
    i) użytkownikach uprawnionych do logowania do oprogramowania na stacji roboczej.
13) Konsola centralnego zarządzania musi pozwalać na wygenerowanie dla każdej zaszyfrowanej stacji płyty ratunkowej.
14) Konsola musi być dostępna z poziomu interfejsu WWW.
15) Administrator musi mieć możliwość zarządzania stacjami klienckimi, które mają dostęp do sieci Internet.
16) Administrator musi mieć możliwość konfiguracji automatycznego szyfrowania pełnej powierzchni dysku po wykonanej instalacji oprogramowania.
17) Konsola centralnego zarządzania musi posiadać możliwość automatycznej aktywacji licencji w ramach kont domenowych.
18) Administrator musi mieć możliwość wykonania poniższych czynności w sposób zdalny:
    a) instalacji klienta na stacji,
    b) zaszyfrowania/odszyfrowania stacji,
    c) wygenerowania klucza aktywacyjnego dla użytkownika,

d) administrowania kluczami szyfrującymi,
e) administrowania użytkownikami, którzy mają dostęp do stacji,
f) administrowania profilem ustawień dla użytkowników,
g) administrowania profilem ustawień dla stacji roboczych,
h) wymuszenia zmiany hasła,
i) zarządzania wieloma organizacjami z poziomu jednej konsoli.

19) Support na oprogramowanie: minimum 36 miesięcy
20) Usługa wdrożenia:

W związku ze specyfiką wdrożenia, osoba wdrażająca musi posiadać aktualne poświadczenie bezpieczeństwa, upoważaniającego do dostępu do danych o klauzuli poufne.

- Instalacja serwera ESET Endpoint Encryption
- Przygotowanie paczki instalacyjnej
- Konfiguracja 2 polityk (użytkowników i stacji)
- Stworzenie grupy kluczy (3 grupy)
- Integracja z AD
- Aktywacja klientów
- Uruchomienie procesu szyfrowania na maksymalnie 10 komputerach.

3. WYMAGANIA SYSTEMOWE APLIKACJI KLIENCKIEJ

1) System szyfrowania danych musi wspierać instalacje aplikacji klienckiej w środowisku Microsoft Windows Vista/7/8/10 32-bit i 64-bit oraz w środowiskach Microsoft Windows Server, 2008 32-bit i 64-bit, 2012 64-bit, 2016 64-bit.
2) System musi posiadać certyfikat FIPS 140-2 Level 1

4. WYMAGANIA DOTYCZĄCE UWIERZYTELNIANIA

1) Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
2) Aplikacja musi umożliwiać określenie, co najmniej 127 unikalnych użytkowników, którzy będą mieć dostęp do chronionej stacji roboczej na poziomie Pre-Boot.
3) Aplikacja musi umożliwiać przetrzymywanie, co najmniej 64 kluczy szyfrujących w jednym pęku kluczy (key file).
4) Dostęp do pliku klucza musi być chroniony przy pomocy hasła. Domyślnie wykorzystywane hasło musi być hasłem systemu Windows.
5) Administrator musi posiadać możliwość modyfikacji ekranu logowania (Pre-boot).

5. WYMAGANIA DOTYCZĄCE USTAWIEŃ APLIKACJI KLIENCKIEJ

1) Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.
2) Defragmentacja dysku nie może mieć negatywnego wpływu na system szyfrowania.

3) Aplikacja musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób:
    a) sektor po sektorze,
    b) kontener.
4) Zaszyfrowany nośnik wymienny oraz nośnik CD/DVD może być odczytany na dowolnej stacji, na której nie ma zainstalowanego klienta systemu szyfrowania. Dostęp do takiego nośnika musi być możliwy po podaniu hasła.
5) Aplikacja musi pozwalać na szyfrowanie wiadomości e-mail wraz z załącznikami.
6) Aplikacja musi umożliwiać automatyczną deszyfrację otrzymywanych wiadomości e-mail.
7) Aplikacja musi pozwalać na szyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.
8) Zaszyfrowany tekst może być odczytany, za pomocą narzędzia, dostarczanego przez producenta, na stacji bez zainstalowanego klienta systemu szyfrowania.
9) Aplikacja musi umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania.
10) Aplikacja musi umożliwiać wybór domyślnego klucza szyfrowania.
11) Aplikacja musi umożliwiać zaszyfrowanie pliku lub folderu z poziomu menu kontekstowego.
12) Możliwe jest utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/odszyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.
13) Aplikacja musi umożliwiać tworzenie wirtualnych partycji. Dostęp do takich partycji ma być możliwy przy użyciu klucza szyfrującego lub hasła.
14) Aplikacja musi umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB.
15) Aplikacja musi umożliwiać tworzenie zaszyfrowanego archiwum. Dostęp do takiego archiwum ma być możliwy, przy użyciu klucza szyfrującego lub hasła.
16) Aplikacja musi umożliwiać trwałe usuwanie danych za pomocą poniższych algorytmów:
    a) Guttman.
    b) US Department of Defence 5220.22-M (8-306. /E).
    c) US Department of Defence 5220.22-M (8-306. /E, CiE).
    d) Kryptograficzne losowe dane liczbowe.
17) Aplikacja musi posiadać dedykowaną wtyczkę co najmniej dla klientów pocztowych MS Outlook 2003 lub nowszych, również dostępnych z poziomu Office 365.
18) Aplikacja musi umożliwiać automatyczne zalogowanie użytkownika do pęku klucza (key file) systemu szyfrowania danych po uruchomieniu systemu operacyjnego.
19) Aplikacja musi umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności użytkownika w systemie.
20) Aplikacja musi posiadać opcję automatycznego odpytywania serwerów producenta o dostępność nowszych wersji.
21) Użytkownik musi posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI.

6. WYMAGANIA DOTYCZĄCE SZYFROWANIA

1) Aplikacja musi dawać możliwość szyfrowania powierzchni dysku sektor po sektorze.
2) Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.
3) Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania powierzchni dysku i jego wznowienie. Proces szyfrowania danych powinien rozpocząć się od momentu, w którym został przerwany.
4) Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania, w sytuacji gdy laptop nie jest podłączony do zasilania. Proces szyfrowania musi zostać wznowiony automatycznie, po podłączeniu zasilacza.
5) Wymagane jest wykorzystanie kluczy szyfrujących, utworzonych przy użyciu jednego z poniższych algorytmów szyfrowania:
    a) AES (Rijndael).
    b) Blowfish.
    c) Triple DES (3DES).
6) Aplikacja musi umożliwiać współpracę z dyskami SSD.
7) Aplikacja musi umożliwiać współpracę z dyskami sprzętowo szyfrowanymi, działającymi w technologii TCG OPAL.
8) Aplikacja musi umożliwiać szyfrowanie danych na komputerach z UEFI.
9) Administrator musi mieć możliwość sprawdzenia, przed zaszyfrowaniem całej powierzchni dysku, czy nie pojawią się problemy po ponownym uruchomieniu komputera.
10) Administrator musi mieć możliwość opcjonalnego szyfrowania niesystemowych partycji dysku.

7. WYMAGANIA DOTYCZĄCE SYTUACJI KRYTYCZNYCH

1) W przypadku utraty hasła, aplikacja musi umożliwiać Administratorowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie zdefiniowanego wcześniej hasła administratora.
2) W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania.