**Załącznik nr 1**
**do „Ogłoszenia o zamówieniu publicznym”**

Nazwa przedmiotu zamówienia:
**„Dostawa wraz z instalacją i konfiguracją urządzenia do backupu oraz rozbudowa posiadanej macierzy o dodatkowe dyski, w budynku Urzędu Miejskiego w Trzebiatowie”**

# Opis przedmiotu zamówienia

1. **Rozbudowa posiadanej macierzy HP MSA 2040 o dodatkowe dyski - 6 szt.**

   Parametry dysku: HP MSA 1.2TB 12G SAS 10K 2.5in ENT HDD [J9F48A]

   Gwarancja producenta: min. 36 miesięcy

2. **Serwerowy system operacyjny (licencja 16 rdzeni procesora) – 2 szt.**

Licencje na serwerowy system operacyjny muszą być przypisane do każdego rdzenia procesora fizycznego na serwerze. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego niezależnie od liczby rdzeni w serwerze fizycznym.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.

8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.

9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:

    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,

    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,

    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,

    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).

10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET

13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:

    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.

16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.

18) Mechanizmy logowania w oparciu o:

    a. Login i hasło,

    b. Karty z certyfikatami (smartcard),

    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..

20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.

23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).

24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.

25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

    a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

    b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

        iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

    c. Zdalna dystrybucja oprogramowania na stacje robocze.

    d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej

    e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

        i. Dystrybucję certyfikatów poprzez http

        ii. Konsolidację CA dla wielu lasów domeny,

        iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

        iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

    f. Szyfrowanie plików i folderów.

g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

i. Serwis udostępniania stron WWW.

j. Wsparcie dla protokołu IP w wersji 6 (IPv6),

k. Wsparcie dla algorytmów Suite B (RFC 4869),

l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

   i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

   ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

   iii. Obsługi 4-KB sektorów dysków

   iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

   v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

   vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).

28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

### 3. Dostawa urządzenia do backupu z deduplikacją - 1 szt.

1) Obudowa przeznaczona do montażu w szafie przemysłowej 19", o wysokość maksymalnie 2U wraz ze wszystkimi elementami niezbędnymi do zamontowania w szafie.
2) Min. 24 TB przestrzeni surowej na zainstalowanych dyskach twardych.
3) Dostępne dla użytkownika min. 12 TB przestrzeni surowej na zainstalowanych dyskach.
4) Dostarczona konfiguracja musi zapewniać min. 7,5 TB przestrzeni na dane (po deduplikacji i kompresji).
5) Możliwość w przyszłości rozbudowy do min. 15 TB przestrzeni na dane.
6) Nominalna wydajność backupu z deduplikacją na urządzeniu – min. 4,6 TB/h.
7) Obsługa technologii pozwalającej na uzyskanie wyższej wydajności przy przeniesieniu procesu deduplikacji na inne urządzenie. Nominalna wydajność backupu z deduplikacją na źródle – min. 12,5 TB/h. Jeśli funkcjonalność wymaga licencji, wymagane jest jej dostarczenie.
8) Powierzchnia dyskowa musi być zabezpieczona mechanizmem RAID. Fizyczne dyski klasy przynajmniej NearLine SAS. Nie są dopuszczalne dyski z interfejsem SATA.
9) Urządzenie powinno wykorzystywać sprzętowy kontroler RAID(obsługiwany RAID 6) z zabezpieczeniem pamięci cache dla zapisu dla dysków z danymi użytkownika. Jeśli odbudowa dysków w RAID odbywa się za pomocą CPU urządzenia,
10) Min. 4 porty typu 1 GbE BaseT z możliwością agregacji mechanizmem LACP (IEEE 802.3ad).
11) Możliwość utworzenia sieciowych zasobów plikowych (protokół CIFS i NFS). Jeśli do realizacji funkcjonalności NAS wymagane są licencje, wymagane jest ich dostarczenie na całą pojemność urządzenia.
12) Blokowa deduplikacja typu inline, niezależna od systemu wykonywania kopii zapasowych. Zmienna wielkość bloku danych, maksymalnie 32kB. Wymagane jest dostarczenie licencji dla tej funkcjonalności dla całej pojemności urządzenia. Możliwość utworzenia udziałów CIFS/NFS i wirtualnych bibliotek bez deduplikacji. Nie jest dopuszczalne rozwiązanie z deduplikacją typu post-process.
13) Musi istnieć możliwość uruchamiania procesu czyszczenia (housekeeping) codziennie, w zadanym oknie czasowym.
14) Graficzny interfejs administracyjny, CLI, SNMP. Powiadamianie o problemach w urządzeniu za pomocą e-mail.
15) Urządzenie musi pozwalać na integrację z Vmware 5.5 oraz Veeam Backup & Replication
16) Gwarancja: 36 miesięczna gwarancja producenta urządzenia , przyjmowanie zgłoszeń w reżimie min. 9x5 Next Business Day czas reakcji następny dzień roboczy, w przypadku awarii dyski twarde pozostają u zamawiającego.
17) Produkt fabrycznie nowy, oznakowany symbolem CE.

4. **System logowania, raportowania i korelacji** – 1 szt.

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM.

**Interfejsy, Dysk:**

System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 500 GB.

**Parametry wydajnościowe:**

1) System musi być w stanie przyjmować minimum 1 GB logów na dzień.
2) Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

**Logowanie**

1) Podgląd logowanych zdarzeń w czasie rzeczywistym.
2) Możliwość przeglądania logów historycznych z funkcją filtrowania.
3) System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
    a. Listę najczęściej wykrywanych ataków.
    b. Listę najbardziej aktywnych użytkowników.
    c. Listę najczęściej wykorzystywanych aplikacji.
    d. Listę najczęściej odwiedzanych stron www.
    e. Listę krajów , do których nawiązywane są połączenia.
    f. Listę najczęściej wykorzystywanych polityk Firewall.
    g. Informacje o realizowanych połączeniach IPSec.
4) Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5) Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6) System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

**Raportowanie**

W zakresie raportowania system musi zapewniać:

1) Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.
2) Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3) Funkcję definiowania własnych raportów.
4) Możliwość spolszczenia raportów.
5) Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

**Korelacja logów**

W zakresie korelacji zdarzeń system musi zapewniać:

1) Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2) Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3) Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
    - Malware.
    - Aplikacje sieciowe.
    - Email.
    - IPS.
    - Traffic.
    - Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

**Zarządzanie**

1) System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
2) System musi umożliwiać zdefiniowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

**Gwarancja oraz wsparcie**

Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

**Wymagania dodatkowe**

1) W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą

jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2) Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

**5. Wkładka SFP 1.25Gbps LC DDM SMF 20km do przełącznika HPE 1810-24G – 2 szt.**

Gwarancja producenta: minimum 12 miesięcy

**6. Patchcord LC/SC. Singlemode Duplex, 3m – 2 szt.**

Gwarancja producenta: minimum 12 miesięcy

**7. Wdrożenie**

- Instalacja i konfiguracja systemu logowania, raportowania i korelacji oraz integracja z posiadanym FortiGate.
- Instalacja dysków w posiadanej macierzy MSA2040. Konfiguracja puli dyskowej, LUN, mapowanie hostów ESXi do LUN. Wystawienie nowej przestrzeni dyskowej w formie datastore z systemem plików vmfs do hostów ESXi.
- Instalacja macierzy dyskowej z deduplikacją w szafie RACK. Podłączenie do LAN w sposób redundantny. Inicjalizacja macierzy i konfiguracja uwierzytelnienia. Wystawienie zasobów jako repozytorium w posiadanym przez zamawiającego systemie Veeam B&R z deduplikacją na źródle. Przekierowanie skonfigurowanych zadań kopii zapasowych na nowe repozytorium. Konfiguracja posiadanego przez Zamawiającego serwera NAS jako drugiej lokalizacji dla plików kopii zapasowych.
- Połączenie dwóch lokalizacji Zamawiającego przy pomocy dostarczonych wkładek i patchcordów do posiadanych przełączników HP 1810-24. Wyeliminowanie obecnie zainstalowanych media konwerterów. Testy komunikacji.
- Szkolenie administratora z obsługi wdrożonych elementów infrastruktury.

**Uwaga!**
Jednocześnie Zamawiający informuje, że ewentualne znaki towarowe i nazwy produktów ujęte w opisie przedmiotu zamówienia służą jedynie określeniu parametrów oraz jakości produktu. W każdym takim przypadku dopuszcza się możliwość zaoferowania produktów równoważnych, przy czym Wykonawca, który powołuje się na rozwiązania równoważne opisanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy, usługi lub roboty budowlane spełniają wymagania określone przez Zamawiającego.