Załącznik 1A do SIWZ

SZCZGÓŁOWY OPIS
PRZEDMIOTU ZAMÓWIENIA

W ramach realizacji przedmiotu zamówienia Zamawiający oczekuje zachowania pełnej kompatybilności z już posiadaną przez Zamawiającego infrastrukturą informatyczną. Każdorazowo, gdy Zamawiający powołuje się w specyfikacji na konkretny model bądź markę, należy interpretować, iż sprzęt ten jest przykładem spełniającym minimalne wymagania techniczne, zarówno wydajnościowe, jak i jakościowe określone przez Zamawiającego, co nie oznacza, że wskazany przykład ogranicza możliwość składania ofert równoważnych (chyba, że Zamawiający w dokumentacji jawnie wskazuje inaczej, np.: w przypadku rozbudowy elementów już posiadanych). Ofertą równoważną jest element o takich samych lub lepszych parametrach technicznych, jakościowych, funkcjonalnych, spełniający ponadto wszystkie minimalne wymagania określone przez Zamawiającego. Zamawiający zastrzega jednak możliwość niedopuszczenia rozwiązań równoważnych, wszędzie tam gdzie ze względu na kompatybilność technologii z rozwiązaniami już posiadanymi, mogłoby w jakimkolwiek stopniu ograniczyć funkcjonalność rozwiązań, czy narazić go na jakiekolwiek dodatkowe koszty, np.: koszty modernizacji, integracji czy koszty szkolenia. Przedmiot dostawy musi być w pełni kompatybilny z już posiadaną przez Zamawiającego infrastrukturą i nie może w żadnym stopniu ograniczać jej funkcjonalności. Elementy, których to dotyczy, pracować będą w środowisku opartym o posiadany przez Zamawiającego kontrolery domeny Active Directory (pracujący na poziomie funkcjonalności Microsoft Windows Server 2012 R2), a dwa podstawowe systemy dziedzinowe działają w oparciu o platformę „Oracle Forms" i bazę „Oracle Database" (środowisko wielowątkowe) oraz platformę „Microsoft .NET 3,5" i „Microsoft SQL Server 2008 R2" (środowisko jednowątkowe), sieć opartą o urządzenia wykonane w technologii CISCO, z centralnymi zabezpieczeniami w technologii FortiNet, system kopii zapasowych Veeam Backup 9.x oraz platformie wirtualizacyjnej VMware vSphere Hypervisor (ESXi) 6.5. Jeśli któryś z elementów systemu będących przedmiotem zamówienia znajduje się na liście „End of Life" (tj. na liście opublikowanej przez producenta urządzenia wskazującej urządzenia dla których kończy się czas życia produktu) należy w ofercie zaproponować upgrade

tego elementu do wersji zapewniającej oczekiwaną funkcjonalność.

PRZEDMIOT NINIEJSZEGO ZAMÓWIENIA STANOWI:

CZĘŚĆ 1.

DOSTAWA URZĄDZEŃ SIECIOWYCH I ZABEZPIECZEŃ UTM**:**

Zamawiający oczekuje dostawy oraz przedłużenia subskrypcji dla posiadanych już urządzeń

a) Zabezpieczenia Centralne

Zamawiający oczekuje:

- Przedłużenia kontraktów serwisowych licencji (nr seryjny FGT6HD3917802871) od dnia 09.10.2020 na urządzenie FortiGate 600D w okresie 36 miesięcy, upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów, Kontrolę Aplikacji, IPS, Antywirus, AntySpam, Web Filtering.
- Aktualizację posiadanego rozwiązania o zapewnienie pracy w trybie HA
- Zapewnienia gwarancji i wsparcia:

  Przedłużenie kontraktu serwisowego o okres kolejnych **36 miesięcy** W ramach tego serwisu producent musi zapewniać dostęp do aktualizacji oprogramowania oraz wsparcie techniczne (poprzez e-mail, telefon, dedykowany portal, połączenie zdalne) co najmniej w trybie 8x5 (5 dni w tygodniu przez 8 godzin dziennie).

- Podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7x4 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7x4.

  Wykonawca winien przedłożyć dokumenty:

  1. Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
  2. Certyfikat ISO 9001 podmiotu serwisującego.

- 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 musi przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

b) [4szt.] Punkty dostępowe (Access Point)

- Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.
- Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
    a. Temperatura -20–45°C,
    b. Wilgotność 5–90%.
- Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington.
- Urządzenie musi być wyposażone w dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
    a. 2.4 GHz 802.11b/g/n,
    b. 5 GHz 802.11a/n/ac,
- Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
- Interfejs Ethernet w standardzie 10/100/1000 Base-TX,
- Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3af lub ze-wnętrzny zasilacz.
- Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych: Tunnel, Bridge, Mesh.
- Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
- Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, Web Captive Portal, MAC blacklist & whitelist, 802.11i, 802.1X (EAP-TLS, EAP-T-TLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
- Interfejs radiowy urządzenia powinien wspierać następujące funkcje:

a) MIMO – 2x2,

b) Transmit Beam Forming (TxBF),

c) Maksymalna przepustowość dla poszczególnych modułów radiowych:

- 400 Mbps;

- 867 Mbps;

d) Wymagana moc nadawania:

- min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;

- min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;

e) Wsparcie dla 802.11n 20/40Mhz HT,

f) Wsparcie dla kanału 80 MHz dla 802.11ac,

g) Anteny – 4 zewnętrzne RP-SMA dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.

h) Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,

i) Maksymalna deklarowana liczba klientów per moduł radiowy – 512.

- Funkcje interfejsu radiowego:
  a. Skaner częstotliwości 2.4 oraz 5 GHz,
  b. Skanowanie w tle podczas obsługi klientów na pasmach 2.4 oraz 5 GHz,
  c. Skaner częstotliwości 2.4 oraz 5GHz w trybie dedykowanego monitora,
- Funkcje dodatkowe:
  a. Low-Density Parity Check (LDPC) Encoding,
  b. Maximum Likelihood Demodulation (MLD),
  c. Maximum Ratio Combining (MRC),
  d. A-MPDU and A-MSDU Packet Aggregation,
  e. MIMO Power Save,
  f. Short Guard Interval,
  g. WME Multimedia Extensions.

- Punkt dostępowy musi być certyfikowanym urządzeniem WiFi Alliance: WiFi certified IEEE Std 802.11a/b/g/n (ac) oraz posiadać certyfikację DFS.
- Kompatybilność w zakresie zarządzania z zabezpieczeń centralnych (Fortigate 600D)
- Gwarancja oraz wsparcie

  Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji, oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w co najmniej w trybie 8x5 (5 dni w tygodniu przez 8 godzin dziennie).

c) [24szt.] Zabezpieczenia dla jednostek podległych

Przedmiotem zamówienia jest dostawa 24 szt. fabrycznie nowych urządzeń klasy UTM (Unified Threat Managment) składającego się na system kompleksowego zabezpieczenia sieci w jednostkach Gminnych z zapewnieniem kompatybilności z zakresie utworzenia połączeń VPN z Centralnymi Zabezpieczeniami w Urzędzie Miejskim w Wołominie.

- **Wymagania Ogólne**

  Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
  System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
  W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.
  System musi wspierać IPv4 oraz IPv6 w zakresie:
  - Firewall.
  - Ochrony w warstwie aplikacji.
  - Protokołów routingu dynamicznego.

- **Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.

- **Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum 7 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

- **Parametry wydajnościowe:**

1. W zakresie Firewall'a obsługa nie mniej niż 1.8 mln jednoczesnych połączeń oraz 21.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 2.5 Gbps.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 450 Mbps.
4. Wydajność szyfrowania IPSec VPN: nie mniej niż 90 Mbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 350 Mbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 160 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 150 Mbps.

- **Funkcje Systemu Bezpieczeństwa:**

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.

7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.

- **Polityki, Firewall**

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    - Translację jeden do jeden oraz jeden do wielu.
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

- **Połączenia VPN**

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
    - Wsparcie dla IKE v1 oraz v2.
    - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
    - Obsługa protokołu Diffie-Hellman grup 19 i 20.
    - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
    - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
    - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
    - Mechanizm „Split tunneling” dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

- **Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
1. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

- **Zarządzanie pasmem**

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

- **Kontrola Antywirusowa**

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

- **Ochrona przed atakami**

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

- **Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

- **Kontrola WWW**

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

- **Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
    - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
    - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
    - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

- **Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

- **Logowanie**

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu

zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

4. Musi istnieć możliwość logowania do serwera SYSLOG.

- **Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.
- ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
- ICSA dla funkcji SSL VPN.

- **Serwisy i licencje**

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

- **Gwarancja oraz wsparcie**

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres [60] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w co najmniej w trybie 8x5 (5 dni w tygodniu przez 8 godzin dziennie).

- **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.

3. Żaden element zaproponowanego systemu w chwili podpisania nie zawierającego zastrzeżeń protokołu odbioru, nie może znajdować się na liście „End of Life" (tj. na liście opublikowanej przez producenta urządzenia wskazującej urządzenia dla których kończy się czas życia produktu).

d) Centralne zarządzania UTM

W ramach postępowania wymaganym jest dostarczenie systemu centralnego zarządzania oraz logowania i raportowania, przystosowanego do współpracy z systemem bezpieczeństwa sieciowego dla posiadanych już rozwiązań oraz nowych będących przedmiotem tego postepowania (np. NGFW).
Rozwiązanie musi zostać dostarczone w postaci platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Specyfikacja:

- **Interfejsy, Dyski:**

1. System musi dysponować co najmniej:
    - 2 portami Gigabit Ethernet RJ-45.
    - 2 gniazdami SFP 1 Gbps.

oraz portem konsoli szeregowej.

2. Powierzchnia dyskowa min. 8 TB.
3. Z punktu widzenia bezpieczeństwa platformy, na których realizowane będą funkcje logowania muszą mieć możliwość rozbudowy o mechanizmy zabezpieczające przed utratą danych w przypadku awarii nośnika – minimum RAID 0,1
4. System musi być wyposażony w zasilanie AC.

- **Parametry wydajnościowe:**

1. System musi umożliwiać zarządzenie co najmniej 30 systemami bezpieczeństwa.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 30 systemów.
3. System musi być w stanie przyjmować minimum 2 GB logów na dzień.

- **Funkcje systemu centralnego zarządzania**

W ramach centralnego systemu zarządzenia muszą być realizowane co najmniej poniższe funkcje:

1. System musi posiadać system zarządzenia zmianami konfiguracji (WorkFlow, mechanizm audytu oraz porównania konfiguracji).

2. System musi dawać możliwość pełnej konfiguracji urządzeń, ze wszystkimi ich funkcjami składowymi.
3. System musi posiadać możliwość skonfigurowania godziny implementacji zmian (harmonogram dla instalowania zmian).
4. System musi przechowywać i implementować polityki bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej.
5. System musi wersjonować polityki w taki sposób, aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości.
6. System musi umożliwiać zarządzenie wersjami firmware'u oraz zapewniać centralną aktualizację oprogramowania.
7. System musi być w stanie wysłać tą samą konfigurację na wiele urządzeń.
8. System musi umożliwiać pracę wielu administratorów jednocześnie (system musi mieć możliwość blokady kontekstu urządzenia).
9. System musi być w stanie zarządzać wersjami baz sygnatur na urządzeniach oraz zdalnymi uaktualnieniami.
10. System musi zapisywać i zdalne wykonywanie skryptów na urządzeniach.
11. System musi monitorować w czasie rzeczywistym stan urządzeń (użycie CPU, RAM).
12. System musi automatyzować proces konfiguracji struktur VPN typu hub-and-spoke oraz full-mash.
13. Konfigurację powiadomień poprzez: e-mail, SNMP v1/v2c/v3 w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.

- **Funkcje logowania**

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.

- **Funkcja raportowania**

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. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

- **Funkcje korelacji**

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.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, TACACS+, PKI.

2. System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do logowanych informacji i elementów zarządzania z perspektywy poszczególnych zarządzanych systemów.
3. System musi posiadać API które umożliwia zarządzenie urządzeniami podłączonymi do systemu za pomocą poleceń REST API.
4. Powinna istnieć możliwość zdefiniowania co najmniej 9 lokalnych kont administracyjnych.

- **Gwarancja oraz wsparcie**

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie w co najmniej w trybie 8x5 (5 dni w tygodniu przez 8 godzin dziennie).

2. Podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5.
3. Wykonawca winien przedłożyć dokumenty:
   a) Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
   b) Certyfikat ISO 9001 podmiotu serwisującego.
   c) Żaden element zaproponowanego systemu w chwili podpisania nie zawierającego zastrzeżeń protokołu odbioru, nie może znajdować się na liście „End of Life" (tj. na liście opublikowanej przez producenta urządzenia wskazującej urządzenia dla których kończy się czas życia produktu).

- **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. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

e) Aktualizacja licencji FortiMail, FortiAnalizer

Zamawiający oczekuje:

- Przedłużenia kontraktów serwisowych licencje (nr seryjny FEVM010000013221) od dnia 08.12.2020 na urządzenie FortiMail VM01 w okresie 36 miesięcy, upoważniające do wsparcia technicznego, korzystania z aktualnych baz funkcji ochronnych producenta i serwisów 8x5 FortiCare plus FortiGuard Bundle Contract, FortiGuard FortiSandbox Cloud Service wraz z autoryzowanym szkoleniem dla jednego administratora FortiMail Email Security (NSE6) prowadzone przez certyfikowanego inżyniera (w postaci vouchera z ważnością co najmniej 6 miesięcy).

- Przedłużenia kontraktów serwisowych licencji (nr seryjny FAZ-VM0000128973) VM Base license + license for adding 5 GB/Day of Logs, 3 TB storage capacity od dnia 08.12.2020 na urządzenie FortiAnalyzer-VM64 w okresie 36 miesięcy, upoważniające do wsparcia technicznego, pobierania aktualizacji i serwisu producenta co najmniej w trybie 8x5 (5 dni w tygodniu przez 8 godzin dziennie) FA-VM 8x5 FortiCare Contract (for 1-6 GB/Day of Logs) 3Y

CZĘŚĆ 2.

DOSTAWA KOMPUTERÓW, DRUKAREK I SKANERÓW

a) **[15 szt.] Komputer typu All-In-One** spełniający co najmniej poniższe parametry:

Atrybut	**Minimalne wymagania parametrów technicznych**	
Typ	Komputer stacjonarny. Typu All in One, komputer wbudowany w monitor. W ofercie wymagane jest podanie modelu i producenta komputera.	
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb dostępu do systemów dziedzinowych opartych o Oracle Forms i Microsoft .NET, aplikacji jednowątkowych i wielowątkowych, aplikacji biurowych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej	
Wydajność obliczeniowa	Procesor osiągający w teście Passmark CPU Mark wynik in 11800 punktów według wyników ze strony https://www.cpubenchmark.net	
Pamięć operacyjna RAM	16GB DDR4 2666MHz możliwość rozbudowy do min 32GB, jeden slot pamięci wolny	
Dysk twardy	Min. 256 GB SSD PCIe NVMe Możliwość instalacji dwóch dysków, w tym min. jednego w złączu M.2	
Wydajność grafiki	Grafika zintegrowana z procesorem ze wsparciem DirectX 11.1, OpenGL 4.0, OpenCL 1.2; pamięć współdzielona z pamięcią RAM, dynamicznie przydzielana	
Matryca	Wielkość i rodzaj	Min.23 ” matryca IPS
	Rozdzielczość	FHD (1920x1080)
	Jasność	min. 250 cd/m²
	Kontrast typowy	Min. 1000:1
	Odświeżanie	min. 60 Hz
	Kąty widzenia pion/poziom	178 / 178
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, 24-bitowa konwersja sygnału cyfrowego na analogowy i analogowego na cyfrowy; wbudowane dwa głośniki min. 3W na kanał Wbudowana w obudowę matrycy kamera cyfrowa 2 MP z dwoma mikrofonami cyfrowymi	

	Czytnik kart SD na bocznej krawędzi obudowy
Obudowa	Typu All-in-One zintegrowana z monitorem min. 23”. Demontaż standu musi odbywać się bez użycia narzędzi, mocowanie standu wyposażone w przycisk zwalniający. Suma wymiarów obudowy (bez podstawy) nie może przekraczać 105cm, Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA 100, Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie oraz wpisanym na stałe w BIOS. Zasilacz wewnętrzny o mocy max. 155W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Obudowa musi posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym producenta komputera Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, system musi sygnalizować minimum: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, uszkodzenie kontrolera video, awarię BIOS’u, awarię procesora Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji. Podstawa umożliwiająca: - pochylenie monitora w zakresie 35 stopni - regulację wysokości w zakresie min. 100mm - pivot - obrót monitora o 45 stopni prawo/lewo
Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą posiadać certyfikat producenta oferowanego systemu operacyjnego, potwierdzający poprawną współpracę oferowanych modeli komputerów z oferowanym systemem operacyjnym (należy załączyć wydruk ze strony producenta oprogramowania)
Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika, dostępny z poziomu szybkiego menu boot, umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych w oferowanym komputerze komponentów, bez konieczności uruchamiania systemu operacyjnego. Minimalna funkcjonalność systemu: testy uruchamiane automatycznie lub w trybie interaktywnym, możliwość powtórzenia testów. podsumowanie testów z możliwością zapisywania wyników, uruchamianie gruntownych testów, uruchamianie szybkich testów lub pojedynczego testu dla

	konkretnego podzespołu, uruchamianie testów zdefiniowanych przez użytkownika, wyświetlanie wiadomości o błędach napotkanych podczas testów. Test musi zawierać informację o nazwie i numerze seryjnym komputera, wersji BIOS oraz wszystkich zainstalowanych komponentach, a w szczególności: numerze seryjnym, typie i pojemności dysku twardego, informacji o obrotach wentylatora CPU, informacji o procesorze (model i taktowanie) informacji o pamięci (wielkość, obsadzenie w konkretnym banku, typ pamięci wraz z taktowaniem), wykaz temperatur CPU, pamięci, temperatury panującej wewnątrz. System działający nawet w przypadku braku dysku twardego, jego uszkodzenia, bez dostępu do internetu i sieci lokalnej pozwalający na uzyskanie wyżej wymienionych funkcjonalności a w szczególności na przetestowanie: procesora i pamięci Pełna funkcjonalność systemu nie może wymagać użycia dodatkowych urządzeń (np. pamięć USB itp.)
Zdalne zarządzanie	Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca: -monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; - zdalną konfigurację ustawień BIOS, - zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; - zdalne przejecie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 1920x1080 włącznie; - zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej. - technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0 (http://www.dmtf.org/standards/mgmt/dash/) - wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego Sprzętowe wsparcie technologii weryfikacji poprawności podpisu cyfrowego wykonywanego kodu oprogramowania, oraz sprzętowa izolacja segmentów pamięci dla kodu wykonywanego w trybie zaufanym wbudowane w procesor, kontroler pamięci, chipset I/O i zintegrowany układ graficzny.

Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu.
BIOS	- BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy (możliwość włączenia/wyłaczenia funkcji BIOS za pomocą urządzenia wskazującego) BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości i prędkości zainstalowanej pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci, typie, ilości rdzeni i prędkości zainstalowanego procesora, pojemności zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA oraz M SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem)) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie jedynie zmienić swoje hasło (bez możliwości zmiany innych parametrów konfiguracji BIOS). Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia kontrolera SATA w trybie RAID, Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość wyłączania portów USB pojedynczo, Funkcja umożliwiająca dokonywania backup’u BIOS wraz z ustawieniami na dysku wewnętrznym lub na urządzeniu zewnętrznym. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia min. : uruchamianie systemu zainstalowanego na HDD, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchamianie systemu z karty SD (funkcja aktywna automatycznie po zainstalowaniu karty SD w czytniku, uruchomienie graficznego systemu diagnostycznego, wejścia do BIOS, upgrade BIOS bez konieczności

	uruchamiania systemu operacyjnego, dostępu do sieci i internetu
Certyfikaty i standardy	- Urządzenie musi być wyprodukowane zgodnie z normą ISO 9001 oraz 50001 – certyfikaty załączyć do oferty - Deklaracja zgodności CE (załączyć do oferty) - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram - Komputer musi spełniać wymogi normy Energy Star min. 6.0 (certyfikat załączyć do oferty) - Certyfikat TCO dla oferowanego modelu – załączyć wydruk ze strony www.tcocertified.com
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy jałowej (IDLE) wynosząca maksymalnie 20 dB (załączyć oświadczenie producenta)
Warunki gwarancji	- 3-letnia gwarancja producenta świadczona na miejscu u klienta, możliwość zgłaszania awarii przez ogólnopolską linię telefoniczną producenta. Czas reakcji serwisu - do końca następnego dnia roboczego Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera . - Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. - W przypadku awarii, dyski twarde zostają u Zamawiającego – do oferty należy załączyć oświadczenie podmiotu realizującego serwis lub producenta o spełnieniu tego warunku. - Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. - Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego)
Wsparcie techniczne producenta	- Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. - Dostęp do najnowszych sterowników i uaktualnień na stronie producenta

	zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony.
System Operacyjny	Zainstalowany system operacyjny Windows 10 Professional 64-bitowy, klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego
Wymagania dodatkowe	Wbudowane porty i złącza: HDMI out, HDMI in, Display Port out, min. 4 porty USB 3.1 gen.1 z tyłu obudowy, min.. 2 porty USB 3.1, w tym min. 1 port USB .1 typ C gen.2 usytuowane w bocznej części obudowy; wymagana ilość i rozmieszczenie portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp., port słuchawkowo-mikrofonowy na przednim/bocznym panelu, port Line-out na tylnym panelu Karta WiFi ac (2x2) + bluetooth 5 Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE, umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem z poziomu konsoli zarządzania - niezależnie od stanu zasilania komputera - łącznie z obsługą stanu S3 (uśpienie) oraz S4-S5 (hibernacja i wyłączenie); Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM, min. 2 złącza M.2 Zintegrowany z płytą główną kontroler RAID 0 i RAID 1 Bezprzewodowy zestaw klawiatura w układzie polski programisty + mysz Wbudowana nagrywarka DVD +/-RW
Dodatkowe oprogramowanie	Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające: - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi: - dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji - sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania) - dostęp do wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o

	zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku *.xml Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku. W ofercie należy podać nazwę oprogramowania

Koniec tabeli

b)**[5 szt.] Notebook** spełniający co najmniej poniższe parametry:

Atrybut	**Minimalne wymagania parametrów technicznych**
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji obliczeniowych, dostępu do internetu, poczty elektronicznej.
Matryca	O przekątnej ekranu od 13 do 14” FHD (1920 x 1080), powłoką przeciwodblaskową
Wydajność	Procesor wielordzeniowy osiągający w teście Passmark CPU Mark wynik min.8000 punktów według wyników ze strony http://www.cpubenchmark.net
Pamięć RAM	16GB DDR4, możliwość rozbudowy do min 32GB, 2 sloty na pamięci w tym min. jeden wolny,
Pamięć masowa	512GB SSD PCIe NVMe
Karta graficzna	Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej
Multimedia	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2x 2W. Obsługująca w pełni co najmniej 2 kanały pod HDMI, cyfrowe mikrofony z funkcją redukcji szumów i poprawy mowy wbudowane w obudowę matrycy. Kamera internetowa z diodą informującą o aktywności, trwale zainstalowana w obudowie matrycy wyposażona w mechaniczną przysłonę. Czytnik kart micro SD, 1 port audio typu combo (słuchawki i mikrofon)
Łączność bezprzewodowa	Karta Wireless AC 2x2, Bluetooth 5.0, Wbudowany modem LTE
Bateria i zasilanie	Min. 60Whr, umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Zasilacz o mocy min. 65W
Waga	Waga max 1,6kg z baterią
Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy

	gumowe uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią. Kąt otwarcia notebooka min 180 stopni.
BIOS	BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i wmontowanego na stałe urządzenia wskazującego oraz samego urządzenia wskazującego. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: dacie produkcji komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i max. osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Funkcje logowania się do BIOS na podstawie hasła użytkownika, administratora (hasła niezależne), informację o stanie naładowania baterii (stanu użycia), podpiętego zasilacza, zarządzanie trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS. Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym.
Certyfikaty	Certyfikat ISO9001 dla producenta sprzętu (załączyć do oferty) Certyfikat ISO 14001 dla producenta sprzętu (załączyć do oferty) Deklaracja zgodności CE (załączyć do oferty) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (załączyć wydruk ze strony producenta oprogramowania) Certyfikat TCO, wymagana certyfikacja na stronie : http://tco.brightly.se/pls/nvp/!tco_search – załączyć do oferty wydruk z strony.
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy jałowej dysku twardego (IDLE) wynosząca maksymalnie 19dB (załączyć oświadczenie producenta)
Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w

	szczególności jego składowych. Działająca w pełni, bez okrojonych funkcjonalności nawet w przypadku uszkodzonego dysku, braku dysku lub sformatowanym dysku.
Bezpieczeństwo	- Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej. Czytnik SmartCard
Zarządzanie zdalne	Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca: monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; zdalną konfigurację ustawień BIOS, zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; zdalne przejecie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 1920x1080 włącznie; zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej. Technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0 (http://www.dmtf.org/standards/mgmt/dash/) Wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego sprzętowy firewall zarządzany i konfigurowany wyłącznie z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji w pełni aktywna konsola zarządzania wyświetlająca informacje i zachowująca pełną funkcjonalność nawet podczas restartów komputera zarządzanego.
Oprogramowanie	Zainstalowany system operacyjny Windows 10 Professional, klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu

	operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające: - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji. - dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji - sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania) - dostęp do wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera - dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku *.xml Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku. W ofercie należy podać nazwę oprogramowania
Wymagania dodatkowe	Wbudowane porty i złącza: 1x HDMI 1.4, 1x RJ-45, 2x USB 3.1 w tym jeden port z zasilaniem, 1x USB TYP-C, port zasilania, złącze na linkę zabezpieczającą Klawiatura w układzie QWERTY, z wbudowanym w klawiaturze podświetleniem, (układ US -QWERTY).. Dedykowana stacja dokująca producenta notebooka z własnym zasilaczem, podłączana przez port USB C wyposażona w minimum: 2x disply Port, HDMI, 3 x USB 3.1, 2x USB C, RJ-45, złącze słuchawkowe
Warunki gwarancyjne, wsparcie techniczne	- 3-letnia gwarancja producenta świadczona na miejscu u klienta. Czas reakcji serwisu - do końca następnego dnia roboczego. - Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. - Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. - W przypadku awarii dysk twardy zostaje u Zamawiającego – do oferty

	należy załączyć oświadczenie podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku. - Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. - Możliwość sprawdzenia kompletnych danych o parametrach komputera na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego)

Koniec tabeli

c)**[4 szt.] Skaner biznesowy** spełniający co najmniej poniższe parametry:

Atrybut	Minimalne wymagania parametrów technicznych
Zastosowanie	Skanery będą wykorzystywane dla potrzeb kancelaryjnych przy bezpośredniej obsłudze interesanta do elektronicznej archiwizacji wszystkich wpływających dokumentów.
Typ skanera	Skaner biznesowy z podajnikiem płaskim oraz automatycznym dostosowany do skanowania dokumentów w formacie A4 o dziennej wydajności nie mniejszej niż 4000 stron.
Rozdzielczość optyczna	Min. 600 x 600 dpi
Automatyczny podajnik dokumentów	Skanowanie dwustronne jednoprzebiegowe formatów dokumentów od min. 50,8 mm x 54 mm do maks 216 mm x 355,6 mm. Pojemność podajnika automatycznego na min. 80 stron.
Podajnik płaski	Przestrzeń robocza skanowania formatu dokumentów A4 o wymiarach min. 210 mm x 297 mm, prędkość skanowania max 1.7 sekundy (200 dpi) Klapa skanera płaskiego nie przytwierdzona na stałe do skanera, Możliwość wygodnego skanu obrazu z trwale złączonego pliku kartek umożliwiająca skan bez deformacji obrazu przy opuszczonej klapie.
Czujnik zacięcia papieru	Ultradźwiękowy
Obsługiwana gramatura papieru dla podajnika automatycznego	Letter: Od 27 g/m² do 413 g/m², Arkusze A8: Od 127 g/m² do 209 g/m²
Wyjściowa głębia kolorów	Kolor: 24-bity, skala szarości: 8-bitów, monochromatyczny: 1-bit
Głębia pikseli	Odcienie szarości: 16 bitów wejście, 8 bitów wyjście,

	Kolor: 48 bitów wejście, 24 bity wyjście
Prędkość skanowania	- Dla formatu A4 w rozdzielczości 200/300 dpi – 60 stron na minutę w trybie jednostronnym w kolorze, skali szarości - Dla formatu A4 w rozdzielczości 200/300 dpi – 120 stron na minutę w trybie dwustronnym w kolorze, skali szarości
Wymiary (szer. x gł. x wys.)	300 mm x 577 mm x 234 mm
Obsługiwane formaty	A4 i mniejsze
Interfejsy	USB 3.0 z kompatybilnością wsteczną do podłączenia z komputerem klasy PC
Sterowniki	TWAIN, ISIS
Działanie w systemach operacyjnych	Windows® 8 / 8.1 (32-/64-bitowy), Windows® 7 (32-/64-bitowy), Windows Vista® (32-/64-bitowy), Windows XP® (32-/64-bitowy),
Gwarancja	Gwarancja minimum 12 miesięcy, wymiana uszkodzonego sprzętu door to door w ciągu 1-2 dni roboczych.
Pakiet oprogramowania	Dostarczenie oprogramowania i sterowników na załączonej do skanera płycie CD / DVD
Wyposażenie dodatkowe	Przewody łączące: min. zasilający i USB 2.0, każdy o długości min. 1.5 m
Wymagania dotyczące zasilania	Zewnętrzny zasilacz w komplecie

Koniec tabeli

d) [6szt.] Drukarki wielofunkcyjne laserowe kolorowe A4

Atrybut	Minimalne wymagania parametrów technicznych
Standard	A4
Funkcja	Drukowanie, kopiowanie, skanowanie
Technologia	Laserowa kolorowa
Obsługiwana wielozadaniowość	Tak
Tryb drukowania	Kolorowa
Liczba tonerów drukujących	4 (czarna, błękitna, purpurowa, żółta)
Duplex	automatyczny
Komunikacja	RJ-45 (10/100/1000 Base-Tx) USB (2.0)
Wyświetlacz	Kolorowy, graficzny ekran dotykowy o przekątnej co najmniej 10 cm
Szybkość procesora	1200 MHz

Pamięć	512MB
Poziom hałasu	Max 49 dB
Obciążalność (zalecana)	Do 50000 stron A4 miesięcznie
Prędkość wydruku i kopiowania	Mono 25-27 str./min. A4 Kolor 25-27 str./min. A4 dwustronne 20-24 str./min. A4
Czas do wydruku pierwszej strony	Mono do 14 sekund Kolor do 16 sekund
Wydajność wkładu	Mono (startowy) do 2400 str. A4 (wg normy producenta, wydruk ciągły) mono (standard) do 7500 str. A4 (wg normy producenta, wydruk ciągły) kolor (startowy) do 1200 str. A4 (wg normy producenta, wydruk ciągły) mono (standard) do 6000 str. A4 (wg normy producenta, wydruk ciągły)
Rozdzielczość wydruku mono	600 x 600 dpi
Rozdzielczość wydruku kolor	600 x 600 dpi
Podajnik papieru	250 arkuszy
Język drukarki	PCL 6, PCL 5c, PDF, URF, Native Office, PWG Raster
Odbiornik papieru	150 arkuszy
Obsługiwane formaty papieru	A4; A5; A6; B5(JIS); koperta C5; koperta C6; koperta DL
Pojemność podajnika kopert	Do 10szt.
Obsługiwane nośniki	papier zwykły, papier bond, papier broszurowy, papier kolorowy,papier błyszczący, papier fotograficzny, papier wstępnie zadrukowany, papier dziurkowany, papier makulaturowy, papier szorstki, pocztówki, etykiety, koperty
Typ skanera	Skaner płaski, automatyczny podajnik dokumentów (ADF na 50 arkuszy)
Dwustronne skanowanie z ADF	Tak
Zapis skanów do plików	JPEG (.jpg), PDF (.pdf), TIFF (.tif)
Rozdzielczość skanowania - optyczna	1200 dpi

Prędkość skanowania (tryb normalny, format A4)	do 8 str./min (200 pikseli na cal, w czerni), do 3,5 str./min (200 pikseli na cal, w kolorze)
Skanowanie do napędów	USB, Komputera
Koszty wydruku (wg karty producenta)	Mono do 10 gr A4 (pokrycie 5%) Kolor do 65 gr A4 (pokrycie 5%)
Rozdzielczość kopii	600 x 600 dpi
Skalowanie kopii	25% do 400%
Zasilanie	100–240 V (+/-10%), 50/60Hz (+/-3 Hz)
Zużycie energii	Średnio 550W, Energy Star
Max. wymiary (szer. × gł. × wys.)	430 × 660 × 420 mm
Waga (netto)	Do 25 kg
Opcjonalnie	Możliwość rozbudowy o dodatkowy podajnik na 550 arkuszy
Sterowniki	Windows 7, 8, 8.1, 10 - 32 oraz 64 bitowe, Mac OS, Android
Fabrycznie zainstalowane tonery startowe	czarny do 2400 stron A4 kolorowe do 1200 stron A4
Gwarancja	Naprawa u klienta 1 rok