Załącznik nr 5 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup sprzętu informatycznego

dla Urzędu Miasta Rawa Mazowiecka

zamówienie realizowane w ramach projektu :

„rawski eUrząd

- wdrożenie elektronicznych usług w Urzędzie Miasta Rawa Mazowiecka”

WYMAGANIA OGÓLNE

I. Zakres zamówienia

Zadanie I Infrastruktura teleinformatyczna

I.1.	Modernizacja serwerowni	1 komplet
I.2.	Szafa rack 42U	1 komplet
I.3.	UPS	1 komplet
I.4.	Zabezpieczenie styku z Internetem	1 komplet
I.5.	Przełącznik dostępowy	4 komplety
I.6.	Acess Point	8 kompletów
I.7.	Kontroler Acess Pointów	1 komplet

Zadanie 2 Sprzęt komputerowy

II.1.	Komputer PC	30 kompletów
II.2.	Laptop typ A	6 kompletów
II.3.	Laptop typ R	20 kompletów

Zadanie 3 Oprogramowanie

III.1.	Pakiet bezpieczeństwa danych	1 sztuka
III.2.	Pakiet biurowy	36 sztuk

II. Wymagany termin realizacji zamówienia. - do 60 dni od daty podpisania umowy (zgodnie z terminem zadeklarowanym przez wykonawce w ofercie)

III. Podmioty biorące udział w zamówieniu - Urząd Miasta Rawa Mazowiecka

IV. Wymagania ogólne dla dostarczanych rozwiązań.

1. Rozwiązania dostarczone i uruchomione w ramach niniejszego zamówienia, musi funkcjonować zgodnie z obowiązującymi w Polsce przepisami prawa.
2. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów sprzętu.
3. Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by były nieużywane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania.
4. Wykonawca zapewnia, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
5. Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
6. Oferowane oprogramowanie w dniu składania ofert nie może być przeznaczone przez producenta do wycofania z produkcji, sprzedaży lub wsparcia technicznego.
7. Do dostarczonego oprogramowania należy dostarczyć licencje potwierdzające legalność użytkowania
8. W ofercie wymagane jest podanie producenta sprzętu, modelu oraz symbolu urządzenia.

V. Warunki gwarancji i rękojmi

1. Zamawiający wymaga udzielenia minimum 36 miesięcznej gwarancji producenta na wszystkie komponenty zaproponowane w ofercie (materiały, urządzenia, oprogramowanie i usługi).
2. Okres trwania gwarancji rozpocznie się z chwilą podpisania Protokołu Odbioru Końcowego.
3. Serwis gwarancyjny musi być świadczony w miejscu instalacji urządzenia (o ile nie określono inaczej), a w przypadku konieczności naprawy uszkodzonego sprzętu poza miejscem jego zainstalowania,
4. Zamawiający wymaga zapewnienia reakcji serwisowej, rozumianej jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym, najpóźniej następnego dnia roboczego po zgłoszeniu awarii, w godzinach pracy Zamawiającego.
5. Usługi gwarancyjne obejmują wykonywanie diagnostyki i napraw, w tym wymianę elementów, uszkodzonych urządzeń lub podzespołów (również zużytych) na nowe o takich samych lub lepszych parametrach.
6. Usługi gwarancyjne dla usług instalacji i konfiguracji obejmują rozwiązywanie i usuwanie problemów wynikających z wykonanych przez Wykonawcę prac.
7. Usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) musi zostać wykonana do końca następnego dnia roboczego od momentu podjęcia reakcji serwisowej.
8. W przypadku urządzenia, dla którego wymagany jest dłuższy czas na naprawę, Zamawiający dopuszcza podstawienie na czas naprawy urządzenia zastępczego o parametrach funkcjonalnych nie gorszych niż urządzenie uszkodzone . Naprawa w takim przypadku nie może przekroczyć 30 dni roboczych od momentu zgłoszenia usterki.
9. Urządzenie zastępcze zostanie podstawione przez podmiot świadczący usługi serwisu gwarancyjnego i skonfigurowane (według wymogów Zamawiającego) do pracy w warunkach produkcyjnych na koszt Wykonawcy. Urządzenie zastępcze nie będzie wymagało dodatkowych prac konfiguracyjnych po stronie Zamawiającego.
10. W przypadku awarii urządzenia, które było naprawiane dwa razy Wykonawca zobowiązany jest wymienić to urządzenia na nowe, wolne od wad.
11. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon w godzinach pracy Zamawiającego oraz przez e-mail lub stronę www przez całą dobę;
12. Wszelkie koszty związane z naprawami gwarancyjnymi, usuwaniem ujawnionych awarii, a także konserwacją i diagnostyką urządzeń, włączając w to koszt części i transportu z i do siedziby Zamawiającego, itp. ponosi Wykonawca.
13. Wykonawca w ramach świadczenia usług gwarancyjnych, zobowiązuje się do zwrotu kosztów naprawy gwarancyjnej zrealizowanej przez Zamawiającego w przypadku, gdy dwukrotnie bezskutecznie wzywał Wykonawcę do jej wykonania, a ten jej nie wykonał lub wykonał nieskutecznie.
14. Wykonawca w ramach świadczenia usług gwarancyjnych, zobowiązuje się do zapewnienia dostępu do najnowszych sterowników i uaktualnień na stronie producenta realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu.
15. Zamawiający wymaga, by usługi gwarancyjne były świadczone przez producenta urządzenia bądź przez podmiot świadczący usługi serwisu gwarancyjnego, który jest autoryzowany przez producenta urządzenia w obszarze usług serwisu gwarancyjnego.
16. Zamawiający wymaga, by dla wszystkich urządzeń wymienionych w rozdziałach II.1 do II.3 usługi gwarancyjne były świadczone przez firmę/firmy serwisujące, które posiadają:
    - 16.1. ISO 9001: 2000 na świadczenie usług serwisowych
    - 16.2. autoryzacje producenta komputera.
    - 16.3. możliwość telefonicznego i przez stronę www sprawdzenia konfiguracji sprzętowej i warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela (należy podać link do strony)
    - 16.4. możliwość dostępu do najnowszych sterowników i uaktualnień na stronie producenta urządzenia, realizowany poprzez podanie na dedykowanej stronie internetowej numeru seryjnego lub modelu komputera (należy podać link do strony)

16.5. Zgłoszenia serwisowe muszą odbywać się w języku polskim, zgłaszane na infolinię w polskiej strefie numeracyjnej (należy podać adres email, nr telefonu i formularz zgłoszeniowy online (link www). pod którymi Zamawiający będzie mógł dokonywać zgłoszeń serwisowych

17. W przypadku wyboru oferty Wykonawcy jako najkorzystniejszej, Wykonawca będzie miał obowiązek dostarczenia dokumentów wymienionych w punktach od 16.1 do 16.5, potwierdzonych za zgodność z oryginałem w dniu dostawy. Niedostarczenie Zamawiającemu choćby jednego dokumentu wymienionego w punktach od 16.1 do 16.5 w wymaganym terminie, będzie skutkowało nieodebraniem sprzętu.

VI. Wymagania związane z promocją unijnego źródła dofinansowania.

Projekt „rawski eUrząd -wdrożenie elektronicznych usług w Urzędzie Miasta Rawa Mazowiecka" jest współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Łódzkiego na lata 2014 – 2020, Osi Priorytetowej VII: Infrastruktura dla usług społecznych, Działania VII.1 Technologie informacyjno-komunikacyjne, Poddziałanie VII.1.1 Technologie informacyjno-komunikacyjne – ZIT, na podstawie umowy o dofinansowanie nr UDA- RPLD.07.01.02-10-0019/17-00 z dnia 1 grudnia 2017 roku.

Do obowiązku Wykonawcy należy oznakowanie sprzętu zgodnie z wymaganiami Instytucji Zarządzającej RPO WŁ na lata 2014-2020. Wszystkie działania promocyjne projektu muszą być zgodne z „Podręcznikiem wnioskodawcy i beneficjanta programów polityki spójności 2014 -2020 w zakresie informacji i promocji" oraz z wymogami, o których mowa w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 1303/2013 z dnia 17 grudnia 2013 roku, Załączniku II do rozporządzenia Wykonawczego Komisji (UE) nr 821/2014 z dnia 28 lipca 2014 roku oraz innymi obowiązującymi regulacjami odwołującymi się do kwestii związanych z promocją.

VII. SZCZEGÓŁOWY OPIS

Zadanie I Infrastruktura teleinformatyczna

W ramach zadania Infrastruktura teleinformatyczna Wykonawca ma obowiązek wykonać wszelkie konieczne do prawidłowego funkcjonowania urządzeń prace instalacyjne i konfiguracyjne oraz dostarczyć sprzęt i urządzenia spełniające minimalne wymagania techniczne i funkcjonalne opisane poniżej.

I.1 Modernizacja serwerowni 1 komplet

Modernizacja istniejącej serwerowni będzie polegała na :

1. Dostawie i montażu drzwi antywłamaniowych. Drzwi antywłamaniowe muszą spełniać wymagania:
   - 1.1. Konstrukcja drzwi zgodna z wymaganiami::
     - 1.1.1. Klasa C według PN-90/B-92270
     - 1.1.2. Klasa EI-30 według PN-B-02871: 1996
     - 1.1.3. Wymiary drzwi w świetle ościeżnicy: 1,00m x 2,00m
     - 1.1.4. Podczas dostawy należy załączyć certyfikaty potwierdzające spełnienie w.w. norm
   - 1.2. Zamek główny rozporowy blokujący w górę, dół i bok
   - 1.3. Samozamykacz przyciągający drzwi.
   - 1.4. Zamek elektroniczny + elektrozaczep
   - 1.5. Akumulator podtrzymujący zasilanie w przypadku braku prądu
2. Dostawie i instalacji klimatyzacji:
   - 2.1. Rodzaj klimatyzacji: stacjonarny typy split
   - 2.2. o mocy minimalnej: 5 kW
3. Wyposażeniu serwerowni w system nadzoru

Do obowiązków Wykonawcy w ramach niniejszego zadania należy instalacja systemu kontroli dostępu zgodnego z wymaganiami rozporządzenia Ministra Spraw Wewnętrznych i Administracji (Dz. U. z dnia z dnia 1 maja 2004 r. oraz Dz. U. z dnia 13.10.2005 r) obejmujący minimum:

- 3.1. Zestaw do kontroli dostępu:
  - 3.1.1. Kontroler ITSupervisor (zasilacz, moduł Ethernet, rack 19" 1U)
  - 3.1.2. Czytnik zbliżeniowy
  - 3.1.3. Karty zbliżeniowe dla min 5 osób
  - 3.1.4. Klawiatura sterująca drzwiami
  - 3.1.5. Możliwość zaprogramowania do 5 użytkowników
- 3.2. instalacja czujników z funkcjami alarmowania administratorów sygnalizujących:
  - 3.2.1. Kontroler temperatury i wilgotności (z wyświetlaczem LED)
  - 3.2.2. Czujnik temperatury (bez wyświetlacza)
  - 3.2.3. Układ kontroli zasilania (trójfazowy)
  - 3.2.4. Czujnik wycieku wody (punktowy) – 3 komplety
  - 3.2.5. Czujka PPOŻ (optyczna, z autoresetem)
  - 3.2.6. Czujnik otwarcia drzwi (kontaktron)
  - 3.2.7. Przycisk resetu sygnalizacji optyczno-dźwiękowej (natynkowy)

I.2 Szafa rack 42U 1 komplet

Dostawa wraz z instalacją szafy przemysłowej typu rack, o następujących parametrach:

1. Szafa typu 19" 42U 800/1000/1980 (szer/gł/wys) RAL7035, profil aluminiowy).
2. Drzwi przednie i tylne metalowo-szklane, zdejmowane, zamykane na klucz.
3. Minimum 3 sztuki listew zasilających z min. 6 gniazdami każda (gniazda typu FR z bolcem) dostarczonych wraz z kompletem uchwytów umożliwiających montaż listew w szafie.
4. Konsola LCD do instalacji w szafie Rack 19" o rozmiarze max. 1U
   4.1. dostarczona wraz z kompletem uchwytów umożliwiających montaż w szafie Rack.
   4.2. konsola LCD o przekątnej wyświetlacza min. 18" wyposażona w klawiaturę wysuwaną w standardzie Qwerty wraz z dotykowym urządzeniem wskazującym typu touchpad.
5. Przełącznik KVM powinien pozwalać na podłączenie do 4 serwerów/komputerów
6. Wraz z przełącznikiem KVM wymagane jest dostarczenie 4 kabli o dł min. 2,1 metra do podłączenia serwerów za pomocą złącz VGA/USB.

I.3 UPS 1 komplet

Dostawa wraz z instalacją urządzenie bezprzerwowego zasilania, o następujących parametrach:

1. Obudowa wolnostojąca lub typu rack do zamontowania w zaoferowanej (pkt 2) szafie rack,
2. Typu smart
3. Moc pozorna - 3000 VA
4. Moc rzeczywista - 2600 Wat
5. Gniazda : 6 x C13 (10A) i 2 x C19 (16A) z podtrzymaniem zasilania i ochroną przepięciową
6. Architektura UPSa: on-line, bypass serwisowy
7. Maks. czas przełączenia na baterię - 0 ms
8. Czas podtrzymania dla obciążenia 100% - 10 min
9. Czas podtrzymania przy obciążeniu 50% - 20 min

I.4 Zabezpieczenie styku z Internetem 1 komplet

1. Wymagania Ogólne
   1.1. 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.
   1.2. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
   1.3. 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. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu.
   1.4. System musi wspierać IPv4 oraz IPv6 w zakresie:
      1.4.1. Firewall.
      1.4.2. Ochrony w warstwie aplikacji.
      1.4.3. Protokołów routingu dynamicznego.

2. Redundancja, monitoring i wykrywanie awarii
   2.1. 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.
   2.2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
   2.3. Monitoring stanu realizowanych połączeń VPN.
   2.4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
3. Interfejsy, Dysk, Zasilanie:
   3.1. System realizujący funkcję Firewall musi dysponować minimum:
      3.1.1. 20 portami Gigabit Ethernet RJ-45.
      3.1.2. 2 gniazdami SFP 1 Gbps.
   3.2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
   3.3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
   3.4. System musi być wyposażony w zasilanie AC.
4. Parametry wydajnościowe:
   4.1. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę.
   4.2. Przepustowość Stateful Firewall: nie mniej niż 7.4 Gbps dla pakietów 512 B.
   4.3. Przepustowość Stateful Firewall: nie mniej niż 4.4 Gbps dla pakietów 64 B.
   4.4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps.
   4.5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 4 Gbps.
   4.6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 1.9 Gbps.
   4.7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps.
   4.8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 190 Mbps.
5. Funkcje Systemu Bezpieczeństwa:
   5.1. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
      5.1.1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
      5.1.2. Kontrola Aplikacji.
      5.1.3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
      5.1.4. Ochrona przed malware – min. dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
      5.1.5. Ochrona przed atakami - Intrusion Prevention System.
      5.1.6. Kontrola stron WWW.
      5.1.7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
      5.1.8. Zarządzanie pasmem (QoS, Traffic shaping).
      5.1.9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

5.1.10. 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.

5.1.11. Analiza ruchu szyfrowanego protokołem SSL.

5.1.12. Analiza ruchu szyfrowanego protokołem SSH.

6. Polityki, Firewall

6.1. System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW.

6.1.1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

6.1.2. musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

6.1.2.1. Translację jeden do jeden oraz jeden do wielu.

6.1.2.2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

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

7. Połączenia VPN

7.1. System musi umożliwiać konfigurację połączeń typu IPSec VPN, w tym:

7.1.1. Wsparcie dla IKE v1 oraz v2.

7.1.2. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).

7.1.3. Obsługa protokołu Diffie-Hellman grup 19 i 20.

7.1.4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.

7.1.5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

7.1.6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

7.1.7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

7.1.8. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.

7.1.9. Mechanizm „Split tunneling" dla połączeń Client-to-Site.

7.2. System musi umożliwiać konfigurację połączeń typu SSL VPN, w tym:

7.2.1. 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.

7.2.2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

8. Routing i obsługa łączy WAN

8.1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

8.1.1. Routingu statycznego.

8.1.2. Policy Based Routingu.

8.1.3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

8.2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

9. Zarządzanie pasmem

9.1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

9.2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
9.3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

10. Kontrola Antywirusowa
10.1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
10.2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
10.3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
10.4. System musi dysponować sygnaturami do ochrony urządzeń mobilnych

11. Ochrona przed atakami
11.1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
11.2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
11.3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz sygnatur.
11.4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
11.5. 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.
11.6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

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

13. Kontrola WWW
13.1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
13.2. 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 avoidance.
13.3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
13.4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
13.5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
13.6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

14. Uwierzytelnianie użytkowników w ramach sesji
    14.1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
        14.1.1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
        14.1.2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
        14.1.3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
    14.2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
    14.3. Możliwość budowy architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
15. Zarządzanie
    15.1. 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.
    15.2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
    15.3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
    15.4. Współpracowa z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
    15.5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
    15.6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
16. Logowanie
    16.1. System musi mieć możliwość logowania do aplikacji udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony system logowania i raportowania w postaci odpowiednio zabezpieczonej, platformy sprzętowej.
    16.2. W ramach logowania system 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
    16.3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
    16.4. Musi istnieć możliwość logowania do serwera SYSLOG.
17. Elementy oferowanego systemu bezpieczeństwa muszą posiadać następujące certyfikacje:
    17.1. ICSA lub EAL4 dla funkcji Firewall.
    17.2. ICSA lub NSS Labs dla funkcji IPS.
    17.3. ICSA dla funkcji IPSec VPN.
    17.4. ICSA dla funkcji SSL VPN.
18. Razem z urządzeniem muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:
        18.1.1. Kontrola Aplikacji,
        18.1.2. IPS,
        18.1.3. Antywirus,
        18.1.4. Antyspam,
        18.1.5. Web Filtering

I.5 Przełącznik dostępowy - 4 komplety

1. Obudowa do montażu w szafie rack 19", o wysokości nie więcej niż 1U, wraz z kompletem szyn.
2. minimum 24 portów GigabitEthernet w standardzie BaseT
3. minimum 2 zintegrowane porty 1Gb Ethernet SFP;
4. minimum 1 port do konfiguracji przełącznika;
5. Przepustowość Non-blocking: min 26Gbps
6. Zdolność Przełączania na poziomie minimum 52 Gbps
7. Prędkość przełączania: minimum 38 Mpps
8. Pobór mocy nie więcej niż 25 W

I.6 Acess Point – 8 kompletów

1. Architektura radiowa i obsługa standardów
   1.1. Obsługa MIMO 2x2:2
   1.2. Moduł radiowy 802.11 b/g/n/ac
2. Obsługa zakresów częstotliwości
   2.1. 2,412 – 2,484 GHz
   2.2. 5,150 – 5,250 GHz (UNII-1)
   2.3. 5,250 – 5,350 GHz (UNII-2)
3. Zasilanie:
   3.1.1.PoE (IEEE 802.3af)
   3.1.2.Adapter AC
4. Interfejs; 1 x 100/1000 Base-T
5. Mechanizmy bezpieczeństwa
   5.1. WEP, WPA, WPA2-PSK, WPA2-Enterprise (802.1X)
   5.2. Szyfrowanie TKIP oraz AES
   5.3. Szyfrowanie IPSec w celu tunelowania danych do koncentratora VPN
   5.4. Blokowanie ruchu między klientami bezprzewodowymi
6. Funkcje ogólne
   6.1. Konfiguracja min. 6 SSID
   6.2. Zarządzanie przez interfejs webowy
   6.3. Logowanie zdarzeń systemowych.

I.7 Kontroler sieci bezprzewodowej – 1 komplet

1. Konfiguracja punktów dostępowych
2. Zarządzanie politykami bezpieczeństwa
3. Zarządzanie politykami QoS
4. Dobór obsługiwanych kanałów na punktach dostępowych
5. Monitorowanie pasma radiowego pod kątem wykrywania interferencji, pomiaru poziomu utylizacji i szumów w celu dynamicznej optymalizacji ustawień parametrów radiowych
6. Zarządzanie mobilnością urządzeń
7. Zarządzanie budową sieci kratowej.

Zadanie II Sprzęt komputerowy

W ramach zadania Sprzęt komputerowy Wykonawca ma obowiązek dostarczyć i skonfigurować w środowisku sieciowym Zamawiającego urządzenia spełniające minimalne wymagania techniczne i funkcjonalne opisane poniżej. W ofercie wymagane jest podanie producenta sprzętu, modelu oraz symbolu proponowanego urządzenia.

II.1 Komputer PC – 30 kompletów

Komputery stacjonarne będą wykorzystywane do pracy z aplikacjami biurowymi, pocztą elektroniczną sieciowymi aplikacji dziedzinowymi oraz do dostępu do zasobów Internetu.

Wymagania minimalne:

1. Typ: Komputer stacjonarny
2. Obudowa:
- **2.1.** małogabarytowa typu Small Form Factor,
- **2.2.** fabrycznie przystosowana do pracy w układzie pionowym i poziomym
- **2.3.** obsługująca karty rozszerzeń o niskim profilu.
- **2.4.** nie dopuszcza się aby w bocznych ściankach obudowy były usytuowane otwory wentylacyjne, cyrkulacja powietrza tylko przez przedni i tylny panel z zachowaniem ruchu powietrza przód -> tył lub tył -> przód.
- **2.5.** otwierana jest bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych)
- **2.6.** umożliwiająca zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady typu Kensington) oraz kłódki (oczko w obudowie do założenia kłódki).

3. Płyta główna - wyposażona w złącza i elementy wewnętrzne, zintegrowane z płytą główną:
- **3.1.** 1 x PCI Express x16 (niski profil),
- **3.2.** 1 x PCI Express x4 (niski profil),
- **3.3.** 2 x DIMM,
- **3.4.** 2 x SATA,
- **3.5.** TPM 2.0

4. Procesor osiągający średni wynik minimum 8000 punktów .Wykonawca ma obowiązek załączyć podczas dostawy wydruk ze strony https://www.cpubenchmark.net/ z datą nie wcześniej niż 14 dni przed dostawą ze wskazaniem wiersza odpowiadającego właściwemu wynikowi testów. Wydruk musi być podpisany przez Wykonawcę. Brak dokumentu potwierdzającego wynik testu, będzie skutkował uznaniem oferowanego urządzenia jako niespełniającego wymagań s.i.w.z.

5. Pamięć operacyjna 8GB RAM DDR4
- **5.1.** możliwość rozbudowy do minimum 32 GB
- **5.2.** Co najmniej jeden bank pamięci wolny

6. Dysk twardy o pojemności min. 1 TB; SATA 3

7. Karta graficzna zintegrowana z procesorem, pamięć współdzielona z pamięcią RAM, dynamicznie przydzielana, umożliwiająca pracę dwumonitorową

8. Karta sieciowa 10/100/1000 Ethernet RJ 45, wspierająca Wake On LAN

9. Karta dźwiękowa minimum 24-bitowa, zgodna z High Definition HD Audio

10. Wbudowane porty i złącza:
- **10.1.** Przód obudowy minimum:
  - 10.1.1. 2 x USB 3.0 (3.1 Gen 1) Typ A,
  - 10.1.2. 2 x USB 2.0,
  - 10.1.3. 1 x złącze mikrofonowe
  - 10.1.4. 1 x złącze słuchawkowe,
- **10.2.** Tył obudowy minimum:
  - 10.2.1. 2 x USB 3.0 (3.1 Gen 1) Typ A,
  - 10.2.2. 2 x USB 2.0,
  - 10.2.3. 1 x RJ-45 Gigabit Ethernet (wsparcie dla WoL oraz PXE 2.1)
  - 10.2.4. 2 x złącza cyfrowe graficzne

11. Zasilacz
- **11.1.** o mocy maksymalnej 250W, 230V 50/60Hz
- **11.2.** o sprawności minimum 92% przy obciążeniu zasilacza na poziomie 50%

12. Dodatkowe wyposażenie:
- **12.1.** Klawiatura USB w układzie QWERTY US. Na klawiszach laserowe nadruki odporne na ścieranie. Wydzielona sekcja klawiszy numerycznych.
- **12.2.** Mysz optyczna USB z dwoma klawiszami oraz rolką.
- **12.3.** Czujnik otwarcia obudowy.
- **12.4.** Wbudowany głośnik.

13. Zainstalowane oprogramowanie:
- **13.1.** typy licencji: licencje bezterminowe
- **13.2.** system operacyjny zgodny z wymaganiami opisanymi w rozdziale III.4
- **13.3.** oprogramowanie administracyjne zapewniające aktualizację sterowników w tym karty graficznej, kontrolera sieci, kontrolera dźwięku oraz aktualizację systemu BIOS poprzez pobranie ręczne i według określonego harmonogramu, ze strony producenta komputera;
- **13.4.** oprogramowanie współpracujące z czujnikiem otwarcia obudowy;

14. Zgodności i Certyfikaty:
- **14.1.** Deklaracja zgodności CE
- **14.2.** Certyfikat ISO 9001:2015 dla producenta sprzętu
- **14.3.** Certyfikat ISO 14001 dla producenta sprzętu
- **14.4.** Certyfikat Energy Star min. 7.0 – komputer musi znajdować się na liście zgodności dostępnej na stronie www.energystar.gov lub www.eu-energystar.org w postaci wydruku ze strony
- **14.5.** Potwierdzenie spełnienia kryteriów środowiskowych - zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta,
- **14.6.** certyfikat TCO, wymagana publikacja na stronie http://tcocertified.com/product-finder/ lub posiada certyfikat EPEAT Gold, wymagana publikacja na stronie https://ww2.epeat.net/searchoptions.aspx (wymagana zgodność płyty głównej) Potwierdzenie kompatybilności komputera z zaoferowanym systemem operacyjnym w postaci wydruku ze strony producenta oprogramowania
- **14.7.** W przypadku wyboru oferty Wykonawcy jako najkorzystniejszej, Wykonawca będzie miał obowiązek dostarczenia dokumentów wymienionych w punktach od 14.1 do 14.6, potwierdzonych za zgodność z oryginałem przez Wykonawcę najpóźniej w dniu dostawy. Niedostarczenie Zamawiającemu choćby jednego dokumentu wymienionego w punktach od 14.1 do 14.6 w wymaganym terminie, będzie skutkowało brakiem podpisania protokołu odbioru.

15. Przewody połączeniowe
- **15.1.** do połączenia sieciowego UTP RJ-45 o długości min. 2,5 m
- **15.2.** przewód zasilający

16. Monitor:
- **16.1.** Rozmiar ekranu: 24'' +/- 0,5"
- **16.2.** Proporcja ekranu 16:9 lub 16:10
- **16.3.** Ekran ciekłokrystaliczny z podświetleniem LED
- **16.4.** Antyodblaskowa powłoka powierzchni ekranu
- **16.5.** Rozdzielczość 1920 x 1080 przy 60Hz
- **16.6.** Maksymalny rozmiar plamki 0,275mm
- **16.7.** Jasność: min. 250 cd/m2
- **16.8.** Kontrast: typowy 1000:1, dynamiczny 20.000:1
- **16.9.** Kąty widzenia (pion/poziom) 178/178 stopni
- **16.10.** Maksymalny czas reakcji matrycy 5 ms
- **16.11.** Pochylenie monitora w zakresie : -5 do 30 stopni
- **16.12.** Wydłużenie w pionie minimum 150 mm
- **16.13.** Funkcja PIVOT
- **16.14.** Głośniki: 2 x 2W

16.15. Złącza:

16.16. 1 x HDMI

16.17. 1 x DVI-D (HDCP)

16.18. 1 x D-SUB

16.19. 1x 3,5mm jack signal input

16.20. 1x 3,5mm jack signal output

16.21. 2 x USB 2.0

16.22. 1 x USB (out)

16.23. Zasilacz wbudowany w monitor

16.24. Przewody sygnałowe:

16.25. przewód zasilający,

16.26. kabel DVI-D

16.27. kabel USB

16.28. kabel audio

16.29. Certyfikaty i standardy:

16.29.1. Certyfikat zgodności z normą ISO 13406-2 lub ISO 9241-307 (pixel fault class 1)

16.29.2. Certyfikat Energy Star min. 7.x– monitor musi znajdować się na liście zgodności dostępnej na stronie www.energystar.gov lub www.eu-energystar.org

16.29.3. Certyfikat TCO Certified Displays 7.0 - wydruk ze strony http://tcocertified.com/ dla oferowanego modelu

16.29.4. W przypadku wyboru oferty Wykonawcy jako najkorzystniejszej, Wykonawca będzie miał obowiązek dostarczenia dokumentów wymienionych w punktach od 16.29.1 do 16.19.3 potwierdzonych za zgodność z oryginałem przez Wykonawcę najpóźniej w dniu dostawy. Niedostarczenie Zamawiającemu choćby jednego dokumentu wymienionego powyżej w wymaganym terminie, będzie skutkowało brakiem podpisania protokołu odbioru.

II.2 Laptop typ A– 6 kompletów

Komputery przenośne będą wykorzystywane do pracy z aplikacjami biurowymi, pocztą elektroniczną sieciowymi aplikacji dziedzinowymi oraz do dostępu do zasobów Internetu.

Wymagania minimalne:

1. Ekran:
   1.1. Ekran o przekątnej 13,3" -15,6"
   1.2. Rozdzielczość 1920 x 1080 pikseli
   1.3. Matryca matrycą antyrefleksyjną lub matową
2. Procesor:
   2.1. procesor klasy x86, zaprojektowany do pracy w komputerach mobilnych
   2.2. osiągający średnią w teście CPU Mark wynik min.: 5000 punktów. Wykonawca ma obowiązek załączyć podczas dostawy wydruk ze strony https://www.cpubenchmark.net/ z datą nie wcześniej niż 14 dni przed dostawą ze wskazaniem wiersza odpowiadającego właściwemu wynikowi testów. Wydruk musi być podpisany przez Wykonawcę. Brak dokumentu potwierdzającego wynik testu, będzie skutkował uznaniem oferowanego urządzenia jako niespełniającego wymagań s.i.w.z.
3. Pamięć RAM: 8GB DDR4 z możliwością rozbudowy do 32 GB, minimum jeden slot wolny z przeznaczeniem do rozbudowy pamięci
4. Dysk twardy:
   4.1. 256 GB SSD zamontowany w złączu M.2
   4.2. zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników
5. Multimedia:
   5.1. Karta graficzna: zintegrowana z możliwością dynamicznego przydzielenia pamięci systemowej na potrzeby grafiki w trybie UMA (Unified Memory Access). Obsługująca funkcje: DirectX 12, OpenGL 4.4, OpenCL 2.0
   5.2. karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition
   5.3. wbudowane w obudowę głośniki stereo
   5.4. mikrofon z funkcją redukcji szumów wbudowany w obudowę matrycy
   5.5. kamera internetowa HD zainstalowana w obudowie matrycy
6. Zintegrowana z płytą główną karta sieci LAN 10/100/1000 Ethernet
7. Zintegrowana z płytą główną karta WLAN, obsługująca standard IEEE 802.11 ac
8. Moduł Bluetooth 4.x zintegrowany z płytą główną
9. Porty i złącza:
   9.1. 1x USB Typ-C,
   9.2. 2x USB 3.0,
   9.3. 1x 19-pin HDMI
   9.4. RJ45 Gigabit Ethernet,
   9.5. 1 x złącze mikrofonowe i 1 x złącze słuchawkowe lub złącze współdzielone typu combo,
   9.6. czytnik kart SD lub microSD.
   9.7. złącze słuchawkowe stereo i złącze mikrofonowe (dopuszczalne także w formie tzw. combo)
10. Klawiatura wyspowa, w układzie US–QWERTY, odporna na zachlapanie,
11. Touchpad wyposażony w 2 niezależne klawisze funkcyjne ze strefą przewijania w pionie, w poziomie wraz ze wsparciem dla technologii multitouch
12. Bateria:
    12.1. o pojemności minimum 50 Wh
    12.2. umożliwiająca pracę przy braku zewnętrznego zasilania przez minimum 12 godzin.
    12.3. Technologia Quick Charge pozwalająca naładować baterie do 80% w 1h.
13. Zasilacz dostosowany mocą do zaoferowanej konfiguracji zgodnie z zaleceniami producenta, wyposażony w kabel zasilający z uziemieniem.
14. Waga: maksymalnie 2 kg z baterią
15. Bezpieczeństwo:
    15.1. Złącze typu Kensington Lock lub równoważne,

15.2. 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.

16. Zainstalowane oprogramowanie:
    16.1. system operacyjny zgodny z wymaganiami opisanymi w rozdziale III.4
17. Teczka na komputer
    17.1. wykonana z trwałego materiału chroniącego komputer przed warunkami pogodowymi,
    17.2. umożliwiająca bezpieczne przenoszenie notebooka w oddzielnej, wyścielanej przegrodzie,
    17.3. umożliwiająca noszenie przy użyciu rączek lub odłączanego, regulowanego paska na ramię
    17.4. posiadająca wyznaczone przegrody na dokumenty i na materiały biurowe;
18. Bezprzewodowa mysz optyczna z dwoma klawiszami oraz rolką (scroll).
19. Gwarancja 36 miesięcy door-to-door, świadczona przez autoryzowany przez producenta serwis.
20. Zgodności i Certyfikaty:
    20.1. Deklaracja zgodności CE
    20.2. Certyfikat ISO 9001:2015 dla producenta sprzętu
    20.3. Certyfikat ISO 14001 dla producenta sprzętu
    20.4. Certyfikat EnergyStar min. 7.0 – komputer musi znajdować się na liście zgodności dostępnej na stronie http://energystar.gov w postaci wydruku z w.w. strony
    20.5. Potwierdzenie spełnienia kryteriów środowiskowych - zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki

II.3 Laptop typ R – 20 kompletów

Komputery przenośne będą wykorzystywane do pracy z aplikacjami biurowymi, pocztą elektroniczną sieciowymi aplikacji dziedzinowymi oraz do dostępu do zasobów Internetu.

Wymagania minimalne:

1. Ekran:
   1.1. Ekran o przekątnej 13,3" z tolerancją -0,3”/+0,7”
   1.2. Rozdzielczość 1920 x 1080 pikseli
   1.3. Matryca matrycą antyrefleksyjną lub matową
2. Procesor:
   2.1. procesor klasy x86, zaprojektowany do pracy w komputerach mobilnych
   2.2. osiągający średnią w teście CPU Mark wynik min.: 4000 punktów. Wykonawca ma obowiązek załączyć podczas dostawy wydruk ze strony https://www.cpubenchmark.net/ z datą nie wcześniej niż 14 dni przed dostawą ze wskazaniem wiersza odpowiadającego właściwemu wynikowi testów. Wydruk musi być podpisany przez Wykonawcę. Brak dokumentu potwierdzającego wynik testu, będzie skutkował uznaniem oferowanego urządzenia jako niespełniającego wymagań s.i.w.z.
3. Pamięć RAM: 8GB DDR4 z możliwością rozbudowy do 32 GB, minimum jeden slot wolny z przeznaczeniem do rozbudowy pamięci
4. Dysk twardy:
   4.1. 256 GB SSD zamontowany w złączu M.2
   4.2. zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników
5. Multimedia:
   5.1. Karta graficzna: zintegrowana z możliwością dynamicznego przydzielenia pamięci systemowej na potrzeby grafiki w trybie UMA (Unified Memory Access). Obsługująca funkcje: DirectX 12, OpenGL 4.4, OpenCL 2.0
   5.2. karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition
   5.3. wbudowane w obudowę głośniki stereo
   5.4. mikrofon z funkcją redukcji szumów wbudowany w obudowę matrycy
   5.5. kamera internetowa HD zainstalowana w obudowie matrycy
6. Zintegrowana z płytą główną karta sieci LAN 10/100/1000 Ethernet
7. Zintegrowana z płytą główną karta WLAN, obsługująca standard IEEE 802.11 ac
8. Moduł Bluetooth 4.x zintegrowany z płytą główną
9. Porty i złącza:
   9.1. 1x USB Typ-C,
   9.2. 2x USB 3.0,
   9.3. 1x 19-pin HDMI
   9.4. RJ45 Gigabit Ethernet,
   9.5. 1 x złącze mikrofonowe i 1 x złącze słuchawkowe lub złącze współdzielone typu combo,
   9.6. czytnik kart SD lub microSD.
   9.7. złącze słuchawkowe stereo i złącze mikrofonowe (dopuszczalne także w formie tzw. combo)
10. Klawiatura wyspowa, w układzie US–QWERTY, odporna na zachlapanie,
11. Touchpad wyposażony w 2 niezależne klawisze funkcyjne ze strefą przewijania w pionie, w poziomie wraz ze wsparciem dla technologii multitouch
12. Bateria:
    12.1. o pojemności minimum 50 Wh
    12.2. umożliwiająca pracę przy braku zewnętrznego zasilania przez minimum 10 godzin.
    12.3. Technologia Quick Charge pozwalająca naładować baterie do 80% w 1h.
13. Zasilacz dostosowany mocą do zaoferowanej konfiguracji zgodnie z zaleceniami producenta, wyposażony w kabel zasilający z uziemieniem.
14. Waga: maksymalnie 2,5 kg z baterią
15. Bezpieczeństwo:
    15.1. Złącze typu Kensington Lock lub równoważne,

15.2. 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.

16. Zainstalowane oprogramowanie:
    16.1. system operacyjny zgodny z wymaganiami opisanymi w rozdziale III.4

17. Teczka na komputer
    17.1. wykonana z trwałego materiału chroniącego komputer przed warunkami pogodowymi,
    17.2. umożliwiająca bezpieczne przenoszenie notebooka w oddzielnej, wyścielanej przegrodzie,
    17.3. umożliwiająca noszenie przy użyciu rączek lub odłączanego, regulowanego paska na ramię
    17.4. posiadająca wyznaczone przegrody na dokumenty i na materiały biurowe;
18. Mysz optyczna USB z dwoma klawiszami oraz rolką (scroll).
19. Gwarancja 36 miesięcy door-to-door, świadczona przez autoryzowany przez producenta serwis.
20. Zgodności i Certyfikaty:
    20.1. Deklaracja zgodności CE
    20.2. Certyfikat ISO 9001:2015 dla producenta sprzętu
    20.3. Certyfikat ISO 14001 dla producenta sprzętu
    20.4. Certyfikat EnergyStar min. 7.0 – komputer musi znajdować się na liście zgodności dostępnej na stronie http://energystar.gov w postaci wydruku z w.w. strony
    20.5. Potwierdzenie spełnienia kryteriów środowiskowych - zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki

Zadanie III *Oprogramowanie*

Wykonawca ma obowiązek wykonać wszelkie konieczne do prawidłowego funkcjonowania prace instalacyjne i konfiguracyjne oraz dostarczyć oprogramowanie spełniające minimalne wymagania techniczne i funkcjonalne opisane poniżej.

III.1 Pakiet bezpieczeństwa danych 1 komplet

1. Do każdego z komputerów stacjonarnych opisanych w rozdziałach II.4, musi być dostarczone oprogramowanie systemu bezpieczeństwa danych (licencja nieograniczona czasowo).
2. Oprogramowanie musi być dostarczone w najnowszej stabilnej wersji systemu, przeznaczone dla architektury 64 bitowej i umożliwiać kompleksowe realizację backupu i odzyskiwania danych.
3. Funkcjonalności:
3.1. Synchronizacja i przywracanie
3.2. Wersjonowanie plików
3.3. Backup przyrostowy i różnicowy
3.4. Harmonogram backupu
3.5. Deduplikacja danych
3.6. Automatyczne przełączanie awaryjne
3.7. Ustawienie prędkości wysyłania
3.8. Ustawienie ilości przechowywanych wersji
3.9. Kontrola wykorzystania procesora
3.10. Transmisja protokołem SSL
3.11. Szyfrowanie algorytmem AES 256
3.12. Kompresja danych
3.13. Backup obrazu dysku

III.2 Pakiet biurowy 36 sztuk

Na komputerach stacjonarnych i przenośnych musi być zainstalowane oprogramowanie systemu biurowego spełniające minimum następujące funkcjonalności:

1. Wymagania ogólne:
   - 1.1. licencja umożliwiający pracę w jednostkach rządowych i samorządowych
   - 1.2. Pełna polska wersja językowa interfejsu użytkownika
   - 1.3. Intuicyjność obsługi,
   - 1.4. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się
   - 1.5. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
     - 1.5.1. posiada kompletny i publicznie dostępny opis formatu,
     - 1.5.2. ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
     - 1.5.3. umożliwia wykorzystanie schematów XML
     - 1.5.4. wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
   - 1.6. Oprogramowanie musi umożliwiać dostosowanie dokumentów do potrzeb oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców
   - 1.7. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy)
   - 1.8. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim
   - 1.9. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
     - 1.9.1. edytor tekstu
     - 1.9.2. arkusz kalkulacyjny
     - 1.9.3. narzędzie do przygotowywania i prowadzenia prezentacji
     - 1.9.4. narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)"
   - 1.10. Wymagania zawarte w specyfikacjach technicznych poszczególnych produktów odnoszą się do natywnej funkcjonalności oferowanego oprogramowania bez użycia dodatkowego oprogramowania.
   - 1.11. Licencja musi uwzględniać prawo (w okresie przynajmniej 3 lat) do bezpłatnej instalacji udostępnianych przez producenta uaktualnień i poprawek krytycznych i opcjonalnych
   - 1.12. Zamawiający wymaga dostarczenia kompletu wymaganych kluczy aktywacyjnych.
   - 1.13. Zamawiający wymaga dostarczenia dokumentów pozwalających na stwierdzenie legalności zakupionego oprogramowania dla celów inwentaryzacyjnych i audytowych
   - 1.14. Telefoniczne wsparcie techniczne w języku polskim w dni robocze zapewniony przez producenta przez co najmniej 3 lat od chwili zakupu
2. Edytor tekstu musi umożliwiać:

2.1. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
2.2. Wstawianie oraz formatowanie tabel
2.3. Wstawianie oraz formatowanie obiektów graficznych
2.4. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
2.5. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
2.6. Automatyczne tworzenie spisów treści
2.7. Formatowanie nagłówków i stopek stron
2.8. Sprawdzanie pisowni w języku polskim
2.9. Śledzenie zmian wprowadzonych przez użytkowników
2.10. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
2.11. Określenie układu strony (pionowa/pozioma)
2.12. Wydruk dokumentów
2.13. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną
2.14. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, Microsoft Word 2007 lub Microsoft Word 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu
2.15. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
2.16. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.
2.17. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.

3. Arkusz kalkulacyjny musi umożliwiać
3.1. Tworzenie raportów tabelarycznych
3.2. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
3.3. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu
3.4. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
3.5. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
3.6. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
3.7. Wyszukiwanie i zmianę danych
3.8. Wykonywanie analiz danych przy użyciu formatowania warunkowego
3.9. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
3.10. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
3.11. Formatowanie czasu, daty i wartości finansowych z polskim formatem
3.12. Zapis wielu arkuszy kalkulacyjnych w jednym pliku

3.13. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, Microsoft Excel 2007oraz Microsoft Excel 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń

3.14. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

4. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać

4.1. Prezentowanie przy użyciu projektora multimedialnego

4.2. Drukowanie w formacie umożliwiającym robienie notatek

4.3. Zapisanie, jako prezentacji tylko do odczytu

4.4. Nagrywanie narracji i dołączanie jej do prezentacji

4.5. Opatrywanie slajdów notatkami dla prezentera

4.6. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo

4.7. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego

4.8. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym

4.9. Możliwość tworzenia animacji obiektów i całych slajdów

4.10. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera

4.11. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i MS PowerPoint 2010

4.12. Możliwość publikacji prezentacji i jej prowadzenie z zewnętrznego źródła internetowego umożliwiającego oglądanie prezentacji przez użytkowników zewnętrznych posługujących się przeglądarką.

5. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:

5.1. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego

5.2. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców

5.3. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną

5.4. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy

5.5. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia

5.6. Zarządzanie kalendarzem

5.7. Udostępnianie kalendarza innym użytkownikom

5.8. Przeglądanie kalendarza innych użytkowników

5.9. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach

5.10. Zarządzanie listą zadań

5.11. Zlecanie zadań innym użytkownikom

5.12. Zarządzanie listą kontaktów

5.13. Udostępnianie listy kontaktów innym użytkownikom

5.14. Przeglądanie listy kontaktów innych użytkowników

5.15. Możliwość przesyłania kontaktów innym użytkowników

III.4 System operacyjny dla komputerów PC

System umożliwiający pracę w jednostkach rządowych i samorządowych.
System przeznaczony dla architektury 64 bitowej, spełniający następujące wymagania poprzez wbudowane mechanizmy (bez użycia dodatkowych aplikacji)

1. Integracja z usługą katalogową (np. Active Directory lub innej opartej na LDAP)
2. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   2.1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   2.2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet,
3. Interfejsy użytkownika dostępne w wielu językach do wyboru
4. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
5. Wbudowany system pomocy w języku polskim;
6. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
7. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
8. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.
9. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
10. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe lokalne i dziedziczone z serwerowego systemu operacyjnego – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
19. Mechanizm pozwalający zarejestrowanemu w systemie użytkownikowi na dostęp do zasobów tego systemu godnie z nadanymi uprawnieniami,
20. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
22. Obsługa standardu NFC (near field communication),
23. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);

24. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
25. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
26. Mechanizmy logowania do domeny w oparciu o:
    26.1. Login i hasło,
    26.2. karty z certyfikatami (smartcard),
27. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
28. Mechanizmy wieloelementowego uwierzytelniania.
29. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
30. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
31. Wsparcie dla algorytmów Suite B (RFC 4869),
32. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
33. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
34. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
35. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
36. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
37. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
38. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
39. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
40. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
41. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
42. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci
43. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.)
44. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
45. Wbudowany mechanizm wirtualizacji typu hypervisor,
46. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
47. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
48. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków.
49. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.