Załącznik nr 1 do umowy

Znak sprawy:
MCPS-WZK/AM/351-46 ZO/D

OPIS PRZEDMIOTU ZAMÓWIENIA

na dostawę urządzeń sieciowych i zasilaczy awaryjnych UPS na potrzeby Mazowieckiego Centrum Polityki Społecznej oraz urządzeń sieciowych, notebooków z oprogramowaniem i projektorów multimedialnych na potrzeby Wojewódzkiego Ośrodka Adopcyjnego w Warszawie

Część I – urządzenia sieciowe

Lp.	Przedmiot zakupu	Liczba szt.
1.	Punkt dostępowy HPE Aruba AP-505 (R2H28A) lub równoważny	5
2.	Przełącznik sieciowy z 48 portami 1G oraz 4 portami 10G SFP+	2
3.	Przełącznik sieciowy od 8 do 16 portów 1G z funkcją POE+ i 2 portami 10G SFP+	2
4.	Urządzenie UTM z funkcją routera	5
5.	Punkt dostępowy WiFi	5

Część II – notebooki z oprogramowaniem i projektory multimedialne

Lp.	Przedmiot zakupu	Liczba szt.
1.	Notebook z oprogramowaniem	6
2.	Mobilny projektor laserowy	3

Część III – zasilacze awaryjne UPS

Lp.	Przedmiot zakupu	Liczba szt.
1.	Zasilacz awaryjny UPS	2

Wymagania ogólne

1. Zaoferowany sprzęt musi spełniać europejskie wymogi bezpieczeństwa, w tym posiadać certyfikat CE.
2. Zamawiający dopuszcza złożenie ofert równoważnych, ale o parametrach nie gorszych niż wyspecyfikowane w dalszej części OPZ.
3. Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta – Zamawiający może wymagać przedstawiania dokumentów w dowolnym momencie realizacji Umowy oraz okresie gwarancji.

4. Firma serwisująca urządzenia musi posiadać certyfikat jakości według normy ISO 9001 lub równoważny certyfikat jakości na świadczenie usług serwisowych – Zamawiający może wymagać przedstawiania certyfikatów w dowolnym momencie realizacji Umowy oraz okresie gwarancji.
5. Sprzęt musi być dostarczony do siedziby Zamawiającego w godzinach jego pracy.
6. W przypadku licencji na oprogramowanie w postaci klucza aktywującego dostawa na e-mail Zamawiającego wskazany w umowie.
7. Wykonawca zapewnia, że dostarczone urządzenia i oprogramowanie będą nowe, nieużywane, będą pochodziły z oficjalnych kanałów dystrybucyjnych producenta i zostały wyprodukowane nie wcześniej niż w 2023 roku.
8. Wykonawca do każdego oferowanego asortymentu załączy kartę katalogową lub inny dokument potwierdzający spełnianie wymagań. W przypadku wątpliwości co do spełnienia wymagań oferta nie będzie oceniana.

Opisy sprzętu

Ad. Cz. I pkt 1. Punkt dostępowy HPE Aruba AP-505 (R2H28A) lub równoważny

1) Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz a/n/ac wave 2/ax, oraz 2.4GHz b/g/n/ax.
2) Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej Aruba
3) <u>Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera:</u>
   a) Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https
   b) Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki
   c) Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania.
4) Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2:
   a) System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego
   b) W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny
   c) Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe
   d) Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję
   e) Tworzenie klastra do 130 urządzeń

5) Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP
6) Punkt dostępowy musi mieć możliwość pracy jako analizator widma
7) W system operacyjny musi być wbudowana pełnostanowa zapora sieciowa
8) W system musi być wbudowany serwer DHCP
9) W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów
10) Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach:
    a) EAP-TLS
    b) PEAP-MSCHAPv2
    c) PEAP-GTC
    d) TTLS-MSCHAPv2
11) Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP
12) Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID
13) Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN
14) Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez:
    a) Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania
    b) Zewnętrzny portal WWW
15) Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT
16) Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne
17) Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:
    a) Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe
    b) Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu
    c) Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma
    d) Wykrywanie interferencji oraz miejsc bez pokrycia sygnału
    e) Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz
    f) Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac wave 2 oraz starszych (802.11b/g)
    g) Wsparcie dla 802.11d oraz 802.11h
    h) Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane
18) Minimalizacja interferencji związanych z sieciami 3G/4G LTE
19) Punkt dostępowy musi mieć wbudowany moduł Bluetooth Low Energy (BLE5.0) (co najmniej 7dBm) wykorzystywany w systemie nawigacji wewnątrzbudynkowej
20) Punkt dostępowy musi mieć wbudowany moduł Zigbee (802.15.4) (co najmniej 6dBm)

21) Obsługa roamingu klientów w warstwie 2
22) Obsługa monitoringu przez SNMP
23) Obsługa logowania na zewnętrznym serwerze SYSLOG
24) W system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci
25) W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci
26) Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:
    a) Widok diagnostyczny prezentujący problemy z sygnałem/prędkością
    b) Wykorzystanie pasma
    c) Ilość klientów korzystających z systemu/interferujących
    d) Ilość ramek wejściowych/wyjściowych dla każdego radia
    e) Ilość odrzuconych/błędnych ramek/s dla każdego radia
    f) Szum tła dla każdego radia
    g) Wyświetlanie logów systemowych
27) Punkt dostępowy musi posiadać co najmniej 2 wbudowane anteny pracujące w trybie 2x2 MIMO, z parametrami co najmniej: 4.3 dBi dla 2,4GHz, 5.5 dBi dla 5 GHz
28) Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac 1 Wave, 802.11ac 2 Wave, 802.11ax
29) Praca w trybie SU MIMO 2X2:2 dla 5GHz
30) Specyfikacja radia 802.11a/n/ac/ax:
    a) Obsługiwana technologia OFDM oraz OFDMA
    b) Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
    c) Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm
    d) Prędkości transmisji:
        - 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a,
        - MCS0-MCS23 (6,5Mbps do 450Mbps) dla 802.11n
        - MCS0-MCS9, NSS = 1-4 (6.5 Mbps do 1733 Mbps) dla 802.11ac
        - MCS0 do MCS11, NSS = 1-2 (3.6 Mbps do 574 Mbps) dla 802.11ax (2,4GHz)
        - MCS0 do MCS11, NSS = 1-4 (3.6 Mbps do 4803 Mbps) dla 802.11ax (5GHz)
    e) Obsługa HT – kanały 20/40MHz dla 802.11n
    f) Obsługa VHT – kanały 20/40/80/160MHz dla 802.11ac
    g) Obsługa HE – kanały 20/40/80/160MHz dla 802.11ax
    h) Wsparcie dla technologii DFS (Dynamic frequency selection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz
    i) Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac
    j) Wsparcie dla:
        - MRC (Maximal ratio combining)
        - CDD/CSD (Cyclic delay/shift diversity)
        - STBC (Space-time block coding)
        - LDPC (Low-density parity check)
        - Technologia TxBF
31) Specyfikacja radia 802.11b/g/n/ax:

a) Technologia direct sequence spread spectrum (DSSS), OFDM, OFDMA
b) Typy modulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM, 256-QAM, 1024-QAM
c) Moc transmisji konfigurowalna przez administratora

32) Punkt dostępowy musi posiadać co najmniej:
a) 1 interfejs 100/1000BaseT
- z funkcją auto-sensing link oraz MDI/MDX
- z funkcją PoE/PoE+
- ze wsparciem dla standardu 802.3az Energy Efficient Ethernet (EEE)

b) interfejs konsoli RS-232 (RJ-45) lub USB
c) interfejs USB 2.0 (Typ-A, niezależny od portu konsoli)
d) przycisk przywracający konfigurację fabryczną
e) slot zabezpieczający Keningston

33) Parametry pracy urządzenia:
a) Temperatura otoczenia (zakres minimalny): 0-50 º C
b) Wilgotność (zakres minimalny): 5% - 92%

34) Obsługiwane standardy:
a) Ethernet IEEE 802.3 / IEEE 802.3u
b) Power-over-Ethernet IEEE 802.3af
c) Wireless IEEE 802.11a/b/g/n/ac/ax
d) Znak CE
e) EN 60601-1-1, EN60601-1-2

35) Punkt dostępowy zasilony przy użyciu zgodnym ze standardem 802.3at PoE lub przy pomocy lokalnego zasilacza DC (zasilacz nie musi być dołączony)
36) Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac
37) Wszystkie dostępne na urządzeniu funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
38) <u>Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni.</u>
39) Punkt dostępowy musi być objęty co najmniej ograniczoną dożywotnią gwarancja producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni przesyła zamiennik. Gwarancja musi być realizowana bezpośrednio przez producenta sprzętu.

Ad. Cz. I pkt 2. Przełącznik sieciowy z 48 portami 1G oraz 4 portami 10G SFP+

1) Minimum 48 portów 10/100/1000BASE-T umieszczonych z przodu obudowy
2) Minimum 4 porty 1/10gigabitowe SFP+ umieszczone z przodu obudowy
3) Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4) Wydajność: minimum 98 Mp/s
5) Bufor pakietów: minimum 12 MB

6) Minimum 4GB pamięci operacyjnej
7) Minimum 16GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash).
8) Dedykowany port konsoli USB
9) Port USB 2.0 (niezależny od portu konsoli USB)
10) Wewnętrzny zasilacz 230V. Pobór mocy nie może być większy niż 50W.
11) Wielkość tablicy routingu: minimum 500 wpisów IPv4, 500 wpisów IPv6
12) Wielkość tablicy ARP co najmniej 1000 wpisów, wielkość tablicy ND co najmniej 500 wpisów
13) Tablica adresów MAC o wielkości minimum 8000 pozycji
14) Obsługa Jumbo Frames co najmniej 9198 bajtów
15) Obsługa sFlow lub Netflow
16) Obsługa REST API
17) Obsługa RMON (minimum grupy 1,2,3 i 9)
18) Obsługa 4094 tagów IEEE 802.1Q oraz 512 jednoczesnych sieci VLAN
19) Obsługa protokołu MVRP
20) Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3
21) Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
22) Obsługa Secure FTP lub SCP
23) Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
24) Obsługa SNTPv4 lub NTP
25) Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)
26) Obsługa protokołów rutingu: ruting statyczny
27) Obsługa ruchu multicast: IGMPv1/v2/v3 (co najmniej 500 grup), MLD (co najmniej 500 grup)
28) Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
29) Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED)
30) Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting
31) Obsługa uwierzytelniania użytkowników zgodna z 802.1x
32) Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS
33) Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW z użyciem zewnętrznego serwera
34) Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie
35) Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+

36) Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+
37) Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego
38) Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
39) Obsługa list kontroli dostępu (ACL)
40) Zakres pracy od 0 do 45°C
41) Przełącznik w obudowie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 25 cm.
42) Jeżeli do działania którejkolwiek z wymaganych funkcji potrzebna jest licencja, należy ją dostarczyć.
43) Wszystkie dostępne na przełączniku funkcje muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji o ile nie wyspecyfikowano inaczej.
44) Producent sprzętu musi być sklasyfikowany co najmniej 5 ostatnich lat (w tym w bieżącym roku) w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure” lub równoważnym i znajdować się w kwadracie liderów (Leaders). Za ranking równoważny Zamawiający uzna ranking klasyfikujący rozwiązania klasy enterprise przewodowych i bezprzewodowych sieci LAN, prowadzony i publikowany przez podmiot niezależny od producentów tych rozwiązań. Zamawiający wymaga, aby ranking taki był aktualizowany w okresach nie dłuższych niż 1 rok i publikowany był od co najmniej 10 lat. Podstawą do sporządzenia raportów muszą być badania polegające na sprawdzeniu jakości oferowanych usług i rozwiązań. Ocena jest prowadzona według kryteriów dotyczących kompletności wizji oferowanych usług, rozwiązań oraz prognoz na przyszłość w tym segmencie rynku oraz zdolności ich realizacji do wdrożenia, są to możliwości finansowe, biznesowe i organizacyjne. Wynik oceny wyznacza miejsce w rankingu w którym znajduje się konkretny dostawca i jego rozwiązanie. Ranking musi uwzględniać co najmniej 4 kategorie, każda z nich ma określać jaką rolę na rynku spełnia dane rozwiązanie/dostawca. Liderzy – najwyższa kategoria, gdzie znajdują się liderzy/producenci danego rozwiązania. Kandydaci – pretendenci pozostający bardzo wysoko w rankingu ze względu na swoje działania i potencjał do dominacji na rynku, w którym działa. Wizjonerzy - firmy rozwiązania posiadający wizję możliwości rynkowych, jednak poprzez realizowane działania nie są oni skuteczni na rynku. Niszowi gracze – rozwiązania skupiające się na niewielkiej części rynku lub nie mających możliwości innowacyjnych do osiągnięcia większych sukcesów rynkowych. Ranking równoważny nie może być wystawiony przez Wykonawcę lub podmiot zależny od Wykonawcy
45) <u>Warunki gwarancji.</u> Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po

dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu.

Ad. Cz. I pkt 3. Przełącznik sieciowy od 8 do 16 portów 1G z funkcją POE+

1) Minimum 8 portów 10/100/1000BASE-T umieszczonych z przodu obudowy ze wsparciem dla protokołu 802.3at (PoE+)
2) Minimum 2 porty 1/10gigabitowe SFP+ umieszczone z przodu obudowy
3) Przepustowość: minimum 68 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4) Wydajność: minimum 45 Mp/s
5) Bufor pakietów: minimum 1 MB
6) Minimum 4GB pamięci operacyjnej
7) Minimum 16GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash).
8) Dedykowany port konsoli USB
9) Port USB 2.0 (niezależny od portu konsoli USB)
10) Wewnętrzny zasilacz 230V zapewniający budżet mocy PoE na poziomie nie niższym niż 130W. Pobór mocy (bez PoE) nie może być większy niż 25W.
11) Wielkość tablicy routingu: minimum 500 wpisów IPv4, 500 wpisów IPv6
12) Wielkość tablicy ARP co najmniej 1000 wpisów, wielkość tablicy ND co najmniej 500 wpisów
13) Tablica adresów MAC o wielkości minimum 8000 pozycji
14) Obsługa Jumbo Frames co najmniej 9198 bajtów
15) Obsługa sFlow lub Netflow
16) Obsługa REST API
17) Obsługa RMON (minimum grupy 1,2,3 i 9)
18) Obsługa 4094 tagów IEEE 802.1Q oraz 512 jednoczesnych sieci VLAN
19) Obsługa protokołu MVRP
20) Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne
21) Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
22) Obsługa Secure FTP lub SCP
23) Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
24) Obsługa SNTPv4 lub NTP

25) Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)
26) Obsługa protokołów rutingu: ruting statyczny
27) Obsługa ruchu multicast: IGMPv1/v2/v3 (co najmniej 500 grup), MLD (co najmniej 500 grup)
28) Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
29) Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED)
30) Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting
31) Obsługa uwierzytelniania użytkowników zgodna z 802.1x
32) Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS
33) Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW z użyciem zewnętrznego serwera
34) Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie
35) Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
36) Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+
37) Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego
38) Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
39) Obsługa list kontroli dostępu (ACL)
40) Zakres pracy od 0 do 45°C
41) Pasywne chłodzenie (brak wentylatorów)
42) Przełącznik w obudowie maksymalnie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 27 cm.
43) Jeżeli do działania którejkolwiek z wymaganych funkcji potrzebna jest licencja, należy ją dostarczyć.
44) Wszystkie dostępne na przełączniku funkcje muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji o ile nie wyspecyfikowano inaczej.
45) Producent sprzętu musi być sklasyfikowany co najmniej 5 ostatnich lat (w tym w bieżącym roku) w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure” lub równoważnym i znajdować się w kwadracie liderów (Leaders). Za ranking równoważny Zamawiający uzna ranking klasyfikujący rozwiązania klasy enterprise przewodowych i bezprzewodowych sieci LAN, prowadzony i publikowany przez podmiot niezależny od producentów tych rozwiązań. Zamawiający wymaga, aby ranking taki był aktualizowany w okresach nie dłuższych niż 1 rok i publikowany był od co najmniej 10 lat.

Podstawą do sporządzenia raportów muszą być badania polegające na sprawdzeniu jakości oferowanych usług i rozwiązań. Ocena jest prowadzona według kryteriów dotyczących kompletności wizji oferowanych usług, rozwiązań oraz prognoz na przyszłość w tym segmencie rynku oraz zdolności ich realizacji do wdrożenia, są to możliwości finansowe, biznesowe i organizacyjne. Wynik oceny wyznacza miejsce w rankingu w którym znajduje się konkretny dostawca i jego rozwiązanie. Ranking musi uwzględniać co najmniej 4 kategorie, każda z nich ma określać jaką rolę na rynku spełnia dane rozwiązanie/dostawca. Liderzy – najwyższa kategoria, gdzie znajdują się liderzy/producenci danego rozwiązania. Kandydaci – pretendenci pozostający bardzo wysoko w rankingu ze względu na swoje działania i potencjał do dominacji na rynku, w którym działa. Wizjonerzy - firmy rozwiązania posiadający wizję możliwości rynkowych, jednak poprzez realizowane działania nie są oni skuteczni na rynku. Niszowi gracze – rozwiązania skupiające się na niewielkiej części rynku lub nie mających możliwości innowacyjnych do osiągnięcia większych sukcesów rynkowych. Ranking równoważny nie może być wystawiony przez Wykonawcę lub podmiot zależny od Wykonawcy

46) <u>Warunki gwarancji.</u> Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Gwarancja musi zapewniać również dostęp do poprawek, wsparcia technicznego i aktualizacji oprogramowania przez cały okres trwania gwarancji. Gwarancja musi być świadczony bezpośrednio przez autoryzowany serwis producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i autoryzowanym serwisem producentem sprzętu.

Ad. Cz. I pkt 4. Urządzenie UTM z funkcją routera

1) Urządzenie musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
2) Urządzenie musi zapewniać możliwość budowy minimum 2 oddzielnych logicznych instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.
3) Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
4) System musi wspierać IPv4 oraz IPv6 w zakresie: Firewall, Ochrony w warstwie aplikacji, Protokołów routingu dynamicznego.
5) Urządzenie musi dysponować 5 portami Gigabit Ethernet RJ-45, w tym 1 dedykowany dla łącza WAN.
6) Urządzenie musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

7) W ramach systemu powinna być możliwość zdefiniowania co najmniej 255 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
8) Urządzenie musi być wyposażone w zasilanie AC.
9) W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
10) Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
11) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
12) Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.
13) 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 1 Gbps.
14) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.
15) Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.
16) W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje:
    - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
    - Kontrola Aplikacji.
    - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
    - Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
    - Ochrona przed atakami - Intrusion Prevention System.
    - Kontrola stron WWW.
    - Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
    - Zarządzanie pasmem (QoS, Traffic shaping).
    - 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.
    - Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
    - Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system
17) Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
18) System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT, a także translację jeden do jeden oraz jeden do wielu oraz dedykowany ALG (Application Level Gateway) dla protokołu SIP

19) W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
20) Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
21) 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.
22) 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.
    - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
23) W zakresie routingu urządzenie powinno zapewniać obsługę:
    - Routingu statycznego.
    - Policy Based Routingu.
    - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
24) System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
25) System musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

26) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
27) System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
28) System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
29) 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.
30) System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
31) Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
32) Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
33) System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
34) Baza sygnatur ataków powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
35) Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
36) System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
37) 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.
38) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
39) Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
40) Baza Kontroli Aplikacji powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
41) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
42) Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
43) Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
44) Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

45) 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.
46) Filtr WWW musi dostarczać kategorii stron zabronionych prawem.
47) Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
48) Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
49) Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
50) W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
51) 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.
    - Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
52) Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
53) 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.
54) Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
55) Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
56) System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
57) System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
58) Element systemu pełniący funkcję firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

59) Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
60) 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.
61) 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.
62) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
63) Musi istnieć możliwość logowania do serwera SYSLOG.
64) W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować kontrolę aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), analizę typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres **12 miesięcy.**
65) <u>Warunki gwarancji.</u> System musi być objęty serwisem gwarancyjnym producenta przez okres **12 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 24x7.

Ad. Cz. I pkt 5. Punkt dostępowy WiFi

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej. **Oferowane punkty dostępowe muszą mieć możliwość zarządzania z poziomu interfejsu urządzenia UTM z funkcją routera z punktu Ad. Cz. I pkt 4. powyżej.**

1) 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%.
2) 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.
3) 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,
4) Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.

5) Interfejs Ethernet w standardzie 10/100/1000 Base-TX,
6) Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3af lub zewnętrzny zasilacz.
7) Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
   a. Tunnel,
   b. Bridge,
   c. Mesh.
8) Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
9) 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-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
10) 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.
11) 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,
12) 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.
13) Punkt dostępowy musi być certyfikowanym urządzeniem WiFi Alliance: WiFi certified IEEE Std 802.11a/b/g/n (ac) oraz posiadać certyfikację DFS.

Ad. Cz. II pkt 1. Notebook z oprogramowaniem

1) Zastosowanie: komputer przenośny wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
2) Ekran 15,6" o rozdzielczości: HD (1920x1080 przy 60Hz) z podświetleniem LED i powłoką przeciwodblaskową.
3) Oferowany komputer przenośny musi osiągać w teście wydajności SYSmark® 25 wyniki minimum:
    a) Overall Rating – 1200 pkt.
    b) Productivity – 1300 pkt.
    c) Creativity – 1100 pkt.
    d) Responsiveness – 1000 pkt.

    Zamawiający zastrzega, że po podpisaniu umowy a przed odbiorem komputerów może zażądać od Wykonawcy dokumentu potwierdzającego spełnianie ww. wymagań w formie wydruku z przeprowadzonego testu, potwierdzonego przez Wykonawcę lub wydruk ze strony: https://results.bapco.com.

    Wymagane testy wydajnościowe muszą być przeprowadzone na automatycznych ustawieniach konfiguratora dołączonego przez BAPCO i rozdzielczości wyświetlacza 1920 x 1080 @ 60 Hz oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).

    Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testu Wykonawca może zostać wezwany do dostarczenia Zamawiającemu oprogramowania testującego, komputera do testów oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego.
4) Procesor powinien osiągać w teście wydajności PassMark Performance Test wynik co najmniej 13000 punktów Passmark CPU Mark.
5) Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia. Wyposażona przez producenta w dedykowany chipset dla oferowanego procesora.
6) Pamięć RAM 16GB DDR4 lub DDR5, wymagane min. 2 sloty na pamięci
7) Dysk min. 500GB SSD
8) Zainstalowany system operacyjny Windows 11 64-bit w wersji Professional lub równoważny, w polskiej wersji językowej. Klucz systemu musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. Licencja wieczysta.

9) Karta graficzna zintegrowana z procesorem, osiągającą min. 2600 punktów w teście PassMark - G3D Mark, wynik testu oferowanego układu graficznego musi być dostępny na stronie: http://www.videocardbenchmark.net/gpu_list.php.
10) Wbudowana karta 802.11 a/b/g/n/ac z możliwością włączania i wyłączenia łączności bezprzewodowej. Wbudowany moduł Bluetooth w wersji min. 5.0 z możliwością włączania i wyłączania łączności bezprzewodowej.
11) Klawiatura wyspowa, z wbudowanym w klawiaturze podświetleniem z możliwością manualnej regulacji zarówno w BIOS jak i spod systemu operacyjnego, (układ US -QWERTY), min. 99 klawiszy.
12) Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki stereo o średniej mocy 2x2W, wbudowany wewnętrzny wzmacniacz głośników.
13) Cyfrowy mikrofon z funkcja redukcji szumów i poprawy mowy wbudowany w obudowę matrycy.
14) Kamera internetowa z diodą informującą o aktywności, o rozdzielczości min. 1280x720 px trwale zainstalowana w obudowie matrycy.
15) Bateria umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin.
16) Dedykowany zasilacz
17) Oferowany komputer przenośny musi osiągać w teście wydajności MobileMark 25 w kategorii Battery Life wynik minimum 400 minut. Zamawiający zastrzega, że po podpisaniu umowy a przed odbiorem komputerów może zażądać od Wykonawcy dokumentu potwierdzającego spełnianie ww. wymagań w formie wydruku z przeprowadzonego testu, potwierdzonego przez Wykonawcę lub wydruk ze strony: https://results.bapco.com.
18) Waga maksymalnie 3kg
19) Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
20) Urządzenie musi posiadać:
    a) zintegrowany układ TPM zgodny ze standardem Trusted Platform Module w wersji min. 2.0;
    b) wbudowaną technologię zarządzania i monitorowania komputerem na poziomie sprzętowym działającą niezależnie od stanu czy obecności OS oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługującą zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, zapewniającą:
        - monitorowanie konfiguracji komponentów komputera, w tym: CPU, Pamięć, HDD, wersja BIOS płyty głównej;
        - zdalną konfigurację ustawień BIOS,
        - zdalne przejęcie konsoli tekstowej systemu,

- zdalne przejęcie 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,

c) wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego.
d) konstrukcję absorbująca wstrząsy;
e) czytnik linii papilarnych;
f) złącze umożliwiające zastosowanie fizycznego zabezpieczenia w postaci linki metalowej.

21) BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Dashboard BIOS'u zbudowany w postaci kombinacji tekstu i grafiki obsługiwany w sposób selektywny i swobodny. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:
a) wersji BIOS,
b) nr seryjnym komputera,
c) model komputera,
d) adresu MAC karty sieciowej,
e) modelu procesora wraz z informacjami o liczbie rdzeni oraz informacjami o:
f) - nominalnej prędkości pracy (w GHz) lub
g) - maksymalnej szybkości zegara, minimalnej szybkości zegara oraz bieżącej szybkości zegara procesora,
h) informacji o ilości pamięci RAM oraz jej taktowaniu,
i) informacji o modelu dysku twardego,
j) informacji o napędzie optycznym (nie dotyczy zewnętrznego napędu USB),
k) informacji o karcie sieciowej Ethernet i karcie dźwiękowej
l) zintegrowanym układzie graficznym,
m) kontrolerze audio,

Zamawiający dopuści jako rozwiązanie równoważne, notebook z BIOS, w którym jest możliwość odczytania informacji o pojemności dysku twardego a informacja o modelu dysku twardego jest widoczna w systemie diagnostycznym, który jest zaimplementowany w tej samej pamięci flash co BIOS.

BIOS musi posiadać następujące funkcje:
a) możliwość wyłączenia/włączenia portów USB;
b) możliwość wyłączenia/włączenia kontrolera SATA (dotyczy notebooka, w którym istnieje możliwość instalacji dysków SATA),
c) możliwość wyłączenia/włączenia karty dźwiękowej,
d) możliwość wyłączenia/włączenia modułu TPM,
e) możliwość wyłączenia/włączenia karty sieciowej Ethernet,

f) możliwość wyłączenia/włączenia bootowania PXE,
g) możliwość włączania/wyłączania funkcji Wake on LAN,
h) możliwość ustawienia preferencji dotyczących sposobu działania i wydajności wentylatora chłodzącego lub możliwość automatycznego sterowania wentylatorem chłodzącym;
i) możliwość ustawienia haseł: Administratora, tzw. „power-on”, pozwalającego na uruchomienie dysku twardego,
j) możliwość ustawienia sekwencji bootowania (wraz z możliwością usunięcia z listy bootowania poszczególnych urządzeń),
k) możliwość uruchamiania systemu z urządzeń zewnętrznych typu HDD-USB, USB Pendrive, CDRW-USB,

22) Certyfikat ISO-9001 lub równoważny certyfikat jakości dla producenta sprzętu oraz certyfikat ISO-14001 lub równoważny certyfikat zarządzania środowiskowego dla producenta sprzętu.
23) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych (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 gramów.
24) Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 22dB.
25) Warunki gwarancji 3-letnia gwarancja. Firma serwisująca musi posiadać certyfikat jakości według normy ISO 9001 na świadczenie usług serwisowych lub równoważny certyfikat jakości oraz posiadać autoryzację producenta komputera. W przypadku wymiany dysku twardego uszkodzony dysk pozostaje u Użytkownika.
26) Dostęp do wsparcia technicznego na stronie producenta komputera realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera, lub innego oznaczenia stosowanego przez producenta komputera do: najnowszych sterowników, uaktualnień, opisu konfiguracji.
27) Płytka TouchPad wielodotykowa ze strefą przewijania.
28) Min. 3 porty USB, w tym min. 2 porty USB 3.2.
29) Porty audio słuchawek i mikrofonu (dopuszcza się tzw. port combo - słuchawka/mikrofon)
30) 1x port HDMI.
31) Czytnik kart multimedialny wspierający karty SD 4.0 lub microSD 4.0,
32) Karta sieciowa 10/100/1000 Ethernet (posiadająca minimum 1 port RJ-45), wspierająca obsługę WoL

33) Dołączony nośnik ze sterownikami lub dostęp do strony internetowej producenta komputera umożliwiający pobranie sterowników,
34) Dołączona dokumentacja w języku polskim, w formie elektronicznej lub papierowej lub dostęp do strony internetowej producenta komputera
35) <u>Dodatkowe wyposażenie:</u>
    a) Mysz optyczna przewodowa min. 1000 dpi USB z rolką, o długości kabla min. 1,5m (bez przedłużaczy).
    b) Torba dedykowana do przenoszenia laptopów o wymiarach ekranu od 15,6”:
        - kolor czarny,
        - regulowany pas na ramię, rączka,
        - kieszenie zewnętrzne,
        - kieszenie wewnętrzne,
        - zamknięcia - zamek błyskawiczny,
        - minimum 2 komory,
        - amortyzacja komory na laptopa fabrycznie wszyta w strukturę torby (nie dopuszcza się uzupełniania w elementy amortyzujące nie będące składnikami fabrycznymi torby oraz nie połączone trwale z torbą);
        - torba musi pomieścić w bezpieczny sposób: laptopa, mysz, dedykowany zasilacz
36) <u>Oprogramowanie dodatkowe:</u>
    a) Oprogramowanie antywirusowe równoważne do Eset Internet Security subskrypcja na 12 miesięcy
    b) Oprogramowanie biurowe równoważne do Microsoft Office Home and Business 2021

Ad. Cz. II pkt 2. Mobilny projektor laserowy

a) Minimalna obsługiwana rozdzielczość natywna: Full HD (1920x1080)
2) Technologia wyświetlania: laser
3) Jasność minimum 3500 lumenów
4) Minimalny kontrast dynamiczny: 2000000:1
5) Żywotność źródła światła minimum 20000 godzin w trybie standardowym pracy
6) Złącza:
    a) minimum wejścia 2x HDMI
    b) minimum 1x USB typu A do zasilania urządzeń zewnętrznych
    c) minimum 1x wyjście audio 3,5 mm mini-jack
7) Wbudowane głośniki o mocy minimum 15W
8) Waga nie większa niż 3kg
9) OSD wyświetlacza musi obsługiwać język polski
10) Urządzenie musi być dostarczone z pełnym zestawem akcesoriów niezbędnych do jego prawidłowej pracy, w tym z kablem zasilającym, pilotem, oraz niezbędnymi instrukcjami w języku polskim.
11) Wymagane jest, aby projektor był fabrycznie nowy, nieużywany i pochodził z autoryzowanej sieci dystrybucyjnej producenta.
12) <u>Do projektora należy dołączyć dedykowaną lub uniwersalną torbę z paskiem na ramię</u>

13) Gwarancja producenta:
   a) 24 miesiące na urządzenie
   b) 5 lat lub 12000h na źródło światła

Ad. Cz. III pkt 1. Zasilacz awaryjny UPS

1) Moc pozorna 1500VA
2) Moc czynna 1500W
3) Kształt napięcia wyjściowego – sinusoida
4) Topologia on-line podwójnej konwersji
5) Napięcie wejściowe 230V
6) Czas podtrzymania przy obciążeniu 100% - co najmniej 5 minut
7) Zabezpieczenia: przeciwprzepięciowe, przeciwprzeciążeniowe, przeciwzwarciowe
8) Typ obudowy rack 19 cali, maksymalnie 3U
9) Minimum 6 gniazd wyjściowych typy IEC 60320 C13
10) Gniazdo zasilania wejściowe IEC 60320 C14
11) Zarządzanie:
   a) panel LCD z przodu obudowy z przyciskami do ustawień
   b) port USB z tyłu obudowy do zarządzania za pomocą dołączonego oprogramowania
   c) wolny slot na kartę rozszerzeń do zarządzania przez sieć LAN
12) Wyposażenie:
   a) nośnik z oprogramowaniem lub możliwość pobrania oprogramowania ze strony producenta
   b) kabel komunikacyjny
   c) instrukcja montażu i obsługi lub możliwość pobrania ze strony producenta
   d) zestaw do montażu w szafie rack
13) Gwarancja producenta:
   a) min. 3 lata na urządzenie
   b) min. 2 lata akumulatory

Warunki i zasady dostarczenia oprogramowania równoważnego

1. **Windows 11 Professional** – licencja na system operacyjny, opis wymagań (wymagania minimalne dla równoważnego oprogramowania, które musi spełniać poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji):
   1) System operacyjny dla komputerów typu desktop i komputerów przenośnych.
   2) System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.
   3) System pozwala na dołączenie komputera do lokalnej domeny Active Directory Zamawiającego na poziomie lasu Windows Serwer 2016 z zarządzaniem nim za pomocą polityk GPO.

4) System musi udostępniać graficzny interfejs użytkownika umożliwiający obsługę przy pomocy klawiatury i myszy.
5) Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim.
6) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe.
7) Wbudowany system pomocy w języku polskim.
8) Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.
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 z ew. ograniczeniem czasowym dostępności nie krótszym niż dla systemu Microsoft Windows 11 Professional.
10) Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
11) Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
12) Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
13) Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
14) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).
15) Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.
16) Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.
17) Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.
18) Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe.
19) Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
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) Mechanizmy logowania do domeny w oparciu o:

a) Login i hasło,

b) Karty z certyfikatami (smartcard),

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

26) Mechanizmy wieloelementowego uwierzytelniania.

27) Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,

28) Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,

29) Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.

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

31) Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,

32) Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.

33) 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.

34) Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,

35) Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.

36) Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, woluminy dyskowe, usługi katalogowe.

37) Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.

38) Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.

39) Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).

40) Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),

41) Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.

42) Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.

43) Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) lub na kluczach pamięci przenośnej USB.

44) Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.

45) Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.

46) Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

47) Wszystkie wymienione parametry, role, funkcje itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

2. **Eset Internet Security** – licencja na oprogramowanie antywirusowe, opis wymagań (wymagania minimalne dla równoważnego oprogramowania, które musi spełniać poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji):

   1) Oprogramowanie musi być kompatybilne i w sposób niezakłócony współdziałać z systemami operacyjnymi Windows 10, 11.

   2) Wersja programu dla stacji roboczych Windows dostępna musi być dostępna w języku polskim

   3) Oprogramowanie musi umożliwiać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji itp.

   4) Oprogramowanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.

   5) Oprogramowanie musi umożliwiać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

6) Oprogramowanie musi umożliwiać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7) Oprogramowanie musi oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
8) Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9) Możliwość skanowania dysków sieciowych i dysków przenośnych.
10) Skanowanie plików spakowanych i skompresowanych.
11) Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
12) Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku ale również ma być możliwe użycie symbolu wieloznacznego „*” zastępującego dowolne znaki w ścieżce.
13) W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
14) Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
15) Oprogramowanie musi posiadać wbudowany konektor dla programów MS Outlook.
16) Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook.
17) Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
18) Automatyczna integracja skanera POP3 i IMAP z klientem pocztowym MS Outlook bez konieczności zmian w konfiguracji.
19) Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.
20) Program musi zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
21) Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik przy próbie dostępu do konfiguracji by proszony o podanie hasła.

22) Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
23) Program musi umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji.
24) Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
25) Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
26) Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
27) Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.

3. **Microsoft Office Home and Business 2021** - licencja bezterminowa – licencja na pakiet oprogramowania biurowego, opis wymagań (wymagania minimalne dla równoważnego oprogramowania, które musi spełniać poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji):
   1) Dostępność pakietu w wersji 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej,
   2) Wymagania odnośnie interfejsu użytkownika:
      a) Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.
      b) Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
   3) Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:
      a) posiada kompletny i publicznie dostępny opis formatu,
      b) ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247 t.j.),
      c) umożliwia kreowanie plików w formacie XML,
      d) wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,

4) Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
5) Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
6) W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
7) Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
8) Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a) Edytor tekstów,
   b) Arkusz kalkulacyjny,
   c) Narzędzie do przygotowywania i prowadzenia prezentacji,
   d) Narzędzie do zarządzania pocztą elektroniczną, kalendarzem, kontaktami i zadaniami,
9) Edytor tekstów musi umożliwiać:
   a) 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,
   b) Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,
   c) Wstawianie oraz formatowanie tabel,
   d) Wstawianie oraz formatowanie obiektów graficznych.
   e) Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),
   f) Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,
   g) Automatyczne tworzenie spisów treści,
   h) Formatowanie nagłówków i stopek stron,
   i) Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie,
   j) Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem,
   k) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
   l) Określenie układu strony (pionowa/pozioma),
   m) Wydruk dokumentów,

n) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną,

o) Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2013, 2016, 2019 i 2021 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu,

p) Zapis i edycję plików w formacie PDF,

q) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,

r) Możliwość jednoczesnej pracy wielu użytkowników na jednym dokumencie z uwidacznianiem ich uprawnień i wyświetlaniem dokonywanych przez nie zmian na bieżąco,

s) Możliwość wyboru jednej z zapisanych wersji dokumentu, nad którym pracuje wiele osób.

10) Arkusz kalkulacyjny musi umożliwiać:

a) Tworzenie raportów tabelarycznych

b) Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych

c) Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.

d) Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych

e) Wyszukiwanie i zamianę danych

f) Wykonywanie analiz danych przy użyciu formatowania warunkowego

g) Tworzenie wykresów prognoz i trendów na podstawie danych historycznych z użyciem algorytmu ETS

h) Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie

i) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności

j) Formatowanie czasu, daty i wartości finansowych z polskim formatem

k) Zapis wielu arkuszy kalkulacyjnych w jednym pliku.

l) Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.

m) Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).

n) Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2013, 2016, 2019 i 2021, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.

o) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

11) Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

a) Przygotowywanie prezentacji multimedialnych, które będą:
   - prezentowane przy użyciu projektora multimedialnego
   - drukowane w formacie umożliwiającym robienie notatek

b) Zapisanie, jako prezentacja tylko do odczytu.

c) Nagrywanie narracji i dołączanie jej do prezentacji

d) Opatrywanie slajdów notatkami dla prezentera

e) Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo

f) Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego

g) Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym

h) Możliwość tworzenia animacji obiektów i całych slajdów

i) Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.

j) Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2013, 2016, 2019 i 2021.

12) Narzędzie do zarządzania pocztą elektroniczną, kalendarzem, kontaktami i zadaniami musi umożliwiać:

a) Uwierzytelnianie wieloskładnikowe poprzez wbudowane wsparcie integrujące z usługą Active Directory,
b) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
c) Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
d) Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
e) Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
f) Automatyczne grupowanie poczty o tym samym tytule,
g) Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
h) Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,

i) Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
j) Zarządzanie kalendarzem,
k) Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
l) Przeglądanie kalendarza innych użytkowników,
m) Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
n) Zarządzanie listą zadań,
o) Zlecanie zadań innym użytkownikom,
p) Zarządzanie listą kontaktów,
q) Udostępnianie listy kontaktów innym użytkownikom,
r) Przeglądanie listy kontaktów innych użytkowników,
s) Możliwość przesyłania kontaktów innym użytkowników,
t) Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

Kryteria równoważności – ocena, zasady, wymagania

1. We wszystkich miejscach niniejszego dokumentu, w których użyto przykładowego znaku towarowego, patentu lub pochodzenia, jest to uzasadnione specyfiką przedmiotu zamówienia i Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń.
2. Wykonawca, który powoła się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać w ofercie, że oferowany przez niego przedmiot dostawy spełnia wymagania określone przez Zamawiającego.
3. Ciężar dowodowy w zakresie udowodnienia równoważności zaoferowanych rozwiązań z rozwiązaniami opisanymi poprzez wskazanie przykładowego znaku towarowego, patentu lub pochodzenia, spoczywa na Wykonawcy, składającym ofertę równoważną.
4. Zamawiający wymaga, aby zaoferowane przez Wykonawcę rozwiązania równoważne nie wiązały się z koniecznością wykonania dodatkowych prac integracyjnych, testowych czy migracyjnych po stronie Zamawiającego, tym samym poniesienia dodatkowych, niezaplanowanych kosztów.
5. W przypadku oferowania rozwiązania równoważnego, wykonawca zobowiązany jest wykazać, że oferowane przez niego rozwiązanie równoważne spełnia wymagania określone przez Zamawiającego, załączając do oferty dowody potwierdzające, że rozwiązanie równoważne spełnia wszystkie parametry równoważności. Dowody powinny zawierać informacje umożliwiające Zamawiającemu weryfikację spełniania przez rozwiązanie równoważne poszczególnych parametrów równoważności.
6. Zaoferowane rozwiązanie równoważne musi być w pełni kompatybilne z istniejącymi rozwiązaniami w środowisku, w tym dedykowanymi ze względu na specyfikę aplikacjami, systemami, także w warstwie aplikacyjnej.

7. Ponadto zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego.
8. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane oprogramowanie.
9. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu oprogramowania równoważnego oraz dostarczy inne rozwiązana spełniające wymagania OPZ.
10. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia/gwarancji producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.
11. Integracja dostarczonego równoważnego oprogramowania nie może wymuszać wykonania dodatkowych zmian programistycznych po stronie posiadanego przez Zamawiającego oprogramowania oraz musi umożliwiać integrację ze wszystkimi rozwiązaniami, które Zamawiający posiada w ramach istniejących środowisk.
12. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.
13. Zamawiający nie dopuszcza dostarczenia licencji dla produktów równoważnych w formie upgradu, licencji czasowej, OEM, z wyłączeniem, w którym Zamawiający określił taki warunek w opisie oprogramowania.
14. Licencje muszą pochodzić z autoryzowanego kanału dystrybucji.
15. Zamawiający nie dopuszcza zaoferowania oprogramowania i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu, z wyłączeniem, w którym Zamawiający określił taki warunek w opisie oprogramowania.
16. Oprogramowanie musi zostać dostarczone w najnowszej dostępnej wersji wydanej przez producenta oprogramowania.