**PAKIET nr 3**

**Załącznik nr 2c – opis przedmiotu zamówienia**

**Wykaz/opis przedmiotu zamówienia**

**Dostawca jest zobowiązany do odbioru sprzętu zużytego w ilości dostarczonego sprzętu, przy czym odbiór sprzętu zużytego może odbywać się w terminie innym niż dostawa nowego sprzętu.**

**Dostawca musi zapewnić możliwość konsultacji przy instalacji sprzętu. Dostawca dostarcza sprzęt posiadający wszystkie konieczne elementy – w tym wszelkiego rodzaju okablowanie, elementy mocujące i zasilające, wentylatory, kable zasilające, zasilacze, oprogramowanie systemowe itp., tak aby sprzęt, po wyjęciu z pudełka/opakowania był gotowy do podłączenia do komputera/sieci Zamawiającego i użytkowania.**

**W specyfikacji zostały wskazane konkretne parametry sprzętu oraz narzędzia, tak aby (zgodnie z wiedzą Zamawiającego) dostarczony sprzęt współpracował z już posiadanym przez Zamawiającego sprzętem. Sprzęt musi być fabrycznie nowy, a korzystanie przez Zamawiającego z dostarczonych produktów nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający nie musi zamówić całego sprzętu wskazanego w specyfikacji.**

1. Specyfikacja dostarczanej infrastruktury informatycznej i architektury technicznej.

W poniższej tabeli przedstawiono typy oraz liczbę zamawianej infrastruktury teleinformatycznej.

*Tabela 1. Typy oraz liczba zamawianej infrastruktury teleinformatycznej.*

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Typ** | **Liczba zamawianego sprzętu (sztuk)** |
|  | Macierz dyskowa - rozbudowa | 1 |
|  | Przełącznik sieciowy – typ 1 | 2 |
|  | Przełącznik sieciowy – typ 2 | 5 |
|  | Przełącznik sieciowy – typ 3 | 1 |
|  | Przełącznik modularny Typ A | 1 |
|  | Przełącznik modularny Typ B | 1 |
|  | System kontroli dostępu | 1 |
|  | UTM | 2 |
|  | Moduł SPF+ | 16 |
|  | Komputer stacjonarny - typ I | 80 |
|  | Komputer stacjonarny - typ II | 16 |
|  | Komputer stacjonarny all-in-one | 4 |
|  | Monitor LCD | 100 |
|  | Urządzenie wielofunkcyjne kolorowe | 12 |
|  | Drukarka biurowa | 20 |
|  | Drukarki kodów kreskowych | 11 |
|  | CAL | 100 |
|  | Oprogramowanie antyspamowe | 1 |
|  | System analizy logów | 1 |
|  | Oprogramowanie biurowe | 100 |

**PAKIET NR 3**

**Wadium:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Przedmiot zamówienia** | **J.m.** | **Ilość** | **Cena jedn. brutto***Wypełnia Wykonawca, który ma siedzibę na terytorium RP* | **Wartość pozycji brutto***Wypełnia Wykonawca, który ma siedzibę na terytorium RP* | **Cena jednostkowa bez podatku VAT***Wypełnia wyłącznie Wykonawca, który nie ma siedziby na terytorium RP* | **Wartość bez podatku VAT***Wypełnia wyłącznie Wykonawca, który nie ma siedziby na terytorium RP* | **Stawka podatku****VAT** *dla wykonawców z terytorium kraju RP lub nie objętych wewnątrzwspólnotowym nabyciem towarów* |
| 1. | Macierz dyskowa - rozbudowa | szt. | 1 |  |  |  |  |  |
| 2. | Przełącznik sieciowy – typ 1 | szt. | 2 |  |  |  |  |  |
| 3. | Przełącznik sieciowy – typ 2 | szt. | 5 |  |  |  |  |  |
| 4. | Przełącznik sieciowy – typ 3 | szt. | 1 |  |  |  |  |  |
| 5. | Przełącznik modularny Typ A | szt. | 1 |  |  |  |  |  |
| 6. | Przełącznik modularny Typ B | szt. | 1 |  |  |  |  |  |
| 7. | System kontroli dostępu | szt. | 1 |  |  |  |  |  |
| 8. | UTM | szt. | 2 |  |  |  |  |  |
| 9. | Moduł SPF+ | szt. | 16 |  |  |  |  |  |
| 10. | Komputer stacjonarny - typ I | szt. | 80 |  |  |  |  |  |
| 11. | Komputer stacjonarny - typ II | szt. | 16 |  |  |  |  |  |
| 12. | Komputer stacjonarny all-in-one | szt. | 4 |  |  |  |  |  |
| 13. | Monitor LCD | szt. | 100 |  |  |  |  |  |
| 14. | Urządzenie wielofunkcyjne kolorowe | szt. | 12 |  |  |  |  |  |
| 15. | Drukarka biurowa | szt. | 20 |  |  |  |  |  |
| 16. | Drukarki kodów kreskowych | szt. | 11 |  |  |  |  |  |
| 17. | CAL | szt. | 100 |  |  |  |  |  |
| 18. | Oprogramowanie antyspamowe | szt. | 1 |  |  |  |  |  |
| 19. | System analizy logów | szt. | 1 |  |  |  |  |  |
| 20. | Oprogramowanie biurowe | szt. | 100 |  |  |  |  |  |
|  | **Suma** | **xxxxx** | **xxxxx** |  |  |  |  | **xxxxxx** |

Cena pakietu z podatkiem VAT (brutto): ……………………………………………………………

Słownie zł: ……………………………………………………………

Cena pakietu bez podatku VAT(netto): …………………………………………………………..

Słownie zł: ……………………………………………………………

| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | **PARAMETRY ZAPROPONOWANE PRZEZ WYKONAWCĘ*****(wypełnia Wykonawca)*** |
| --- | --- | --- | --- |
| **Macierz dyskowa - rozbudowa** | **Model i producent sprzętu:** |
|  | Rozbudowa macierzy DELLEMC UNITY 300: | 1. Półka dyskowa 25 dysków o rozmiarze 2,5”
2. Półka dyskowa 15 dysków o rozmiarze 3,5”
3. 13 sztuk dysków 6TB NLSAS
4. 19 dysków 1,8TB 10K SAS
5. 6 dysków 3,2TB SSD
6. 2 kontrolery 10Gb ISCSI SFP+
 |  |
|  | Licencje pojemnościowe | Należy je dostarczyć, jeżeli są wymagane |  |
|  | Wymagania dotyczące instalacji i konfiguracji | 1. Instalacja półek dyskowych
2. Konfiguracja LUN
3. Migracja danych z posiadanej przez zamawiającego macierzy dyskowej HP2040
4. Podniesienie wersji firmware macierzy Unity 300
5. Podniesienie wersji firmware hostów ESX przynajmniej do wersji 6.5
6. Podniesienie wersji Vcenter do wersji przynajmniej 6.5
 |  |
| **Przełącznik sieciowy – typ 1** | **Model i producent sprzętu:** |
|  | Wymagania | 1. Minimum 24 porty 10/100/1000BaseT ze wsparciem dla standardu PoE+ (802.3at)
2. Minimum 4 porty Gigabitowe SFP, niezależne od wymaganych portów 10/100/1000BaseT
3. Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT
4. Wydajność przełączania co najmniej 56 Gbps oraz przepustowość 41,6 Mpps dla pakietów 64 bajtowych
5. Obsługa 4094 tagów IEEE 802.1Q oraz minimum 512 jednoczesnych sieci VLAN
6. Automatyczne wykrywanie punktów bezprzewodowych podłączonych do przełącznika (w szczególności posiadanych przez Zamawiającego punktach Aruba AP315) automatyczne konfigurowanie portów, do których są one podłączone (minimum sieć VLAN, CoS, budżet mocy PoE, priorytet PoE)
7. Funkcja automatycznej aprowizacji i konfiguracji przełącznika przy jego pierwszym podłączeniu do sieci bez konieczności wykonywania wstępnej, ręcznej konfiguracji
	1. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
8. Budżet mocy PoE nie może być mniejszy niż 190W
9. Bufor pakietów nie mniejszy niż 1,5MB
10. Minimum 128MB pamięci Flash
11. Dostęp do urządzenia przez konsolę szeregową (linia komend umożliwiająca pełne zarządzanie przełącznikiem), HTTPS, SSHv2 i SNMPv3
	1. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
	2. Obsługa Secure FTP
	3. Obsługa 802.3ad Link Aggregation Protocol (LACP)
	4. Obsługa Simple Network Time Protocol (SNTP) v4
12. Wielkość tablicy adresów MAC: minimum 16000
13. Obsługa LLDP i LLDP-MED
14. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting
15. Funkcja autoryzacji użytkowników zgodna z 802.1x
16. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+,
17. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
18. Obsługa list kontroli dostępu (ACL)
19. Obsługa protokołu TR-069
20. Obudowa wieżowa 1U umożliwiająca instalację w szafie 19" o głębokości nie większej niż 35 cm.
21. Maksymalny pobór mocy (bez PoE) nie większy niż 60W
22. Minimalny zakres pracy od 0°C do 45°C
23. Wymagane jest aby wszystkie dostarczone przełączniki były obsługiwane w zakresie monitoringu i zarządzania przez posiadane przez Zamawiającego oprogramowanie do zarządzania infrastrukturą sieciową HPE Intelligent Management Center Standard. W szczególności wymagane jest wsparcie w zakresie: wykrywania urządzeń i prezentacji ich topologii, alarmów, serwera syslog, archiwizacji, przywracania i porównywania konfiguracji, aktualizacji oprogramowania, konfiguracji VLAN, konfiguracji ACL, konfiguracji QoS.
24. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i niewyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
 |  |
|  | Gwarancja | 1. 3 letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory).
2. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia. Wymagane jest zapewnienie (niezależnego od zgłaszania usterek) wsparcia telefonicznego w trybie 8x5 przez okres trwania gwarancji.
3. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis.
4. Zamawiający musi mieć bezpośredni dostęp do zespołu wsparcia technicznego producenta w ramach i w okresie trwania gwarancji.
 |  |
|  | Wymagania dotyczące odbioru, instalacji i konfiguracji | 1. Weryfikacja ilościowa i jakościowa dostarczanego sprzętu.
2. Aktualizacja firmware do najnowszego stabilnego wydania.
3. Konfiguracja dostępu dla administratorów z wykorzystaniem protokołu TACACS+.
4. Konfiguracja adresacji, vlanów, portów, funkcji Spanning tree itp. zgodnie ze standardem wykorzystywanym w sieci Zamawiającego.
5. Wymiana przełączników w miejscach wskazanych przez Zamawiającego.
6. Weryfikacja poprawności działania przełączników.
7. Uaktualnienie informacji o urządzeniach w systemie monitoringu.
 |  |
| **Przełącznik sieciowy – typ 2** | **Model i producent sprzętu:** |
|  | Wymagania | 1. Co najmniej 10 portów gigabitowych w standardzie 10/100/1000BaseT z czego minimum 8 ze wsparciem dla standardu PoE+ (802.3at)
2. Co najmniej 2 porty 1000BaseX ze stykiem definiowanym przez SFP (dopuszcza się porty typu Combo, współdzielone z portami 10/100/1000BaseT).
3. Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT
4. Wydajność przełączania co najmniej 20 Gbps oraz przepustowość 14,8 Mpps dla pakietów 64 bajtowych
5. Obsługa 4094 tagów IEEE 802.1Q oraz minimum 512 jednoczesnych sieci VLAN
6. Automatyczne wykrywanie punktów bezprzewodowych podłączonych do przełącznika (w szczególności posiadanych przez Zamawiającego punktach Aruba AP315), automatyczne konfigurowanie portów, do których są one podłączone (minimum sieć VLAN, CoS, budżet mocy PoE, priorytet PoE)
7. Funkcja automatycznej aprowizacji i konfiguracji przełącznika przy jego pierwszym podłączeniu do sieci bez konieczności wykonywania wstępnej, ręcznej konfiguracji
8. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
9. Bufor pakietów nie mniejszy niż 1,5MB
10. Minimum 128MB pamięci Flash
11. Budżet mocy PoE nie może być mniejszy niż 60W
12. Dostęp do urządzenia przez konsolę szeregową (linia komend umożliwiająca pełne zarządzanie przełącznikiem), HTTPS, SSHv2 i SNMPv3
13. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
14. Obsługa Secure FTP
15. Obsługa 802.3ad Link Aggregation Protocol (LACP)
16. Obsługa Simple Network Time Protocol (SNTP) v4
17. Wielkość tablicy adresów MAC: minimum 16000
18. Obsługa LLDP i LLDP-MED
19. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting
20. Funkcja autoryzacji użytkowników zgodna z 802.1x
21. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+,
22. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
23. Obsługa list kontroli dostępu (ACL)
24. Obsługa protokołu TR-069
25. Wysokość w szafie 19” – 1U. Kompaktowa obudowa o szerokości nie większej niż 13” i głębokości nie większej niż 16 cm. Na wyposażeniu powinny również znajdować się elementy do montażu w standardowej szafie 19”
26. Pasywne chłodzenie – brak wentylatora
27. Minimalny zakres pracy od 0°C do 45°C
28. Maksymalny pobór mocy (bez PoE) nie większy niż 20W
29. Wymagane jest, aby wszystkie dostarczone przełączniki były obsługiwane w zakresie monitoringu i zarządzania przez posiadane przez Zamawiającego oprogramowanie do zarządzania infrastrukturą sieciową HPE Intelligent Management Center Standard. W szczególności wymagane jest wsparcie w zakresie: wykrywania urządzeń i prezentacji ich topologii, alarmów, serwera syslog, archiwizacji, przywracania i porównywania konfiguracji, aktualizacji oprogramowania, konfiguracji VLAN, konfiguracji ACL, konfiguracji QoS. Zamawiający wymaga, aby z przełącznikiem zostały dostarczone licencje dostępowe HPE IMC Standard lub równoważne w ilości pokrywającej zapotrzebowanie przedmiotowego postępowania.
30. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i niewyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
 |  |
|  | Gwarancja | 3 letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia. W ramach gwarancji wymagane jest zapewnienie (niezależnego od zgłaszania usterek) wsparcia telefonicznego w trybie 8x5 przez okres trwania gwarancji. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do zespołu wsparcia technicznego producenta w ramach i w okresie trwania gwarancji. |  |
|  | Wymagania dotyczące odbioru instalacji i konfiguracji | 1. Weryfikacja ilościowa i jakościowa dostarczanego sprzętu.
2. Aktualizacja firmware do najnowszego stabilnego wydania.
3. Konfiguracja dostępu dla administratorów z wykorzystaniem protokołu TACACS+.
4. Konfiguracja adresacji, vlanów, portów, funkcji Spanning tree itp. zgodnie ze standardem wykorzystywanym w sieci Zamawiającego.
5. Wymiana przełączników w miejscach wskazanych przez Zamawiającego.
6. Weryfikacja poprawności działania przełączników.
7. Uaktualnienie informacji o urządzeniach w systemie monitoringu.
 |  |
| **Przełącznik sieciowy – typ 3** | **Model i producent sprzętu:** |
|  | Wymagania | 1. Minimum 48 portów 100/1000BaseT ze wsparciem dla standardu 802.3at (PoE+)
2. Minimum 4 porty 10Gb SFP+
3. Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT
4. Wydajność przełączania co najmniej 176 Gbps oraz przepustowość 112 Mpps
5. Obsługa 4094 tagów IEEE 802.1Q oraz minimum 500 jednoczesnych sieci VLAN
6. Obsługa protokołu IEEE 802.1v
7. Automatyczne wykrywanie punktów bezprzewodowych podłączonych do przełącznika (w szczególności posiadanych przez Zamawiającego punktach Aruba AP315), automatyczne konfigurowanie portów, do których są one podłączone (minimum sieć VLAN, CoS, budżet mocy PoE, priorytet PoE)
8. Funkcja automatycznego provisioningu i konfiguracji przełącznika przy jego pierwszym podłączeniu do sieci bez konieczności wykonywania wstępnej, ręcznej konfiguracji
9. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
10. Bufor pakietów nie mniejszy niż 12MB
11. Minimum 4GB pamięci typu Flash
12. Minimum 1GB pamięci operacyjnej typu RAM
13. Obsługa protokołów rutingu: ruting statyczny (wraz w ECMP), RIP v1, RIP v2
14. Wielkość tablicy rutingu: minimum 2000 wpisów IPv4 i 1000 wpisów IPv6
15. Dostęp do urządzenia przez konsolę szeregową (linia komend umożliwiająca pełne zarządzanie przełącznikiem), HTTPS, SSHv2 i SNMPv3
16. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
17. Obsługa protokołów GVRP i MVRP
18. Obsługa Secure FTP
19. Obsługa 802.3ad Link Aggregation Protocol (LACP)
20. Obsługa Simple Network Time Protocol (SNTP) v4
21. Wielkość tablicy adresów MAC: minimum 16000
22. Obsługa LLDP i LLDP-MED
23. Wbudowany serwer DHCP
24. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting
25. Funkcja autoryzacji użytkowników zgodna z 802.1x
26. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+,
27. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
28. Ochrona serwerów DHCP
29. Obsługa list kontroli dostępu (ACL)
30. Obsługa ramek Jumbo o wielkości co najmniej 9200 bajtów
31. Obsługa IP SLA dla ruchu typu VoIP (co najmniej monitoring jakości połączeń głosowych przy pomocy testów jitter UDP)
32. Obudowa wieżowa 1U umożliwiająca instalację w szafie 19" o głębokości nie większej niż 45 cm.
33. Wewnętrzny zasilacz 230V zapewniający budżet mocy PoE na poziomie nie niższym niż 370W
34. Maksymalny pobór mocy (bez PoE) nie większy niż 100W
35. Minimalny zakres pracy od 0°C do 45°C
36. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i niewyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
37. Wymagane jest, aby wszystkie dostarczone przełączniki były obsługiwane w zakresie monitoringu i zarządzania przez posiadane przez Zamawiającego oprogramowanie do zarządzania infrastrukturą sieciową HPE Intelligent Management Center Standard. W szczególności wymagane jest wsparcie w zakresie: wykrywania urządzeń i prezentacji ich topologii, alarmów, serwera syslog, archiwizacji, przywracania i porównywania konfiguracji, aktualizacji oprogramowania, konfiguracji VLAN, konfiguracji ACL, konfiguracji QoS.
38. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i niewyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
 |  |
|  | Gwarancja | 3 letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia. Wymagane jest zapewnienie (niezależnego od zgłaszania usterek) wsparcia telefonicznego w trybie 8x5 przez okres trwania gwarancji. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do zespołu wsparcia technicznego producenta w ramach i w okresie trwania gwarancji. |  |
|  | Wymagania dotyczące, odbioru instalacji i konfiguracji | 1. Weryfikacja ilościowa i jakościowa dostarczanego sprzętu.
2. Aktualizacja firmware do najnowszego stabilnego wydania.
3. Konfiguracja dostępu dla administratorów z wykorzystaniem protokołu TACACS+.
4. Konfiguracja adresacji, vlanów, portów, funkcji Spanning tree itp. zgodnie ze standardem wykorzystywanym w sieci Zamawiającego.
5. Wymiana przełączników w miejscach wskazanych przez Zamawiającego.
6. Weryfikacja poprawności działania przełączników.
7. Uaktualnienie informacji o urządzeniach w systemie monitoringu.
 |  |
| **Przełącznik modułowy – typ A** | **Model i producent sprzętu:** |
|  | Wymagania | 1. Przełącznik o budowie modularnej pozwalającej na instalację minimum 288 portów gigabitowych, 96 portów 10-gigabitowych SFP+, 96 portów miedzianych 1/2,5/5/10-gigabitowych z negocjacją prędkości oraz obsługą standardu PoE+, 24 porty 40-gigabitowych lub ich kombinacji.
2. Przełącznik musi posiadać moduł zarządzający wyposażony w minimum 1GB pamięci stałej (typu Flash) oraz minimum 4GB pamięci operacyjnej (typu RAM) oraz możliwość instalacji drugiego, redundantnego modułu to takich samych parametrach jak moduł podstawowy
3. Przełącznik wyposażony w:
	1. Minimum 48 porty100BaseTX/1000BaseT
	2. Minimum 24 porty 100BaseTX/1000BaseT ze wsparciem dla standardu 802.3 at (PoE+)
	3. Minimum 24 porty gigabitowe SFP
	4. Minimum 32 porty 1/10-gigabitowymi SFP+. Dla zapewnienia redundancji porty SFP+ muszą być rozdzielone na co najmniej dwa różne moduły.
4. Redundantne, wewnętrzne, modularne, zasilacze wspierające standard 802.3at (PoE+) zapewniające minimum 500W dla PoE oraz zapewniające redundancję zasilania i budżetu mocy w trybie N+N.
5. Wolne sloty umożliwiające dalszą rozbudowę do zadanej minimalnej liczby portów
6. Musi być możliwe zainstalowanie w przełączniku posiadanych przez Zamawiającego modułów zl v2:
	1. HPE 8-port 10GbE SFP+ v2 zl Module J9538A
	2. HPE 24x SFP J9550A
	3. HPE 24-port Gig-T J9537A
7. Modularną wentylację (zapewniające redundancję wentylatory umieszczone na dedykowanym module)
8. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych
9. Obsługa ramek typu Jumbo
10. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 2 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster)
11. Obsługa sFlow oraz RMON (minimum grupy 1,2,3 i 9) Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT
12. Obsługa 4094 tagów IEEE 802.1Q oraz 4094 jednoczesnych sieci VLAN
13. Obsługa standardu IEEE 802.1v
14. Wsparcie dla VxLAN
15. Obsługa MAC forwarding table per vlan (możliwość używania takiego samego adresu MAC na różnych portach w różnych VLANach).
16. Dostęp do urządzenia przez konsolę szeregową (RS-232 i USB), HTTPS, SSHv2 i SNMPv3
17. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
18. Obsługa Secure FTP
19. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
20. Obsługa dystrybuowanych łączy agregowanych LACP – łączy agregowanych wychodzących z dwóch, różnych, niezależnych i oddzielnie zarządzanych (niepołączonych w stos) przełączników (tzw. Multi-chassis Link Aggregation, MLAG, MC-LAG, Distributed Trunking)
21. Obsługa Simple Network Time Protocol (SNTP) v4
22. Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping)
23. Obsługa protokołów rutingu: ruting statyczny, RIP v1, RIP v2, OSPF, OSPFv3, VRRP, PIM-SM, PIM-DM, BGP
24. Obsługa **802.1ad (Q-in-Q)**
25. Wielkość tablicy rutingu: minimum 10000 wpisów IPv4 i 5000 wpisów IPv6
26. Wielkość tablicy MAC: minimum 60000 wpisów
27. Prędkość matrycy przełączającej nie mniejsza niż 2000 Gb/s
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) oraz CDPv2
30. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting
31. Obsługa uwierzytelniania użytkowników zgodna z 802.1x
32. Obsługa uwierzytelniania użytkowników w oparciu o lokalną bazę adresów MAC
33. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS
34. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW
35. Obsługa różnych metod uwierzytelniania (802.1x, MAC, WWW) w tym samym czasie na tym samym porcie
36. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie
37. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
38. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+
39. Wbudowany serwer DHCP
40. Obsługa funkcji User Datagram Protocol (UDP) helper
41. Obsługa blokowania nieautoryzowanych serwerów DHCP
42. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
43. Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP
44. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD), Device Link Detection Protocol (DLDP) lub równoważnego
45. Obsługa mechanizmu wykrywania usterek kabla dla standardów 100/1000BaseT -Time Domain Reflectometry (TDR)
46. Obsługa protokołu OpenFlow w wersji co najmniej 1.0 i 1.3
47. OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic.
48. Musi być możliwe wielotablicowe przetwarzanie zapytań Open Flow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP)
49. Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow.
50. Musi być możliwe tworzenie logicznych tuneli poprzez komunikaty SNMP i możliwość ich wykorzystania w kierowaniu ruchem w sposób sterowany za pomocą protokołu OpenFlow.
51. Obsługa standardu 802.3az Energy Efficient Ethernet
52. Obsługa standardu 802.1AE MACsec
53. Obsługa ochrony procesora
54. Obudowa maksymalnie 7U umożliwiająca instalację w szafie 19" o głębokości nie większej niż 46 cm.
55. Minimalny zakres pracy od 0°C do 45°C
56. Wymagane jest, aby wszystkie dostarczone przełączniki były obsługiwane w zakresie monitoringu i zarządzania przez posiadane przez Zamawiającego oprogramowanie do zarządzania infrastrukturą sieciową HPE Intelligent Management Center Standard. W szczególności wymagane jest wsparcie w zakresie: wykrywania urządzeń i prezentacji ich topologii, alarmów, serwera syslog, archiwizacji, przywracania i porównywania konfiguracji, aktualizacji oprogramowania, konfiguracji VLAN, konfiguracji ACL, konfiguracji QoS.
57. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i niewyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji
 |  |
|  | Gwarancja | 3-letniagwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia. Wymagane jest zapewnienie (niezależnego od zgłaszania usterek) wsparcia telefonicznego w trybie 8x5 przez okres trwania gwarancji. Całość świadczeń gwarancyjnych musi być realizowana przez serwis producenta. |  |
|  | Wymagania dotyczące odbioru, instalacji i konfiguracji | 1. Weryfikacja ilościowa i jakościowa dostarczanego sprzętu.
2. Montaż przełączników w szafach RACK w dwóch serwerowniach.
3. Aktualizacja firmware do najnowszego stabilnego wydania.
4. Połączenie w klaster niezawodnościowy.
5. Konfiguracja dostępu dla administratorów z wykorzystaniem protokołu TACACS+.
6. Odwzorowanie konfiguracji z obecnie wykorzystywanych przełączników głównych.
7. Przeniesienie wszystkich połączeń na nowe urządzenia.
8. Weryfikacja poprawności działania sieci.
9. Uaktualnienie informacji o urządzeniach w systemie monitoringu.
 |  |
| **Przełącznik modułowy – typ B** | **Model i producent sprzętu:** |
|  | Wymagania | 1. Przełącznik o budowie modularnej pozwalającej na instalację minimum 288 portów gigabitowych, 96 portów 10-gigabitowych SFP+, 96 portów miedzianych 1/2,5/5/10-gigabitowych z negocjacją prędkości oraz obsługą standardu PoE+, 24 porty 40-gigabitowych lub ich kombinacji.
2. Przełącznik musi posiadać moduł zarządzający wyposażony w minimum 1GB pamięci stałej (typu Flash) oraz minimum 4GB pamięci operacyjnej (typu RAM) oraz możliwość instalacji drugiego, redundantnego modułu to takich samych parametrach jak moduł podstawowy
3. Przełącznik wyposażony w:
	1. Minimum 24 portów (porty) 100BaseTX/1000BaseT
	2. Minimum 24 porty 100BaseTX/1000BaseT ze wsparciem dla standardu 802.3at (PoE+)
	3. Minimum 24 porty gigabitowe SFP
	4. Minimum 32 porty 1/10-gigabitowymi SFP+. Dla zapewnienia redundancji porty SFP+ muszą być rozdzielone na co najmniej dwa różne moduły.
4. Redundantne, wewnętrzne, modularne, zasilacze wspierające standard 802.3at (PoE+) zapewniające minimum 500W dla PoE oraz zapewniające redundancję zasilania i budżetu mocy w trybie N+N.
5. Wolne sloty umożliwiające dalszą rozbudowę do zadanej minimalnej liczby portów
6. Musi być możliwe zainstalowanie w przełączniku posiadanych przez Zamawiającego modułów zl v2:
	1. HPE 8-port 10GbE SFP+ v2 zl Module J9538A
	2. HPE 24x SFP J9550A
	3. HPE 24-port Gig-T J9537A
7. Modularną wentylację (zapewniające redundancję wentylatory umieszczone na dedykowanym module)
8. Dołączone wkładki:
	1. 10G SFP+ LC SR 300m MMF Transceiver – 4 szt
	2. 10G SFP+ LC LR 10km SMF Transceiver – 12 szt
9. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych
10. Obsługa ramek typu Jumbo
11. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 2 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster)
12. Obsługa sFlow oraz RMON (minimum grupy 1,2,3 i 9) Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT
13. Obsługa 4094 tagów IEEE 802.1Q oraz 4094 jednoczesnych sieci VLAN
14. Obsługa standardu IEEE 802.1v
15. Wsparcie dla VxLAN
16. Obsługa MAC forwarding table per vlan (możliwość używania takiego samego adresu MAC na różnych portach w różnych VLANach).
17. Dostęp do urządzenia przez konsolę szeregową (RS-232 i USB), HTTPS, SSHv2 i SNMPv3
18. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
19. Obsługa Secure FTP
20. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
21. Obsługa dystrybuowanych łączy agregowanych LACP – łączy agregowanych wychodzących z dwóch, różnych, niezależnych i oddzielnie zarządzanych (niepołączonych w stos) przełączników (tzw. Multi-chassis Link Aggregation, MLAG, MC-LAG, Distributed Trunking)
22. Obsługa Simple Network Time Protocol (SNTP) v4
23. Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping)
24. Obsługa protokołów rutingu: ruting statyczny, RIP v1, RIP v2, OSPF, OSPFv3, VRRP, PIM-SM, PIM-DM, BGP
25. Obsługa 802.1ad (Q-in-Q)
26. Wielkość tablicy rutingu: minimum 10000 wpisów IPv4 i 5000 wpisów IPv6
27. Wielkość tablicy MAC: minimum 60000 wpisów
28. Prędkość matrycy przełączającej nie mniejsza niż 2000 Gb/s
29. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
30. Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED) oraz CDPv2
31. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting
32. Obsługa uwierzytelniania użytkowników zgodna z 802.1x
33. Obsługa uwierzytelniania użytkowników w oparciu o lokalną bazę adresów MAC
34. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS
35. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW
36. Obsługa różnych metod uwierzytelniania (802.1x, MAC, WWW) w tym samym czasie na tym samym porcie
37. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie
38. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
39. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+
40. Wbudowany serwer DHCP
41. Obsługa funkcji User Datagram Protocol (UDP) helper
42. Obsługa blokowania nieautoryzowanych serwerów DHCP
43. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
44. Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP
45. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD), Device Link Detection Protocol (DLDP) lub równoważnego
46. Obsługa mechanizmu wykrywania usterek kabla dla standardów 100/1000BaseT -Time Domain Reflectometry (TDR)
47. Obsługa protokołu OpenFlow w wersji co najmniej 1.0 i 1.3
48. OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic.
49. Musi być możliwe wielotablicowe przetwarzanie zapytań Open Flow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP)
50. Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow.
51. Musi być możliwe tworzenie logicznych tuneli poprzez komunikaty SNMP i możliwość ich wykorzystania w kierowaniu ruchem w sposób sterowany za pomocą protokołu OpenFlow.
52. Obsługa standardu 802.3az Energy Efficient Ethernet
53. Obsługa standardu 802.1AE MACsec
54. Obsługa ochrony procesora
55. Obudowa maksymalnie 7U umożliwiająca instalację w szafie 19" o głębokości nie większej niż 46 cm.
56. Minimalny zakres pracy od 0°C do 45°C
57. Wymagane jest aby wszystkie dostarczone przełączniki były obsługiwane w zakresie monitoringu i zarządzania przez posiadane przez Zamawiającego oprogramowanie do zarządzania infrastrukturą sieciową HPE Intelligent Management Center Standard. W szczególności wymagane jest wsparcie w zakresie: wykrywania urządzeń i prezentacji ich topologii, alarmów, serwera syslog, archiwizacji, przywracania i porównywania konfiguracji, aktualizacji oprogramowania, konfiguracji VLAN, konfiguracji ACL, konfiguracji QoS.
58. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i niewyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji
 |  |
|  | Gwarancja | 3-letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia. Wymagane jest zapewnienie (niezależnego od zgłaszania usterek) wsparcia telefonicznego w trybie 8x5 przez okres trwania gwarancji. Całość świadczeń gwarancyjnych musi być realizowana przez serwis producenta. |  |
|  | Wymagania dotyczące instalacji i konfiguracji | 1. Weryfikacja ilościowa i jakościowa dostarczanego sprzętu.
2. Montaż przełączników w szafach RACK w dwóch serwerowniach.
3. Aktualizacja firmware do najnowszego stabilnego wydania.
4. Połączenie w klaster niezawodnościowy.
5. Konfiguracja dostępu dla administratorów z wykorzystaniem protokołu TACACS+.
6. Odwzorowanie konfiguracji z obecnie wykorzystywanych przełączników głównych.
7. Przeniesienie wszystkich połączeń na nowe urządzenia.
8. Weryfikacja poprawności działania sieci.
9. Uaktualnienie informacji o urządzeniach w systemie monitoringu.
 |  |
| **System NAC**  | **Model i producent sprzętu:** |
|  | Wymagania | System do kontroli dostępu musi charakteryzować się następującymi cechami:1. Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor)
2. System musi odsługiwać minimum 300 urządzeń klienckich (w tym gości). Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia
3. Praca jako maszyna wirtualna
4. Musi posiadać wbudowany serwer Radius oraz TACACS +
5. Musi wspierać RADIUS VSA co najmniej 100 producentów, w tym:
	1. Cisco Systems
	2. Fortinet
	3. Microsoft
	4. Alcatel-lucent Enterprise
	5. Aruba Networks
	6. Huawei
	7. Extreme Networks
	8. PaloAlto
	9. Producenta posiadanych przez Zamawiającego urządzeń firm: Hewlett Packard Enterprise i Aruba Networks
6. System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera.W szczególności, musi współpracować w tym zakresie z posiadanymi przez Zamawiającego kontrolerami Aruba 7205
7. System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego. W szczególności, musi współpracować w tym zakresie z posiadanymi przez Zamawiającego kontrolerami Aruba 7205
8. Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.
9. Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych
	1. Microsoft Active Directory
	2. Radius
	3. Kerberos
	4. LDAP
	5. ODBC
	6. Współpraca z serwerami tokenów
10. Musi obsługiwać metody profilowania
	1. DHCP
	2. TCP
	3. MAC OUI
	4. SNMP
	5. Cisco device sensor
11. Wspierać protokoły
	1. Radius, Radius CoA, TACACS +, web authentication, SAML v2.0
	2. EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
	3. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)
	4. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)
	5. EAP-TLS
	6. PAP, CHAP, MSCHAPv1 i v2, EAP-MD5
	7. NAC, Microsoft NAP
	8. Windows machine authentication
	9. MAC Auth
	10. Audit (role oparte na porcie oraz skanowanie podatności)
	11. OCSP (Online Certificate Status Protocol)
	12. SNMP generic MIB, SNMP private MIB
	13. CEF (Common Event Format), LEEF (Log Event Extended Format)
	14. TLS 1.2
12. Funkcja integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami
13. Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych
	1. Co najmniej ESXi 5.0 do 6.
	2. Co najmniej Hyper-V 2012 R2, Hyper-V 2016, Hyper-V 2019 oraz Windows Server 2012 R2, Windows Server 2016
	3. KVM
14. Posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (300). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte.
15. System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności
	1. Samodzielna rejestracja klientów gościnnych w oparciu o:
	2. Adres e-mail
	3. Numer telefonu (wiadomość SMS)
	4. Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link)
	5. Logowanie w oparciu o portale społecznościowe
	6. Funkcja integracji z systemami trzecimi poprzez API
	7. Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do płatności systemy płatności karta kredytową
	8. Wbudowany system reklamowy umożliwiający integrację z zewnętrznymi serwisami umożliwiającymi w prosty sposób promowanie ofert promocyjnych, materiałów multimedialnych oraz aplikacji mobilnych.
	9. Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.
	10. Funkcja personalizacji strony gościnnej
16. Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.
17. Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działo IT
18. System musi wspierać obsługę następujących systemów operacyjnych
	1. MS Windows
	2. Mac OS X
	3. iOS
	4. Android
	5. Chromebook
	6. Ubuntu
19. Umożliwienie klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci
20. Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej
21. Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu.
22. Funkcja tworzenia unikalnych certyfikatów dla urządzeń.
23. Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń
24. Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID
25. Posiadać możliwość rozbudowy o moduł odpowiedzialny za kontrolę końcówek klienckich. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji
26. System kontroli końcówek klienckich musi mieć następujące funkcjonalności
	1. System musi wspierać następujące systemy operacyjne
		1. Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis)
		2. Apple MacOS X 10.10 i nowsze
		3. Red HAT Enterprise Linux 5 i nowsze
		4. CentOS 5 (Community Enterprise Operating System) i nowsze
		5. Fedora Core 24 i nowsze
		6. SUSE linux 12.x i nowsze
	2. Funkcja kontroli stanu oprogramowania anty-wirusowego, anty-spyware, firewall
	3. Wyświetlanie informacji on-line o statusie monitorowanych końcówek
	4. System powinien obsługiwać agenta w formie
		1. Stałej (Presistent Agent)
		2. Tymczasowej (Dissolvabe Agent)
		3. Agenta NAP
27. Do rozwiązania musi być dostępna publicznie, na stronie producenta, dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu) (nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Zamawiający zastrzega sobie prawo do weryfikacji spełnienia wymagań.
28. Oferta musi zawierać kompletne zestawianie numerów katalogowych produktów i wszystkich jego dodatkowych składników umożliwiających ich jednoznaczną identyfikację u producenta sprzętu Zamawiający może zażądać przed dostawą przeprowadzenia testów wybranych funkcji sprzętu i oprogramowania wymaganych w niemniejszym postępowaniu. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Zamawiającego w terminie nie dłużysz niż 2 tygodnie od chwili zażądania przez Zamawiającego ich przeprowadzenia. Nieprzystąpienie do testów lub nieskuteczne ich przeprowadzenie (brak potwierdzenia przez Zamawiającego, że testy zostały zakończone pomyślnie) skutkować będzie odrzuceniem oferty.
 |  |
|  | Gwarancja | Minimum 3-letniagwarancja producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć w ramach gwarancji bezpośredni dostęp do zespołu wsparcia technicznego producenta. |  |
|  | Wymagania dotyczące instalacji i konfiguracji | 1. - Instalacja maszyny wirtualnej w środowisku Zamawiającego.
2. - Konfiguracja sieciowa urządzenia.
3. - Konfiguracja usługi TACACS+ do autoryzacji administratorów na urządzeniach sieciowych.
4. - Konfiguracja dynamicznego przydzielania vlanu w oparciu o rodzaj konta czy sieci bezprzewodowej.
5. - Konfiguracja autoryzacji do wewnętrznej sieci bezprzewodowej szpitala z wykorzystaniem adresów MAC oraz kont Active Directory.
6. -W związku z posiadanym przez zamawiającego środowiska AD wymaga się, przeprowadzenia następujących działań:
* Audyt aktualnych ustawień: lasu, domeny, relacji zaufania, poziomów funkcjonalnych, rozmieszczenia kontrolerów i ról FSMO, roli global catalog, hierarchi czasu, lokalizacji i przypisań kontrolerów do lokalizacji, topologii replikacji i połączeń site link, serwerów bridgehead, a także podsieci IP.
* Przedstawienie projektu środowiska zgodnego z najlepszymi praktykami, i rekonfiguracja aktualnego środowiska zgodnie z zaakceptowanym projektem.
* Audyt stref i ustawień DNS, ich konfiguracji i replikacji. Zaproponowanie zmian zgodnych z najlepszymi praktykami,i ich wdrożenie.
* Audyt wszystkich polityk GPO, dokumentację ich funkcjii przedstawienie projektu konsolidacji polityk dla całego środowiska, celem redukcji ilości posiadanych polityk przy zachowaniu obecnej funkcjonalności.
* Audyt wszystkich skryptów logowania, dokumentację ich funkcji i przepisanie ich na polityki GPO.
* Upgrade poziomu funkcjonalnego lasu i domeny.
* Przygotowanie pełnej dokumentacji wdrożonego środowiska, łącznie ze wszystkimi politykami GPO.
1. - Konfiguracja autoryzacji do sieci bezprzewodowej dla gościw oparciu o adresy mailowe.
2. - Przeprowadzenie testów poprawności działania systemu autoryzacji.
 |  |
| **UTM** | **Model i producent sprzętu:** |
|  | Wymagania ogólne | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: 1. Routera z funkcją NAT,
2. Transparentnym
3. Monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.System musi wspierać IPv4 oraz IPv6 w zakresie:1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.

Opis przedmiotu zamówienia (nie techniczny, tylko ogólny):* 1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
	2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
 |  |
|  | Redundancja, monitoringi wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
 |  |
|  | Interfejsy, Dysk, Zasilanie | 1. System realizujący funkcję Firewall musi dysponować minimum:
	1. 10 portami Gigabit Ethernet RJ-45.
	2. 8 gniazdami SFP 1 Gbps.
	3. 2 gniazdami SFP+ 10 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.
 |  |
|  | Parametry wydajnościowe | 1. W zakresie Firewall’a obsługa nie mniej niż 8 mln jednoczesnych połączeń oraz 300.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 36 Gbps.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 14 Gbps.
4. Wydajność szyfrowania IPSec VPN: nie mniej niż 18 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5.2 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 4.7 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 5.7 Gbps.
 |  |
|  | Funkcje SystemuBezpieczeństwa | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.
 |  |
|  | Polityka Firewall | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
	1. Translację jeden do jeden oraz jeden do wielu.
	2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
 |  |
|  | Połączenia VPN | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
	1. Wsparcie dla IKE v1 oraz v2.
	2. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
	3. Obsługa protokołu Diffie-Hellman grup 19 i 20.
	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.
	5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
	6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
	7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
	8. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
	9. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
	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.
	2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
 |  |
|  | Routing i obsługa łączy WAN | 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
	1. Routingu statycznego.
	2. Policy Based Routingu.
	3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
 |  |
|  | Zarządzanie pasmem | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
 |  |
|  | Kontrola Antywirusowa | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania zamawiających nie wymaga dostarczenia licencji.
 |  |
|  | Ochrona przed atakami | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
 |  |
|  | Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnaturi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
 |  |
|  | Kontrola WWW | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotnez punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
 |  |
|  | Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
	1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
	2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
	3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
 |  |
|  | Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jaki powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
 |  |
|  | Logowanie | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
3. Musi istnieć możliwość logowania do serwera SYSLOG.
 |  |
|  | Certyfikaty | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:* 1. ICSA lub EAL4 dla funkcji Firewall.
	2. ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
	3. ICSA dla funkcji SSL VPN.
 |  |
|  | Serwisy i licencje | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:* 1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy
 |  |
|  | Gwarancja  | 1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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 gwarancyjne w trybie 24x7.
2. Oferent winien przedłożyć dokumenty:
	1. Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego usługi gwarancyjne, o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu gwarancyjnego.
	2. Certyfikat ISO 9001 lub równoważny podmiotu serwisującego.
 |  |
|  | Akcesoria | 1.Wkładka typu SFP+ 10G przeznaczona do transmisji podwójnym (duplex) światłowodem wielomodowym (MM). 2.Kompatybilna z dostarczonymi urządzeniami firewall |  |
|  | Wymagania dotyczące odbioru, instalacji i konfiguracji | 1. Weryfikacja ilościowa i jakościowa dostarczanego sprzętu.
2. Montaż urządzeń UTM w dwóch serwerowniach.
3. Podłączenie firewalli do istniejącej infrastruktury sieciowej.
4. Aktualizacja firmware do najnowszego stabilnego wydania.
5. Przeniesienie konfiguracji z obecnych jednostek firewall, w szczególności:
	1. Konfiguracja profili zabezpieczających (antywirus, filtr stron internetowych, kontrola aplikacji, IPS) zgodnie z dobrymi praktykami i wymaganiami klienta.
	2. Konfiguracja autoryzacji użytkowników za pomocą SSO.
	3. Konfiguracja tuneli IPSec VPN do firm zewnętrznych.
	4. Konfiguracja routingu.
	5. Konfiguracja polityk dostępowych do Internetu i pomiędzy vlanami.
6. Przeprowadzenie testów poprawności działania nowych jednostek.
7. Uaktualnienie informacji o urządzeniach w systemie monitoringu.
 |  |
| **Moduł SPF+** | **Model i producent sprzętu:** |
|  | Typ | 1. Wkładka typu SFP+ 10G przeznaczona do transmisji podwójnym (duplex) światłowodem jednomodowym (SM) na odległość do 10 km. Długość fali TX 1310nm.
2. Kompatybilna z dostarczonym przełącznikiem modułowym Typu B
 |  |
| **Komputer stacjonarny - typ I** | **Model i producent sprzętu:** |
|  | Typ | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta |  |
|  | Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |  |
|  | Procesor | Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 9700 punktów wynik dostępny na stronie https://www.cpubenchmark.net/cpu\_list.php |  |
|  | Pamięć operacyjna RAM | 8GB DDR4 2666MHz non-ECC możliwość rozbudowy do min 32GB, jeden slot wolny |  |
|  | Parametry pamięci masowej | 1. Min.M.2 256 GB SSD SATA
2. Komputer musi umożliwiać instalację min 2 HDD
 |  |
|  | Wydajność grafiki | Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik min 1300 punktów w G3D Rating, wynik dostępny na stronie : <http://www.videocardbenchmark.net/gpu_list.php> |  |
|  | Wyposażenie multimedialne | Min 24-bitowa Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik 2W w obudowie komputera Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. audio out. |  |
|  | Obudowa | Typu Small form factor z obsługą kart PCI Express wyłącznie o niskim profilu, wyposażona w min. 1 wnękę wewnętrznie umożliwiającą montaż dysku 3,5” lub 2 dysków 2,5”. Napęd optyczny w dedykowanej wnęce zewnętrznej slim. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Wyposażona w dystanse gumowe zapobiegające poślizgom obudowy i zarysowaniu lakieru. 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. Suma wymiarów obudowy nie może przekraczać 70cm, waga max 8 kg, Zasilacz o mocy min. 200W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, EPA BRONZEZasilacz w oferowanym komputerze musi się znajdować na stronie <http://www.plugloadsolutions.com/80pluspowersupplies.aspx>, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus, w przypadku, kiedy u producenta występuje kilka zasilaczy które są montowane na etapie produkcji w fabryce załączyć wydruki dla wszystkich zasilaczy.Wydruki 80plus musza być potwierdzone przez producenta lub dołączone oświadczenie producenta komputera, iż wskazane zasilacze przez wykonawcę spełniają 80plus.Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego, dysku 3,5” oraz 2,5”, bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych, śrub radełkowych). Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej raz kłódki (oczko w obudowie do założenia kłódki). Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED np. przycisk POWER [tzn. barw i miganie] w szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej [ w tym również portów I/O, chipset ], awarię CMOS baterii, awarię BIOS’u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. |  |
|  | Zgodność z systemami operacyjnymi | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera ). |  |
|  | Bezpieczeństwo | Ukryty w laminacie płyty głównej 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. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot lub z samego środowiska BIOS umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System oparty o test procesora, pamięci Ram, dysku, układu graficznego. Uruchamiane automatycznie lub w trybie interaktywnym, możliwość powtórzenia testów, podsumowanie testów. Uruchamianie testów zdefiniowanych przez użytkownika. Wyświetlanie wiadomości o błędach, które informują o problemach napotkanych podczas testów.Test musi zawierać informację o nazwie komputera, podawać dokładne informacje o wszystkich zainstalowanych komponentach, a w szczególności zawierać informacje o numerze seryjnym, typie i pojemności dysku twardego, informacji o obrotach wentylatora CPU, informacji o pamięci w tym wielkość podana w MB, oraz SN i PN, wykaz temperatur CPU, pamięci, temperatury panującej wewnątrz obudowy. System posiadający pełną funkcjonalność wymienioną powyżej nawet w przypadku braku dysku twardego, uszkodzenia, sformatowania. Nie dopuszcza się stosowania dodatkowych nośników zewnętrznych (np. pamięci USB flash) oraz konieczności podłączenia jednostki do sieci lokalnej i internetu.  |  |
|  | Wirtualizacja | Sprzętowe wsparcie technologi wirtualizacji realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |  |
|  | BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera, Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy ( przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury).. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności : procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego ) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, dacie produkcji komputera, włączonej lub wyłączonej funkcji aktualizacji BIOS, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, aktywnym kanale – dual channel, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, maksymalnej osiąganej prędkości zainstalowanego procesora, pamięci cache L2 zainstalowanego procesora, pamięci cache L3 zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dyskach twardych podpiętych do dostępnych na płycie głównej portów SATA oraz M.2, rodzajach napędów optycznych, MAC adresie zintegrowanej karty sieciowej,zintegrowanym układzie graficznym, kontrolerze audio.Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.Możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) oraz uprawniającego do samodzielnej zmiany tego hasła przez użytkownika (bez możliwości zmiany innych parametrów konfiguracji BIOS) przy jednoczesnym zdefiniowanym haśle administratora i/lub zdefiniowanym haśle dla dysku Twardego. Użytkownik po wpisaniu swojego hasła jest wstanie jedynie zmienić hasło dla dysku twardego.Możliwość włączenia/wyłączenia kontrolera SATA ( w tym w szczególności pojedynczo)Możliwość włączenia/wyłączenia kontrolera audio,Możliwość włączenia/wyłączenia układu TPM.Możliwość włączenia/wyłączenia wzbudzania komputera za pośrednictwem portów USB,Możliwość włączenia/wyłączenia funkcjonalności Wake On LAN i WLANMożliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia funkcji VT dla Direct I/OMożliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia dodatkowych funkcji sprzętowych Virtual Machine Mnitor (MVMM)Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.Funkcja zbierania i zapisywania incydentów, Możliwość przeglądania i kasowania zdarzeń przebiegu procedury POST. Funkcja ta obejmuje datę i godzinę oraz opis incydentu kodu wizualnego systemu diagnostycznego. Funkcja pozwalająca na włączenie/wyłączenie automatycznego tworzenia recovery BIOS na dysku twardym lub na urządzeniu zewnętrznym podpiętym przez USBMożliwość wyłączania portów USB pojedynczo.Funkcja bezpiecznego usuwania danych oparta o JEDECOferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia min. : uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, wejścia do BIOS, upgrade BIOS bez konieczności uruchamiania systemu operacyjnego.  |  |
|  | Certyfikaty i standardy | Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 (załączyć dokument potwierdzający spełnianie wymogu)Deklaracja zgodności CE (załączyć do oferty)Certyfikat TCO, wymagana certyfikacja na stronie : [http://tco.brightly.se/pls/nvp/!tco\_search](http://tco.brightly.se/pls/nvp/%21tco_search) – załączyć do oferty wydruk z stronyPotwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram |  |
|  | Ergonomia | 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 22 dB (załączyć oświadczenie  |  |
|  | Warunki gwarancji | Firma serwisująca musi posiadać wdrożony system zgodny z ISO 9001:2008 lub równoważną na świadczenie usług gwarancyjnych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że serwis gwarancyjny urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.Minimalny czas trwania gwarancji producenta wynosi 3 lata.**Sposób realizacji usług gwarancji:**Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17. Dedykowany bezpłatny portal online do zgłaszania usterek i zarządzania zgłoszeniami.Usługi gwarancyjne dla sprzętu będą dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii. W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzień roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego.Możliwość sprawdzenia aktualnego okresu i poziomu gwarancji dla urządzeń za pośrednictwem strony internetowej producenta.Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń po zakończeniu okresu gwarancji.Dostawca zapewni bezpłatne oprogramowanie do automatycznej diagnostyki i zdalnego zgłaszania awarii.Zamawiający wymaga od podmiotu realizującego serwis gwarancyjny lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym gwarancją, uszkodzony dysk twardy pozostaje u Zamawiającego. |  |
|  | System operacyjny | Zainstalowany system operacyjny o parametrach:System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Interfejs graficzny użytkownika pozwalający na obsługę:
	1. Klasyczną przy pomocy klawiatury i myszy,
	2. Dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim,
3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe,
4. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje,
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 z mechanizmem sprawdzającym, które z poprawek są potrzebne,
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. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
21. 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,
22. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
23. Obsługa standardu NFC (near field communication),
24. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
25. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
26. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
27. Mechanizmy uwierzytelniania w oparciu o:
	1. Login i hasło,
	2. Karty z certyfikatami (smartcard),
	3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
	4. Wirtualnej tożsamości użytkownika potwierdzanej za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być ze specyfikacją FIDO.
28. Mechanizmy wieloskładnikowego 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. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji,
33. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku
34. Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym,
35. Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny,
36. Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0,
37. Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji,
38. Możliwość konfiguracji trybu „kioskowego” dającego dostęp tylko do wybranych aplikacji i funkcji systemu,
39. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
40. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
41. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
42. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
43. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
44. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego. (provisioning)
45. 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,
46. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
47. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
48. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
49. Udostępnianie wbudowanego modemu,
50. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
51. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
52. 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.),
53. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
54. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
55. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
56. 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.
57. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
58. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
59. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
 |  |
|  | Wymagania dodatkowe | 1. Wbudowane porty:
	1. 1x DisplayPort v1.1a
	2. 1x HDMI 1.4
	3. 1x LAN 10/100/1000 wspierająca obsługęWoL (funkcja włączana przez użytkownika),
2. Porty USB
	1. Panel przedni
		1. - 4x USB TYP-A w układzie 2x USB 3.1 i 2x USB 2.0
	2. Panel Tylny
		1. - 4x USB TYP-A w układzie 2x USB 3.1 i 2x USB 2.0
3. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB TYP-A nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Wszystkie wymagane porty mają być w sposób stały zintegrowane z obudową (wlutowane w laminat płyty głównej).
4. Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w:
	1. 1 złącza PCI Express x16 Gen.3,
	2. 1 złącza PCI Epress x 1,
	3. 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM,
	4. 2 złącza SATA w tym 1 szt SATA 3.0
	5. 1 złącze M.2 2280 dedykowane dla syków M.2 SATA lub NVMe
	6. 1 złącze M.2 WLAN
	7. 1 konektor do realizacji funkcji clear CMOS
	8. 1 konektor do realizacji funkcji clear Password
5. Klawiatura USB w układzie polski programisty
6. Karta WiFi ac + bluetooth 5 (zainstalowana fabrycznie przez producenta komputera)
7. Mysz USB z rolką (scroll)
8. Nagrywarka DVD +/-RW o prędkości min. 8x
9. Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.
10. Dostarczona licencja dostępowa na urządzenie do posiadanego przez zamawiającego systemu windows server 2016.
11. Dostarczony czytnik do kart stykowych o parametrach:
	1. interfejs 2.0 (zgodny z USB 3.0)
	2. Prędkość transmisji -12 Mbps (pełna prędkość USB 2.0)
	3. Kabel połączeniowy USB typ A (długość min 150 cm)
	4. Interfejs kart stykowych (SMARTCARD) CCID
	5. Standardy ISO 7816 A/B/C lub równoważną
	6. Protokoły T=0, T=1
	7. Rozmiar karty ID-1 (pełny rozmiar)
	8. Prędkość interfejsu min 420 Kbps
	9. Częstotliwość taktowania do 8 MHz
	10. Obsługiwane typy kart 5V, 3V, 1,8V
	11. Dopuszczalny pobór prądu dla karty 60 mA
	12. wykrywanie włożenia karty do czytnika, automatyczny power-off, wykrywanie typu karty, system przeciwzwarciowy i ochrona termiczna
12. Typ styków (8pin) - C4 / C8
 |  |
| **Komputer stacjonarny – typ II** | **Model i producent sprzętu:** |
|  | Typ | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta |  |
|  | Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |  |
|  | Procesor | Procesor wielordzeniowy ze zintegrowaną grafik Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 13 800 punktów, wynik dostępny na stronie: https://www.cpubenchmark.net/cpu\_list.php |  |
|  | Pamięć operacyjna RAM | 8GB DDR4 2666MHz non-ECC możliwość rozbudowy do min 32GB, jeden slot wolny |  |
|  | Parametry pamieci masowej | 1. Min.M.2 256 GB SSD SATA
2. Komputer musi umożliwiać instalację min 2 HDD
 |  |
|  | Wydajność grafiki | Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik min 1300 punktów w G3D Rating, wynik dostępny na stronie : <http://www.videocardbenchmark.net/gpu_list.php> |  |
|  | Wyposażenie multimedialne | Min 24-bitowa Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik 2W w obudowie komputera Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. audio out.  |  |
|  | Obudowa | Typu Small form factor z obsługą kart PCI Express wyłącznie o niskim profilu, wyposażona w min. 1 wnękę wewnętrznie umożliwiającą montaż dysku 3,5” lub 2 dysków 2,5”. Napęd optyczny w dedykowanej wnęce zewnętrznej slim. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Wyposażona w dystanse gumowe zapobiegające poślizgom obudowy i zarysowaniu lakieru. 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. Suma wymiarów obudowy nie może przekraczać 70cm, waga max 8 kg, Zasilacz o mocy min. 200W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, EPA BRONZEZasilacz w oferowanym komputerze musi się znajdować na stronie <http://www.plugloadsolutions.com/80pluspowersupplies.aspx>, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus, w przypadku, kiedy u producenta występuje kilka zasilaczy które są montowane na etapie produkcji w fabryce załączyć wydruki dla wszystkich zasilaczy.Wydruki 80plus musza być potwierdzone przez producenta lub dołączone oświadczenie producenta komputera, iż wskazane zasilacze przez wykonawcę spełniają 80plus.1. Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego, dysku 3,5” oraz 2,5”, bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych, śrub radełkowych). Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej raz kłódki (oczko w obudowie do założenia kłódki). Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED np. przycisk POWER [tzn. barw i miganie] w szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej [ w tym również portów I/O, chipset ], awarię CMOS baterii, awarię BIOS’u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
 |  |
|  | Zgodność z systemami operacyjnymi | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera ). |  |
|  | Bezpieczeństwo | Ukryty w laminacie płyty głównej 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. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot lub z samego środowiska BIOS umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System oparty o test procesora, pamięci Ram, dysku, układu graficznego. Uruchamiane automatycznie lub w trybie interaktywnym, możliwość powtórzenia testów, podsumowanie testów. Uruchamianie testów zdefiniowanych przez użytkownika. Wyświetlanie wiadomości o błędach, które informują o problemach napotkanych podczas testów.Test musi zawierać informację o nazwie komputera, podawać dokładne informacje o wszystkich zainstalowanych komponentach, a w szczególności zawierać informacje o numerze seryjnym, typie i pojemności dysku twardego, informacji o obrotach wentylatora CPU, informacji o pamięci w tym wielkość podana w MB, oraz SN i PN, wykaz temperatur CPU, pamięci, temperatury panującej wewnątrz obudowy. System posiadający pełną funkcjonalność wymienioną powyżej nawet w przypadku braku dysku twardego, uszkodzenia, sformatowania. Nie dopuszcza się stosowania dodatkowych nośników zewnętrznych (np. pamięci USB flash) oraz konieczności podłączenia jednostki do sieci lokalnej i internetu.  |  |
|  | Wirtualizacja | Sprzętowe wsparcie technologi wirtualizacji realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |  |
|  | BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera, Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy ( przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury).. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności : procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego ) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, dacie produkcji komputera, włączonej lub wyłączonej funkcji aktualizacji BIOS, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, aktywnym kanale – dual channel, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, maksymalnej osiąganej prędkości zainstalowanego procesora, pamięci cache L2 zainstalowanego procesora, pamięci cache L3 zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dyskach twardych podpiętych do dostępnych na płycie głównej portów SATA oraz M.2, rodzajach napędów optycznych, MAC adresie zintegrowanej karty sieciowej,zintegrowanym układzie graficznym, kontrolerze audio.Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.Możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) oraz uprawniającego do samodzielnej zmiany tego hasła przez użytkownika (bez możliwości zmiany innych parametrów konfiguracji BIOS) przy jednoczesnym zdefiniowanym haśle administratora i/lub zdefiniowanym haśle dla dysku Twardego. Użytkownik po wpisaniu swojego hasła jest wstanie jedynie zmienić hasło dla dysku twardego.Możliwość włączenia/wyłączenia kontrolera SATA ( w tym w szczególności pojedynczo)Możliwość włączenia/wyłączenia kontrolera audio,Możliwość włączenia/wyłączenia układu TPM.Możliwość włączenia/wyłączenia wzbudzania komputera za pośrednictwem portów USB,Możliwość włączenia/wyłączenia funkcjonalności Wake On LAN i WLANMożliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia funkcji VT dla Direct I/OMożliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia dodatkowych funkcji sprzętowych Virtual Machine Mnitor (MVMM)Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.Funkcja zbierania i zapisywania incydentów, Możliwość przeglądania i kasowania zdarzeń przebiegu procedury POST. Funkcja ta obejmuje datę i godzinę oraz opis incydentu kodu wizualnego systemu diagnostycznego. Funkcja pozwalająca na włączenie/wyłączenie automatycznego tworzenia recovery BIOS na dysku twardym lub na urządzeniu zewnętrznym podpiętym przez USBMożliwość wyłączania portów USB pojedynczo.Funkcja bezpiecznego usuwania danych oparta o JEDECOferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia min. : uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, wejścia do BIOS, upgrade BIOS bez konieczności uruchamiania systemu operacyjnego.  |  |
|  | Certyfikaty i standardy | Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 (załączyć dokument potwierdzający spełnianie wymogu)Deklaracja zgodności CE (załączyć do oferty)Certyfikat TCO, wymagana certyfikacja na stronie : [http://tco.brightly.se/pls/nvp/!tco\_search](http://tco.brightly.se/pls/nvp/%21tco_search) – załączyć do oferty wydruk z strony1. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram
 |  |
|  | Ergonomia | 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 22 dB (załączyć oświadczenie  |  |
|  | Warunki gwarancji | 1. Firma świadcząca usługi gwarancyjne musi posiadać ISO 9001:2008 lub równoważny na świadczenie usług gwarancyjnych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
2. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że usługi gwarancyjne urządzeń będą realizowane bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
3. Minimalny czas trwania gwarancji producenta wynosi 3 lata.
4. Sposób realizacji usług gwarancyjnych:
	1. Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17.
	2. Dedykowany bezpłatny portal online do zgłaszania usterek i zarządzania zgłoszeniami.
5. Usługi gwarancyjne dla sprzętu będą dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii.
6. W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzień roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego.
7. Możliwość sprawdzenia aktualnego okresu i poziomu gwarancji dla urządzeń za pośrednictwem strony internetowej producenta.
8. Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń po okresie gwarancji.
9. Dostawca zapewni bezpłatne oprogramowanie do automatycznej diagnostyki i zdalnego zgłaszania awarii.
10. Zamawiający wymaga od podmiotu realizującego gwarancję lub producenta sprzętu, dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym gwarancją, uszkodzony dysk twardy pozostaje u Zamawiającego.
 |  |
|  | System operacyjny | Zainstalowany system operacyjny o parametrach:System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Interfejs graficzny użytkownika pozwalający na obsługę:
	1. Klasyczną przy pomocy klawiatury i myszy,
	2. Dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim,
3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe,
4. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje,
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 z mechanizmem sprawdzającym, które z poprawek są potrzebne,
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. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
21. 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,
22. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
23. Obsługa standardu NFC (near field communication),
24. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
25. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
26. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
27. Mechanizmy uwierzytelniania w oparciu o:
	1. Login i hasło,
	2. Karty z certyfikatami (smartcard),
	3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
	4. Wirtualnej tożsamości użytkownika potwierdzanej za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być ze specyfikacją FIDO.
28. Mechanizmy wieloskładnikowego 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. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji,
33. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku
34. Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym,
35. Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny,
36. Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0,
37. Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji,
38. Możliwość konfiguracji trybu „kioskowego” dającego dostęp tylko do wybranych aplikacji i funkcji systemu,
39. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
40. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
41. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
42. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
43. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
44. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego. (provisioning)
45. 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,
46. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
47. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
48. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
49. Udostępnianie wbudowanego modemu,
50. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
51. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
52. 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.),
53. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
54. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
55. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
56. 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.
57. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
58. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
59. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
 |  |
| 17 | Wymagania dodatkowe | 1. Wbudowane porty:
	1. 1x DisplayPort v1.1a
	2. 1x HDMI 1.4
	3. 1x LAN 10/100/1000 wspierająca obsługęWoL (funkcja włączana przez użytkownika),
2. Porty USB
	1. Panel przedni
		1. - 4x USB TYP-A w układzie 2x USB 3.1 i 2x USB 2.0
	2. Panel Tylny
		1. - 4x USB TYP-A w układzie 2x USB 3.1 i 2x USB 2.0
3. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB TYP-A nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Wszystkie wymagane porty mają być w sposób stały zintegrowane z obudową (wlutowane w laminat płyty głównej).
4. Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w :
	1. 1 złącze PCI Express x16 Gen.3,
	2. 1 złącze PCI Epress x 1,
	3. 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM,
	4. 2 złącza SATA w tym 1 szt. SATA 3.0
	5. 1 złącze M.2 2280 dedykowane dla syków M.2 SATA lub NVMe
	6. 1 złącze M.2 WLAN
	7. 1 konektor do realizacji funkcji clear CMOS
	8. 1 konektor do realizacji funkcji clear Password
5. Klawiatura USB w układzie polski programisty
6. Karta WiFi ac + bluetooth 5 (zainstalowana fabrycznie przez producenta komputera)
7. Mysz USB z rolką (scroll)
8. Nagrywarka DVD +/-RW o prędkości min. 8x
9. Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.
10. Dostarczona licencja dostępowa na urządzenie do posiadanego przez zamawiającego systemu windows server 2016.
11. Dostarczony czytnik do kart stykowych o parametrach:
	1. interfejs 2.0 (zgodny z USB 3.0),
	2. Prędkość transmisji -12 Mbps (pełna prędkość USB 2.0),
	3. Kabel połączeniowy USB typ A (długość min 150 cm),
	4. Interfejs kart stykowych (SMARTCARD) CCID,
	5. Standardy ISO 7816 A/B/C, lub równoważne
	6. Protokoły T=0, T=1,
	7. Rozmiar karty ID-1 (pełny rozmiar),
	8. Prędkość interfejsu min 420 Kbps,
	9. Częstotliwość taktowania do 8 MHz,
	10. Obsługiwane typy kart 5V, 3V, 1,8V,
	11. Dopuszczalny pobór prądu dla karty 60 mA,
	12. wykrywanie włożenia karty do czytnika, automatyczny power-off, wykrywanie typu karty, system przeciwzwarciowy i ochrona termiczna,
12. Typ styków (8pin) - C4 / C8.
 |  |
| **Komputer stacjonarny All-in-one** | **Model i producent sprzętu:** |
|  | Typ | Komputer stacjonarny all-in-one. W ofercie wymagane jest podanie modelu, symbolu oraz producenta |  |
| 2. | Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |  |
| 3. | Procesor | Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 9000 punktów, wynik dostępny na stronie: https://www.cpubenchmark.net/cpu\_list.php |  |
| 4. | Pamięć operacyjna RAM | Min 8GB DDR4 2666MHz non-ECC  |  |
| 5. | Parametry pamieci masowej | Min.M.2 256 GB SSD nvme |  |
| 6. | Obudowa | Typu all in one z ekranem dotykowym.Matryca:- min FULLHD (1920x1080)- 21,5cal.- 10 punktowa obsługa wielodotykowa |  |
| 7. | Warunki gwarancji | 1. Minimalny czas trwania gwarancji producenta wynosi 3 lata.
2. Sposób realizacji usług gwarancyjnych:
3. Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17.
4. Dedykowany bezpłatny portal online do zgłaszania usterek i zarządzania zgłoszeniami.
5. Usługi gwarancyjne dla sprzętu będą dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii.
6. W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzień roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego.
7. Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń po okresie gwarancji.
 |  |
| 8. | System operacyjny | Zainstalowany system operacyjny o parametrach:System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Interfejs graficzny użytkownika pozwalający na obsługę:
	1. Klasyczną przy pomocy klawiatury i myszy,
	2. Dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim,
3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe,
4. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje,
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 z mechanizmem sprawdzającym, które z poprawek są potrzebne,
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. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
21. 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,
22. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
23. Obsługa standardu NFC (near field communication),
24. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
25. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
26. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
27. Mechanizmy uwierzytelniania w oparciu o:
	1. Login i hasło,
	2. Karty z certyfikatami (smartcard),
	3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
	4. Wirtualnej tożsamości użytkownika potwierdzanej za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być ze specyfikacją FIDO.
28. Mechanizmy wieloskładnikowego 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. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji,
33. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku
34. Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym,
35. Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny,
36. Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0,
37. Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji,
38. Możliwość konfiguracji trybu „kioskowego” dającego dostęp tylko do wybranych aplikacji i funkcji systemu,
39. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
40. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
41. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
42. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
43. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
44. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego. (provisioning)
45. 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,
46. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
47. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
48. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
49. Udostępnianie wbudowanego modemu,
50. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
51. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
52. 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.),
53. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
54. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
55. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
56. 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.
57. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
58. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.

Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu. |  |
| 9. | Wymagania dodatkowe | 1. Wbudowane porty:

a) USB 3.1 Gen 2 z RapidChargeb) USB-Cc) Gniazdo słuchawek/mikrofonud) Port szeregowye) DisplayPortf) 4x usb 3.1 Gen1g) RJ-451. Karta WiFi ac + bluetooth 5 (zainstalowana fabrycznie przez producenta komputera)
2. Mysz USB z rolką (scroll)
3. Dostarczona licencja dostępowa na urządzenie do posiadanego przez zamawiającego systemu windows server 2016.
4. Dostarczony czytnik do kart stykowych o parametrach:
	1. interfejs 2.0 (zgodny z USB 3.0),
	2. Prędkość transmisji -12 Mbps (pełna prędkość USB 2.0),
	3. Kabel połączeniowy USB typ A (długość min 150 cm),
	4. Interfejs kart stykowych (SMARTCARD) CCID,
	5. Standardy ISO 7816 A/B/C, lub równoważne
	6. Protokoły T=0, T=1,
	7. Rozmiar karty ID-1 (pełny rozmiar),
	8. Prędkość interfejsu min 420 Kbps,
	9. Częstotliwość taktowania do 8 MHz,
	10. Obsługiwane typy kart 5V, 3V, 1,8V,
	11. Dopuszczalny pobór prądu dla karty 60 mA,
	12. wykrywanie włożenia karty do czytnika, automatyczny power-off, wykrywanie typu karty, system przeciwzwarciowy i ochrona termiczna,

Typ styków (8pin) - C4 / C8. |  |
| **Monitor LCD** | **Model i producent sprzętu:** |
|  | Typ ekranu | Ekran ciekłokrystaliczny z aktywną matrycą min. 21,5” (16:9). |  |
|  | Rozmiar plamki | 0,248 mm |  |
|  | Jasność | 250 cd/m2 |  |
|  | Kontrast | Typowy 1000:1 |  |
|  | Kąty widzenia (pion/poziom) | 160/170 stopni |  |
|  | Czas reakcji matrycy | Max 5ms (Black to White) |  |
|  | Rozdzielczość maksymalna | 1920 x 1080 przy 60Hz |  |
|  | Color Gamut | 1. 83% (CIE 1976)

72% (CIE 1931) |  |
|  | Zużycie energii | Normalne działanie 19W (typowe), 24W (maksymalne), tryb wyłączenia aktywności mniej niż 0,3W |  |
|  | Powłoka powierzchni ekranu | 1. Antyodblaskowa utwardzona
 |  |
|  | Podświetlenie | System podświetlenia LED |  |
|  | Bezpieczeństwo | 1. Monitor musi być wyposażony w tzw. Kensington Slot - gniazdo zabezpieczenia przed kradzieżą.

Wbudowane w monitor narzędzie diagnostyczne umożliwiające zdiagnozowanie problemu wyświetlania obrazu na ekranie (kwestia karty graficznej czy monitora) |  |
|  | Waga bez podstawy | Maksymalnie 2,85 kg |  |
|  | Waga z podstawą + kable | 1. Maksymalnie 3,70 kg
 |  |
|  | Zakres regulacji Tilt | Wymagany, od -5 do +21  |  |
|  | Kolor obudowy | Czarny |  |
|  | Złącze  | 1. 1x 15-stykowe złącze D-Sub,
2. 1x DisplayPort
 |  |
|  | Gwarancja | 1. 3 lata na miejscu u klienta
2. Firma świadcząca usługi gwarancji musi posiadać wdrożony system zgodny z ISO 9001:2000 lub równoważny na świadczenie usług serwisu gwarancyjnego oraz posiadać autoryzacje producenta– dokumenty potwierdzające załączyć do oferty.
3. Oświadczenie producenta, że w przypadku nie wywiązywania się z  obowiązków gwarancyjnych oferenta lub firmy świadczącej usługi gwarancji, przejmie na siebie wszelkie zobowiązania związane z serwisem gwarancyjnym.
 |  |
|  | Certyfikaty | TCO , ISO 13406-2 lub ISO 9241, EPEAT Gold, Energy Star 5.2 lub nowszy- lub równoważne |  |
|  | Inne | Zdejmowana podstawa oraz otwory montażowe w obudowie VESA 100mm |  |
| **Urządzenie wielofunkcyjne kolorowe** | **Model i producent sprzętu:** |
|  | Technologia druku | Laser, kolor |  |
|  | Funkcje standardowe | Kopiarka, drukarka sieciowa, skaner sieciowy, faks  |  |
|  | Format oryginału | A4 |  |
|  | Format kopii | A4-A6 |  |
|  | Prędkość druku | 26 stron A4 / min. |  |
|  | Dostępne rozdzielczości drukowania | 600, 1200 dpi  |  |
|  | Czas wydruku pierwszej strony w kolorze | maks. 11 sek. |  |
|  | Czas nagrzewania | maks. 30 sek.  |  |
|  | Kopiowanie wielokrotne | 1- 999 kopii |  |
|  | Pamięć RAM | min. 512 MB (możliwość rozbudowy do min. 1,5 GB) |  |
|  | Zoom | 25-400%  |  |
|  | Panel operatora | wyposażony w kolorowy ekran dotykowy LCD, opisy na panelu oraz komunikaty na ekranie w języku polskim |  |
|  | Drukowanie dwustronne | automatyczne, w standardzie |  |
|  | Podajnik dokumentów | automatyczny, dwustronny jednoprzebiegowy na min. 50 ark. (80 g/m2), w standardzie  |  |
|  | Podajniki papieru | min. 1 kaseta na min. 250 ark. A5-A4 (80 g/m2), 60-160 g/m2;taca uniwersalna na min. 50 ark. A6-A4 (80 g/m2), 60-220 g/m2 |  |
|  | Funkcja druku sieciowego | w standardzie |  |
|  | Emulacje | PCL 6, PostScript 3 |  |
|  | Interfejsy | USB 2.0, Ethernet 10BaseT/100BaseTX/1000BaseT, USB dla pamięci przenośnej, gniazdo karty SD |  |
|  | Funkcja skanowania sieciowego | w standardzie, skanowanie pełno-kolorowe  |  |
|  | Funkcje skanowania | skanowanie do e-mail, do FTP, do-SMB, TWAIN, WSD, do pamięci przenośnej USB |  |
|  | Rozdzielczość skanowania | 600 dpi  |  |
|  | Prędkość skanowania | W trybie mono: min. 30 obrazów/min. (A4, 300 dpi), W trybie kolorowym: min. 20 obrazów/ min. (A4, 300 dpi) |  |
|  | Typy plików | PDF, JPEG, TIFF, XPS |  |
|  | Funkcja faksu | Wymagany wewnętrzny, zintegrowany faks analogowy zapewniający wysyłanie i odbiór dokumentów papierowych przy pomocy linii telefonicznej, funkcja PC-faks. |  |
|  | Możliwość rozbudowy | Dodatkowy podajnik na min. 250 ark. formatu A4 – A5, 80 g/m2 |  |
|  | Materiały eksploatacyjne jako wyposażenie standardowe (dostarczone w komplecie w ramach oferowanej ceny jednostkowej). | 1. **Tonery** - właściwa ilość, która zapewni wydrukowanie minimum 1 000 stron A4 przy pokryciu zgodnie z ISO19752.
2. **Bębny** - właściwa ilość, która zapewni wydrukowanie minimum 100 000 stron A4. Dostarczone materiały muszą być nowe i nieużywane, pierwszej kategorii oraz wyprodukowane przez producenta oferowanych urządzeń.
 |  |
|  | Wymagania dodatkowe | Oświadczenie producenta oferowanego sprzętu lub jego autoryzowanego przedstawiciela w Polsce, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy świadczącej usługi gwarancyjne, przejmie na siebie wszelkie zobowiązania związane z serwisem. Konieczność nie zachodzi w przypadku autoryzowanego przedstawiciela producenta.Certyfikat ISO 9001:2008 lub równoważny producenta oferowanego sprzętuCertyfikat ISO 14001:2004 lub równoważny producenta oferowanego sprzętu |  |
| **Drukarka biurowa czarno-biała** | **Model i producent sprzętu:** |
|  | Technologia druku | Laserowa/ LED |  |
|  | Rodzaj druku | Monochromatyczny |  |
|  | Rozdzielczość | 600 x 600 dpi |  |
|  | Format wydruku | A4 |  |
|  | Prędkość druku | 30 stron A4/minutę przy zachowaniu rozdzielczości 600x600 dpi |  |
|  | Czas wydruku pierwszej strony | Maksymalnie 7 sekund |  |
|  | Obciążalność miesięczna | 50 000 stron A4 w miesiącu. |  |
|  | Pamięć RAM zainstalowana | 256 MB  |  |
|  | Emulacje | PCL 6, PCL 5e, PostScript3 lub emulacja. |  |
|  | Interfejsy | USB 2.0, Gigabit Ethernet (10BaseT/100BaseTX/1000BaseT). |  |
|  | Obsługiwane systemy operacyjne | Windows 7/8/10 |  |
|  | Gramatura papieru | 60 – 160 g/m2 |  |
|  | Podajniki papieru | 1 podajnik w formie zamkniętej kasety na minimum 250 arkuszy A4,1 podajnik wielofunkcyjny na minimum 100 arkuszy A4. |  |
|  | Odbiornik papieru umieszczony na górze drukarki | Min. 250 arkuszy A4 80 g/m2 |  |
|  | Technologia druku | Rozdzielność bębna i tonera |  |
|  | Poziom hałasu | W trakcie drukowania nieprzekraczający 50 dB(A). |  |
|  | Maksymalne wymiary urządzenia (szerokość x głębokość x wysokość) | 380 x 400 x 280 mm. |  |
|  | Materiały eksploatacyjne jako wyposażenie standardowe drukarki (dostarczone w komplecie w ramach oferowanej ceny jednostkowej) | Drukarka powinna mieć w standardzie toner startowy na min. 3000 wydruków zgodnie z normą ISO/IEC 19752. Dodatkowo powinna być w stanie obsługiwać standardowy toner na min. 7000 wydruków zgodnie z normą ISO/IEC 19752.Bębny pozwalające wydrukować min. 100 000 wydruków. |  |
|  | Procesor | 800 MHz |  |
|  | Waga | Do 15 kg |  |
|  | Wydruk dwustronny | Automatyczny |  |
|  | Gwarancja | 36 miesięcy |  |
|  | Oświadczenie | Oświadczenie producenta oferowanego sprzętu lub jego autoryzowanego przedstawiciela w Polsce, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy świadczącej usługi gwarancyjne, przejmie na siebie wszelkie zobowiązania związane z serwisem gwarancyjnym. Konieczność nie zachodzi w przypadku autoryzowanego przedstawiciela producenta. |  |
|  | Certyfikat | 1. Certyfikat ISO 140001:2004 lub równoważny producenta oferowanego sprzętu.
2. Certyfikat ISO 9001:2008 lub równoważny producenta oferowanego sprzętu.
 |  |
| **Drukarka kodów kreskowych** | **Model i producent sprzętu:** |
|  | Druk | Termiczny |  |
|  | Rozdzielczość | 8 pkt/mm (203 dpi) |  |
|  | Prędkość druku | Min. 150mm/s |  |
|  | Max szerokość nośników | 108 mm |  |
|  | Max długość nośników | 990 mm. |  |
|  | Maksymalne wymiary rolki z nośnikiem | Średnica zew. 127 mm na rdzeniu o średnicy, wew. 25,4 mm lub 38 mm. |  |
|  | Waga | Max 1,5 kg. |  |
|  | Wymiary, obudowa | 1. Max. 160 x 175 x 210 mm.
2. Obudowa plastikowa.
 |  |
|  | Temperatura pracy | 4,4˚C– 41˚C |  |
|  | Wilgotność pracy | 5% – 95% |  |
|  | Procesor | RISC 32- bitowy |  |
|  | Język programowania | EPL, EPL2, ZPL2 |  |
|  | Pamięć | Flash 4 MB, SDRAM 8 MB |  |
|  | Interfejs | 1. Porty równoległe Centronics® (36-pinowe).
2. Interfejs szeregowy RS-232.
3. Interfejs USB 1.1, dwukierunkowy.
 |  |
|  | Zasilacz | 100- 240V 50=60Hz |  |
|  | Drukowane kody kreskowe | 1. Stosunek kresek: 2:1 (bez rotacji) i 3:1.
2. Kody liniowe: Code 11, Code 39, Code 93, Code 128, UPC-A, UPC-E, EAN-8, EAN-13, EAN-14, UPC-A and UPC-E with EAN 2 or 5 digit extensions, Plessey, POSTNET, Standard 2 of 5, Industrial 2 of 5, Interleaved 2 of 5, LOGMARS, MSI, Codabar i GS1 DataBar®.
3. (formerly RSS).
4. Kody dwuwymiarowe: PDF417, MicroPDF-417, Code 49,
5. Maxicode, Codablock, Data Matrix, QR code, Aztec.
 |  |
| **CAL** |  |
|  | Oprogramowanie | MS Windows Server 2019 CAL lub równoważne\* |  |
|  | Inne | Wykonawca zapewni dostęp do spersonalizowanej strony producenta produktów pozwalającej upoważnionym osobom ze strony Zamawiającego na:1. Pobieranie zakupionego oprogramowania,
2. Pobieranie kluczy aktywacyjnych do zakupionego oprogramowania,

Sprawdzanie liczby zakupionych licencji w wykazie zakupionych produktów. |  |
|  | Sposób licencjonowania | 1. Zamawiający nie dopuszcza licencji OEM
2. Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu.
3. Zamawiający wymaga licencji grupowej (jeden klucz na wszystkie produkty).
4. Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta.
5. Licencja ma umożliwiać downgrade do poprzednich wersji licencji oraz uprawniać do dostępu do zasobów serwera dla określonej liczby urządzeń.
6. Licencja powinna zapewnić (w zgodzie z wymaganiami licencyjnymi producenta) możliwość równoległego zarządzania wybranymi usługami przez administratorów serwera, a także dostęp do zasobów serwera dla określonej liczby urządzeń.
 |  |
|  | Kompatybilność | Zamawiający wymaga, aby licencja była kompatybilna z Serwerowym Systemem Operacyjnym Microsoft Windows Server 2019 DataCenter lub równoważnym zgodnie z powyższymi wymaganiami. |  |
| **Oprogramowanie antyspamowe** | **Model i producent sprzętu:** |
|  | Wymagania ogólne | System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM.Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Opisy do wymagań ogólnych1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. **System antyspam musi integrować się z posiadanymi przez zamawiającego jednostkami FortiGate 300C.**
 |  |
|  | Parametry fizyczne systemuantyspamowego | System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 2 TB. |  |
|  | Kontrola antywirusowai ochrona przed malware | W tym zakresie dostarczony system ochrony poczty musi zapewniać:1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. 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. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
7. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
8. Ochronę typu wirus outbrake.
 |  |
|  | Kontrola antyspamowa | System musi zapewniać poniższe funkcje i metody filtrowania spamu:* 1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
	2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
	3. Szczegółowa kontrola nagłówka wiadomości.
	4. Analiza Heurystyczna.
	5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
	6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
	7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
	8. Wykrywanie spamu w oparciu a analizę plików graficznych oraz plików PDF.
	9. Kontrola w oparciu o Greylisting oraz SPF.
	10. Filtrowanie treści wiadomości i załączników.
	11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
	12. Ochrona typu outbrake.
	13. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
	14. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
 |  |
|  | Ochrona przed atakami na usługę poczty | System musi zapewniać poniższe funkcje i metody filtrowania:1. Ochrona przed atakami na adres odbiorcy.
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.
 |  |
|  | Funkcje logowania i raportowania | W tym zakresie dostarczony system ochrony poczty musi zapewniać:1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
 |  |
|  | Funkcje pracy w trybie wysokiej dostępności (HA) | System ochrony poczty musi zapewniać poniższe funkcje:1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.
 |  |
|  | Aktualizacje sygnatur, dostęp do bazy spamu | W tym zakresie dostarczony system ochrony poczty musi zapewniać:1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
 |  |
|  | Zarządzanie | System ochrony poczty musi zapewniać poniższe funkcje:1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 7 lokalnych kont administracyjnych.
 |  |
|  | Certyfikaty | Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:* 1. VBSpam,
	2. VB100 rated,
	3. Common Criteria NDPP,
	4. FIPS 140-2 Certified.
 |  |
|  | Serwisy i licencje | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:* 1. Kontrola Antyspam,
	2. URL Filtering,
	3. Kontrola antywirusowa,
	4. Ochrona typu virus outbrake, na okres 36 miesięcy.
 |  |
|  | Wymagania dotyczące instalacji i konfiguracji | 1. Instalacja maszyny wirtualnej w środowisku Zamawiającego.
2. Konfiguracja sieciowa urządzenia.
3. Konfiguracja chronionej domeny mailowej.
4. Konfiguracja profili dostępowych dla administratorów.
5. Integracja systemu z Active Directory za pomocą protokołu LDAP.
6. Konfiguracja profili zabezpieczających przed złośliwym oprogramowaniem, spamem oraz niedozwolonymi treściami.
7. Konfiguracja kwarantanny.
8. Konfiguracja reguł pocztowych z użyciem zdefiniowanych profili zabezpieczających.
9. Konfiguracja logowania zdarzeń i raportowania,
10. Testy i monitorowanie po przełączeniu produkcyjnym.
 |  |
| **System analizy logów** | **Model i producent sprzętu:** |
|  | Wymagania ogólne | W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM. |  |
|  | Interfejsy, Dysk | System musi obsługiwać, co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 1 TB. |  |
|  | Parametry wydajnościowe | 1. System musi być w stanie przyjmować minimum 2 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów, z co najmniej 1000 systemów
 |  |
|  | Logowanie | 1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować, co najmniej:
	1. Listę najczęściej wykrywanych ataków.
	2. Listę najbardziej aktywnych użytkowników.
	3. Listę najczęściej wykorzystywanych aplikacji.
	4. Listę najczęściej odwiedzanych stron www.
	5. Listę krajów, do których nawiązywane są połączenia.
	6. Listę najczęściej wykorzystywanych polityk Firewall.
	7. Informacje o realizowanych połączeniach IPSec.
4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
 |  |
|  | Raportowanie | W zakresie raportowania system musi zapewniać:1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.
 |  |
|  | Korelacja logów | W zakresie korelacji zdarzeń system musi zapewniać:1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
	1. Malware.
	2. Aplikacje sieciowe.
	3. Email.
	4. IPS.
	5. Traffic.
	6. Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
 |  |
|  | Zarządzanie | 1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
	1. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
2. System musi umożliwiać zdefiniowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
 |  |
|  | Gwarancja | 1. System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz usług gwarancyjnych w trybie 8x5.

Opisy do wymagań ogólnych1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. System logowania musi integrować się z posiadanymi przez zamawiającego jednostkami FortiGate 300C.
 |  |
|  | Wymagania dotyczące instalacji i konfiguracji | 1. Instalacja maszyny wirtualnej w środowisku Zamawiającego.
2. Podstawowa konfiguracja systemu.
3. Konfiguracja wysyłania logów z Fortigate posiadanych przez Zamawiającego.
4. Uruchomienie systemu Syslog i dodanie podanych przez Zamawiającego urządzeń sieciowych.
5. Zdefiniowanie cyklicznych raportów.
6. Konfiguracja powiadomień o wybranych zdarzeniach.
 |  |
| **Oprogramowanie biurowe** | **Model i producent sprzętu:** |
|  | Minimalne wymagania | Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej,
2. Wymagania odnośnie interfejsu użytkownika:
	1. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.
	2. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
	3. 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.
3. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi katalogowej Active Directory.
4. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.
5. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:
	1. posiada kompletny i publicznie dostępny opis formatu,
	2. 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. 2012, poz. 526),
	3. umożliwia kreowanie plików w formacie XML,
	4. wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES.
6. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
7. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
8. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
9. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
10. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
	1. Edytor tekstów.
	2. Arkusz kalkulacyjny.
	3. Narzędzie do przygotowywania i prowadzenia prezentacji.
	4. Narzędzie do tworzenia drukowanych materiałów informacyjnych.
	5. Narzędzie do tworzenia i pracy z lokalną bazą danych.
	6. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).
	7. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.
	8. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.
11. Edytor tekstów musi umożliwiać:
	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. 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.
	3. Wstawianie oraz formatowanie tabel.
	4. Wstawianie oraz formatowanie obiektów graficznych.
	5. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
	6. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
	7. Automatyczne tworzenie spisów treści.
	8. Formatowanie nagłówków i stopek stron.
	9. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
	10. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.
	11. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
	12. Określenie układu strony (pionowa/pozioma).
	13. Wydruk dokumentów.
	14. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
	15. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
	16. Zapis i edycję plików w formacie PDF.
	17. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
	18. Możliwość jednoczesnej pracy wielu użytkowników na jednym dokumencie z uwidacznianiem ich uprawnień i wyświetlaniem dokonywanych przez nie zmian na bieżąco,
	19. Możliwość wyboru jednej z zapisanych wersji dokumentu, nad którym pracuje wiele osób.
12. Arkusz kalkulacyjny musi umożliwiać:
	1. Tworzenie raportów tabelarycznych.
	2. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
	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.
	4. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).
	5. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
	6. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.
	7. Wyszukiwanie i zamianę danych.
	8. Wykonywanie analiz danych przy użyciu formatowania warunkowego.
	9. Tworzenie wykresów prognoz i trendów na podstawie danych historycznych z użyciem algorytmu ETS.
	10. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
	11. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
	12. Formatowanie czasu, daty i wartości finansowych z polskim formatem.
	13. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
	14. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
	15. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).
	16. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
	17. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
13. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
	1. Przygotowywanie prezentacji multimedialnych, które będą:
	2. Prezentowanie przy użyciu projektora multimedialnego
	3. Drukowanie w formacie umożliwiającym robienie notatek
	4. Zapisanie jako prezentacja tylko do odczytu.
	5. Nagrywanie narracji i dołączanie jej do prezentacji
	6. Opatrywanie slajdów notatkami dla prezentera
	7. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
	8. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
	9. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
	10. Możliwość tworzenia animacji obiektów i całych slajdów
	11. 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.
	12. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.
14. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:
	1. Tworzenie i edycję drukowanych materiałów informacyjnych
	2. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.
	3. Edycję poszczególnych stron materiałów.
	4. Podział treści na kolumny.
	5. Umieszczanie elementów graficznych.
	6. wykorzystanie mechanizmu korespondencji seryjnej
	7. Płynne przesuwanie elementów po całej stronie publikacji.
	8. Eksport publikacji do formatu PDF oraz TIFF.
	9. Wydruk publikacji.
	10. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.
15. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
	1. Uwierzytelnianie wieloskładnikowe poprzez wbudowane wsparcie integrujące z usługą Active Directory,
	2. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
	3. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
	4. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
	5. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
	6. Automatyczne grupowanie poczty o tym samym tytule,
	7. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
	8. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
	9. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
	10. Zarządzanie kalendarzem,
	11. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
	12. Przeglądanie kalendarza innych użytkowników,
	13. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
	14. Zarządzanie listą zadań,
	15. Zlecanie zadań innym użytkownikom,
	16. Zarządzanie listą kontaktów,
	17. Udostępnianie listy kontaktów innym użytkownikom,
	18. Przeglądanie listy kontaktów innych użytkowników,
	19. Możliwość przesyłania kontaktów innym użytkowników,
	20. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.
 |  |