**Sfinansowano w ramach reakcji Unii na pandemię COVID-19**

WRG.271.9.2022

# Załącznik nr 1 do SWZ
# OPIS PRZEDMIOTU ZAMÓWIENIA - OPIS TECHNICZNY

**„Dostawa sprzętu komputerowego i oprogramowania w ramach projektu grantowego pn. „Cyfrowa Gmina”**

## Część 1: Dostawa stacji roboczych, komputerów przenośnych i oprogramowania.

### Stacje robocze typ I (komputery stacjonarne z systemem operacyjnym, klawiaturą, myszką i monitorem)

| Obszar wymagań | Wymagane minimalne |
|---|---|
| **Typ urządzenia** | **Komputer stacjonarny** |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do sieci Internet oraz sieci wewnętrznej, poczty elektronicznej oraz świadczenia szeregu usług publicznych dla ludności na drodze teleinformatycznej. |
| Wydajność | Procesor wielordzeniowy zaprojektowany do pracy w komputerach stacjonarnych, który uzyskuje wynik co najmniej **16000** punktów **w teście PassMark – CPU Mark**, według wyników opublikowanych na stronie internetowej http://www.cpubenchmark.net/cpu_list.php. Wynik w okresie nie wcześniej niż 21 dni przed terminem składania ofert. **Do oferty należy dołączyć wydruk z powyższej strony. Zamawiający dopuszcza wydruk w języku angielskim.** |
| Obudowa | Typ obudowy dostosowany do oferowanych parametrów zestawu, o minimalnych wymiarach (wysokość/szerokość/głębokość) 250 mm/80 mm/200 mm, mierzone w orientacji pionowej obudowy. Suma wymiarów nie może przekraczać 750 mm. Miejsce na porty USB zarówno na przednim (min. 2 sztuki) oraz tylnym panelu (min. 4 sztuki). Gniazdo słuchawkowe port combo lub słuchawki plus mikrofon na przednim panelu. Na obudowie trwale umieszczony niepowtarzalny numer seryjny każdego komputera, który powinien być wpisany na stałe w BIOS. |
| Zasilacz | Zasilacz wewnętrzny pracujący w sieci 230V 50/60 Hz prądu zmiennego. Moc adekwatna do proponowanego zestawu, umożliwiająca pracę komputera przy pełnym wyposażeniu w dodatkowe urządzenia podpięte przez porty i sloty rozszerzeń. |

| | |
|---|---|
| Pamięć operacyjna | Zainstalowana pamięć o pojemności co najmniej 16 GB.<br>Ilość zajętych slotów pamięci 2 sztuki. |
| Dyski twarde | Dysk półprzewodnikowy SSD M.2 NVMe o pojemności min. 512 GB zawierający RECOVERY umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
| Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu, dynamicznie rozdzielaną na potrzeby grafiki – z możliwością dynamicznego przydzielania pamięci. |
| Karta dźwiękowa | Zintegrowana z płytą główną, co najmniej dwukanałowa. Gniazdo słuchawek i mikrofonu znajdujące się na obudowie podłączone do karty. |
| Karta sieciowa LAN | LAN 10/100/1000 Mbit/s – złącze RJ45<br>Wspierająca obsługę Wake on LAN - włączana przez użytkownika. |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, z pełną obsługą za pomocą klawiatury i myszy. Możliwość ustawienia hasła administratora, oraz blokady aktualizacji bez podania hasła administratora. |
| Zintegrowany system diagnostyczny | Pełny system diagnostyczny dostępny z poziomu BIOS lub menu boot, umożliwiający pełne przetestowanie komponentów komputera nawet bez użycia: dysku twardego, dostępu do sieci i Internetu, urządzeń zewnętrznych typu pendrive itp. Działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera. |
| Bezpieczeństwo | Moduł TPM znajdujący się na płycie głównej. |
| System operacyjny | System operacyjny w wersji odpowiedniej dla jednostki samorządu terytorialnego, musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:<br>1. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.<br>2. Internetowa aktualizacja systemu w języku polskim.<br>3. Graficzne środowisko instalacji i konfiguracji systemu dostępne w języku polskim.<br>4. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji.<br>5. Bezpłatne aktualizacje w ramach wersji systemu operacyjnego przez Internet z możliwością wyboru instalowanych poprawek.<br>6. Aktualizacja sterowników urządzeń możliwa przez Internetową witrynę producenta systemu.<br>7. Interfejs użytkownika dostępny w wielu językach do wyboru – w |

| | |
|---|---|
| | tym polskim i angielskim.<br>8. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie, praca systemu w trybie ochrony kont użytkowników.<br>9. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. Zapora zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.<br>10. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.<br>11. Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta.<br>12. Wbudowany system pomocy w języku polskim.<br>13. 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.<br>14. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). Funkcjonalność rozpoznawania mowy, pozwalająca na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.<br>15. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.<br>16. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (tj. drukarek, urządzeń wielofunkcyjnych, urządzeń sieciowych, standardów: USB, Plug&Play, Wi-Fi). Automatyczna zmiana domyślnej drukarki w zależności do sieci, o której podłączony jest komputer.<br>17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.<br>18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.<br>19. 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.).<br>20. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.<br>21. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.<br>22. Narzędzie służące do automatycznego tworzenia obrazu systemu wraz z aplikacjami. Możliwość wdrożenie nowego obrazu poprzez zdalną instalację.<br>23. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.<br>24. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.<br>25. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).<br>26. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.<br>27. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.<br>28. Możliwość zarządzania stacją roboczą poprzez polityki – reguły definiujące lub ograniczające funkcjonalność systemu lub aplikacji. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.<br>29. Automatyczne występowanie i używanie (wstawianie) certyfikatów PKI X.509.<br>30. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM.<br>31. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot).<br>32. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.<br>33. Zarządzanie komputerami, kontami i grupami użytkowników.<br>34. Wsparcie dla Sun Java i NET Framework 1.x, 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych |

| | |
|---|---|
| | środowiskach.<br>35. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.<br>**Oferowany system operacyjny powinien być nieużywany tzn. klucz systemu nie może być wykorzystany wcześniej do aktywacji na innym urządzeniu.** |
| Wymagania dodatkowe | Płyta główna komputera wyposażona w niezbędne okablowanie i sterowniki. Chipset adekwatny do zaproponowanego procesora.<br>Złącza cyfrowe wideo zgodnie z zaoferowanym monitorem.<br>Podłączony co najmniej jeden port HDMI na tylnym panelu.<br>Wiele różnych wbudowanych portów/złącz umożliwiających elastyczne podłączenie urządzenia bez stosowania przejściówek.<br>Ponadto, co najmniej 6 x USB w tym 2 wprowadzane na przedzie obudowy, oraz 4 USB na tylnym panelu.<br>Na tylnym panelu wejście RJ45.<br>Wymagana ilość oraz rozmieszczenie wszystkich w/w portów nie może być osiągnięta w wyniku stosowania konwerterów, przewodów połączeniowych, przejściówek itp. |
| Niezawodność/jakość wytwarzania | Potwierdzona certyfikatem ISO 9001 lub równoważnym dla producenta sprzętu. **(należy dołączyć do oferty)**<br>Deklaracja zgodności CE. **(należy dołączyć do oferty)** |
| Gwarancja producenta | Minimum trzyletnia gwarancja producenta, obejmująca wszystkie komponenty komputera. |
| Wsparcie techniczne producenta | Dedykowany numer telefonu oraz adres email lub portal techniczny (dokładny adres strony internetowej) producenta umożliwiający zgłaszanie awarii, wsparcie techniczne i informacji produktowej, w tym konfiguracji fabrycznej oferowanego sprzętu.<br><br>Dostęp do aktualnych sterowników zainstalowanych w komputerze urządzeń realizowany poprzez podanie identyfikatora klienta lub modelu komputera lub numeru seryjnego komputera, na dedykowanej przez producenta stronie internetowej. |
| **Typ urządzenia** | **Klawiatura/Mysz** |
| Zastosowanie | Urządzenia peryferyjne wykorzystywane do normalnego użytkowania powyższego komputera stacjonarnego. |
| Klawiatura<br>Mysz | Klawiatura przewodowa w układzie US.<br>Mysz optyczna przewodowa USB. |

**Sfinansowano w ramach reakcji Unii na pandemię COVID-19**

WRG.271.9.2022

| **Typ urządzenia** | **Monitor** |
|---|---|
| Zastosowanie | Monitor będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do sieci Internet oraz sieci wewnętrznej, poczty elektronicznej oraz świadczenia szeregu usług publicznych dla ludności na drodze teleinformatycznej. |
| Wielkość ekranu | Przekątna co najmniej 27” nie więcej niż 32’’. |
| Matryca | IPS, PLS, VA, TN z podświetleniem LED o wykończeniu matowym (nie dopuszcza się naklejek matowiących matrycę). |
| Rozdzielczość podstawowa | 1920 x 1080 pikseli |
| Typ ekranu | Płaski |
| Janość | Przynajmniej 250 cd/$m^2$ |
| Kontrast typowy | Przynajmniej 1000:1 |
| Czas reakcji | Maksymalnie 5ms |
| Certyfikaty i standardy | Certyfikat ISO 9001 lub równoważny dla producenta sprzętu. **(należy dołączyć do oferty)**<br>Deklaracja zgodności CE. **(należy dołączyć do oferty)** |
| Gwarancja producenta | Minimum dwuletnia gwarancja producenta. |
| Wsparcie techniczne producenta | Dedykowany numer telefonu oraz adres email lub portal techniczny (dokładny adres strony internetowej) producenta umożliwiający zgłaszanie awarii, wsparcie techniczne, weryfikację kompletnych danych o modelu monitora. |
| Inne | Złącze cyfrowe zgodnie z oferowanym komputerem bez konieczności stosowania przejściówek (przynajmniej jeden port HDMI).<br>W zestawie wymagany kabel do połączenia z komputerem stacjonarnym.<br>Posiadanie funkcji podziału ekranu. |

WRG.271.9.2022

## Stacje robocze typ II (komputery stacjonarne z systemem operacyjnym, klawiaturą, myszką i monitorem)

| Obszar wymagań | Wymagane minimalne |
|---|---|
| **Typ urządzenia** | **Komputer stacjonarny** |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, czytania i obróbki map, programów graficznych, dostępu do sieci Internet oraz sieci wewnętrznej, poczty elektronicznej, stacja programistyczna oraz świadczenia szeregu usług publicznych dla ludności na drodze teleinformatycznej. |
| Wydajność | Procesor wielordzeniowy zaprojektowany do pracy w komputerach stacjonarnych, który uzyskuje wynik co najmniej **17000** punktów **w teście PassMark – CPU Mark**, według wyników opublikowanych na stronie internetowej http://www.cpubenchmark.net/cpu_list.php. Wynik w okresie nie wcześniej niż 21 dni przed terminem składania ofert. **Do oferty należy dołączyć wydruk z powyższej strony. Zamawiający dopuszcza wydruk w języku angielskim.** |
| Obudowa | Typ obudowy dostosowany do oferowanych parametrów zestawu, o minimalnych wymiarach (wysokość/szerokość/głębokość) 250 mm/80 mm/200 mm, mierzone w orientacji pionowej obudowy. Suma wymiarów nie może przekraczać 780 mm. Miejsce na porty USB zarówno na przednim (min. 2 sztuki) oraz tylnym panelu (min. 4 sztuki). Gniazdo słuchawkowe port combo lub słuchawki plus mikrofon na przednim panelu. Na obudowie trwale umieszczony niepowtarzalny numer seryjny każdego komputera, który powinien być wpisany na stałe w BIOS. |
| Zasilacz | Zasilacz wewnętrzny pracujący w sieci 230V 50/60 Hz prądu zmiennego. Moc adekwatna do proponowanego zestawu, umożliwiająca pracę komputera przy pełnym wyposażeniu w dodatkowe urządzenia podpięte przez porty i sloty rozszerzeń. |
| Pamięć operacyjna | Zainstalowana pamięć o pojemności co najmniej 16 GB. Ilość zajętych slotów pamięci 2 sztuki. |
| Dyski twarde | Dysk półprzewodnikowy SSD M.2 NVMe o pojemności min. 512 GB zawierający RECOVERY umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
| Karta graficzna | Zewnętrzna karta graficzna z min. 4 GB pamięci własnej niewspółdzielonej. |

| | |
|---|---|
| Karta dźwiękowa | Zintegrowana z płytą główną, co najmniej dwukanałowa. Gniazdo słuchawek i mikrofonu znajdujące się na obudowie podłączone do karty. |
| Karta sieciowa | LAN 10/100/1000 Mbit/s – złącze RJ45<br>Wspierająca obsługę Wake on LAN - włączana przez użytkownika. |
| Napęd optyczny | Nagrywarka DVD+/-RW umieszczona w kieszeni obudowy komputera, kolor zgodny z kolorem obudowy. |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, z pełną obsługą za pomocą klawiatury i myszy. Możliwość ustawienia hasła administratora, oraz blokady aktualizacji bez podania hasła administratora. |
| Zintegrowany system diagnostyczny | Pełny system diagnostyczny dostępny z poziomu BIOS lub menu boot, umożliwiający pełne przetestowanie komponentów komputera nawet bez użycia: dysku twardego, dostępu do sieci i Internetu, urządzeń zewnętrznych typu pendrive itp. Działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera. |
| Bezpieczeństwo | Moduł TPM znajdujący się na płycie głównej. |
| System operacyjny | System operacyjny w wersji odpowiedniej dla jednostki samorządu terytorialnego, musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:<br>1. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.<br>2. Internetowa aktualizacja systemu w języku polskim.<br>3. Graficzne środowisko instalacji i konfiguracji systemu dostępne w języku polskim.<br>4. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji.<br>5. Bezpłatne aktualizacje w ramach wersji systemu operacyjnego przez Internet z możliwością wyboru instalowanych poprawek.<br>6. Aktualizacja sterowników urządzeń możliwa przez Internetową witrynę producenta systemu.<br>7. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim.<br>8. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie, praca systemu w trybie ochrony kont użytkowników.<br>9. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. Zapora zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. |

| | |
|---|---|
| | 10. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.<br>11. Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta.<br>12. Wbudowany system pomocy w języku polskim.<br>13. 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.<br>14. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). Funkcjonalność rozpoznawania mowy, pozwalająca na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.<br>15. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.<br>16. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (tj. drukarek, urządzeń wielofunkcyjnych, urządzeń sieciowych, standardów: USB, Plug&Play, Wi-Fi). Automatyczna zmiana domyślnej drukarki w zależności do sieci, o której podłączony jest komputer.<br>17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.<br>18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.<br>19. 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.).<br>20. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie |

| | |
|---|---|
| | zapasowe.<br>21. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.<br>22. Narzędzie służące do automatycznego tworzenia obrazu systemu wraz z aplikacjami. Możliwość wdrożenie nowego obrazu poprzez zdalną instalację.<br>23. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.<br>24. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.<br>25. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).<br>26. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.<br>27. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.<br>28. Możliwość zarządzania stacją roboczą poprzez polityki – reguły definiujące lub ograniczające funkcjonalność systemu lub aplikacji. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.<br>29. Automatyczne występowanie i używanie (wstawianie) certyfikatów PKI X.509.<br>30. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM.<br>31. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot).<br>32. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.<br>33. Zarządzanie komputerami, kontami i grupami użytkowników.<br>34. Wsparcie dla Sun Java i NET Framework 1.x, 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.<br>35. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.<br>**Oferowany system operacyjny powinien być nieużywany tzn. klucz systemu nie może być wykorzystany wcześniej do aktywacji na innym urządzeniu.** |

| | |
|---|---|
| Wymagania dodatkowe | Płyta główna komputera wyposażona w niezbędne okablowanie i sterowniki. Chipset adekwatny do zaproponowanego procesora.<br>Złącza cyfrowe wideo zgodnie z zaoferowanym monitorem.<br>Podłączony co najmniej jeden port HDMI.<br>Wiele różnych wbudowanych portów/złącz umożliwiających elastyczne podłączenie urządzenia bez stosowania przejściówek.<br>Ponadto, co najmniej 6 x USB w tym 2 wprowadzane na przedzie obudowy, oraz 4 USB na tylnym panelu.<br>Na tylnym panelu wejście RJ45.<br>Wymagana ilość oraz rozmieszczenie wszystkich w/w portów nie może być osiągnięta w wyniku stosowania konwerterów, przewodów połączeniowych, przejściówek itp. |
| Niezawodność/jakość wytwarzania | Potwierdzona certyfikatem ISO 9001 lub równoważnym dla producenta sprzętu. **(należy dołączyć do oferty)**<br>Deklaracja zgodności CE. **(należy dołączyć do oferty)** |
| Gwarancja producenta | Minimum trzyletnia gwarancja producenta, obejmująca wszystkie komponenty komputera. |
| Wsparcie techniczne producenta | Dedykowany numer telefonu oraz adres email lub portal techniczny (dokładny adres strony internetowej) producenta umożliwiający zgłaszanie awarii, wsparcie techniczne i informacji produktowej, w tym konfiguracji fabrycznej oferowanego sprzętu.<br><br>Dostęp do aktualnych sterowników zainstalowanych w komputerze urządzeń realizowany poprzez podanie identyfikatora klienta lub modelu komputera lub numeru seryjnego komputera, na dedykowanej przez producenta stronie internetowej. |
| **Typ urządzenia** | **Klawiatura/Mysz** |
| Zastosowanie | Urządzenia peryferyjne wykorzystywane do normalnego użytkowania powyższego komputera stacjonarnego. |
| Klawiatura<br>Mysz | Klawiatura przewodowa w układzie US.<br>Mysz optyczna przewodowa USB. |
| **Typ urządzenia** | **Monitor** |
| Zastosowanie | Monitor będzie wykorzystywany dla potrzeb aplikacji biurowych, czytania i obróbki map, programów graficznych, dostępu do sieci Internet oraz sieci wewnętrznej, poczty elektronicznej, oraz świadczenia szeregu usług publicznych dla ludności na drodze |

| | |
|---|---|
| | teleinformatycznej. |
| Wielkość ekranu | Przekątna co najmniej 27” nie więcej niż 32’’. |
| Matryca | IPS, PLS, VA, TN z podświetleniem LED o wykończeniu matowym (nie dopuszcza się naklejek matowiących matrycę). |
| Rozdzielczość podstawowa | 1920 x 1080 pikseli |
| Typ ekranu | Płaski |
| Janość | Przynajmniej 250 cd/$m^2$ |
| Kontrast typowy | Przynajmniej 1000:1 |
| Czas reakcji | Maksymalnie 5ms |
| Certyfikaty i standardy | Certyfikat ISO 9001 lub równoważny dla producenta sprzętu. **(należy dołączyć do oferty)**<br>Deklaracja zgodności CE. **(należy dołączyć do oferty)** |
| Gwarancja producenta | Minimum dwuletnia gwarancja producenta. |
| Wsparcie techniczne producenta | Dedykowany numer telefonu oraz adres email lub portal techniczny (dokładny adres strony internetowej) producenta umożliwiający zgłaszanie awarii, wsparcie techniczne, weryfikację kompletnych danych o modelu monitora. |
| Inne | Złącze cyfrowe zgodnie z oferowanym komputerem bez konieczności stosowania przejściówek (przynajmniej jeden port HDMI).<br>W zestawie wymagany kabel do połączenia z komputerem stacjonarnym.<br>Posiadanie funkcji podziału ekranu. |

## Komputery przenośne z systemem operacyjnym

| Obszar wymagań | Wymagane minimalne |
|---|---|
| **Typ urządzenia** | **Komputer przenośny typu laptop** |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do sieci Internet oraz sieci wewnętrznej, poczty elektronicznej, świadczenia szeregu usług publicznych dla ludności na drodze teleinformatycznej oraz pracy zdalnej wykonywanej przez pracowników Zamawiającego. |

| | |
|---|---|
| Wydajność | Procesor wielordzeniowy zaprojektowany do pracy w komputerach stacjonarnych, który uzyskuje wynik co najmniej **10000** punktów **w teście PassMark – CPU Mark**, według wyników opublikowanych na stronie internetowej http://www.cpubenchmark.net/cpu_list.php. Wynik w okresie nie wcześniej niż 21 dni przed terminem składania ofert. **Do oferty należy dołączyć wydruk z powyższej strony. Zamawiający dopuszcza wydruk w języku angielskim.** |
| Obudowa | Obudowa powinna charakteryzować się wzmocnioną konstrukcją i być wykonana z materiałów o podwyższonej odporności na uszkodzenia mechaniczne. |
| Zasilacz | Zasilacz dedykowany przez producenta. |
| Bateria | Pojemność minimum 40 Wh. **Do oferty należy dołączyć dokumentację producenta potwierdzającą spełnianie powyższego parametru.** |
| Ekran | Matryca z podświetleniem w technologii LED, o przekątnej co najmniej 15,6”, powłoka matowa. Rozdzielczość co najmniej 1920 x 1080. |
| Pamięć operacyjna | Zainstalowana pamięć o pojemności co najmniej 16 GB. |
| Dyski twarde | Dysk półprzewodnikowy SSD o pojemności min. 256 GB ze złączem M.2 RECOVERY umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
| Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu, dynamicznie rozdzielaną na potrzeby grafiki – z możliwością dynamicznego przydzielania pamięci. |
| Audio/Video | Karta dźwiękowa zintegrowana, co najmniej dwukanałowa. Wbudowane głośniki stereo, wbudowany mikrofon. Wbudowana kamera internetowa. |
| Klawiatura<br>Mysz | W układzie US.<br>Oddzielna dodatkowa mysz optyczna przewodowa USB. |
| Karta sieciowa | Wbudowana karta LAN 1000 Mbit/s<br>Wbudowana karta sieciowa, pracująca w standardzie AC z antenami 2x2 za pomocą Wi-Fi. |
| Bluetooth | Wbudowany moduł Bluetooth |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, z pełną obsługą za pomocą klawiatury i myszy. Możliwość ustawienia hasła administratora, oraz blokady aktualizacji bez podania hasła administratora. |
| Zintegrowany system diagnostyczny | Pełny system diagnostyczny dostępny z poziomu BIOS lub menu boot, umożliwiający pełne przetestowanie komponentów |

| | |
|---|---|
| | komputera nawet bez użycia: dysku twardego, dostępu do sieci i Internetu, urządzeń zewnętrznych typu pendrive itp. Działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera. |
| Bezpieczeństwo | Moduł TPM znajdujący się na płycie głównej. |
| System operacyjny | System operacyjny w wersji odpowiedniej dla jednostki samorządu terytorialnego, musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:<br>1. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.<br>2. Internetowa aktualizacja systemu w języku polskim.<br>3. Graficzne środowisko instalacji i konfiguracji systemu dostępne w języku polskim.<br>4. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji.<br>5. Bezpłatne aktualizacje w ramach wersji systemu operacyjnego przez Internet z możliwością wyboru instalowanych poprawek.<br>6. Aktualizacja sterowników urządzeń możliwa przez Internetową witrynę producenta systemu.<br>7. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim.<br>8. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie, praca systemu w trybie ochrony kont użytkowników.<br>9. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. Zapora zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.<br>10. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.<br>11. Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta.<br>12. Wbudowany system pomocy w języku polskim.<br>13. 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.<br>14. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). Funkcjonalność rozpoznawania mowy, pozwalająca na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.<br>15. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.<br>16. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (tj. drukarek, urządzeń wielofunkcyjnych, urządzeń sieciowych, standardów: USB, Plug&Play, Wi-Fi). Automatyczna zmiana domyślnej drukarki w zależności do sieci, o której podłączony jest komputer.<br>17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.<br>18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.<br>19. 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.).<br>20. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.<br>21. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.<br>22. Narzędzie służące do automatycznego tworzenia obrazu systemu wraz z aplikacjami. Możliwość wdrożenie nowego obrazu poprzez zdalną instalację.<br>23. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.<br>24. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.<br>25. Możliwość blokowania lub dopuszczania dowolnych urządzeń |

| | |
|---|---|
| | peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).<br>26. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.<br>27. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.<br>28. Możliwość zarządzania stacją roboczą poprzez polityki – reguły definiujące lub ograniczające funkcjonalność systemu lub aplikacji. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.<br>29. Automatyczne występowanie i używanie (wstawianie) certyfikatów PKI X.509.<br>30. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM.<br>31. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot).<br>32. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.<br>33. Zarządzanie komputerami, kontami i grupami użytkowników.<br>34. Wsparcie dla Sun Java i NET Framework 1.x, 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.<br>35. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.<br>36. Dostępne dwa rodzaje graficznego interfejsu użytkownika:<br>- klasyczny, umożliwia obsługę przy pomocy klawiatury i myszy,<br>- dotykowy, umożliwia sterowanie dotykiem.<br>**Oferowany system operacyjny powinien być nieużywany tzn. klucz systemu nie może być wykorzystany wcześniej do aktywacji na innym urządzeniu.** |
| Wymagania dodatkowe | Płyta główna komputera wyposażona w niezbędne okablowanie i sterowniki. Chipset adekwatny do zaproponowanego procesora. Ponadto, co najmniej 3 porty USB, złącze słuchawek i mikrofonu, HDMI, RJ-45.<br>Posiada urządzenie wskazujące. |
| Niezawodność/jakość wytwarzania | Potwierdzona certyfikatem ISO 9001 lub równoważnym dla producenta sprzętu. **(należy dołączyć do oferty)**<br>Deklaracja zgodności CE. **(należy dołączyć do oferty)** |
| Gwarancja producenta | Minimum trzyletnia gwarancja producenta, obejmująca wszystkie komponenty komputera. |

| | |
|---|---|
| Wsparcie techniczne producenta | Dedykowany numer telefonu oraz adres email lub portal techniczny (dokładny adres strony internetowej) producenta umożliwiający zgłaszanie awarii, wsparcie techniczne i informacji produktowej, w tym konfiguracji fabrycznej oferowanego sprzętu.<br>Dostęp do aktualnych sterowników zainstalowanych w komputerze urządzeń realizowany poprzez podanie identyfikatora klienta lub modelu komputera lub numeru seryjnego komputera, na dedykowanej przez producenta stronie internetowej. |

## Pakiety oprogramowania biurowego

| Obszar wymagań | Wymagane minimalne |
|---|---|
| **Typ oprogramowania** | **Pakiet oprogramowania biurowego** |
| Zawartość pakietu | Pakiet musi zawierać:<br>1) edytor tekstów,<br>2) arkusz kalkulacyjny,<br>3) narzędzie do przygotowania i prowadzenia prezentacji,<br>4) narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami). |
| Edytor tekstów | Edytor tekstów musi umożliwiać:<br>a) edycję i formatowanie tekstu w języku polskim, angielskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,<br>b) wstawianie oraz formatowanie tabel,<br>c) wstawianie oraz formatowanie obiektów graficznych,<br>d) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),<br>e) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,<br>f) tworzenie i modyfikację stylów tekstu przez użytkownika,<br>g) automatyczne tworzenie spisów treści,<br>h) formatowanie nagłówków i stopek stron,<br>i) śledzenie i porównywanie zmian wprowadzonych przez |

| | |
|---|---|
| | użytkowników,<br>j) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,<br>k) określenie układu strony (pionowa/pozioma).<br>l) wydruk dokumentów,<br>m) wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną,<br>n) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. |
| Arkusz kalkulacyjny | Arkusz kalkulacyjny musi umożliwiać:<br>a) tworzenie raportów tabelarycznych,<br>b) tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych,<br>c) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,<br>d) tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice),<br>e) tworzenie i edycję kwerend bazodanowych i webowych,<br>f) narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych,<br>g) tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,<br>h) wyszukiwanie i zamianę danych,<br>i) wykonywanie analiz danych przy użyciu formatowania warunkowego,<br>j) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,<br>k) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,<br>l) formatowanie czasu, daty i wartości finansowych z polskim formatem, |

| | |
|---|---|
| | m) zapis wielu arkuszy kalkulacyjnych w jednym pliku,<br>n) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. |
| Narzędzie do przygotowywania i prowadzenia prezentacji | Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:<br>a) przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego,<br>b) drukowanie w formacie umożliwiającym robienie notatek,<br>c) zapisanie jako prezentacja tylko do odczytu,<br>d) nagrywanie narracji i dołączanie jej do prezentacji,<br>e) opatrywanie slajdów notatkami dla prezentera,<br>f) umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,<br>g) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,<br>h) odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,<br>i) możliwość tworzenia animacji obiektów i całych slajdów,<br>j) prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. |
| Narzędzie do zarządzania informacją osobistą | Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:<br>a) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,<br>b) przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,<br>c) filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,<br>d) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,<br>e) automatyczne grupowanie poczty o tym samym tytule,<br>f) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, |

| | |
|---|---|
| | g) oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,<br>h) mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,<br>i) zarządzanie kalendarzem,<br>j) udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,<br>k) przeglądanie kalendarza innych użytkowników,<br>l) zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,<br>m) zarządzanie listą zadań,<br>n) zlecanie zadań innym użytkownikom,<br>o) zarządzanie listą kontaktów. |
| Wymagania dla pakietu | Pakiet oprogramowania biurowego musi posiadać pełną polską wersję językową interfejsu użytkownika.<br>Zamawiający wymaga dostarczenia licencji odpowiedniej dla jednostek samorządu terytorialnego, która obejmuje najnowszą wersję oprogramowania dostępną na dzień składania oferty.<br>**Licencja musi uprawniać Zamawiającego do bezterminowego, nieograniczonego czasowo korzystania z funkcji oprogramowania.**<br>Pakiet oprogramowania powinien umożliwiać przeprowadzenie instalacji na stacji roboczej/komputerze przenośnym lokalnie.<br>Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.1). |

## System ochrony antywirusowej z zaporą ogniową

| Obszar wymagań | Wymagane minimalne |
|---|---|
| **Typ oprogramowania** | **Oprogramowanie antywirusowe.** |
| Licencja | System ochrony antywirusowej z zaporą ogniową w wersji polskiej z subskrypcją jednoroczną z możliwością instalacji na 60 urządzeniach (minimum 55 na stacjach roboczych i 5 na serwerach). |

| | |
|---|---|
| Funkcjonalność | 1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy.<br>2. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.<br>3. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan".<br>4. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie pliku offline ze strony producenta i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.<br>5. Możliwość wywołania skanowania komputera na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.<br>6. Możliwość wywołania skanowania komputera w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.<br>7. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.<br>8. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.<br>9. Mikrodefinicje wirusów – przyrostowe (inkrementalne) - pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).<br>10. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.<br>11. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.<br>12. Heurystyczna technologia do wykrywania nowych, |

| | |
|---|---|
| | nieznanych wirusów.<br>13. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit".<br>14. Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie.<br>15. Ochrona pliku 'hosts' przed niepożądanymi wpisami.<br>16. Mechanizm centralnego zarządzania elementami kwarantanny znajdującymi się na stacjach klienckich.<br>17. Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona.<br>18. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.<br>19. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.<br>20. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.<br>21. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.<br>22. Automatyczne uruchamianie procedur naprawczych.<br>23. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.<br>24. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).<br>25. Automatyczne powiadomienie użytkowników oraz administratora o wykrytych zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.<br>26. Możliwość zablokowania wychodzącej wiadomości e-mail, jeżeli zostanie w niej wykryty zainfekowany załącznik.<br>27. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http. |

| | |
|---|---|
| | 28. Blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.<br>29. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez serwery reputacyjne producenta.<br>30. Automatyczna kwarantanna blokująca ruch przychodzący i wychodzący, włączająca się w momencie, gdy stacja robocza posiada stare sygnatury antywirusowe.<br>31. Wsparcie dla technologii Microsoft Network Access Protection (NAP).<br>32. Ochrona przeglądarki internetowej, w tym: blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX i pobieranych plików.<br>33. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie Network Interceptor Framework (niezależnie od rodzaju i wersji przeglądarki).<br>34. Możliwość zabezpieczenia połączenia do witryn skategoryzowanych przez producenta, jako ‘bankowość elektroniczna’ poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z bankiem.<br>35. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z daną witryną HTTPS.<br>36. Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębny plik wykonywalny dostarczony przez producenta.<br>37. Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji.<br>38. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną. |

| | |
|---|---|
| | 39. Osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.<br>40. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.<br>41. Możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).<br>42. Blokowanie dostępu do witryn WWW na podstawie dostarczonych przez producenta kategorii bez konieczności ręcznego wpisywanie poszczególnych adresów.<br>43. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii musi zostać powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.<br>44. Możliwość blokowania witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.<br>45. Brak konieczności restartu komputera po zainstalowaniu aplikacji w środowisku Windows<br>46. Moduł kontroli urządzeń zapewniający możliwość zezwolenia lub zablokowania dostępu do urządzeń zewnętrznych (np. napędy USB, urządzenia bluetooth, czytniki kart pamięci, napędy CD/DVD, stacje dyskietek).<br>47. Moduł kontroli urządzeń zarządzany z poziomu konsoli centralnego zarządzania.<br>48. Moduł kontroli urządzeń umożliwia dodanie ‘zaufanego urządzenia’ poprzez podanie jego identyfikatora sprzętowego.<br>49. Moduł aktualizatora aplikacji, który okresowo skanuje i umożliwia aktualizację do najnowszych wersji aplikacji firm trzecich.<br>50. Aktualizator aplikacji powinien spełniać role programu łatającego podatności a nie tylko i wyłącznie pasywnego skanera luk w bezpieczeństwie aplikacji.<br>51. Administrator ma możliwość wykluczenia aplikacji, które mają |

| | |
|---|---|
| | nie podlegać aktualizacji poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.<br>52. System raportowania powinien pokazywać status podatności aplikacji na komputerach dotyczące całej domeny lub pojedynczych komputerów.<br>53. Aktualizator aplikacji nie może wymagać instalowania dodatkowych agentów oprócz agenta AV.<br>54. Aktualizator powinien dać możliwość aktualizacji poprawek w sposób akcji wymuszonej lub reguły wykonującej się w sposób zaplanowany: dzień, godzina, opcje restartu komputera, wykluczenia aplikacji.<br>55. Administrator konsoli zarządzającej powinien mieć możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.<br>56. Aktualizator aplikacji nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces. |
| Wymagania dotyczące system ochrony anty wirusowej z zaporą ogniową dla stacji roboczych | 1. Ochrona antywirusowa systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli.<br>2. Możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach.<br>3. Polski interfejs użytkownika aplikacji ochronnej. |
| Wymagania dotyczące systemu zarządzania centralnego | 1. System centralnego zarządzania może być zainstalowany na wersjach serwerowych Microsoft Windows.<br>2. Konsola zarządzania umożliwia eksport pakietu instalacyjnego dla klienta w formacie Microsoft Installer (MSI) i JAR lub też bezpośrednią instalację zdalną nienadzorowaną.<br>3. Narzędzie instalacyjne musi sprawdzać istnienie poprzednich wersji oprogramowania. W przypadku znalezienia poprzedniej wersji instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie z klienta lub serwera i instalować nowe wersję.<br>4. Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem). |

| | |
|---|---|
| | 5. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi.<br>6. Pełne centralne zarządzanie dla środowisk Windows Server.<br>7. Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta.<br>8. Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa.<br>9. Centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy.<br>10. Możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów).<br>11. Tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach.<br>12. Możliwość importu struktury drzewa z Microsoft Active Directory.<br>13. Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników.<br>14. Możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający.<br>15. Możliwość instalacji i konfiguracji wewnętrznego serwera aktualizacji, łączącego się z serwerem aktualizacji producenta i aktualizacja serwerów, serwera zarządzającego oraz stacji roboczych z wewnętrznego serwera aktualizacji.<br>16. Możliwość ustalenia dodatkowego harmonogramu pobierania przez serwery plików i stacje robocze aktualizacji z serwera producenta.<br>17. Funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych |

| | |
|---|---|
| | dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania.<br>18. Dane muszą być przesyłane do serwera zarządzania podczas kolejnego połączenia.<br>19. Możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich.<br>20. Umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe.<br>21. Automatyczne wykrywanie i usuwanie oprogramowanie innych wiodących producentów systemów antywirusowych (min. 3 inne) podczas instalacji.<br>22. Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej, niż co 7 dni (zalecane codzienne aktualizacje).<br>23. Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe.<br>24. Możliwość eksportu raportów z pracy systemu do pliku HTML.<br>25. Możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich.<br>26. Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”.<br>27. Program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa.<br>28. Program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe.<br>29. Program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy).<br>30. Program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów.<br>31. Dedykowany system raportowania dostępny przez przeglądarkę internetową umożliwiający podgląd statystyk dotyczących wykrytych wirusów, przeprowadzonych ataków, zainstalowanego oprogramowania oraz statystyk połączenia stacji klienckich. |

| | |
|---|---|
| | 32. System raportowania umożliwiający wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora.<br>33. Zarządzanie zdarzeniami i raportowanie – natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta elektroniczna, powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania.<br>34. Możliwość przekierowania alertów bezpośrednio do serwera Syslog.<br>35. Możliwość tworzenia wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).<br>36. System umożliwiający wykonanie pełnej kopii bazy danych systemu zarządzania centralnego bez konieczności ręcznego wyłączania programu.<br>37. Pełna kopia bazy danych systemu zarządzania centralnego może być wykonywana automatycznie zgodnie z harmonogramem określonym przez administratora.<br>38. Administrator ma możliwość określenia liczby kopii bazy danych, jaka będzie przetrzymywana. |
| Kompatybilność | Oprogramowanie antywirusowe musi umożliwiać ochronę antywirusową posiadanych przez Zamawiającego stacji roboczych, które są wyposażone w następujące systemy operacyjne:<br>1) Microsoft Windows 7 (32-bit i 64-bit),<br>2) Microsoft Windows 8.1 (32-bit i 64-bit),<br>3) Microsoft Windows 10 (32-bit i 64-bit) i nowsze. |

WRG.271.9.2022

## Oprogramowanie do zdalnej pracy na stacjach roboczych i komputerach przenośnych

| **Obszar wymagań** | **Wymagania minimalne** |
|---|---|
| **Typ oprogramowania** | **Oprogramowanie służące do bezpiecznego zdalnego dostępu na stacjach roboczych i komputerach przenośnych** |
| Licencja | Wymagane dostarczenie licencji na oprogramowanie do bezpiecznego zdalnego dostępu na stacjach roboczych (dalej: Oprogramowanie) zlokalizowanych w jednostce Zamawiającego. Jedna licencja musi pozwalać na dostęp do co najmniej 10 urządzeń zarządzanych. W przypadku dostarczenia licencji ograniczonej czasowo licencja powinna umożliwiać korzystanie z oprogramowania przez co najmniej 3 lata. |
| Funkcjonalność | Oprogramowanie musi umożliwiać:<br>1) przejęcie zdalnej kontroli nad innym urządzeniem, na którym jest zainstalowane to oprogramowanie,<br>2) zainstalowanie jako usługi systemowej,<br>3) bezpośrednie połączenia LAN przez TCP/IP i kanał wirtualnej sieci prywatnej (VPN),<br>4) działanie przez zapory ogniowe i automatycznie wykrywać dowolną konfigurację serwera proxy,<br>5) wykrywanie urządzeń znajdujących się w pobliżu,<br>6) komunikację z użytkownikami sieci, np. w formie czatu,<br>7) nawiązanie wielu połączeń jednocześnie i przełączanie się między nimi,<br>8) obsługę zdalnego budzenie komputera (Wake-on-LAN), oraz zdalny restart z automatycznym wznowieniem połączenia,<br>9) wygaszanie ekranu komputera zdalnego,<br>10) obsługę kilku ekranów komputera zdalnego,<br>11) zapewnienie bezpieczeństwa połączeń:<br>a) wykorzystywać algorytm wymiany kluczy publicznych/prywatnych RSA 2048 i szyfrowania sesji w systemie E2EE zgodnie ze standardem AES (256-bitowy),<br>b) wykorzystywać losowe hasła jednorazowego dostępu,<br>c) umożliwiać uwierzytelnianie dwuskładnikowe,<br>d) umożliwiać zdefiniowanie zaufanych urządzeń i kontrolę dostępu poprzez zaufane urządzenia,<br>e) umożliwiać stosowanie białych list,<br>12) zapisywanie ustawień połączeń,<br>13) zdalne uaktualnienia i instalację. |

| | |
|---|---|
| Kompatybilność | Oprogramowanie musi zapewniać połączenia pomiędzy różnymi platformami: z komputera PC na komputer PC, z komputera PC na komputer przenośny, z komputera przenośnego na komputer PC. Oprogramowanie musi zapewniać połączenia z urządzeniami pracującymi pod kontrolą systemów: Windows 11/10/8.1/7, Windows Server 2012/2019 i nowsze. |

WRG.271.9.2022

## Część 2: Dostawa sprzętu serwerowego i sieciowego oraz oprogramowania.

### Serwery z systemem operacyjnym

| Obszar wymagań | Wymagane minimalne |
|---|---|
| **Typ urządzenia** | **Komputer Serwer** |
| Zastosowanie | Serwer będzie wykorzystywany do przechowywania baz danych oraz aplikacji wykorzystywanych w Urzędzie. |
| Wydajność | Procesor wielordzeniowy (jeden lub więcej) zaprojektowany do pracy w komputerach typu serwer, który uzyskuje wynik co najmniej **22117 p**unktów **w teście PassMark – CPU Mark**, według wyników opublikowanych na stronie internetowej http://www.cpubenchmark.net/cpu_list.php. Wynik w okresie nie wcześniej niż 21 dni przed terminem składania ofert. **Do oferty należy dołączyć wydruk z powyższej strony. Zamawiający dopuszcza wydruk w języku angielskim.** |
| Obudowa | Obudowa Rack o wysokości minimum 2U z możliwością instalacji dysków 2,5” HotPlug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Możliwość instalacji co najmniej 12 dysków. Posiadająca dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera. Panel LCD umieszczony na froncie informujący o parametrach serwera. |
| Zasilacz | Zasilanie wewnętrzne pracujące w sieci 230V 50/60 Hz prądu zmiennego. Moc i liczba adekwatna do proponowanego serwera. Minimum dwa nadmiarowe zasilacze Hot-plug z możliwością wymiany bez wyłączania systemu. |
| Pamięć operacyjna | Zainstalowana pamięć o pojemności co najmniej 64 GB. Maksymalna obsługiwana pojemność minimum 512 GB. |
| Dyski twarde | Możliwość instalacji dysków twardych SSD SATA. Zainstalowane 4 dyski twarde SSD SATA o pojemności każdego z nich min. 800 GB. |
| Karta graficzna | Zintegrowana karta graficzna umożliwiająca wyświetlanie w rozdzielczości minimum 1280x1024. |
| Kontroler dysków | Sprzętowy kontroler dyskowy posiadający co najmniej 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. |

| | |
|---|---|
| Interfejsy sieciowe | Wbudowane co najmniej dwa interfejsy sieciowe po 1 Gb/s Ethernet. |
| Zarządzanie | Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania o funkcjonalnościach:<br>1) niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera,<br>2) dedykowane złącze RJ-45 z tyłu obudowy do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym,<br>3) dostęp poprzez przeglądarkę Web (także SSL, SSH),<br>4) zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii,<br>5) zarządzanie alarmami (zdarzenia poprzez SNMP),<br>6) sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych),<br>7) oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.),<br>8) możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania,<br>9) możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN,<br>10) możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewnętrznych i zewnętrznych, itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji,<br>11) możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w |

| | |
|---|---|
| | obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą. |
| System operacyjny | System operacyjny odpowiedni dla komputerów typu serwer, w wersji odpowiedniej dla jednostki samorządu terytorialnego, musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:<br>1. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu zarządzana przez administratora systemu Zamawiającego.<br>2. Internetowa aktualizacja systemu w języku polskim.<br>3. Graficzne środowisko instalacji i konfiguracji systemu dostępne w języku polskim.<br>4. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji.<br>5. Bezpłatne aktualizacje w ramach wersji systemu operacyjnego poprzez Internet z możliwością wyboru instalowanych poprawek.<br>6. Aktualizacja sterowników urządzeń możliwa przez Internetową witrynę producenta systemu.<br>7. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim.<br>8. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie, praca systemu w trybie ochrony kont użytkowników.<br>9. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. Zapora zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.<br>10. Zintegrowane z systemem operacyjnym narzędzie zwalczające złośliwe oprogramowanie, z dostępnymi aktualizacjami u producenta bez ograniczeń czasowych.<br>11. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.<br>12. Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. |

| | |
|---|---|
| | 13. Wbudowany system pomocy w języku polskim.<br>14. 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.<br>15. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). Funkcjonalność rozpoznawania mowy, pozwalająca na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.<br>16. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.<br>17. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (tj. drukarek, urządzeń wielofunkcyjnych, urządzeń sieciowych, standardów: USB, Plug&Play, Wi-Fi). Automatyczna zmiana domyślnej drukarki w zależności do sieci, o której podłączony jest komputer.<br>18. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.<br>19. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.<br>20. 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.).<br>21. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.<br>22. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.<br>23. Narzędzie służące do automatycznego tworzenia obrazu systemu wraz z aplikacjami. Możliwość wdrożenie nowego obrazu poprzez zdalną instalację.<br>24. Możliwość przywracania obrazu plików systemowych do |

| | |
|---|---|
| | uprzednio zapisanej postaci.<br>25. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.<br>26. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).<br>27. Wbudowany mechanizm wirtualizacji typu hypervisor.<br>28. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.<br>29. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.<br>30. Możliwość zarządzania stacją roboczą poprzez polityki – reguły definiujące lub ograniczające funkcjonalność systemu lub aplikacji. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.<br>31. Automatyczne występowanie i używanie (wstawianie) certyfikatów PKI X.509.<br>32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM.<br>33. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot).<br>34. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.<br>35. Wsparcie dla Sun Java i NET Framework 1.x, 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.<br>36. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.<br>37. Dostępne dwa rodzaje graficznego interfejsu użytkownika:<br>- klasyczny, umożliwia obsługę przy pomocy klawiatury i myszy,<br>- dotykowy, umożliwia sterowanie dotykiem.<br>38. Możliwość uruchomienia programów 64 bitowych.<br>39. Wymagana licencja na wszystkie rdzenie procesorowe zainstalowane w serwerze.<br>**Oferowany system operacyjny powinien być nieużywany tzn. klucz systemu nie może być wykorzystany wcześniej do aktywacji na innym urządzeniu.** |
| Wymagania dodatkowe | Chipset adekwatny do zaproponowanego procesora.<br>Ponadto, co najmniej 4 x USB, w tym min. 1 x USB na froncie obudowy serwera, 2 x porty RJ-45, 1 port VGA, min. 1 x port |

| | |
|---|---|
| | RS-232 lub inny o tej samej funkcji.<br>Wymagana ilość oraz rozmieszczenie wszystkich w/w portów nie może być osiągnięta w wyniku stosowania konwerterów, przewodów połączeniowych, przejściówek itp. |
| Niezawodność/jakość wytwarzania | Certyfikat ISO 9001 lub równoważny dla producenta sprzętu. **(należy dołączyć do oferty)**<br>Deklaracja zgodności CE. **(należy dołączyć do oferty)** |
| Gwarancja producenta | Minimum trzyletnia gwarancja producenta, obejmująca wszystkie komponenty komputera. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. |
| Wsparcie techniczne producenta | Dedykowany numer telefonu oraz adres email lub portal techniczny (dokładny adres strony internetowej) producenta umożliwiający zgłaszanie awarii, wsparcie techniczne i informacji produktowej, w tym konfiguracji fabrycznej oferowanego sprzętu.<br><br>Dostęp do aktualnych sterowników zainstalowanych na serwerze urządzeń realizowany poprzez podanie identyfikatora klienta lub modelu komputera lub numeru seryjnego, na dedykowanej przez producenta stronie internetowej, nawet po wygaśnięciu okresu**.** |
| **Licencje Dostępowe - tylko do jednego z serwerów** | |
| Opis licencji | Licencja Dostępowa, którą można przypisać odpowiednio do użytkownika. Licencja użytkownika umożliwia jednemu użytkownikowi dostęp z dowolnego urządzenia do odpowiedniej wersji oprogramowania serwerowego lub jego wersji wcześniejszych. Licencje Dostępowa umożliwiają dostęp do oprogramowania serwerowego działającego wyłącznie na Licencjonowanych Serwerach. |

WRG.271.9.2022

## Serwery NAS

| Obszar wymagań | Wymagane minimalne |
|---|---|
| **Typ urządzenia** | **Serwer NAS (Network Attached Storage – sieciowa pamięć masowa)** |
| Zastosowanie | Urządzenia do przechowywania danych i tworzenia kopii zapasowych. Działający jako media serwer, serwer baz danych, serwer FTP, serwer plików, serwer VPN, serwer WWW, stacja: monitoringu, fotograficzna, pobierająca dane. |
| Wydajność | Procesor wielordzeniowy (jeden lub więcej) zaprojektowany do pracy w serwerach NAS. |
| Obudowa | Obudowa Rack o wysokości 2U z możliwością instalacji min. 8 dysków 3,5” lub 2,5” HotPlug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack 19” i wysuwanie serwera do celów serwisowych. Konstrukcja modułowa w zakresie obudowy dla instalacji i obsługi dysków zapewniającą wyjątkową wydajność systemu oraz możliwość rozbudowy wejść/wyjść. |
| Zasilacz | Zasilanie wewnętrzne pracujące w sieci 230V 50/60 Hz prądu zmiennego. Moc i liczba adekwatna do proponowanego serwera. |
| Pamięć operacyjna | Zainstalowana pamięć o pojemności co najmniej 4 GB. |
| Dyski twarde | Możliwość instalacji dysków twardych SATA dedykowanych do urządzenia NAS.<br>Zainstalowane co najmniej 4 dyski twarde o pojemności 6 TB na każdym dysku. |
| Zabezpieczenie | Urządzenie musi zapewniać poziom zabezpieczenia danych na dyskach o poziomach RAID: 0, 1, 5, 6, 10, JBOD. |
| Interfejsy sieciowe | Urządzenie powinno być wyposażone w min. 2 porty Gigabit sieci Ethernet (RJ45). |
| System operacyjny | Serwer NAS musi posiadać dedykowany system operacyjny. Komunikacja z wbudowanym oprogramowaniem zarządzającym serwerem musi odbywać się w trybie graficznym poprzez przeglądarkę WWW oraz w trybie tekstowym. |
| Niezawodność/jakość wytwarzania | Certyfikat ISO 9001 lub równoważny dla producenta sprzętu. **(należy dołączyć do oferty)**<br>Deklaracja zgodności CE. **(należy dołączyć do oferty)** |
| Gwarancja producenta | Minimum trzyletnia gwarancja producenta, obejmująca wszystkie komponenty serwera. |

| | |
|---|---|
| Wsparcie techniczne producenta | Dedykowany numer oraz adres email lub portal techniczny (dokładny adres strony internetowej) producenta umożliwiający zgłaszanie awarii, wsparcie techniczne i informacji produktowej, w tym konfiguracji fabrycznej oferowanego sprzętu.<br>Dostęp do poprawek i nowych wersji wbudowanego oprogramowania realizowany na dedykowanej przez producenta stronie internetowej, nawet po wygaśnięciu okresu gwarancji. |

## Przełącznik wraz z konsolą KVM

| Obszar wymagań | Wymagane minimalne |
|---|---|
| **Typ urządzenia** | **Przełącznik KVM** |
| Zastosowanie | Urządzenie umożliwiające podłączenie do jednej konsoli (klawiatury, monitora i myszy) większej liczby urządzeń np. serwerów, rejestratorów IP z łatwym przełączaniem się między nimi. |
| Sposób montażu | Szafa Rack 19”. |
| Ilość obsługiwanych urządzeń | Przełącznik powinien obsługiwać 16 urządzeń. |
| Rozdzielczość obrazu | Kompatybilna z oferowanym serwerem. |
| Porty konsoli | 1 x VGA, 1 x USB |
| Porty PC | 16 x VGA |
| **Typ urządzenia** | **Konsola KVM**<br>**W ofercie należy podać nazwę producenta, typ, model** |
| Zastosowanie | Urządzenie sterujące Przełącznikiem KVM. |
| Sposób montażu | Szafa Rack 19”. |
| Ilość obsługiwanych urządzeń | 1 |
| Przekątna ekranu | Min. 17” |
| Porty | 1 x VGA, 1 x USB, SPHD x 1, PS/2 x 1 |
| **UWAGA: Zamawiający wymaga żeby oferowana konsola KVM była kompatybilna z oferowanym przełącznikiem KVM.** | |

WRG.271.9.2022

## Urządzenie sieciowe – SWITCH

| Obszar wymagań | Wymagane minimalne |
|---|---|
| **Typ urządzenia** | **Urządzenie typu SWITCH** |
| Zastosowanie | Przełącznik łączący segmenty sieci w Urzędzie Miasta. |
| Sposób montażu | Każdy przełącznik o wysokości 1U, przystosowany do montażu do Szafa Rack 19” oraz posiada oprzyrządowanie niezbędne do zamocowania w w/w szafie . |
| Ilość portów dostępowych | Min. 24 RJ45 Ethernet 10/100/1000Base-T |
| Ilość złącz SFP | Min. 2 |
| Architektura portów | Przełącznik musi posiadać architekturę umożliwiającą przełączanie w warstwie minimum 2 Ethernet. |
| Zasilanie | Przełącznik musi być wyposażony w minimum jeden zasilacz AC, przystosowany do zasilania z sieci 230V/50Hz. |
| Pozostałe | Stackowalny, stos zarządzany za pomocą jednego adresu IP. Urządzenie powinno być zarządzalne lokalnie: poprzez port szeregowy (CLI), interfejs graficzny (WWW) oraz zdalnie: SSH (CLI).<br>Porty bez zasilania PoE. |

## Serwerowe zasilacze awaryjne

| Obszar wymagań | Wymagania minimalne |
|---|---|
| **Funkcja urządzenia** | Urządzenie służące utrzymaniu zasilania urządzeń znajdujących się w serwerowni Urzędu Miasta. |
| Obudowa | Obudowa typu rack, co najmniej 2U do szaf 19 cali |
| Moc | Moc pozorna co najmniej 3000 VA, moc rzeczywista min. 2000 W |
| Topologia | Line-interactive |
| Czas przełączania | Maksymalnie 6 ms |
| Czas podtrzymania | 7 min. dla obciążenia 50% lub więcej<br>3 min. dla obciążenia 100% lub więcej |
| Gniazda | Co najmniej 1 x IEC-C19 i co najmniej 6 x IEC-C13 |
| Funkcje i cechy | Automatyczna regulacja napięcia (AVR)<br>Funkcja korekcji niskich i wysokich napięć<br>Filtrowanie napięcia<br>Ładowanie akumulatorów dostosowane do temperatury<br>Automatyczne włączenie po powrocie zasilania<br>Automatyczny test<br>Zarządzalny sieciowo przez złącze RJ45 |

| | |
|---|---|
| | Akumulatory wymienialne przez użytkownika<br>Akumulatory wymienialne "na gorąco"<br>Bezpiecznik automatyczny<br>Regulowane punkty przełączania napięcia<br>Regulowana czułość na napięcie |
| Komunikacja | Port szeregowy<br>Złącze USB |
| Sygnalizacja | Alarmy dźwiękowe<br>Wskaźnik statusu LED<br>Powiadomienie o awarii akumulatora<br>Powiadomienie o rozłączeniu akumulatora |
| Gwarancja producenta | Co najmniej 24-miesięczna gwarancja producenta. |

## System klasy UTM – system bezpieczeństwa

| Obszar wymagań | Wymagane minimalne |
|---|---|
| **Typ urządzenia** | **System klasy UTM (Unified Threat Management – ujednolicone zarządzanie zagrożeniami)** |
| 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.<br>System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.<br>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 4 administratorów do poszczególnych instancji |

| | |
|---|---|
| | systemu.<br>System musi wspierać IPv4 oraz IPv6 w zakresie:<br>1) Firewall,<br>2) ochrony w warstwie aplikacji,<br>3) protokołów routingu dynamicznego. |
| Parametry wydajnościowe | 1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.<br>2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.<br>3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.<br>4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.<br>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 1.4 Gbps.<br>6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.<br>7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps. |
| Funkcje systemu bezpieczeństwa | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:<br>1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.<br>2. Kontrola Aplikacji.<br>3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.<br>4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.<br>5. Ochrona przed atakami - Intrusion Prevention System.<br>6. Kontrola stron WWW.<br>7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.<br>8. Zarządzanie pasmem (QoS, Traffic shaping). |

| | |
|---|---|
| | 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).<br>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.<br>11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.<br>12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. |
| Polityki firewall | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.<br>2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:<br>a) translację jeden do jeden oraz jeden do wielu,<br>b) dedykowany ALG (Application Level Gateway) dla protokołu SIP.<br>3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.<br>4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hashe złośliwych plików.<br>5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu:<br>a) Amazon Web Services (AWS),<br>b) Microsoft Azure,<br>c) Google Cloud Platform (GCP),<br>d) OpenStack, |

| | |
|---|---|
| | e) VMware NSX. |
| Połączenia VPN | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:<br>a) wsparcie dla IKE v1 oraz v2,<br>b) obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM),<br>c) obsługa protokołu Diffie-Hellman grup 19 i 20,<br>d) wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE,<br>e) tworzenie połączeń typu Site-to-Site oraz Client-to-Site,<br>f) monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności,<br>g) możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego,<br>h) obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth,<br>i) mechanizm „Split tunneling" dla połączeń Client-to-Site.<br>2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:<br>a) 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,<br>b) pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.<br>Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |

| | |
|---|---|
| Routing i obsługa łączy WAN | W zakresie routingu rozwiązanie powinno zapewniać obsługę:<br>a) routingu statycznego,<br>b) Policy Based Routingu,<br>c) protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |
| Funkcje SD-WAN | 1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.<br>2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. |
| Zarządzanie pasmem | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.<br>2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.<br>System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |
| Ochrona przed malware | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).<br>2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.<br>3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).<br>4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.<br>5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.<br>Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. |

| | |
|---|---|
| Ochrona przed atakami | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.<br>2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.<br>3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.<br>4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.<br>5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.<br>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.<br>2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.<br>3. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.<br>Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |
| Kontrola WWW | 1. Moduł kontroli WWW musi korzystać z bazy adresów URL pogrupowanych w kategorie tematyczne.<br>2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.<br>3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.<br>4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.<br>5. Funkcja Safe Search – przeciwdziałająca pojawieniu się |

| | |
|---|---|
| | niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.<br>6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.<br>W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |
| Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:<br>a) haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.<br>b) haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.<br>c) haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.<br>2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.<br>3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.<br>Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.<br>2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.<br>3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.<br>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.<br>5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent |

| | |
|---|---|
| | udostępnia dokumentację.<br>6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.<br>Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |
| Logowanie | 1. W ramach logowania system pełniący funkcję firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.<br>2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.<br>Musi istnieć możliwość logowania do serwera SYSLOG. |
| Licencje | Z urządzeniem należy dostarczyć licencje upoważniające do korzystania w okresie jednego roku na urządzenie z aktualnych baz funkcji ochronnych producenta i serwisów w zakresie: kontrola aplikacji, IPS, antywirus z uwzględnieniem sygnatur do ochrony urządzęń mobilnych, analiza typu antyspam, web filtering, bazy reputacyjne adresów IP/domen. |
| Gwarancja producenta | Co najmniej 3 letnia gwarancja producenta. |

WRG.271.9.2022

## Oprogramowanie do tworzenia kopii zapasowych

| Obszar wymagań | Wymagane minimalne |
|---|---|
| **Typ oprogramowanie** | System Backup – oprogramowanie do automatyzacji kopii zapasowych. |
| Funkcjonalność - tworzenie kopii zapasowych | 1. Możliwość backupu obejmującego kopie całego systemu operacyjnego wraz z konfiguracją oraz zainstalowanymi aplikacjami i plikami.<br>2. Możliwość skonfigurowania różnych schematów wykonywania backupu: w trybie pełnym, backupy przyrostowe lub tryb mieszany. Harmonogram przyrostowy powinien umozliwiać backup z częstotliwością min. co 15 minut.<br>3. Możliwość wykonywania backupów pełnych i przyrostowych na dyski lokalne, dyski sieciowe, SAN, NAS, dyski USB, Firewire.<br>4. Możliwość wykonywania kopie zapasowe (backupy) na poziomie sektorów, czyli backup przyrostowy, zawierający tylko zmienione sektory na dysku, a nie np. całe pliki.<br>5. Program nie może wymagać oddzielnego serwera zarządzającego backupem, a harmonogram zadań tworzenia backupów dla danej maszyny ma być przechowywany bezpośrednio na tej maszynie.<br>6. Tworzenie kopii zapasowej w automatycznym trybie hot backupu (bez korzystania ze skryptów zamykających i uruchamiających bazy czy programy). Hot backup powinien pozwalać na backup systemu, aplikacji i baz danych takich jak MS SQL, MS Exchange, Active Directory, Share Point, Oracle od wersji 11g.<br>7. Możliwość wykonywania kopii zapasowej dysku bez konieczności uruchamiania systemu operacyjnego za pomocą bootowalnej płyty lub pendrive'a z systemem i oprogramowaniem dostarczanym przez producenta rozwiązania backupowego.<br>8. Rozwiązanie musi pozwalać na okresową weryfikację, konsolidację oraz retencję łańcucha backupu przyrostowego z możliwością konfiguracji po jakim czasie mają się one wykonać.<br>9. Rozwiązanie musi umożliwiać tworzenie backupu przez łącze 3G i WiFi.<br>10. Podczas tworzenia kopii zapasowej program musi generować plik sumy kontrolnej (md5) dla pliku backupu w celu kontroli |

| | |
|---|---|
| | plików backupu.<br>11. Program musi posiadać narzędzie pozwalające na automatyczną weryfikację tworzonych plików backupu za pomocą okresowego uruchamiania backupowanego systemu operacyjnego w maszynie wirtualnej, oraz wysłanie zrzutu ekranu z tak uruchomionego systemu do administratora za pomocą wiadomości email.<br>12. Program musi umożliwiać konwersje kopii zapasowej do plików dysków maszyn wirtualnych w formacie VHD, VMDK, VHDX.<br>Program musi umożliwiać replikację wykonanych plików kopii zapasowych na dyski lokalnie, dyski sieciowe lub do lokalizacji zdalnych na serwer FTP. |
| Funkcjonalność - przywracanie z kopii zapasowych | 1. Możliwość przywrócenia backupu całego obrazu dysku/partycji na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników do nowego sprzętu lub możliwość dodania sterowników przez użytkownika. Komputer powinien zostać uruchomiony z bootowalnej płyty CD lub pendrive'a, z którego bezpośrednio zostaje uruchomiony proces odzyskiwania obrazu dysku z backupu.<br>2. Program musi pozwalać na dowolne odtwarzanie maszyn fizycznych na inną fizyczną lub do maszyny wirtualnej oraz z maszyny wirtualnej do innej maszyny wirtualnej lub na fizyczną.<br>3. Bez względu na rozmiar backupu, program musi umożliwiać automatyczne uruchomienie systemu z backupu jako maszyny wirtualnej w środowiskach VirtualBox, VMware vSphere lub Hyper-V bez konieczności wcześniejszej konwersji pliku backupu do postaci wirtualnej.<br>4. Program musi umożliwiać zamontowanie pliku backupu jako dysku wirtualnego w trybie odczyt/zapis lub tylko do odczytu. Tak podłączony dysk logiczny umożliwia przeglądanie, wyszukiwanie i odzyskiwanie plików, folderów a także modyfikowanie zawartości.<br>5. Podczas przywracania obrazu dysku/partycji z kopii zapasowej, program musi umożliwiać: uaktywnienie wybranej partycji, przywrócenia sektora MBR, przywrócenie sygnatur dysku, przywrócenie ukrytych ścieżek na dysku, dezaktywację licencji systemu Windows. Program musi pozwalać na zdefiniowanie |

| | |
|---|---|
| | procesu tworzenia kolejnych backupów przyrostowych, które w sposób automatyczny będą odtwarzane po określonym przez administratora czasie na innej maszynie fizycznej lub wirtualnej (VMDK, VHD, VHDX). Musi istnieć możliwość zdefiniowania opóźnienia z jakim kopie przyrostowe będą przenoszone na nowy wolumin w zakresie od 1 godziny do 30 dni. |
| Funkcjonalność – zdalne zarządzanie | 1. Program musi umożliwiać pełną konfigurację i pełne zarządzanie zadaniami wykonywania kopii zapasowej na innych komputerach w sieci lokalnej, w zakresie identycznym jak z lokalnej konsoli administracyjnej.<br>2. Musi być dostępne narzędzie dające możliwość tworzenia zadań backupu za pomocą polityk dla grup stacji z poziomu konsoli webowej.<br>3. Konsola webowa musi umożliwiać instalację oraz aktualizację zdalną oprogramowania na punktach końcowych.<br>4. Konsola webowa musi umożliwiać podgląd dzienników zdarzeń na stacjach końcowych.<br>5. Program musi umożliwiać wysłanie powiadomień w postaci wiadomości e-mail gdy: zadanie backupu zakończyło się niepowodzeniem, po zakończeniu zadania tworzenia backupu, oraz podsumowanie aktywności dziennej, tygodniowej i miesięcznej. Musi istnieć możliwość pobrania ze strony producenta konsoli zarządzającej w postaci pliku ISO. |
| Kompatybilność | Pełne wsparcie dla system operacyjnego zainstalowanego na oferowanym serwerze.<br>Wsparcie dla 32 i 64-bitowych systemów Microsoft.<br>Wsparcie systemów plików: FAT16, FAT16X, FAT32, FAT32X, NTFS.<br>Wsparcie dla dysków z tablicą partycji MBR oraz GPT.<br>Wsparcie systemów plików: ext2, ext3, ext4, XFS.<br>Wsparcie dla 32 i 64-bitowych systemów Microsoft: Windows 10, Windows 11. |
| Licencja | Licencja wieczysta musi umożliwiać tworzenie kopii zapasowych na 60 urządzeniach, w tym dla 5 serwerów.<br>Oprogramowanie w języku polskim i możliwość uzyskania pomocy technicznej w języku polskim. |

WRG.271.9.2022

## Część 3: Dostawa urządzeń wielofunkcyjnych i skanerów.

### Urządzenia wielofunkcyjne A3

| Obszar wymagań | Wymagane minimalne |
|---|---|
| **Typ urządzenia** | **Urządzenie wielofunkcyjne** |
| Zastosowanie | Sieciowe urządzenie wielofunkcyjne umożliwiające wykonywanie wydruków kolorowych, oraz kopiowanie i skanowanie dokumentów, zdjęć, planów, rysunków itp. na potrzeby Urzędu Miasta. |
| Drukowanie | Druk laserowy kolorowy, automatyczny druk dwustronny. Rozdzielczość druku minimalna 1200 x 1200 dpi. |
| Kopiowanie | Liczba kopii, zmniejszanie/powiększanie, przyciemnianie/rozjaśnianie, kopiowanie dokumentów wielostronicowych. |
| Skanowanie | Skaner płaski o minimalnej rozdzielczości skanowania 600 x 600 dpi (w kolorze i w czerni), skanowanie dwustronne. Skanowanie do folderu sieciowego, do wiadomości e-mail, do lokalnego komputera PC. Automatyczny podajnik dokumentów do skanowania wielu stron. Zapisywanie w postaci plików (PDF, JPEG). |
| Obsługiwany format papieru | A3, A4, B5 |
| Pamięć | Minimum 1200 MB |
| Rodzaj połączenia | Port USB 2.0<br>Port sieciowy Ethernet<br>Wbudowana karta sieciowa |
| Protokoły sieciowe | TCP/IP, IPv4 |
| Ekran | Dotykowy LCD, kolorowy, ułatwiający obsługę urządzenia |
| Zarządzanie | Możliwość zarządzania urządzeniem przez przeglądarkę WWW. |
| Zasilacz | Przystosowany do prądu zmiennego 220-230 V.<br>Kabel zasilający w wyposażeniu. |
| Wymagania dodatkowe | W zestawie oprogramowanie sterujące i tonery. |
| Niezawodność/jakość wytwarzania | Potwierdzona certyfikatem ISO 9001 lub równoważnym dla producenta sprzętu. **(należy dołączyć do oferty)**<br>Deklaracja zgodności CE. **(należy dołączyć do oferty)** |
| Gwarancja producenta | Minimum dwuletnia gwarancja producenta. |

WRG.271.9.2022

## Urządzenia wielofunkcyjne A4

| Obszar wymagań | Wymagane minimalne |
|---|---|
| **Typ urządzenia** | **Urządzenie wielofunkcyjne** |
| Zastosowanie | Sieciowe urządzenie wielofunkcyjne umożliwiające wykonywanie wydruków monochromatycznych, oraz kopiowanie i skanowanie dokumentów, zdjęć itp. na potrzeby Urzędu Miasta. |
| Drukowanie | Druk laserowy monochromatyczny, automatyczny druk dwustronny. Rozdzielczość druku minimalna 1200 x 1200 dpi. |
| Kopiowanie | Liczba kopii, zmniejszanie/powiększanie, przyciemnianie/rozjaśnianie, kopiowanie dokumentów wielostronicowych. |
| Skanowanie | Skaner płaski o minimalnej rozdzielczości skanowania 600 x 600 dpi (w czerni i w kolorze). Skanowanie do folderu sieciowego, do wiadomości e-mail, do lokalnego komputera PC. Automatyczny podajnik dokumentów do skanowania wielu stron. Zapisywanie w postaci plików (PDF, JPG). |
| Obsługiwany format papieru | A4 - maksymalny, B5 |
| Pamięć operacyjna | Minimum 512 MB |
| Rodzaj połączenia | Port USB 2.0<br>Port sieciowy Ethernet 10/100/1000 Mb/s<br>Wbudowana karta sieciowa |
| Protokoły sieciowe | TCP/IP, IPv4 |
| Ekran | Dotykowy LCD, kolorowy, ułatwiający obsługę urządzenia |
| Zarządzanie | Możliwość zarządzania urządzeniem przez przeglądarkę WWW. |
| Zasilacz | Przystosowany do prądu zmiennego 220-230 V.<br>Kabel zasilający w wyposażeniu. |
| Wymagania dodatkowe | W zestawie oprogramowanie sterujące i tonery. |
| Niezawodność/jakość wytwarzania | Potwierdzona certyfikatem ISO 9001 lub równoważnym dla producenta sprzętu. **(należy dołączyć do oferty)**<br>Deklaracja zgodności CE. **(należy dołączyć do oferty)** |
| Gwarancja producenta | Minimum dwuletnia gwarancja producenta. |

WRG.271.9.2022

## Skanery

| Obszar wymagań | Wymagane minimalne |
|---|---|
| **Typ urządzenia** | **Skaner ADF** |
| Zastosowanie | Skaner umożliwiający skanowanie dokumentów, zdjęć itp. na potrzeby Urzędu Miasta. |
| Skanowanie | Skaner o minimalnej rozdzielczości skanowania 600 x 600 dpi (w kolorze i w czerni), skanowanie dwustronne. Skanowanie do folderu sieciowego, do wiadomości e-mail, do lokalnego komputera PC. Automatyczny podajnik dokumentów do skanowania wielu stron. Zapisywanie w postaci plików (PDF). |
| Obsługiwany format papieru | A4, Koperty |
| Rodzaj połączenia | Port USB<br>Wi-Fi |
| Ekran | Ekran dotykowy |
| Wymagania dodatkowe | W zestawie oprogramowanie sterujące. |
| Zasilacz | Przystosowany do prądu zmiennego 220-230 V.<br>Kabel zasilający w wyposażeniu. |
| Niezawodność/jakość wytwarzania | Potwierdzona certyfikatem ISO 9001 lub równoważnym dla producenta sprzętu. **(należy dołączyć do oferty)**<br>Deklaracja zgodności CE. **(należy dołączyć do oferty)** |
| Gwarancja producenta | Minimum dwuletnia gwarancja producenta. |

## Skanery

| Obszar wymagań | Wymagane minimalne |
|---|---|
| **Typ urządzenia** | **Skaner płaski** |
| Zastosowanie | Skaner umożliwiający skanowanie dokumentów, zdjęć itp. na potrzeby Urzędu Miasta. |
| Skanowanie | Skaner o minimalnej rozdzielczości skanowania 600 x 600 dpi (w kolorze i w czerni). Zapisywanie w postaci plików (PDF, JPEG). |
| Obsługiwany format papieru | A4 |
| Rodzaj połączenia | Port USB |
| Wymagania dodatkowe | W zestawie oprogramowanie sterujące. |
| Zasilacz | Przystosowany do prądu zmiennego 220-230 V.<br>Kabel zasilający w wyposażeniu. |

**Sfinansowano w ramach reakcji Unii na pandemię COVID-19**

WRG.271.9.2022

| | |
|---|---|
| Niezawodność/jakość wytwarzania | Potwierdzona certyfikatem ISO 9001 lub równoważnym dla producenta sprzętu. **(należy dołączyć do oferty)**<br>Deklaracja zgodności CE. **(należy dołączyć do oferty)** |
| Gwarancja producenta | Minimum dwuletnia gwarancja producenta. |