Załącznik nr 10 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup sprzętu IT dla szkół do nauki zdalnej oraz zakup zabezpieczenia UTM w ramach projektu „Cyfrowa Gmina”

1. Przedmiotem zamówienia jest dostawa sprzętu komputerowego wraz z oprogramowaniem dla szkół podstawowych w ramach projektu grantowego **„Cyfrowa Gmina”**, która obejmuje:
   - Komputer All-in-One - szt. 80,
   - System wielofunkcyjnej zapory sieciowej - szt. 1.
2. Adres dostawy: Urząd Gminy Czernikowo, ul. Słowackiego 12, 87-640 Czernikowo.
3. **Zamawiający informuje, że zestawy komputerów stacjonarnych z uwagi na ich przeznaczenie dla placówek oświatowych należy zgodnie z zapisami art. 83 ust. 1 pkt 26 lit. a ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz. U. z 2021 r. poz. 685 z późn. zm.) objąć zerową stawką podatku VAT.**
4. Wymagania ogólne:
   - całość przedmiotu zamówienia musi być dostarczona zgodnie z zapisami Specyfikacji warunków zamówienia,
   - Zamawiający wymaga dostawy przedmiotu zamówienia fabrycznie nowego, wolnego od obciążeń osób trzecich, wad fizycznych i prawnych, objętego gwarancją producenta oraz posiadającego wszelkie wymagane przepisami prawa pozwolenia, atesty i certyfikaty niezbędne do korzystania przez Zamawiającego oraz osoby trzecie,
   - przedmiot zamówienia musi odpowiadać parametrom ilościowym i jakościowym określonym przez Zamawiającego oraz posiadać znak bezpieczeństwa „CE”,
   - urządzenia muszą być dostarczone w oryginalnych opakowaniach fabrycznych wraz z kompletem standardowej dokumentacji dla użytkownika oraz nośnikami zawierającymi oprogramowanie zainstalowane w urządzeniu (jeśli dotyczy),
   - każde urządzenie musi być oznakowane przez producenta w sposób umożliwiający jego jednoznaczną identyfikację, tj. posiadać nazwę producenta, model oraz numer seryjny,
   - Zamawiający wymaga, aby dostarczone urządzenia, system operacyjny i oprogramowanie były fabrycznie nowe, wcześniej nieużywane oraz nieaktywowane nigdy wcześniej na innym urządzeniu. Ponadto muszą pochodzić z oficjalnego kanału dystrybucji producentów urządzeń i oprogramowania na teren Unii Europejskiej i posiadać pakiet usług gwarancyjnych kierowanych do użytkowników z obszaru Rzeczypospolitej Polskiej. Nie dopuszcza się zaoferowania oprogramowania używanego i aktywowanego wcześniej na innym urządzeniu. Zamawiający wymaga aby zaoferowane oprogramowanie systemu operacyjnego i inne oprogramowanie było zgodne z zasadami licencjonowania wymaganymi przez ich producentów,

- Zamawiający wymaga aby oprogramowanie systemowe było fabrycznie preinstalowane przez producenta komputera,
- Zamawiający wymaga, aby oprogramowanie było dostarczone wraz ze stosownymi, oryginalnymi atrybutami legalności np. certyfikatami autentyczności (tzw. COA), o ile producent oprogramowania przewidział dla danego rodzaju oprogramowania tego rodzaju potwierdzenie jego autentyczności,
- Zamawiający w trakcie odbioru końcowego przewiduje możliwość sprawdzenia i weryfikacji dostarczonego sprzętu oraz oprogramowania,
- Zamawiający dopuszcza możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów komputerowych u producenta oprogramowania, jako elementu procedury odbioru,
- Zamawiający zastrzega weryfikację u producenta sprzętu czy dostarczony przedmiot zamówienia pochodzi z oficjalnego kanału dystrybucji producenta na teren Unii Europejskiej i posiada pakiet usług gwarancyjnych kierowanych do użytkowników z obszaru Rzeczypospolitej Polskiej,
- naprawy gwarancyjne muszą być realizowane przez producenta lub autoryzowanego partnera serwisowego producenta,
- urządzenia muszą posiadać instrukcje obsługi oraz dokumenty gwarancyjne w języku polskim,
- do wszystkich urządzeń należy dołączyć wszelkie kable niezbędne do ich prawidłowego użytkowania.

5. Wymagania stawiane Wykonawcy:
   - Wykonawca jest odpowiedzialny za jakość, zgodność z warunkami technicznymi i jakościowymi opisanymi dla przedmiotu zamówienia,
   - Wykonawca dostarczy przedmiot zamówienia własnym transportem, na własny koszt i na własne ryzyko, w miejsce wskazane przez Zamawiającego,
   - Wykonawca będzie zobowiązany zagwarantować we wskazanym miejscu rozładunek i wniesienie przedmiotu zamówienia do siedziby Gminy Czernikowo, ul. Słowackiego 12, 87-640 Czernikowo.
6. Przedmiot zamówienia obejmuje również pełną i bezwarunkową gwarancję, w tym wszelkie koszty związane z naprawami gwarancyjnymi przedmiotu zamówienia w miejscu użytkowania. W przypadku zaistnienia w okresie gwarancyjnym konieczności przemieszczania przedmiotu zamówienia do punktu serwisowego lub siedziby Wykonawcy w związku ze stwierdzeniem wad lub usterek, których nie można usunąć w miejscu użytkowania, koszty przemieszczenia przedmiotu zamówienia od i do Zamawiającego ponosi Wykonawca, przy czym dysk twardy na czas naprawy pozostaje u Zamawiającego. Przekazanie przedmiotu zamówienia Wykonawcy na czas naprawy i jego odbiór musi nastąpić protokolarnie. Zamawiający wymaga reakcji serwisu najpóźniej do końca następnego dnia roboczego.
7. Zgodnie z art. 100 ust. 1 ustawy Pzp Zamawiający wymaga aby przedmiot zamówienia został zrealizowany z uwzględnieniem wymagań w zakresie zapewnienia dostępności dla osób niepełnosprawnych zawartych w Szczegółowym opisie przedmiotu zamówienia.
8. Zamawiający ustala minimalny okres gwarancji na komputery All-in-One na 24 miesiące a maksymalny na 36 miesięcy zgodnie z przyjętym kryterium oceny ofert „Okres gwarancji”.

   Okres gwarancji należy podać w pełnych miesiącach w postaci liczby całkowitej. Minimalny okres jaki

może zaoferować Wykonawca to 24 miesiące, a maksymalny okres wynosi 36 miesięcy.

Bieg terminu gwarancji rozpoczyna się od daty odbioru i przekazania w użytkowanie całego przedmiotu zamówienia.

9. W sytuacji, gdy gwarancja udzielona przez producenta jest dłuższa od gwarancji udzielonej przez Wykonawcę, obowiązuje gwarancja producenta.
10. Zamawiającemu przysługują pełne uprawnienia z tytułu rękojmi za wady fizyczne wynikające z przepisów kodeksu cywilnego, niezależnie od uprawnień z tytułu gwarancji.
11. Ilekroć w niniejszej specyfikacji podane są nazwy własne, typy urządzeń oraz ich producenci lub konkretne wymiary należy traktować je jako przykładowe określenie cech technicznych oraz pożądanego standardu i jakości.

    Zamawiający dopuszcza możliwość złożenia oferty równoważnej tj. zaproponowania rozwiązań równoważnych w stosunku do opisanych, z zastosowaniem tych samych standardów technicznych i jakościowych niezbędnych do prawidłowego funkcjonowania przedmiotu zamówienia. Poprzez pojęcie rozwiązań równoważnych należy rozumieć rozwiązania zapewniające uzyskanie wymaganych cech i parametrów technicznych, jakościowych i użytkowych nie gorszych niż założone w opisie przedmiotu zamówienia, a ponadto muszą to być urządzenia dopuszczone do obrotu i stosowania zgodnie z obowiązującym prawem.

    W sytuacji, gdy Zamawiający opisał przedmiot zamówienia przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, lub opisał przedmiot zamówienia przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy Pzp, Wykonawca powinien przyjąć, że wskazaniu takiemu lub odniesieniu towarzyszą wyrazy „lub równoważny/równoważne”, a działanie takie miało na celu wyłącznie wskazanie oczekiwanych przez Zamawiającego cech dostaw. Wykonawca w każdym przypadku może zaproponować urządzenia równoważne, które posiadają co najmniej takie same lub lepsze normy, parametry techniczne; jakościowe, funkcjonalne, będą tożsame tematycznie i o takim samym przeznaczeniu oraz nie obniżą określonych w dokumentach zamówienia standardów.

    Jeżeli Zamawiający dopuszcza rozwiązania równoważne opisywanym w dokumentach zamówienia, ale nie podaje minimalnych parametrów, które by tę równoważność potwierdzały – Wykonawca obowiązany jest zaoferować produkt o właściwościach zbliżonych, nadający się funkcjonalnie do zapotrzebowanego zastosowania (arg. na podstawie sentencji wyroku Krajowej Izby Odwoławczej z dnia 14 października 2013 r. sygn. akt: KIO 2315/13).
12. Zamawiający ma prawo zwrócić się do producenta oferowanego przez Wykonawcę przedmiotu zamówienia w celu weryfikacji spełniania wymagań określonych w Opisie przedmiotu zamówienia.
13. Wykonawca ponosi odpowiedzialność cywilną za wszelkie szkody osobiste i majątkowe wobec osób trzecich, które mogą powstać w związku z wykonywaniem przedmiotu zamówienia.
14. **Zamawiający wymaga, aby Wykonawca w Arkuszu cenowym (Załącznik nr 1.1 do SWZ) podał nazwę producenta oraz typ, model lub numer katalogowy oferowanego przedmiotu zamówienia.** Złożenie oferty poprzez wpisanie wyrażeń typu „zgodnie z dokumentacją postępowania” jest niewystarczające i sama deklaracja realizacji zamówienia zgodnie z SWZ bez podania nazwy producenta, typu, modelu lub numeru katalogowego oferowanego przedmiotu zamówienia stanowi niezgodność treści oferty z warunkami zamówienia i skutkuje odrzuceniem oferty na podstawie ar. 226 ust. 1 pkt 5 ustawy Pzp.

15. Wykonawca jest zobowiązany wykonać zamówienie **w terminie do 2 miesięcy od dnia zawarcia umowy**. Za dzień wykonania zobowiązań należy rozumieć ostateczny termin fizycznego dostarczenia przez Wykonawcę przedmiotu zamówienia odpowiadającego wymaganiom Zamawiającego, zgodnego z ofertą, czego potwierdzeniem będzie podpisany przez przedstawicieli Stron protokół odbioru.

Szczegółowy opis przedmiotu zamówienia, ilość, parametry:

1. **Komputer All-In-One – 80 szt.**

Lp.	Atrybut	Minimalne wymagane parametry techniczne / funkcje
1	Typ	komputer stacjonarny typu All in One, komputer wbudowany w monitor
2	Zastosowanie	komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
3	Wydajność obliczeniowa	procesor osiągający na wybrany dzień począwszy od dnia zamieszczenia ogłoszenia o zamówieniu w BZP do dnia składania ofert w teście PassMark CPU Mark wynik min. 7 500 punktów według wyników ze strony https://www.cpubenchmark.net
4	Płyta główna	dedykowana dla danego urządzenia; wyposażona w min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 1 złącze M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi
5	Wbudowane porty	– 1x DP++ 1.4/HDCP 2.3 – 1x USB 3.2 Gen 2 Type-C port – 3x USB 3.2 Gen 1 Type-A port – 2x USB 2.0 – wymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hub’ów itp. Wszystkie porty dostępne dla użytkownika w najniższej możliwej regulacji wysokości – 1x Universal audio jack – 1x Line-out audio – 1x RJ-45 port 10/100/1000 Mbps – czytnik kart SD 4.0 – karta WiFi ax+ bluetooth 5.1
6	Pamięć RAM	8GB DDR4 2666MHz, możliwość rozbudowy do 64GB, jeden slot wolny
7	Pamięć masowa	dysk 256GB SSD M.2 NVMe, możliwość instalacji dodatkowego dysku twardego
8	Wydajność grafiki	grafika zintegrowana z procesorem powinna umożliwiać pracę min. dwumonitorową, współdzielona i dynamicznie przydzielana pamięć z RAM
9	Matryca	– rozmiar matrycy / plamki: min. 23,8” / max. 0,275mm – rozdzielczość: FHD (1920x1080) – jasność typowa: 250 cd/m² – kontrast typowy: 700:1 – barwa koloru (typowa): 72% NTSC – kąty Horizontal/Vertical: 178(+/- 89) / 178 (+/-89) – rodzaj matrycy: matowa IPS
10	Załączone peryferia	– klawiatura USB w układzie polski programisty – mysz optyczna USB z dwoma przyciskami oraz rolką (scroll)
11	Wyposażenie multimedialne	– karta dźwiękowa zintegrowana z płytą główną, – wbudowane dwa głośniki min. 2W na kanał, – wbudowana w obudowę matrycy cyfrowa kamera 2,0 MP, mechaniczna chowana w obudowie (nie dopuszcza się kamer przekręcanych i wystających poza obrys obudowy), – wbudowane w obudowę dwa mikrofony

12	Obudowa	– typu All-in-One zintegrowana z monitorem, – obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki), – demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi, – wbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System musi zapisywać logi zdarzeń w BIOS. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji, – każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz wpisanym na stałe w BIOS, – podstawa jednostki typu All-in-One musi umożliwiać: • regulację pochyłu pionowego w zakresie od -5 do 30 stopni, • regulację wysokości w zakresie min. 10 cm, • ustawienie jednostki w trybie Pivot, • obrót podstawy w lewą oraz prawą stronę.
13	Zasilacz	wewnętrzny o mocy min. 155W o efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%
14	Zdalne zarządzanie	wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca min.: – monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej, – zdalną konfigurację ustawień BIOS, – zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego, – zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej.
15	Bezpieczeństwo	– płyta główna zawierająca układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. – zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot’owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego. – czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS
16	Wirtualizacja	sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu
17	BIOS	– BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta

		komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. – Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. – Możliwość uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. – Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła systemowego/ użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu hasła systemowego/ użytkownika w BIOS jest wstanie zidentyfikować ustawienia oraz dokonać zmiany hasła systemowego/ użytkownika. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość ustawienia portów USB w trybie „no BOOT” (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. – Dedykowane pole inwentarzowe umożliwiające wpisanie oznaczenia sprzętu. Pole po nadaniu numeru nie może być edytowalne. – Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS.
18	Certyfikaty i standardy	– oferowane urządzenia muszą być wyprodukowane zgodnie z normą ISO 9001 oraz ISO 50001 – Deklaracja zgodności CE – potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki lub Wykonawcy (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram

19	Ergonomia	głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy jałowej dysku twardego (IDLE) wynosząca maksymalnie 24 dB
20	System operacyjny	– zainstalowany system operacyjny Windows 10/11 Professional lub dowolny inny równoważny w rozumieniu Zamawiającego. Równoważność zdefiniowano wymogami minimalnymi (*), – klucz licencyjny zapisany trwale w BIOS, musi umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego
21	Dodatkowe oprogramowanie	Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające: – upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, – sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi, – dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne, – włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji, – sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania), – dostęp do wykazu wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml, – dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku *.xml. Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku.
22	Warunki gwarancji	– minimalny punktowany okres gwarancji udzielonej przez Wykonawcę wynosi 24 miesiące, – maksymalny punktowany okres gwarancji udzielonej przez Wykonawcę wynosi 36 miesięcy, – gwarancja producenta świadczona na miejscu u klienta, – możliwość zgłaszania awarii przez ogólnopolską linię telefoniczną producenta, – czas reakcji serwisu - do końca następnego dnia roboczego, – dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów, – możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).

2. **System wielofunkcyjnej zapory sieciowej – 1 szt.**

Lp.	Atrybut	Minimalne wymagane parametry techniczne / funkcje
1	Wymagania ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: Firewall, ochrony w warstwie aplikacji, protokołów routingu dynamicznego.
2	Redundancja, monitoring i wykrywanie awarii	– w przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall, – monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych, – monitoring stanu realizowanych połączeń VPN.
3	Interfejsy, dysk, zasilanie	– system realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45, – system Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB, – w ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q, – system musi być wyposażony w zasilanie AC.
4	Parametry wydajnościowe	– w zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę, – przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B, – przepustowość Stateful Firewall: nie mniej niż 6 Gbps dla pakietów 64 B, – przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 1518 B, – przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps, – wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps, – 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, – wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps, – wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

5	Funkcje Systemu Bezpieczeństwa	– Kontrola dostępu - zapora ogniowa klasy Stateful Inspection, – Kontrola Aplikacji, – poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN, – ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS, – ochrona przed atakami - Intrusion Prevention System, – kontrola stron WWW, – kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, – zarządzanie pasmem (QoS, Traffic shaping), – mechanizmy ochrony przed wyciekiem poufnej informacji (DLP), – dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site, – analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2, – funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
6	Polityki, Firewall	– polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń, – system musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz translację jeden do jeden oraz jeden do wielu, dedykowany ALG (Application Level Gateway) dla protokołu SIP, – w ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN, – możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików, – 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: Amazon Web Services (AWS), Microsoft Azure, Cisco ACI, Google Cloud Platform (GCP), Nuage Networks VSP, OpenStack, VMware vCenter (ESXi), VMware NSX, VMware NSX.Nutanix, VMware NSX.IBM Cloud.
7	Połączenia VPN	– System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • wsparcie dla IKE v1 oraz v2, • obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM), • obsługa protokołu Diffie-Hellman grup 19 i 20, • wsparcie dla pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE, • tworzenie połączeń typu Site-to-Site oraz Client-to-Site, • monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności, • możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego,

		• obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth, • mechanizm „Split tunneling” dla połączeń Client-to-Site. – System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0, • pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta, • producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwią realizację połączeń IPSec VPN lub SSL VPN.
8	Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie powinno zapewniać obsługę: Routingu statycznego, Policy Based Routingu, Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
9	Funkcje SD-WAN	– system powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN, – reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu, – rozwiązanie powinno wspierać funkcję Forward Error Correctionm na tunelach IPSec, – funkcja monitorowania łącza w oparciu o rzeczywisty ruch bez konieczności tworzenia dedykowanych detektorów.
10	Zarządzanie pasmem	– system Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu, – musi istnieć możliwość określania pasma dla poszczególnych aplikacji, – system musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
11	Ochrona przed malware	– silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021), – system musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR, – system musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android), – 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, – system musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików, – możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
12	Ochrona przed atakami	– ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych, – system powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach, – baza sygnatur ataków powinna zawierać minimum 10 000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora, – Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur,

		– system musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS, – 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, – wykrywanie i blokowanie komunikacji C&C do sieci botnet.
13	Kontrola aplikacji	– Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP, – Baza Kontroli Aplikacji powinna zawierać minimum 4 000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora, – Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików, – Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P, – Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
14	Kontrola WWW	– moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne, – 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, – filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard, – Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL, – funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo, – system musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii, – Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania, – w ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji, – filtrowanie treści wideo w oparciu o kategorie - co najmniej dla serwisów youtube, vimeo, – blokowanie wysyłania poświadczeń firmowych do obcych serwisów.

15	Uwierzytelnianie użytkowników w ramach sesji	– system Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu, • haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, • haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych, – musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego, – rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API, – uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
16	Zarządzanie	– 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, – komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów, – powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego, – system musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow, – system musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację, – element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall, – element systemu realizujący funkcję Firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
17	Logowanie	– elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. – 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, – logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu, – musi istnieć możliwość logowania do serwera SYSLOG.
18	Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać certyfikacje ICSA dla funkcji Firewall.
19	Serwisy i licencje	W ramach przedmiotu zamówienia należy dostarczyć licencje na okres **60 miesięcy**, upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu

		Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.
20	Gwarancja oraz wsparcie	– system musi być objęty serwisem gwarancyjnym producenta przez okres **60 miesięcy**, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. – dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym na okres minimum 1 roku, gwarantującym w przypadku awarii wymianę sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji. – do zamawianego sprzętu Wykonawca zapewni usługę wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Partnera Serwisowego Producenta świadczoną w języku polskim w zakresie: • wsparcie telefoniczne zespołu certyfikowanych inżynierów, • pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu, • doradztwo w zakresie konfiguracji, • zdalne wsparcie techniczne, • pomoc w zakładaniu zgłoszeń serwisowych u producenta, • pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą), • przygotowanie urządzenia do zdalnej konfiguracji, • zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika, • minimum 10 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika, – dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. – Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji winien być nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

(*)
Windows 10/11 Professional PL 64bit jest preferowany ze względu na dotychczasowe używanie systemów rodziny Windows, a tym samym: przystosowanie środowiska informatycznego pod ten system (narzędzia sieciowe, stosowane specjalistyczne oprogramowanie). Jeżeli Wykonawca zaproponuje inne rozwiązanie niż Windows 10/11 Professional PL 64bit zgodne z wymienionymi kryteriami równoważności musi zapewnić pełne wdrożenie oferowanego rozwiązania, przeszkolenie użytkowników i administratorów systemu oraz zapewnić współpracę z używanym obecnie środowiskiem informatycznym.

Za równoważny system Zamawiający uzna taki, który współpracuje z Active Directory i realizuje wszystkie jego funkcje.

Za oprogramowanie równoważne Microsoft Windows 10 Professional Zamawiający przyjmuje oprogramowanie, które spełnia następujące wymagania:

1) Obsługa trybu Windows XP (XP Mode).
2) Pełna zgodność z domeną Active Directory w wersji na Windows 2003 Serwer i późniejszymi.
3) Współpraca z następującymi aplikacjami (obsługa natywna, bez wspierania się emulatorem): Microsoft Office 95/97/2000/XP/2003/2010/2013/2016.
4) Zaimplementowana w systemie obsługa aplikacji zgodnych z podsystemami Win16 i Win32.
5) Możliwość zainstalowania Microsoft .NET Framework.

6) Obsługa rozszerzonego pulpitu.
7) Personalizacja pulpitu.
8) Zintegrowana z systemem pełna obsługa stylów wizualnych oraz napędów CD-RW, DVD-RW (odczyt i zapis).
9) Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek.
10) Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu.
11) Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW.
12) Internetowa aktualizacja zapewniona w języku polskim.
13) Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
14) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe.
15) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).
16) Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.
17) Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta.
18) Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.
19) Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
20) Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.
21) Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych.
22) Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego.
23) Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.
24) Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
25) Wbudowany system pomocy w języku polskim.
26) Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
27) Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.
28) Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
29) Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
30) Wsparcie dla logowania przy pomocy smartcard.
31) Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.
32) System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.
33) Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
34) Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.

35) Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
36) Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.
37) Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.
38) Graficzne środowisko instalacji i konfiguracji.
39) Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
40) Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
41) Udostępnianie modemu.
42) Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
43) Możliwość przywracania plików systemowych.
44) System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
45) Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).