Załącznik nr 4 do SIWZ

Opis przedmiotu zamówienia

w postępowaniu o udzielenie zamówienia publicznego na:

„**Dostawa sprzętu komputerowego na potrzeby realizacji projektu pt: e-Myślenice – wdrożenie e-usług w Gminie Myślenice**”

1 Spis treści

1 SPIS TREŚCI 2

1. LOKALIZACJA PROJEKTU 3

2 WYKAZ ZADAŃ DO WYKONANIA 3

3 TERMIN REALIZACJI ZAMÓWIENIA 3

4 RÓWNOWAŻNOŚĆ 3

5 WYMAGANIA DOTYCZĄCE SPRZĘTU 4

5.1 WYMAGANIA OGÓLNE 4
5.2 WYMAGANIA DOTYCZĄCE INSTALACJI 4
5.3 WYMAGANIA MINIMALNE SPRZĘTU 5
5.4 WYMAGANIA DOTYCZĄCE GWARANCJI 12

1. Lokalizacja Projektu

Infrastruktura dostarczone w ramach realizacji projektu będzie umiejscowiona siedzibie Zamawiającego:

Urząd Miasta i Gminy w Myślenicach

Rynek 8/9, 32- 400 Myślenice

2 Wykaz zadań do wykonania

W celu prawidłowego funkcjonowania planowanych do wdrożenia przez e-usług konieczny jest zakup wyspecyfikowanego sprzętu informatycznego.

L.p.	Przedmiot zamówienia	Ilość szt.
1	Przełączniki sieciowe	6
2	Urządzenia ochrony sieci – UTM + 2AP	1
3	Zasilacz awaryjny UPS	1
4	Skaner dokumentów	2

3 Termin realizacji zamówienia

Przedmiot umowy musi zostać zrealizowany zgodnie ze złożoną ofertą, nie później niż do dnia 01 września 2017r. Płatności będą realizowane w terminie 30 od daty otrzymania prawidłowo wystawionej faktury VAT. Wystawienie faktur nastąpi po podpisaniu bez uwag przez Zamawiającego Protokołu Odbioru Przedmiotu Zamówienia.

4 Równoważność

W celu zachowania reguły konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych w treści niniejszego OPZ, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności przez to rozwiązanie oferowanych, nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym.

W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób. Za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie

wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, identycznych dla obu rozwiązań, dla których to warunków rozwiązania te są dedykowane.

Rozwiązanie równoważne musi zawierać dokumentację dostarczoną przez Wykonawcę potwierdzającą, iż spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego

5 Wymagania dotyczące sprzętu

5.1 Wymagania ogólne

Wymaganie	Minimalne parametry
WO.1	Zakupione w ramach niniejszego zamówienia sprzęt i oprogramowanie zostanie dostarczone, zainstalowane, wdrożone i skonfigurowane przez Wykonawcę w lokalizacji wskazanej przez Zamawiającego pod adresem: Rynek 8/9 Myślenice. Przeprowadzony zostanie również instruktaż stanowiskowy.
WO.2	Cały dostarczony sprzęt musi być fabrycznie nowy, tzn. nieużywany przed dniem dostarczenia, z wyłączeniem używania niezbędnego dla przeprowadzenia testów jego poprawnej pracy.
WO.3	Dostarczone elementy oraz dostarczone wraz z nimi oprogramowanie muszą pochodzić z oficjalnych kanałów dystrybucyjnych producenta, zapewniających w szczególności realizację uprawnień gwarancyjnych.
WO.4	Cały dostarczony sprzęt musi zostać wyprodukowany nie dalej niż 6 miesięcy przed dniem dostarczenia.
WO.5	Sprzęt i oprogramowanie powinno posiadać dokumenty dopuszczające do stosowania w Unii Europejskiej
WO.6	
WO.7	Cały dostarczony sprzęt musi zawierać wszelkie niezbędne do realizacji założonych funkcjonalności licencje na czas nieograniczony.

5.2 Wymagania dotyczące instalacji

Wymaga-nie	Minimalne parametry
WI.1	Cały dostarczony sprzęt musi zostać zamontowany w szafach RACK (jeśli dotyczy), w wymaganej lokalizacji, podłączony do wszystkich wymaganych instalacji teletechnicznych, podłączony ze sobą, skonfigurowany, uruchomiony i przetestowany.
WI.2	Wszystkie urządzenia muszą zawierać wszystkie niezbędne do podłączenia kable

	dostarczone przez producenta urządzenia.

5.3 Wymagania minimalne sprzętu

	Zasilacz awaryjny UPS	
Wymaganie	Wymagania minimalne	
UPS.1	Napięcie wyjściowe 230V.	
UPS.2	W serwerowni zostanie zamontowany zasilacz awaryjny UPS o mocy znamionowej 5 kVA/4 kW, pozwalający na autonomię podczas pracy awaryjnej nie mniej niż 15 min, o wydajności przy pełnym obciążeniu 96%, pracujący w trybie pracy true on-line. Urządzenie ma zapewnić podtrzymanie zasilania po zaniku zasilania głównego dla urządzeń zamontowanych w serwerowni.	
UPS.3	Zniekształcenia napięcia wyjściowego <5% przy pełnym obciążeniu.	
UPS.4	Tolerancja częstotliwości wejściowej 47-53 Hz.	
UPS.5	Wyświetlacz statusu LED ze wskaźnikiem pracy online: Zasilanie akumulatorowe: Wskaźniki Wymień baterię i Przeciążenie.	
UPS.6	Możliwość zdalnego zarządzanie UPS-em przez sieć LAN.	
UPS.7	Maksymalna wysokość 5U.	
UPS.8	Zgodność ze standardami CE, EN 50091-1, EN 50091-2 lub równoważnych	
Urządzenia aktywne sieci (przełączniki)		
Wymaganie	Komponent	Minimalne wymagania
UAS.1	Obsługa Routingu IPv4	1. Sprzętowa obsługa routingu IPv4 – forwarding. 2. Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 16 wpisów. 3. Routing statyczny. 4. Obsługa routingu dynamicznego IPv4 a. RIPv1/v2; b. OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania.
UAS.2	Ogólne	Sieć komputerowa zostanie wyposażona w zarządzane przełączniki sieciowe spełniające minimalne wymagania: 1. Przełącznik o wysokości 1U musi posiadać 24 portów 100/1000BASE-T z czego 4 porty muszą mieć możliwość zamiany na interfejsy Gigabit Ethernet SFP. 2. Nieblokująca architektura o wydajności przełączania min. 85 Gb/s. 3. Szybkość przełączania min. 60 Milionów pakietów na sekundę. 4. Wbudowany dedykowane porty umożliwiające łącznie przełączników w stos. Wydajność połączenia w stos min. 40 Gb/s.

		5. Możliwość łączenia do 8 przełączników w stos. 6. Tablica MAC adresów min. 16k. 7. Pamięć operacyjna: min. 512MB pamięci DRAM. 8. Pamięć flash: min. 512MB pamięci Flash. 9. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094. 10. Obsługa sieci wirtualnych protokołowych IEEE 802.1v. 11. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci. 12. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów). 13. Obsługa Q-in-Q IEEE 802.1ad, Obsługa Quality of Service 14. IEEE 802.1p; DiffServ; Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB. Obsługa LLDP Media Endpoint Discovery (LLDP-MED) . 15. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora. 16. Przełącznik musi posiadać możliwość dołączenia redundantnego systemu zasilania. 17. Wbudowany DHCP Serwer i klient. 18. Możliwość instalacji min. dwóch wersji oprogramowania – firmware. 19. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash. 20. Możliwość monitorowania zajętości CPU. 21. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring). 22. Wbudowany dodatkowy port do zarządzania poza pasmem - out of band management.
UAS.3	Obsługa Routingu IPv6	1. Sprzętowa obsługa routingu IPv6 – forwarding. 2. Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 16 wpisów. 3. Routing statyczny. 4. Obsługa routingu dynamicznego dla IPv6 a. Ring; b. OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania. 5. Telnet Serwer/Klient dla IPv6. 6. SSH2 Serwer/Klient dla IPv6. 7. Ping dla IPv6. 8. Tracert dla IPv6. 9. Obsługa MLDv1 (Multicast Listener Discovery version 1).
UAS.4	Obsługa Multicastów	1. Filtrowanie IGMP. 2. Obsługa Multicast VLAN Registration – MVR. 3. Obsługa IGMP v1/v2/v3 snooping.
UAS.5	Bezpieczeństwo	1. Obsługa Network Login a. IEEE 802.1x - RFC 3580; b. Web-based Network Login ;

		c. MAC based Network Login; 2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants). 3. Obsługa Guest VLAN dla IEEE 802.1x. 4. Obsługa Identity Management. 5. Wbudowana obrona procesora urządzenia przed atakami Dos. 6. Obsługa TACACS+ (RFC 1492). 7. Obsługa RADIUS 8. Bezpieczeństwo MAC adresów a. ograniczenie liczby MAC adresów na porcie; b. zatrzaśnięcie MAC adresu na porcie; c. możliwość wpisania statycznych MAC adresów na port/vlan. 9. Możliwość wyłączenia MAC learning. 10. Obsługa SNMPv1/v2/v3. 11. Klient SSH2. 12. Zabezpieczenie przełącznika przed atakami DoS 13. Listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 a. Adres MAC źródłowy i docelowy plus maska; b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6; c. Protokół – np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.; d. Numery portów źródłowych i docelowych TCP, UDP; e. Zakresy portów źródłowych i docelowych TCP, UDP; f. Identyfikator sieci VLAN – VLAN ID; g. Flagi TCP; h. Obsługa fragmentów. 14. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika. 15. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI. – możliwość rozszerzenia przez licencję oprogramowania. 16. Obsługa bezpiecznego transferu plików SCP/SFTP. 17. Obsługa IP Security.
UAS.6	Bezpieczeństwo sieciowe	1. Możliwość konfiguracji portu głównego i zapasowego. 2. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania. 3. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D. 4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w. 5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE

		802.1s. 6. Obsługa PVST+. 7. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619. 8. Obsługa G.8032 v1/v2. 9. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP 10. Obsługa MLAG - połączenie link aggregation do dwóch niezależnych przełączników.
UAS.7	Zarządzanie	1. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol). 2. Obsługa synchronizacji czasu NTP. 3. Zarządzanie przez SNMP v1/v2/v3. 4. Zarządzanie przez przeglądarkę WWW – protokół http i https. 5. Telnet Serwer/Klient dla IPv4 / IPv6. 6. SSH2 Serwer/Klient dla IPv4 / IPv6. 7. Ping dla IPv4 / IPv6. 8. Traceroute dla IPv4 / IPv6. 9. Obsługa SYSLOG z możliwością definiowania wielu serwerów. 10. Obsługa RMON, Obsługa RMON2 (RFC 2021).
UAS.8	Inne	1. Obsługa skryptów CLI. 2. Obsługa funkcji TCL/Tk w skryptach CLI. 3. Możliwość edycji skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych). 4. Możliwość uruchamiania skryptów: • ręcznie; • o określonym czasie lub co wskazany okres czasu; • na podstawie wpisów w logu systemowym. 5. Przełącznik musi być wyposażony w kabel stakujący za pomocą, którego można połączyć ze sobą przełączniki w stos.
Urządzenia bezpieczeństwa UTM		
Wymaganie	Komponent	Minimalne wymagania
UTM.1	Tryby pracy	Rozwiązanie musi wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy (część, jako router, część jako bridge).
UTM.2	Ogólne	System ochrony sieci musi być dostarczony w postaci platformy sprzętowej z zabezpieczonym systemem operacyjnym obsługującej w ramach jednego urządzenia

		funkcjonalności: 1. firewall, 2. IPS, 3. antywirus, 4. antyspam, 5. kontrola treści (WWW i aplikacji), 6. poufność danych – IPSec VPN oraz SSL VPN, z uwzględnieniem identyfikacji poszczególnych użytkowników lub grup użytkowników.
UTM.3	Porty/interfejsy	Urządzenie musi być wyposażone w 8 portów 10/100/1000 Mbps musi: 1. Udostępniać nie mniej niż 512 interfejsów wirtualnych definiowanych, jako VLANy w oparciu o standard IEEE802.1q. 2. Obsługiwać nie mniej niż 50 000 nowych połączeń na sek. oraz nie mniej niż 1500 000 jednoczesnych połączeń. 3. Zapewniać przepustowość nie mniejszą niż: a. Firewall: 18 000 Mbps; b. IPS: 7 000 Mbps; c. Antywirus: 2 000 Mbps; d. IPSec VPN: 3 000 Mbps.
UTM.4	Dodatkowe funkcjonalności	Urządzenie musi: 1. Pozwalać na utworzenie tuneli IPSec VPN: nie mniej niż 1000. 2. Być wyposażone w dysk twardy (minimum 120 GB) do celów logowania i raportowania. 3. Wspierać funkcje load balancing i failover dla przynajmniej 2 łącz internetowych 4. Wspierać algorytm WRR (weighted round robin) dla funkcji load balancing. 5. Zapewniać możliwość przełączania na inne łącze w przypadku awarii podstawowego łącza. 6. Wysyłać do administratora powiadomienie o zmianie statusu urządzenia Autoryzacja użytkowników: Uwierzytelnianie użytkowników poprzez Active Directory, LDAP, Radius oraz lokalną bazę użytkowników.

		Automatyczne uwierzytelnianie użytkowników w oparciu o Single Sign On.
UTM.5	Moduł Antywirusa	Skanowane protokoły: SMTP (z możliwością włączenia/wyłączenia skanowania dla autoryzowanego ruchu), POP3, IMAP.
UTM.6	Moduł Antyspam	1. Skanowane protokoły: SMTP, POP3. 2. Współpraca z bazą RBL. 3. Tworzenie białych i czarnych list adresów IP i e-mail. 4. Wykrywanie spamu niezależnie od stosowanego języka.
UTM.7	Moduł Firewall	1. Możliwość określania nazw użytkowników, adresów źródłowych, docelowych i podsieci, jako kryteriów przy tworzeniu reguł na firewallu. 2. Możliwość określania przepustowości łącza dla konkretnej aplikacji np. Skype. 3. Wspierane protokoły routingu: RIP, OSPF, BGP4. 4. Obsługa translacji adresów NAT, PAT.
UTM.8	Moduł filtrowania WWW	1. 50 kategorii stron WWW, umożliwiać tworzenie własnych kategorii stron WWW 2. Blokowanie wysyłania treści poprzez HTTP i HTTPS. 3. Blokada stron HTTPS. 4. Blokowanie anonimowe proxy działające poprzez HTTP i HTTPS. 5. Definiowanie polityk dostępu do internetu w oparciu o harmonogramy dzienne/tygodniowe/miesięczne/roczne dla użytkowników i grup użytkowników. 6. Wyświetlanie komunikatów o przyczynie zablokowania dostępu do strony www. Administrator ma możliwość edytowania treści komunikatu i dodania logo organizacji.
UTM.9	Moduł kontroli aplikacji	1. Identyfikacja aplikacji niezależnie od wykorzystywanego portu, protokołu, szyfrowania. 2. Rozpoznawanie przynajmniej 1000 aplikacji. 3. Blokowanie: • aplikacji, które pozwalają na transfer plików (np. P2P) • komunikatorów internetowych, przynajmniej Skype, Gadu-gadu • proxy uruchamianych poprzez przeglądarki internetowe

		• streaming media (radio internetowe, Youtube, Vimeo) • kontrola dostępu do Facebooka.
UTM.10	Moduł IPS	1. Baza 2000 sygnatur. 2. Tworzenie własnych sygnatur IPS. 3. Automatyczne pobieraanie aktualizacji. 4. Generowanie alertów w przypadku prób ataków.
UTM.11	VPN	1. Wsparcie dla połączeń VPN: IPsec, L2TP i PPTP. 2. Wsparcie dla algorytów: DES, 3DES, AES. 3. Wsparcie dla lokalnych i zewnętrznych centrów certyfikacji. 4. Obsługa ogólnodostępnych klientów IPSec VPN. 5. Wbudowany moduł SSL VPN. 6. Możliwość skanowania antywirusowego i antyspamowego tuneli VPN (IPsec/L2TP/PPTP). 7. VPN failover.
UTM.12	Zarządzanie	1. Możliwość tworzenia kont administracyjnych o różnych uprawnieniach. 2. Możliwość automatycznego wylogowanie administratora po określonym czasie bezczynności. 3. Możliwość definiowanie polityk hasłowych dla administratorów. 4. Wsparcie zarządzania poprzez bezpieczny kanał komunikacji: HTTPS, SSH i konsolę 5. Wsparcie SNMP. 6. Możliwość monitorowania w czasie rzeczywistym stanu urządzenia 7. Możliwość automatycznego wykonywania kopii zapasowej konfiguracji systemu.
UTM.13	Logowanie oraz raportowanie	1. System musi umożliwiać składowanie oraz archiwizację logów. 2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników. 3. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących. 4. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania

		danych (długoterminowe przechowywanie danych). 5. Rozwiązanie musi generować raporty w HTML. 6. Rozwiązanie musi wspierać wiele serwerów syslog (przynajmniej 2).
UTM.14	Certyfikaty	dla funkcjonalności Firewall - ICSA lub EAL4 lub równoważne.
Skaner dokumentów		
Wymaganie	Komponent	Minimalne wymagania
SD.1	Ogólne	Do celów digitalizacji korespondencji oraz dokumentów tradycyjnych przewiduje się instalację w Biurze Obsługi Klienta skanera do dokumentów A4.
SD.2	Podajnik	Podajnik ADF na mini 80 kartek.
SD.3	Skanowanie	Skanowanie jedno i dwustronne w rozdzielczości 600dpi.
SD.4	Obsługiwane nośniki	Urządzenie musi umożliwiać skanowanie standardowych kartek, faktur, listów przewozowych, kopert, wizytówek, czy nawet kart kredytowych lub dowodów osobistych.
SD.5	Obsługiwane formaty skanowania	Obsługa formatów A8-A4 oraz możliwość skanowania dokumentów A3 składanych w dostarczanej folii „carrier sheet”.
SD.6	Prędkość skanowania	Skanowanie z prędkością 60 kartek na minutę w trybie SIMPLEX lub 120 obrazów na minutę dwustronnie: zarówno w bieli/czerni jak i trybie kolorowym (przy rozdzielczości 200/300dpi).
SD.7	Gramatura	od 30 do 400 g/m2.
SD.8	Inne	Funkcja wykrywania zablokowanej strony.

5.4 Wymagania dotyczące gwarancji

Wymagania ogólne	
WU.1	Zamawiający wymaga, aby wszystkie dostarczane urządzenia posiadały gwarancję na okres minimum 36 miesięcy. Gwarancja będzie liczona od daty odbioru potwierdzającego instalację urządzeń. Gwarancja ma być oparta na autoryzowanym kanale producenta lub poprzez serwis bezpośrednio producenta.

WU.2	Zamawiający wymaga na okres 5 lat wsparcia technicznego na produkt, aktualizacji wewnętrznego oprogramowania. 5-letnie wsparcie techniczne obejmuje aktualizację oprogramowania. Wsparcie techniczne musi być realizowane mailowo i telefonicznie w języku polskim.
WU.3	Zamawiający dopuszcza świadczenie usługi w trybie minimum 8 x 5, co oznacza, że powyższa gwarancja i wsparcie musi być realizowana 5 dni w tygodniu w godzinach pracy Urzędu.
WU.4	Wykonawca zapewni usługę wsparcia poprzez: 1. Udostepnienie usługi typu helpdesk. 2. Help Desk musi posiadać stronę webową, za pomocą której każdy użytkownik może sprawdzić status zainicjowanego przez siebie zgłoszenia. 3. Help Desk musi być usługą udostępnioną pod adresem e-mail, numerem telefonu i numerem faksu. 4. Portal typu helpdesk musi być dostępny on-line w trybie 356/7/24. 5. Portal musi pozwalać na dokonywane zgłoszenia Usterek/Awarii/Wad.
WU.5	Wykonawca zobowiązany jest do potwierdzenia w ciągu 4 godzin w czasie okna dostępności usługi gwarancyjnej przyjęcie Zgłoszenia reklamacyjnego oraz jego klasyfikację. Potwierdzenie zostanie wysłane przez Wykonawcę do zgłaszającego.
WU.6	Wsparcie użytkowników obejmuje świadczenie usługi wsparcia technicznego, merytorycznego oraz konsultacji w celu utrzymania poprawnej pracy zgodnej z wymaganiami zamówienia. W ramach usługi Wykonawca zobowiązany jest do udzielania odpowiedzi na pytania Użytkowników i Administratorów związane z bieżącą eksploatacją.
WU.7	Wykonawca zapewni w godzinach pracy Urzędu w dni robocze dostępność specjalistów mających niezbędną wiedzę i doświadczenie z zakresu eksploatacji Systemów.
WU.8	Wykonawca zapewni wystarczającą ilość konsultantów do zapewnienia ciągłości usługi gwarancji.