



**Rzeczpospolita  
Polska**

**Unia Europejska**  
Europejski Fundusz  
Rozwoju Regionalnego



Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA  
dla I i II i III części przedmiotu zamówienia

## Wstęp

Niniejszy dokument określa minimalne wymagania dla przedmiotu zamówienia dotyczącego realizacji projektu pn.: „Cyfrowa Gmina” realizowanego przez Gminę Piaski.

Zakup jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczący realizacji projektu grantowego „Cyfrowa Gmina” dla Gminy Piaski o numerze: POPC.05.00-00-001/21-00.

## Spis treści

<b>WSTĘP</b>	<b>2</b>
<b>CZĘŚĆ I PRZEDMIOTU ZAMÓWIENIA</b>	<b>4</b>
1. PRZEŁĄCZNIKI ZARZĄDZALNE	4
2. SERWER Z OPROGRAMOWANIEM	5
3. OPROGRAMOWANIE DO BACKUPU	8
<b>CZĘŚĆ II PRZEDMIOTU ZAMÓWIENIA</b>	<b>10</b>
4. SKANER	10
<b>CZĘŚĆ III PRZEDMIOTU ZAMÓWIENIA</b>	<b>11</b>
5. AUDYT	11
<b>ROZWIĄZANIA RÓWNOWAŻNE</b>	<b>13</b>

Część I przedmiotu zamówienia

1. Przełączniki zarządzalne

Nazwa	Minimalne wymagania dla sprzętu
<b>Obudowa</b>	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn lub uchwytów montażowych, wyposażona w zintegrowany zasilacz lub wymienny hot-swap w obudowie urządzenia.
<b>Porty</b>	Minimum 24 porty 10/100/1000Mbps RJ45, minimum 2 porty SFP/SFP+ 1/10GbE, 1 port konsolowy Obsługa modułów SFP: 1000BASE-SX, 1000BASE-LX Obsługa modułów SFP+: 10GbE, SR, LR, ER
<b>Wydajność przełącznika</b>	Minimum 8000 adresów MAC Switch fabric capacity min. 80Gbps Forwarding rate min. 80Mpps Pamięć flash min. 128MB
<b>Funkcjonalność warstwy II</b>	Obsługa minimum 256 wirtualnych sieci Wsparcie dla agregacji LACP (802.3ad) Obsługa 8 grup LACP i 8 portów fizycznych per grupa Obsługa technologii port mirroring oraz remote port mirroring Obsługa funkcjonalności Voice VLAN
<b>Funkcjonalność warstwy III</b>	Obsługa minimum 64 wpisów routingu statycznego IPv4 Obsługa minimum 64 wpisów routingu dynamicznego IPv4 Obsługa protokołu RIP2
<b>Inne Funkcjonalności</b>	Możliwość połączenia w stos do 4 urządzeń tego samego typu Wydajność połączenia pomiędzy przełącznikami w stosie min. 20Gbps Obsługa 802.1x, Mac Based Authentication Bypass Obsługa list kontroli dostępu opartych o adresy MAC i IP
<b>Zgodność z protokołami</b>	802.1AB LLDP 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority (User Provisioning and Mapping) 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP 802.1S Multiple Spanning Tree (MSTP) 802.1v Protocol-based VLANs 802.1W Rapid Spanning Tree (RSTP) 802.1X Network Access Control, Auto VLAN 802.2 Logical Link Control 802.3 10BASE-T 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ac Frame Extensions for VLAN Tagging 802.3ad Link Aggregation with LACP 802.3ae 10 Gigabit Ethernet (10GBASE-X) 802.3AX LAG Load Balancing 802.3az Energy Efficient Ethernet (EEE)

	802.3u Fast Ethernet (100BASE-TX) on Management Ports 802.3x Flow Control 802.3z Gigabit Ethernet (1000BASE-X)
<b>Zgodność ze standardami RFC w zakresie zarządzania siecią i bezpieczeństwa</b>	1155 SMIV1 1157 SNMPv1 1212 Concise MIB Definitions 1213 MIB-II 1215 SNMP Traps 1286 Bridge MIB 1442 SMIV2 1908 Coexistence Between SNMPv1/v2 2011 IP MIB 2012 TCP MIB 2013 UDP MIB 2096 IP Forwarding Table MIB 2233 Interfaces Group using SMIV2 2246 TLS v1 2271 SNMP Framework MIB 2618 RADIUS Authentication MIB 2620 RADIUS Accounting MIB 2819 RMON MIB (groups 1, 2, 3, 9) 2863 Interfaces MIB 2865 RADIUS 2866 RADIUS Accounting 2868 RADIUS Attributes for Tunnel Prot. 2869 RADIUS Extensions 3410 Internet Standard Mgmt. Framework 3411 SNMP Management Framework 3413 SNMP Applications 3416 SNMPv2 3418 SNMP MIB 3580 802.1X with RADIUS 4251 SSHv2 Protocol 4252 SSHv2 Authentication 4253 SSHv2 Transport 4254 SSHv2 Connection Protocol 4419 SSHv2 Transport Layer Protocol 4716 SECSH Public Key File Format 6101 SSL
<b>Inne</b>	Przystosowanie do pracy w temperaturze 0-40 stopni Celsjusza
<b>Ilość</b>	3 szt.

## 2. Serwer z oprogramowaniem

Parametr	Charakterystyka (wymagania minimalne)
----------	---------------------------------------

<b>Obudowa</b>	Obudowa typu Tower z możliwością instalacji min 8 dysków twardech 3,5".
<b>Płyta główna</b>	Z możliwością instalacji dwóch fizycznych procesorów, posiadająca minimum 16 slotów na pamięć RAM RDIMM z możliwością zainstalowania do minimum 1TB pamięci RAM, możliwe zabezpieczenia pamięci: ECC. Płyta główna zaprojektowana przez producenta serwera.
<b>Procesor</b>	Procesor Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.5GHz, klasy x86 dedykowane do pracy z zaferowanym serwerem umożliwiające osiągnięcie wyniku min. 106 w teście SPECrate2017_int_base, dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> dla konfiguracji dwuprocesorowej. Wydruk ze strony należy dołączyć do oferty.
<b>RAM</b>	Minimum 64GB pamięci RAM UDIMM o częstotliwości taktowania minimum 3200MHz
<b>Gniazda PCI</b>	minimum 5 slotów PCI Express trzeciej generacji
<b>Interfejsy sieciowe</b>	Minimum dwa interfejsy sieciowe 1Gb/s Ethernet nie zajmujące żadnego z dostępnych slotów PCI Express oraz złącz USB. Dodatkowa 2 portowa karta 10GbE BaseT
<b>Wewnętrzna pamięć masowa</b>	Możliwość instalacji dysków twardech 3,5" typu: SATA, NearLine SAS, SAS, SSD.  Zainstalowane co najmniej 3 dyski SAS o pojemności min. 1.2TB 10K Hot-Plug  Możliwość instalacji dodatkowej wewnętrznej pamięci masowej typu flash, dedykowanej dla hypervisora wirtualizacyjnego, wyposażonej w 2 nośniki typu flash o pojemności min. 64GB, umożliwiającej konfigurację zabezpieczenia typu "mirror" lub RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości minimalnej ilości wewnętrznej pamięci masowej w serwerze.  Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 240GB oraz możliwość konfiguracji w RAID1.
<b>Kontroler pamięci masowej</b>	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących
<b>System operacyjny/dodatkowe oprogramowanie</b>	Zainstalowany Windows Server 2022 Standard  Dodatkowo należy dostarczyć:  Nośnik do downgrade-u do wersji Windows Server 2019 Standard

	VMware vSphere 7 Essentials Kit for 3 Hosts (Max 2 CPU per host. 32 cores/CPU) – licencja i subskrypcja na min. 3 lata
<b>Wbudowane porty</b>	Minimum 8 portów USB z czego min. 3 w technologii 3.0 (porty nie mogą zostać osiągnięte poprzez zastosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń) 1x RS-232, 1x VGA D-Sub
<b>Karta graficzna</b>	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli
<b>Chłodzenie i zasilanie</b>	Wentylator, zasilacze o mocy minimum 495W (redundantne) wraz z kablami zasilającymi.
<b>Diagnostyka i bezpieczeństwo</b>	<ul style="list-style-type: none"> <li>- możliwość wyposażenia w moduł TPM 2.0</li> <li>- wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</li> <li>- fizyczne zabezpieczenie dedykowane przez producenta serwera uniemożliwiające wyjęcie dysków twardych umieszczonych na froncie obudowy przez nieuprawnionych użytkowników.</li> </ul>
<b>Karta Zarządzania</b>	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:</p> <ul style="list-style-type: none"> <li>• zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</li> <li>• zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);</li> <li>• szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;</li> <li>• wsparcie dla IPv6;</li> <li>• wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;</li> <li>• możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;</li> <li>• integracja z Active Directory;</li> <li>• wsparcie dla dynamic DNS;</li> <li>• wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.</li> <li>• możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera</li> <li>• możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera</li> </ul>
<b>Certyfikaty/normy</b>	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 lub inną równoważną (dokumenty załączyć do oferty)

	<p>Serwer musi posiadać deklaracja CE lub inny równoważną. (należy załączyć do oferty)</p> <p>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019.</p>
<p><b>Warunki gwarancji</b></p>	<p>Minimum roczna gwarancja producenta realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Możliwość zgłaszania awarii 24x7x365 poprzez linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do 3 lat.</p> <p>Zamawiający wymaga dołączenia dokumentów potwierdzających, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p> <p>Firma serwisująca musi posiadać certyfikat ISO 9001:2008 lub inny równoważny na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.</p> <p>Wymagane dołączenie do oferty dokumentów potwierdzających, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p> <p>Możliwość telefonicznego i elektronicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta oraz poprzez stronę internetową producenta lub jego przedstawiciela.</p> <p>Dokumentacja dostarczona wraz z serwerem dostępna w języku polskim lub angielskim.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie najnowszych uaktualnień oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.</p>

### 3. Oprogramowanie do backupu

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie do backupu i archiwizacji komputerów w sieciach LAN



<p><b>Wymagania funkcjonalne</b></p>	<ul style="list-style-type: none"> <li>• Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich</li> <li>• Program serwerowy kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology</li> <li>• Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11, Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology</li> <li>• Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików)</li> <li>• Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)</li> <li>• Automatyczny backup przy wyłączeniu komputera</li> <li>• Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i ?</li> <li>• Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows)</li> <li>• Backup baz danych i plików poczty w trybie online i offline</li> <li>• Kopie rotacyjne (wersjonowanie)</li> <li>• Zapis archiwów w otwartym formacie (ZIP 64-bit)</li> <li>• Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore)</li> <li>• Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej</li> <li>• Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych</li> <li>• Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO</li> <li>• Kompresja po stronie stacji roboczej</li> <li>• Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP,</li> <li>• Replikacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows)</li> <li>• Centralne sterowanie całym Systemem z jednego miejsca</li> <li>• Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników</li> <li>• Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN</li> <li>• Wysyłanie Alertów administracyjnych na e-mail</li> <li>• Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych</li> <li>• Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki</li> <li>• Automatyczna aktualizacja oprogramowania na komputerach zdalnych</li> </ul>
<p><b>Licencja</b></p>	<p>Licencja dla:</p>

	35 stanowisk klienckich oraz 1 serwera oraz 5 maszyn wirtualnych Bezterminowa licencja - licencja nie może być ograniczona czasowo z dodatkowym wsparciem technicznym producenta na okres minimum 12 miesięcy
<b>Ilość</b>	1 kpl.

## Część II przedmiotu zamówienia

### 4. Skaner

Nazwa	Minimalne wymagania dla oprogramowania
Wspierane systemy operacyjne	Windows 10, Windows 11
Dysk twardy	min. 500 Gb
Ilość pamięci RAM	pamięć fizyczna min. 2 Gb
Technologia druku	atramentowa pigmentowa
Liczba głowic drukujących	min. 1 szt
liczba zbiorników z atramentem	min. 5, możliwość wymiany atramentu podczas drukowania bez zatrzymania urządzenia Urządzenie musi obsługiwać również tusze p pojemności min. 700ml każdy
Dokładność linii	+/-0,1% lub mniej
Rozdzielczość druku	min. 2400 x 1200 dpi
Obsługa papieru	automatyczny podajnik 2-rolkowy, automatyczne ładowania papieru z przodu urządzenia
Rodzaje nośników	obsługa rolek do 44"
Szerokość rolki	max. 1118mm
Panel sterowania urządzeniem (interfejs)	Zintegrowany z urządzeniem wyświetlacz dotykowy - 15,6 cala. Komunikacja w języku
Sterowniki	w języku polskim
Automatyczna obcinarka papieru	tak
Szybkość skanera	szybkość skanowania mono (200 dpi) - min. 25 cm/sek szybkość skanowania kolor (200 dpi) - min. 7 cm/sek/
Rozdzielczość skanera	min. 600 dpi
Technologia skanowania	CIS, SingleSensor
Szerokość skanowania	min. 914 mm
Format skanowania	JPG,TIF,PDF
Interfejsy	LAN,USB
Wyposażenie standardowe	Niezbędne przewody, głowica drukująca, komplet atramentów startowych min. 1500 ml tuszu łącznie. Uchwyt na tuby papieru, podstawa.

Wyposażenie dodatkowe	dotatkowy komplet atramentów o min. pojemności 330 mln każdy
Gwarancja	Okres gwarancji 12 miesięcy, obejmująca cały system MFP
Inne	<ul style="list-style-type: none"> <li>• Urządzenie musi pochodzić z legalnego, autoryzowanego kanału sprzedaży.</li> <li>• Wykonawca dostarczy, wniesie, zainstaluje oraz skonfiguruje urządzenie w siedzibie i miejscu wskazanym przez Zamawiającego</li> <li>• Wykonawca przeprowadzi szkolenie pracowników w zakresie prawidłowej obsługi systemu w siedzibie Zamawiającego</li> </ul>

### Część III przedmiotu zamówienia

#### 5. Audyt

Nazwa	Minimalne wymagania dla usługi
<b>Typ</b>	<p>Wykonanie audytu cyberbezpieczeństwa, zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 do dokumentacji konkursowej - Cyfrowa Gmina.</p> <p>Audyt cyberbezpieczeństwa powinien zostać przeprowadzony w terminie do 60 dni od podpisania umowy.</p> <p>Wynikiem przeprowadzenia diagnozy musi być raport dotyczący audytowanego środowiska oraz wypełnienie formularza audytu i dostarczenia go za pomocą elektronicznej skrzynki podawczej ePUAP do NASK na adres skrzynki: /NASK-Institut/SkrytkaESP.</p>
<b>Plan audytu</b>	<p>Audyt musi składać się z minimum:</p> <ol style="list-style-type: none"> <li>1. Audyt dokumentacji i procesów: <ul style="list-style-type: none"> <li>- ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)</li> <li>- ocena wybranych aspektów bezpieczeństwa systemów informatycznych</li> <li>- ocena dojrzałości wybranych procesów bezpieczeństwa</li> <li>- opracowanie raportu z audytu oraz uzupełnienie arkusza do oceny</li> </ul> </li> <li>2. Testy penetracyjne infrastruktury sieciowej <ul style="list-style-type: none"> <li>- Weryfikacja dokumentacji sieci, topologii sieci, kluczowych elementów sieci</li> <li>- skanowanie sieci, rekonesans sieci (skanowanie musi zostać powtórzone dla każdej wskazanej przez Zamawiającego sieci)</li> <li>- skanowanie najistotniejszych hostów w sieci (serwery, kluczowe stacje końcowe, kamery, rejestratory), który zostały wybrane na podstawie wcześniejszej analizy</li> <li>- sprawdzenie domyślnych haseł dla najistotniejszych hostów w sieci (serwery, bramy, switche, access point), które zostały wybrane na podstawie wcześniejszej analizy</li> <li>- sprawdzenie możliwości wylistowania użytkowników oraz zdobycia haseł</li> <li>- weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych</li> </ul> </li> </ol>

	<ul style="list-style-type: none"> <li>- weryfikacja zabezpieczeń urządzeń sieciowych</li> <li>- testy sieci bezprzewodowej oraz weryfikacja zabezpieczeń sieci bezprzewodowej</li> <li>- wykonanie raportu zawierającego minimum: <ul style="list-style-type: none"> <li>• opis wszystkich elementów, które zostały poddane audytowi</li> <li>• podział podatności ze względu na ryzyko: wysoki, średni, niski</li> <li>• wskazanie zaleceń, rekomendacji, najlepszych praktyk – dla każdej znalezionej podatności</li> <li>• wylistowanie wszystkich podatności ze względu na ryzyko: wysoki, średni, niski</li> <li>• określenie bezpieczeństwa informatycznego w organizacji poprzez wskazanie ilości i rodzaju znalezionych podatności</li> </ul> </li> <li>- Wsparcie poaudytowe - Wykonawca ma obowiązek na udzielenie informacji na temat audytowanych elementów wynikających z raportu w terminie maksymalnie 7 dni od wykonania raportu.</li> </ul>
<p><b>Wymagania dla audytora</b></p>	<p>Audyt musi zostać przeprowadzony przez osobę posiadającą uprawnienia wskazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu:</p> <ol style="list-style-type: none"> <li>1. Certified Internal Auditor (CIA);</li> <li>2. Certified Information System Auditor (CISA);</li> <li>3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;</li> <li>4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;</li> <li>5. Certified Information Security Manager (CISM);</li> <li>6. Certified in Risk and Information Systems Control (CRISC);</li> <li>7. Certified in the Governance of Enterprise IT (CGEIT);</li> <li>8. Certified Information Systems Security Professional (CISSP);</li> <li>9. Systems Security Certified Practitioner (SSCP);</li> <li>10. Certified Reliability Professional;</li> <li>11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert</li> </ol>

## Wymagania dodatkowe

Wykonawca zobowiązany jest do ustalenia terminów dostaw z zamawiającym, we wskazanym przez niego miejscu, z uwzględnieniem charakteru pracy Urzędu.

## Rozwiązania równoważne

1. Jeżeli w opisie przedmiotu zamówienia zamawiający odnosi się do norm, specyfikacji technicznych zamawiający nie może odrzucić oferty dlatego, że oferowane dostawy są z nimi niezgodne pod warunkiem, że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107 Pzp, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia. Wykonawca oferując rozwiązanie równoważne do opisanego w opisie przedmiotu zamówienia jest zobowiązany wykazać równoważność w zakresie wskazanych parametrów, które muszą być na poziomie nie gorszym niż parametry wskazane przez zamawiającego. Zamawiający będzie oceniał zaproponowane rozwiązania z uwzględnieniem wyżej opisanej zasady.
2. W przypadku, gdy w opisie przedmiotu zamówienia znajdują się odniesienia do norm, specyfikacji technicznych zamawiający dopuszcza rozwiązania równoważne opisywanym, a odniesieniu temu towarzyszą wyrazy „ lub równoważne”.
3. Jeżeli w opisie przedmiotu zamówienia znajdują się jakiegokolwiek odniesienia do wielkości fizycznych ciała lub zjawiska, którą można określić ilościowo, czyli zmierzyć za pomocą jednostki miary (o ile nie wskazano inaczej) – należy przyjąć, iż jako równoważne zamawiający uzna ofertę, która uwzględni wymiary wraz z dopuszczonymi odchyleniami od wymiarów podanych w opisie przedmiotu zamówienia mieszczące się w granicach tolerancji określonych normą/standardem, dla której/którego wypracowano system normalizacji i certyfikacji na poziomie co najmniej międzynarodowym. Norma/standard musi być obowiązujący wg przepisów prawa na dzień wyceny.