

**Załącznik nr 1.1 do SIWZ**

**Program Funkcjonalno Użytkowy:**

**Modernizacja sieci teleinformatycznej w Urzędzie Gminy w Starej Kamienicy**

**adres obiektu budowlanego, którego dotyczy program funkcjonalno użytkowy :** Gmina Stara Kamienica  
58-512 Stara Kamienica 41

**Zamawiający:** Gmina Stara Kamienica  
58- 512 Stara Kamienica 41

**Program opracował:** Mariusz Marek

**Wspólny Słownik Zamówień (CPV):**

45000000-7 Roboty budowlane  
45300000-0 Roboty instalacyjne w budynku  
45311000-0 Roboty w zakresie okablowania strukturalnego oraz instalacji elektrycznych  
45314300-4 Instalowanie infrastruktury okablowania  
45314310-7 Układanie kabli  
45314320-0 Instalowanie okablowania komputerowego  
45314300-4 Instalowanie infrastruktury okablowania  
45400000-1 Roboty wykończeniowe w zakresie obiektów budowlanych  
45453000-7 Roboty remontowe i renowacyjne  
71000000-8 Usługi architektoniczne, budowlane, inżynieryjne i kontrolne  
71024000-2 Usługi architektoniczne, inżynieryjne i planowania  
71200000-0 Usługi architektoniczne i podobne  
71220000-6 Usługi projektowania architektonicznego  
712 23000-7 Usługi architektoniczne w zakresie rozbudowy obiektów budowlanych  
71320000-7 Usługi inżynieryjne w zakresie projektowania

Stara Kamienica 4 kwietnia 2017 r.

Spis treści:

1. Skrócony opis przedmiotu zamówienia.....	3
2. Minimalne wymagania zamawiającego, sposób wykonania i standardy dotyczące systemu okablowania.....	3
3. Szczegóły dotyczące budowy sieci informatycznej.....	4
3.1. Założenia ogólne.....	4
3.2. Okablowanie strukturalne.....	5
4. Opis stanu istniejącego.....	10
5. Gwarancja.....	10
6. Pomiary.....	10
7. Normy i przepisy prawne.....	11
8. Oświadczenie.....	12
9. Rysunki.....	12

## **1. Skrócony opis przedmiotu zamówienia:**

Przedmiotem niniejszego opracowania jest program funkcjonalno użytkowy dotyczący wykonanie niezbędnych prac projektowych, adaptacyjnych, montażowo – instalacyjnych, rozruchowych, specjalistycznych pomiarów, pozwalających uruchomić instalacje okablowania teleinformatycznego w budynku Urzędu Gminy w Starej Kamienicy.

Podane, w niniejszym PFU nazwy własne lub minimalne wymagania mają jedynie charakter pomocniczy dla określenia podstawowych parametrów. Zamawiający dopuszcza zastosowanie rozwiązań równoważnych. Produkt równoważny to taki, który ma te same cechy funkcjonalne, co wskazany w opisie produkt. Jego jakość nie może być gorsza, od jakości określonego w specyfikacji produktu oraz powinien mieć parametry nie gorsze niż wskazany produkt. Cechy techniczne i jakościowe zaoferowanego sprzętu powinny być zgodne z Polskimi Normami przenoszonymi normy europejskie lub w przypadku uczestniczenia w przetargu firm zagranicznych, normy innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszących te normy.

Należy zaprojektować i wykonać sieć informatyczna kategorii 6/klasa E. Serwerownię wyposażać w elementy pasywne i aktywne niezbędne do prawidłowego funkcjonowania sieci wraz z zasilaczem UPS. Ponadto do serwerowni należy dostarczyć i zainstalować klimatyzację.

## **2. Minimalne wymagania Zamawiającego, sposób wykonania i standardy dotyczące systemu okablowania:**

- a) Instalacji okablowania strukturalnego w budynku Urzędu gminy w Starej Kamienicy, ogółem 107 gniazd teleinformatycznych typu RJ45 kat 6e. Na etapie projektu należy skonfigurować gniazda końcowe wg. wytycznych Zamawiającego. Wszystkie elementy okablowania muszą być zgodne z wymaganiami norm na min kategorię 6 wg. ISO /IEC 11801:2002, PN-EN 50173-1:2004
- b) dostawa, montaż 2 switchy 48 portowych,
- c) dostawa i montaż klimatyzacji
- d) wszelkie wykonywane prace nie mogą pogorszyć stanu obecnie funkcjonującej sieci teleinformatycznej,
- e) Zamawiający nie dopuszcza połączeń stanowisk lub poszczególnych elementów sieci za pomocą połączeń bezprzewodowych.
- f) Zamawiający nie dopuszcza montażu torów kablowych na żadnym odcinku na kleje natynkowe, a jedynie za pomocą kołków rozporowych,
- g) Wykonawca prowadząc tory kablowe dla sieci strukturalnej winien zachować szczególną ostrożność w czasie prowadzenia odwiertów w ścianach i stropach w zakresie istniejących instalacji, których położenie w budynku nie jest udokumentowane schematami instalacyjnymi.

- h) Wszelkie uszkodzenia infrastruktury podczas prowadzonych prac przez wykonawcę obciążają jego samego i muszą być usunięte w terminie natychmiastowym po ich stwierdzeniu.
- i) Wykonawca sporządzi projekt wykonawczy instalacji okablowania strukturalnego sieci LAN, zawierający:
- ✓ opis z zestawieniem materiałowym
  - ✓ rozmieszczenie punktów stanowiskowych o schematy ideowe projektowanych instalacji,
  - ✓ specyfikację techniczną wykonania i odbioru robót, oraz plan bezpieczeństwa i ochrony zdrowia
- j) Wykonawca sporządzi dokumentację powykonawczą która, musi zawierać w szczególności:
- ✓ raporty z pomiarów dynamicznych okablowania,
  - ✓ rzeczywiste trasy rozmieszczenia instalacji,
  - ✓ lokalizowania punktów stanowiskowych z naniesioną numeracją gniazd,
  - ✓ schematy ideowe wykonanych instalacji.
  - ✓ lokalizację przebiegów przez ściany i stropy,
  - ✓ listę materiałów oraz wszelkie karty katalogowe, instrukcje montażu i eksploatacji oraz certyfikaty wystawione przez akredytowane niezależne laboratoria testowe i inne dokumenty pozwalające ocenić zgodność proponowanego rozwiązania z wymaganiami niniejszego dokumentu.
  - ✓ projekt wykonawczy oraz dokumentacja powykonawcza, muszą być wykonane przez osoby posiadające stosowne uprawnienia, określone przepisami prawa budowlanego.
- k) Wykonawca przed przystąpieniem do prac projektowych zobowiązany jest do doprecyzowania dokładnego rozmieszczenia punktów w poszczególnych pomieszczeniach. Przykładowy schemat został zamieszczony w inwentaryzacji.

### 3. Szczegóły dotyczące budowy sieci teleinformatycznej:

#### 3.1. Założenia ogólne:

- ✓ Ilość stanowisk:

Lp.	Nazwa pomieszczenia	Ilość stanowisk	Ilość gniazd teleinformatycznych pojedynczych
1.	Pomieszczenie biurowe nr 1	1	6
2.	Pomieszczenie biurowe nr 2	1	4
3.	Pomieszczenie biurowe nr 3	2	4
4.	Pomieszczenie biurowe nr 4	2	4
5.	Pomieszczenie socjalne		4
6.	Pomieszczenie biurowe nr 8	1	4
7.	Pomieszczenie biurowe nr 9	2	6
8.	Pomieszczenie biurowe nr 10	2	6
9.	Pomieszczenie biurowe nr 11	1	6
10.	Pomieszczenie biurowe nr 12	5	14
11.	Pomieszczenie biurowe nr 13	2	4

12.	Pomieszczenie biurowe nr 14	1	4
13.	Pomieszczenie gospodarcze nr 15	1	4
14.	Pomieszczenie biurowe nr 16	1	6
15.	Pomieszczenie biurowe nr 17	2	6
16.	Pomieszczenie biurowe nr 18	1	4
17.	Sala konferencyjna nr 23	1	5
18.	Pomieszczenie biurowe nr 24	2	4
19.	Pomieszczenie biurowe nr 25	1	6
20.	Pomieszczenie biurowe nr 26	1	6

Serwerownię należy wyposażyć w nową klimatyzację dedykowaną do serwerowni. Klimatyzacja musi spełniać wszelkie normy bezpieczeństwa oraz umożliwić utrzymanie zadanej temperatury serwerowni w ciągu całego roku.

Minimalne parametry klimatyzacji:

Wydajność:

chłodzenie w zakresie 0,9-2,50 [kW],

grzanie w zakresie 0,9 – 3,2 [kW],

zasilanie – 220 [V/Hz/Ø],

poziom hałasu jedn. wew/zew - 20 - 25 - 33 / 47 [dB(A),odl.1m]

Wymiary:

jedn. wew. [dł x wys x gł] - 800 x 300 x 200 dopuszczalna różnica 10% [mm]

jedn. zewn. [dł x wys x gł] - 700 x 480 x 230 dopuszczalna różnica 10% [mm]

waga jedn. wew/zew – 8,0 / 30 dopuszczalna różnica 15% [kg]

Kolor - biały

### 3.2. Okablowanie strukturalne

#### ✓ Okablowanie poziome

Okablowanie strukturalne obejmuje 107 gniazd logicznych, podzielonych zgodnie z wymaganiami użytkowymi i charakterystyką pomieszczeń. Gniazda rozmieszczone są na dwóch kondygnacjach budynku. Okablowanie poziome zostanie rozprowadzone w pomieszczeniach w torach kablowym zgodnie z wytycznymi z poprzednich punktów opracowania, nad lub pod którymi należy zamontować puszki natynkowe z gniazdami. Prowadzenie tras kablowych, kanałów musi zostać ustalone z użytkownikiem podczas projektowania instalacji.

Kabel ten ma spełniać wymagania stawiane komponentom opisanym w punkcie 2, równocześnie zapewniając pełną zgodność z niższymi kategoriami okablowania. Kable instalacyjne należy zakończyć w szafie kablowej na panelach 24 – portowych. Ponadto panele krosowe dodatkowo muszą posiadać boczne wieszaki po bokach. Wykonawca zobowiązany jest także do pozostawienia wolnych portów krosowych w ilości 10% wszystkich portów.

## ✓ Punkt dystrybucyjny

Instalacja sieci będzie przez jeden punkt dystrybucyjny do którego zbiegać się będą wszystkie linie okablowania strukturalnego. Punkt dystrybucyjny będzie składał się z szafy stojącej 37 U 800x1000, standard 19" Szafę zakupi i dostarczy wykonawca:

- nośność statyczna: do 800kg,
- drzwi przednie przeszklone z zamkiem, drzwi tylne stalowe z zamkiem, drzwi boczne z możliwością montażu zamka – stopień ochrony min IP20
- otwory na przewody: od góry, od dołu
- otwory wentylacyjne: w ścianach bocznych, w drzwiach
- zamontowane 4 wentylatory,
- listwa zasilająca,
- organizery kablowe 4szt,
- patchpanel – 4 szt. o parametrach – 24 porty RJ45 w kategorii 6 dla nieekranowanej skrętki 4 parowej o wysokości 1U)
- kable krosowe kat. 6A w ilości odpowiedniej do uruchomienia wszystkich gniazd sieci LAN,

Do szafy należy dostarczyć i zamontować UPS zapewniający podtrzymanie pracy aktywnych urządzeń sieciowych o parametrach co najmniej:

- moc pozorna – min. 1000 VA,
- moc rzeczywista – min. 600 Wat,
- typowy czas przełączenia na baterię 2 ms,
- liczba i rodzaj gniazdek z utrzymaniem zasilania – 2xPL (10A)
- czas podtrzymywania dla obciążenia 100% - nie mniej niż 2 min,
- czas podtrzymania przy obciążeniu 50 % - nie mniej niż 12 min,
- zakres napięcia wejściowego – 170 – 260 V,
- zimny start – TAK,
- alarmy – niski poziom baterii, przeciążenie,
- diody sygnalizacyjne – praca na baterii oraz przeciążenie,
- obudowa – Rack, max. 2U
- gwarancja – min 2 lata

## ✓ Konfiguracja

Wykonawca zobowiązany jest do skonfigurowania wszystkich urządzeń aktywnych wg. zaleceń zamawiającego

## ✓ Urządzenia aktywne

Urządzenia winny być zamontowane w Punkcie Dystrybucyjnym w pomieszczeniu serwerowni oznaczonym nr 19 w załączonej inwentaryzacji. Urządzenia aktywne muszą być zarządzane poprzez interfejs sieciowy pozwalający na zdalną konfigurację każdego urządzenia w sieci. Urządzenia muszą być dobrane w ilości zapewniającej obsługę

wszystkich portów sieci komputerowej w ilości wskazanej przez użytkownika z zapasem 10% dodatkowych portów.

a) Switch 48 portowy – 2 szt:

Specyfikacja:

Typ przełącznika	- Managed
Przełącznik wielowarstwowy	- L3
Obsługa MIB	- Tak
obsługa jakość serwisu (QoS)	- Tak
Podstawowe przełączania Ethernet RJ-45 porty typ	- Gigabit Ethernet (10/100/1000)
Liczba portów SFP Combo	- 2
Ilość slotów Modułu SFP+	- 2
Technologia okablowania Copper Ethernet	- 1000BASE-T,100BASE-TX,10BASE-T
Ilość portów Gigabit Ethernet	- 52
Gniazdko wyjścia CD	- TAK
Standardy komunikacyjne	- IEEE 802.1D,IEEE 802.1Q,IEEE 802.1s,IEEE 802.1w,IEEE 802.1x,IEEE 802.3,IEEE 802.3ab,IEEE 802.3ad,IEEE 802.3u,IEEE 802.3x,IEEE 802.3z
Blokowanie head-of-line (HOL)	- Tak
Podpora kontroli przepływu	- Tak
Dublowanie portów	- Tak
Agregator połączenia	- Tak
Kontrola wzrostu natężenia ruchu	- Tak
Limit częstotliwości	- Tak
Klient DHCP	- Tak
Protokół drzewa rozpinającego	- Tak
Obsługa sieci VLAN	- Tak
Szybkość transmisji danych	- 10/100/1000Mbps
Przepustowość rutowania/przełączania	- Min 120 Gbit/s
Przepustowość	- Min 77 Mpps
Wielkość tabeli adresów	- 16000 wejścia
Liczba VLANs	- 4096
Liczba kolejek	- 4
Maksymalna szybkość przesyłania danych	- 1 Gbit/s
Zgodny z Jumbo Frames	- Tak
Szyfrowanie / bezpieczeństwo obsługuje SSH/SSL	- 802.1x RADIUS,MD5
Obsługiwane protokoły sieciowe	- Tak
	- TCP/IP, ARP, DHCP, HTTP, UDP, ICMP, IPv6
Stackowalny	- Tak
Procesor wbudowany	- ARM albo kompatybilny
Taktowanie procesora	- Min 800 Mhz
Pojemność pamięci wewnętrznej	- Min 256 MB
Aktualizacje oprogramowania urządzenia	- Tak
Pamięci bufora pakietów	- Min 16 MB

Napięcie wejściowe AC	- 100-240 V
Minimalne wymagania systemowe	Mozilla Firefox 3.6, Microsoft Internet Explorer 7 \nEthernet Cat 5
System operacyjny	- Microsoft Windows, Linux, Mac OS X
Prędkość transmisji pakietu	- Min 77.38 mpps
Wskaźnik LED zasilania	- Tak

b) Zapora sieciowa FIREWALL

<b>Zapora sieciowa: 1 szt.</b>	
<b>Parametr</b>	<b>Wartości minimalne</b>
<b>TYP</b>	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
	<ul style="list-style-type: none"> <li>- monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych;</li> <li>- monitoring stanu realizowanych połączeń VPN;</li> <li>- system realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym;</li> <li>- system realizujący funkcję Firewall powinien dysponować minimum 10 portami Ethernet 10/100/1000 Base-TX;</li> <li>- system powinien umożliwiać zdefiniowanie co najmniej 250 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q;</li> <li>- w zakresie zapory sieciowej obsługa nie mniej niż 1,3 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę;</li> <li>- przepustowość Firewall'a: nie mniej niż 3 Gbps;</li> <li>- wydajność szyfrowania VPN IPSec: nie mniej niż 2 Gbps;</li> <li>- system realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 128 GB. System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej;</li> <li>- system realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanymi dotąd zagrożeń;</li> <li>- w ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych: <ul style="list-style-type: none"> <li>• kontrola dostępu - zapora ogniowa klasy Stateful Inspection</li> </ul> </li> </ul>



	<ul style="list-style-type: none"> <li>• ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS,</li> <li>• poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN,</li> <li>• ochrona przed atakami - Intrusion Prevention System,</li> <li>• kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM,</li> <li>• kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP,</li> <li>• kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma,</li> <li>• kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&amp;C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów),</li> <li>• możliwość analizy ruchu szyfrowanego protokołem SSL,</li> <li>• mechanizmy ochrony przed wyciekiem poufnej informacji (DLP);</li> <li>- baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW;</li> <li>- automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL;</li> <li>- system zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż:             <ul style="list-style-type: none"> <li>- haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu,</li> <li>• haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP,</li> <li>• haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych,</li> <li>• rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory;</li> </ul> </li> <li>- poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:             <ul style="list-style-type: none"> <li>• ICSA lub EAL4 dla funkcji Firewall,</li> <li>• ICSA lub NSS Labs dla funkcji IPS,</li> <li>• ICSA dla funkcji: SSL VPN, IPSec VPN;</li> </ul> </li> <li>- Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów;</li> </ul>
<p><b>SERWISY I LICENCJE</b></p>	<p>- w ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres min. 3 lat lub dłużej zgodnie ze złożoną ofertą);</p>

<b>SZKOLENIE</b>	- w ramach postępowania powinno zostać przeprowadzone minimum trzy dniowe szkolenie prowadzone przez producenta sprzętu lub autoryzowanego partnera producenta oferowanego sprzętu;
<b>GWARANCJA I WSPARCIE</b>	- system powinien być objęty serwisem gwarancyjnym przez okres 3 lat (lub dłużej zgodnie ze złożoną ofertą), realizowanym na terenie Rzeczypospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.

#### 4. Opis stanu istniejącego

Budynek dwukondygnacyjny konstrukcji murowanej, stropy żelbetowe. W budynku istnieje okablowanie, lecz nie spełnia ono dzisiejszych standardów okablowania strukturalnego. W budynku nie ma dedykowanej sieci zasilającej dla sprzętu komputerowego. Na parterze budynku znajduje się rozdzielnica główna. Rozdzielnica jest w wykonaniu podtynkowym.

#### 5. Gwarancja

Należy zapewnić objęcie wykonanej instalacji gwarancją

systemową producenta, gdzie okres gwarancji udzielonej bezpośrednio przez producenta nie może być krótszy niż 25 lat (wymagany certyfikat gwarancyjny producenta okablowania udzielony bezpośrednio Użytkownikowi końcowemu i stanowiący 25-letnie zobowiązanie gwarancyjne producenta w zakresie dotrzymania parametrów wydajnościowych, jakościowych, funkcjonalnych i użytkowych wszystkich elementów oddzielnie i całego systemu okablowania).

25 letnia gwarancja systemowa producenta ma obejmować:

- a) gwarancję materiałową (Producent zagwarantuje, że jeśli w jego produktach podczas dostawy, instalacji bądź 25-letniej eksploatacji wykryte zostaną wady lub usterki fabryczne, to produkty te zostaną naprawione bądź wymienione);
- b) gwarancję parametrów łącza/kanału (Producent zagwarantuje, że łącze stałe bądź kanał transmisyjny zbudowany z jego komponentów przez okres 25 lat będzie charakteryzował się parametrami transmisyjnymi spełniającymi wymogi stawiane przez normę PN-EN 50173-1:2011 dla klasy A);
- c) gwarancję aplikacji (Producent zagwarantuje, że na jego systemie okablowania przez okres 25 lat będą pracowały dowolne aplikacje (współczesne i opracowane w przyszłości), które zaprojektowane były (lub będą) dla systemów okablowania klasy A (w rozumieniu normy PN-EN 50173-1:2011).

#### 6. Pomiary

Urządzenia pomiarowe stosowane do testowania sieci teleinformatycznej muszą być zaakceptowane przez producenta systemu okablowania strukturalnego a wyniki pomiarów przeprowadzonych przy ich pomocy stanowią podstawę do udzielenia certyfikatu gwarancyjnego. Wyniki testów muszą zostać przekazane w formie papierowej oraz elektronicznej wraz z programem do obsługi danych. Testy końcowe muszą być wykonane po ukończeniu realizacji. Wszystkie błędy i uszkodzenia muszą być zdiagnozowane, naprawione i ponownie przetestowane z powodzeniem. Urządzenie pomiarowe musi posiadać aktualne świadectwo kalibracji (należy okazać kopię świadectwa kalibracji, w przypadku dostarczenia dokumentów obcojęzycznych należy dostarczyć tłumaczenia wykonane przez tłumacza przysięgłego).

## **7. Normy i przepisy prawne**

Projekt wykonawczy oraz wykonane instalacje muszą być zgodne z obowiązującymi przepisami i normami m.in.:

- Ustawa, Prawo budowlane (tekst jednolity Dz.U Nr 207 z 2003 r poz. 2016 z późniejszymi zmianami)
- Rozporządzenie MI z dnia 2.09.2004 roku w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznej wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego ( Dz.U. Nr 202 z 2004 r poz. 2072)
- Rozporządzenie MI z dnia 18.05.2004 roku w sprawie określenia metod i podstaw sporządzania kosztorysu inwestorskiego (Dz. U. Nr 130 z 2004 r poz. 1389)
- PN-EN 50173-1:2007 Technika informatyczna - Systemy okablowania strukturalnego
- PN-EN 50174-2 Technika informatyczna. Planowanie i wykonawstwo instalacji wewnątrz budynków.
- PN ISO IEC 27001 Technika informatyczna - Techniki bezpieczeństwa Systemy zarządzania bezpieczeństwem informacji
- Polskie Normy i Normy Branżowe
- Aprobaty techniczne

## 8. Oświadczenie

### OŚWIADCZENIE

Zgodnie z Rozporządzenia Ministra Infrastruktury dnia 2 września 2004 r. w sprawie szczegółowego zakresu form dokumentacji projektowej, specyfikacji technicznych i odbioru robót budowlanych oraz programu funkcjonalno–użytkowego (Dz. U. Nr 202 poz.2072) oświadczam, że

Wykonanie programu funkcjonalno – użytkowego dla zadania polegającego na modernizacji sieci informatycznej budynku Urzędu Gminy w starej Kamienicy

Budynek Urzędu Gminy w Starej Kamienicy  
58-512 Stara Kamienica 41

został sporządzony zgodnie z obowiązującymi przepisami oraz zasadami wiedzy technicznej.

.....  
/podpis projektanta/

## 9. Rysunki