ZP/UR/171/2014 **Załącznik nr 2.1 do SIWZ**

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA (parametry i wymagania minimalne)

Przedmiotem zamówienia jest remont istniejącej sieci internetowej w DS LAURA i DS Filon w Rzeszowie, ul. Cicha 2,4.

Miejsce realizacji:
Dom Studencki "Laura", 35-326 Rzeszów, ul. Cicha 2
Dom Studencki "Filon", 35-326 Rzeszów, ul. Cicha 4

Wymagania dodatkowe:

1. Oferowany sprzęt musi być fabrycznie nowy i nie używany.
2. Zamawiający wymaga aby oferowany sprzęt pochodził z oficjalnego i legalnego kanału dystrybucyjnego.
3. Wykonawca przed odbiorem przedmiotu zamówienia dostarczy potwierdzenie producenta, że dostarczony sprzęt pochodził z oficjalnego i legalnego kanału dystrybucyjnego.
4. Wykonawca opracuje dokumentację powykonawczą w 4 egzemplarzach.

Pozycja nr 1: Dostawa fabrycznie nowego, nie używanego różnego sprzętu komputerowego i sieciowego wraz z montażem, instalacją, konfiguracją, uruchomieniem i wdrożeniem

Pozycja nr 2: Konieczne do wykonania roboty instalacyjne związane z podłączeniem ułożeniem kabli strukturalnych i montaż gniazd

Opis minimalnych wymagań dotyczących pozycji nr 1:

W celu realizacji projektu należy dostarczyć niżej wymiennie urządzenia.

System Firewall – sztuk 2

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. Dopuszcza się, aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Minimalna liczba interfejsów i modułów:

- Minimalna liczba interfejsów GE RJ45 8
- Minimalna liczba interfejsów GE SFP 8
- Co najmniej jeden port konsoli
- Urządzenie wyposażone, w co najmniej jeden dysk SSD o pojemności nie mniejszej niż. 100GB

Wydajność firewall-a (minimalne wartości):

- Przepustowość IPv4 dla pakietów 1518 bajtów nie mniejsza niż 15Gbps
- Opóźnienie dla pakietów 64 bajty nie mniejsze niż 3us
- Przepustowość liczona w pakietach/s nie mniejsza niż 22Mpps
- W zakresie Firewall'a obsługa nie mniej niż 5 mln jednoczesnych połączeń oraz 250 tys. nowych połączeń na sekundę
- Możliwość tworzenia, co najmniej 8000 polityk bezpieczeństwa
- Wydajność dla połączeń VPN IPSEC nie mniejsza niż 12Gbps
- Wydajność dla połączeń VPN SSL, co najmniej na poziomie 400Mbps
- Obsługa, co najmniej 400 użytkowników korzystających z połączeń VPN SSL
- Wydajność IPS-a nie mniejsza niż 4,5Gbps
- Możliwość podłączenia AP-tów(funkcja kontrolera), co najmniej 500 AP-tów w tym, co najmniej 250 w trybie tunelowania
- Możliwość pracy w klastrze Active-Active oraz Active-standby

W ramach dostarczanego systemu ochrony musi być możliwość realizowania wszystkich z poniższych funkcjonalności:

- Antywirus – skanowanie ruchu w poszukiwaniu zainfekowanych plików
- IPS – skanowanie ruchu, detekcja anomalii
- Kontrola stron Internetowych – możliwość filtracji, monitorowania, blokowania stron internetowych
- Kontrola aplikacji – możliwość monitorowania/blokowania ruchu w tym rozpoznawanie aplikacji P2P
- Ochrona przed wyciekiem danych
- Kontroler sieci bezprzewodowej, możliwość podłączenia i zarządzania AP-tami oraz możliwość kreowania sieci bezprzewodowych z poziomu firewall-a
- Praca w trybie NAT/transparent
- Optymalizacja WAN
- Możliwość monitorowania i raportowania w „Chmurze"
- Możliwość autoryzacji z wykorzystaniem token-ów
- Możliwość tworzenia VPN-ów IPSec Site-to-Site
- Możliwość tworzenia VPN-ów IPSec Klient-to-Site

- Możliwość tworzenia VPN-ów SSL-owych
- W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
    - Tworzenie połączeń w topologii Site-to-Site oraz możliwość definiowania połączeń Client-to-Site
    - Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    - Praca w topologii Hub and Spoke oraz Mesh
    - Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
    - Obsługa SSL VPN w trybach portal oraz tunel
- Integracja ze środowiskiem Active Directory, z możliwością autoryzacji użytkowników w trybie SSO
- Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
- Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
- Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
- Możliwość budowy min. 2 oddzielnych instancji systemów bezpieczeństwa (fizycznych lub logicznych) w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
- Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
- Ochrona IPS powinna opierać się, co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać, co najmniej 4500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
- Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
- Baza filtra WWW o wielkości, co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne – min 50 kategorii. W ramach filtra powinny być dostępne m.in. kategorie spyware, malware, spam, proxy avoidance, sieci społecznościowe, zakupy. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
- Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.

- System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
    - 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
    - Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory

Wymagane wsparcie techniczne/suport na urządzenie Firewall

W ramach dostawy należy dostarczyć 12 miesięczny suport producenta Firewall realizowany w minimalnym reżimie czasowym 8x5 (8 godzin x 5 dni w tygodniu) dla funkcjonalności co najmniej IPS, Application Control, AV, Web Filtering i Antispam Services.

System zbierania logów – sztuk 1

Urządzenie musi pochodzić od tego samego producenta, co firewall. Urządzenie musi spełniać następujące minimalne wymagania:

- Minimum 3 porty 1 Gbps
- Zainstalowany min. dwa dyski twarde o pojemności nie mniejszej niż 2 tera każdy
- Możliwość zapisu, co najmniej 14GB logów na dzień
- Obsługa, co najmniej 50 milionów sesji/dzień
- System musi posiadać predefiniowane raporty dostosowane do potrzeb administratorów umożliwiające min.:
    - Monitorowanie wykorzystania polityk
    - Identyfikowanie wzorców ataków
- Korelacja zdarzeń sieciowych umożliwiająca szybką identyfikację na zagrożenia i zdarzenia bezpieczeństwa
- Możliwość przeglądania logów wysyłanych z urządzeń w podziale min. na
    - Rodzaj urządzenia
    - Log z ruchu użytkowników
    - Log zdarzeń zarejestrowanych przez urządzenie
    - Log z profili ochrony
- Możliwość archiwizacji(http, FTP, MAIL)

Wymagane wsparcie techniczne/suport na urządzenie

W ramach dostawy należy dostarczyć 12 miesięczny suport producenta Systemu zbierania logów realizowany w minimalnym reżimie czasowym 8x5 (8 godzin x 5 dni w tygodniu).

Przełączniki sieciowe – wymagania

W ramach realizacji projektu należy dostarczyć 3 rodzaje przełączników. Przełączniki te musza pochodzić od jednego producenta oraz muszą mieć możliwość klastrowania/łączenia urządzeń w stos po linkach 10Gbps. Należy również dostarczyć moduły, kable i inne elementy niezbędne do podłączenia urządzeń w stos/klaster oraz połączenia urządzeń ze sobą po linkach światłowodowych. Sposób łączenia został opisany w projekcie.

Przełącznik sw_type_1 o parametrach – sztuk 12:

- Wyposażony w minimum 48 portów 10/100/1000Base-T
- Musi posiadać możliwość zasilania urządzeń końcowych jak AP-ty, telefony z przełącznika poprzez funkcję PoE+
- Minimum 4 porty SFP+
- Minimum jeden zasilacz o mocy nie mniejszej niż 350W
- Możliwość instalacji modułów 1Gbps SFP oraz modułów 10Gbps SFP+
- Możliwość łączenia urządzeń tego samego typu w jeden logiczny przełącznik po linkach 10Gbps,
- Wyposażony w min. 1GB pamięci RAM
- Wyposażony w min. 128 MB pamięci flash
- Wydajność na poziomie nie mniejszym niż 130 Mpps
- Wydajność przełączania nie mniejsza niż 170Gbps
- Wsparcie dla protokołu Openflow
- Musi posiadać możliwość zarządzania minimum przez protokoły:
    - SSH
    - WEB
    - SNMP v2 oraz SNMP v3
    - Specjalizowane oprogramowanie producenta sprzętu
- Obsługa routingu statycznego, protokołu routingu RIP
- Musi minimalnie wspierać protokoły/standardy:
    - IEEE 802.1w
    - IEEE 802.1ad Q-in-Q
    - IEEE 802.1D MAC Bridges
    - IEEE 802.1p Priority
    - IEEE 802.1Q VLANs
    - IEEE 802.1s Multiple Spanning Trees

- IEEE 802.3ab 1000BASE-T
- IEEE 802.3ad Link Aggregation Control Protocol(LACP)
- IEEE 802.3ae 10-Gigabit Ethernet
- IEEE 802.3af Power over Ethernet
- IEEE 802.3u 100BASE-X
- IEEE 802.3x Flow Control
- IEEE 802.3z 1000BASE-X
- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 854 TELNET

Przełącznik sw_type_2 o parametrach – sztuk 11:

- Minimum 48 portów 10/100/1000Base-T
- Minimum 4 porty SFP+
- Minimum jeden zasilacz o mocy nie mniejszej niż 350W
- Możliwość instalacji modułów 1Gbps SFP oraz modułów 10Gbps SFP+
- Możliwość łączenia urządzeń tego samego typu w jeden logiczny przełącznik(klastrowanie) po linkach 10Gbps,
- Możliwość kastrowania do 9 przełączników tego samego typu po linkach 10Gbps
- Wyposażony w min. 1GB pamięci RAM
- Wyposażony w min. 128 MB pamięci flash
- Wydajność na poziomie nie mniejszym niż 130 Mpps
- Wydajność przełączania nie mniejsza niż 170Gbps
- Musi posiadać możliwość zarządzania minimum przez protokoły:
    - SSH
    - WEB
    - SNMP v2 oraz SNMP v3
    - Specjalizowane oprogramowanie producenta sprzętu
- Obsługa routingu statycznego, protokołu routingu RIP
- Musi minimalnie wspierać protokoły/standardy:
    - IEEE 802.1w
    - IEEE 802.1ad Q-in-Q
    - IEEE 802.1D MAC Bridges
    - IEEE 802.1p Priority
    - IEEE 802.1Q VLANs
    - IEEE 802.1s Multiple Spanning Trees
    - IEEE 802.3ab 1000BASE-T
    - IEEE 802.3ad Link Aggregation Control Protocol(LACP)
    - IEEE 802.3ae 10-Gigabit Ethernet
    - IEEE 802.3u 100BASE-X
    - IEEE 802.3x Flow Control
    - IEEE 802.3z 1000BASE-X
    - RFC 768 UDP

- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 854 TELNET

Przełącznik sw_type_3 o parametrach – sztuk 1:

- Musi posiadać minimum 4 porty SFP+
- Musi posiadać minimum 16 portów SFP 1Gbps
- Musi posiadać minimum 8 portów 100/1000Base-T
- Musi być wyposażony w minimum dwa zasilacz wbudowane umożliwiające redundancje na wypadek awarii jednego z nich
- Możliwość łączenia urządzeń tego samego typu w jeden logiczny przełącznik(klastrowanie) po linkach 10Gbps,
- Wyposażony w min. 1GB pamięci RAM
- Wyposażony w min. 128 MB pamięci flash
- Wydajność na poziomie nie mniejszym niż 95 Mpps
- Wydajność przełączania nie mniejsza niż 120Gbps
- Musi posiadać możliwość zarządzania minimum przez protokoły:
    - SSH
    - WEB
    - SNMP v2 oraz SNMP v3
    - Specjalizowane oprogramowanie producenta sprzętu
- Obsługa routingu statycznego, protokołu routingu RIP
- Musi minimalnie wspierać protokoły/standardy:
    - IEEE 802.1w
    - IEEE 802.1ad Q-in-Q
    - IEEE 802.1D MAC Bridges
    - IEEE 802.1p Priority
    - IEEE 802.1Q VLANs
    - IEEE 802.1s Multiple Spanning Trees
    - IEEE 802.3ab 1000BASE-T
    - IEEE 802.3ad Link Aggregation Control Protocol(LACP)
    - IEEE 802.3ae 10-Gigabit Ethernet
    - IEEE 802.3u 100BASE-X
    - IEEE 802.3x Flow Control
    - IEEE 802.3z 1000BASE-X
    - RFC 768 UDP
    - RFC 791 IP

- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 854 TELNET

Oprogramowanie do monitorowania i zarządzania dostarczanymi przełącznikami

System musi być zbudowany w architekturze klient – serwer. Licencja na system powinna umożliwiać zarządzanie min. 50 urządzeniami sieciowymi różnych producentów. System musi minimalnie wspierać instalację części serwerowej min. na platformach Windows Server 2003 SP2 oraz Red Hat Enterprise Linux 5. System musi być zbudowany modułowo tak, aby możliwe było doinstalowanie modułu dającego dodatkową funkcjonalność.
System zarządzania musi spełniać podstawowe funkcje:

- Automatyczne wykrywanie topologii sieci z użyciem przynajmniej protokołów SNMP, Telnet
- Monitorowanie stanu urządzeń po protokole SNMP
- Konfiguracja urządzeń po protokole SNMP
- Konfiguracja list dostępu (ACL) na zarządzanych urządzeniach
- Konfiguracja VLAN-ów na zarządzanych urządzeniach
- Zarządzenie konfiguracją urządzeń, tworzenie backupów oraz grupowe implementowanie konfiguracji przechowywanych w systemie zarządzania
- Zarządzenie zdarzeniami, przypisywanie alarmów do różnego rodzaju zdarzeń
- Zarządzenie infrastrukturą Wi-Fi z wykorzystaniem kontrolerów bezprzewodowych
- Możliwość wysyłania alarmów np. mailem lub SMS'em
- Generowanie raportów w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta
- Obrazowanie sieci w postaci mapki wraz z wyróżnianiem kolorami występujących alarmów
- Lokalizowanie użytkowników po adresie IP lub MAC
- Możliwość zdefiniowania polityki zmieniającej ustawienia sieci w przypadku wykrycia ataku sieciowego
- Możliwość utworzenia mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym
- Funkcja Telnet / SSH proxy umożliwiająca zarządzanie CLI przez przeglądarkę Internetową.
- Funkcja zarządzania za pomocą urządzeń mobilnych tj. iPhone oraz urządzeniami z systemem android.
- Dla wszystkich obsługiwanych standardowo urządzeń musi być dostępnie nie tylko monitorowanie, ale również zarządzanie, czyli możliwość modyfikacji konfiguracji urządzeń.
- Dostęp do sytemu zarządzania musi być realizowany przez przeglądarkę internetową.

- Niezbędne jest, aby system zarządzania był w stanie podłączyć się i importować dane z LDAP / Active Directory
- System powinien mieć możliwość autentykacji użytkowników w oparciu o LDAP i Radius
- System powinien mieć możliwość zbierania informacji o konfiguracji urządzeń w sieci dzienników zdarzeń systemu, informacji o zasobach (np. mapy topologii sieci) i przesyłania tych informacji min. za pomocą FTP, SFTP, Email.
- Wymagana jest możliwość tworzenia kont administratorskich z różnymi poziomami uprawnień, z możliwością przypisywania administratorów do grup urządzeń
- System powinien mieć możliwość zarządzania siecią wirtualną poprzez integracje SOAP z VMWare VirtualCenter Server oraz Microsoft Hyper-V vManager.
- System powinien mieć możliwość zarządzania siecią wirtualną dla serwerów Microsoft Hyper-V poprzez profil Power shell oraz WMI.
- System powinien wspierać zarządzanie, co najmniej dla 6000 modeli urządzeń.
- System powinien mieć możliwość automatycznej aktualizacji przez Internet.
- System powinien mieć możliwość implementacji rozproszonej, wykorzystując różne serwery do instalacji swoich komponentów.
- System powinien posiadać kontekstową funkcje pomocy zmieniającą zawartość w zależności od wyświetlanego kontekstu.

Muszą być dostępne moduły umożliwiające rozbudowę i integrację systemu o następujące funkcjonalności:

- Zarządzanie dostępem użytkowników z wykorzystaniem 802.1x
- Zarządzanie klientami na stacjach roboczych w ramach implementacji technologii Network Access Control
- Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA
- Obsługa informacji przesyłanych z wykorzystaniem sFlow oraz Netstream z urządzeń sieciowych oraz obrazowanie wyników
- Zarządzenie systemem telefonii IP
- Zarządzenie sieciami MPLS oraz sieciami VPN w oparciu o MPLS oraz VPLS
- Zarządzanie dostępem zdalnym IPSec/VPN
- Audyt użytkowników z wykorzystaniem informacji z logów, przepływów sieciowych SFLOW, NetSream v5 oraz analizy kontentu pakietów SMTP, FTP, http

Access Point-y – sztuk 90

W ramach realizacji projektu należy dostarczyć AP-ty o parametrach nie gorszych niż:

- Access Point do zastosowań wewnątrz budynków
- Minimalna liczba modułów radiowych: 2
- Minimalna liczba anten wewnętrznych/wbudowanych: 4
- Częstotliwości dla radia 1-wszego:
    - 2.4 GHz b/g/n lub 5 GHz a/n
- Częstotliwości dla radia 2-go:
    - 5 GHz a/n/ac
- Minimalna wydajność dla:
    - Radio 1 – do to 300 Mbps,
    - Radio 2 – do to 500 Mbps
- Minimalne jeden port 10/100/1000Base-T
- Strumienie TX / RX:
    - 2x2 MIMO
- Możliwość zasilenia AP-ta przez PoE
- Liczba jednoczesnych SSID: minimum 13
- Wsparcie minimum dla protokołów EAP: EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST
- Minimum wsparcie dla autentykacja użytkowników/urządzeń: WPA, WPA2 z 802.1x lub Preshared key, WEP, Web Captive Portal
- Minimum wsparcie dla standardów IEEE: 802.11a, 802.11b, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11n, 802.1X, 802.3af, 802.11ac
- Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej. W celu zapewnienia spójności zarządzania i uzyskania wymaganego poziomu bezpieczeństwa kontroler sieci Wif-Fi ma być uruchomiony w obrębie systemu realizującego funkcję firewall/ platformy bezpieczeństwa gwarantującej ochronę dla obsługiwanych sieci bezprzewodowych i przewodowych.
- Kompaktowa obudowa z tworzywa sztucznego umożliwiającą montaż na suficie lub ścianie wewnątrz budynku. Wymaga się, aby interfejs sieciowy i inne gniazda - jeśli występują - zlokalizowane były na ściance od strony montażowej urządzenia.

Serwer – sztuk 1

Należy dostarczyć serwer o parametrach:

LP	Parametr lub warunek	**Minimalne wymagania**
1	Obudowa	-Typu Rack, wysokość min. 2U; -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack oraz ramieniem porządkującym ułożenie przewodów w szafie rack;
3	Procesory	-Zainstalowany procesor w architekturze x86
4	Pamięć RAM	-Zainstalowane min. 24 GB pamięci RAM min. DDR3 LV Registered -Wsparcie dla technologii zabezpieczania pamięci min. Advanced ECC, Memory Scrubbing, SDDC; -Wsparcie dla konfiguracji pamięci w trybie „Rank Sparing”; -min. 24 gniazda pamięci RAM na płycie głównej, obsługa min. do 1536GB pamięci RAM;
5	Kontrolery dyskowe, I/O	-Zainstalowany kontroler SAS 2.0 min. RAID 0,1,5,6,50,60, min. 1024MB pamięci podręcznej cache,
6	Dyski twarde	-Zainstalowane min. 3 dyski SAS 2.0 o pojemności min. 300GB każdy, min. 10K RPM dyski Hotplug; -Minimum 8 wnęk dla dysków twardych Hotplug 2,5; -Obsługa dysków min. SAS, SATA, SSD; -Możliwość rozbudowy dostarczonego serwera do obsługi 16 wewnętrznych dysków twardych Hotplug 2,5;
7	Kontrolery LAN	-min. 2x 1Gb/s LAN, ze wsparciem min. iSCSI i iSCSI boot i teamingu, RJ-45;
8	Porty	-zintegrowana karta graficzna ze złączem VGA; -min. 7x USB 2.0, w tym minimum 2 na panelu przednim, minimum 4 z tyłu; -min. 1x RS-232;
10	Zasilanie, chłodzenie	-Redundantne zasilacze hotplug -Redundantne wentylatory hotplug;

11	Zarządzanie	-Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera -Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; Dostęp poprzez przeglądarkę Web (także SSL, SSH) Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii Zarządzanie alarmami (zdarzenia poprzez SNMP) Możliwość przejęcia konsoli tekstowej Opcjonalne przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
12	Wspierane OS	-Windows 2012 Hyper-V, VMWare
13	Oprogramowanie	Wraz z serwerem należy dostarczyć licencje oprogramowania potrzebnego do uruchomienia systemu MGMT i Radius.

Wymagane wsparcie techniczne/suport na urządzenie

Gwarancja na serwer musi być świadczona w miejscu jego instalacji.

Komputer stacjonarny do prezentacji informacji – sztuk 2

Komputer stacjonarny do prezentacji informacji (Kiosk informacyjny) wyposażony w klawiaturę metalową, o wzmocnionej konstrukcji odpornej na uszkodzenia mechaniczne o poniższych minimalnych parametrach:

Element	**Opis wymagań minimalnych**	
Obudowa	• konstrukcja wykonana z blachy stalowej • monitor odchylony od pionu pod kątem 45 stopni (+/- 5 stopni) • dostęp serwisowy realizowany od tyłu kiosku przez drzwi uchylne stalowe, zamykane zamkiem. • podstawa kiosku dwuwarstwowa stalowa, malowana proszkowo • kolorystyka dopasowana do wymagań Zamawiającego • wymagana możliwość demontażu (wymiany) wszystkich elementów poszycia kiosku bez użycia elektronarzędzi. • podświetlane logo (każdy komputer/terminal zostanie w pełni spersonalizowany poprzez polakierowanie na dowolny, wskazany przez Zamawiającego, kolor z palety, jak również umieszczenie na nim elementów identyfikacji wizualnej w formie podświetlanego logo zgodne z wymogami Zamawiającego – księga znaku). Personalizacja zostanie uzgodniona z oferentem.	
Monitor	monitor dotykowy - przekątna monitora min : 21''	
Jednostka sterująca kioskiem	Procesor	Procesor zgodny z architekturą x64
	Pamięć RAM	Minimum 4 GB; z możliwością rozbudowy do min. 32 GB, min. 2 wolne złącza dla rozszerzeń pamięci
	Dysk twardy	Min. 320GB, min. 32MB Cache,
	Karta dźwiękowa	zintegrowana
	Porty I/O	minimum 8 portów USB min. 2.0
	Karta sieciowa	Zintegrowana minimum 10/100/1000 MBit/s
	Karta graficzna	Karta graficzna zintegrowana, z możliwością dynamicznego przydzielania pamięci.
Wyposażenie dodatkowe	• wrzutnik monet • Głośniki • Czytnik kart stykowych (smartcard) zamontowany z przodu Kiosku • Klawiatura o wzmocnionej konstrukcji odpornej na uszkodzenia mechaniczne z manipulatorem kulkowym	
Zasilanie	• 230V, 50 Hz,	
Certyfikaty i dokumenty	• Deklaracja zgodności CE	

Do oferty należy dołączyć projekt (wizualizację) komputera stacjonarnego do prezentacji informacji.

a) Parametry funkcjonującego u Zamawiającego Systemu Kiosków Informacyjnych

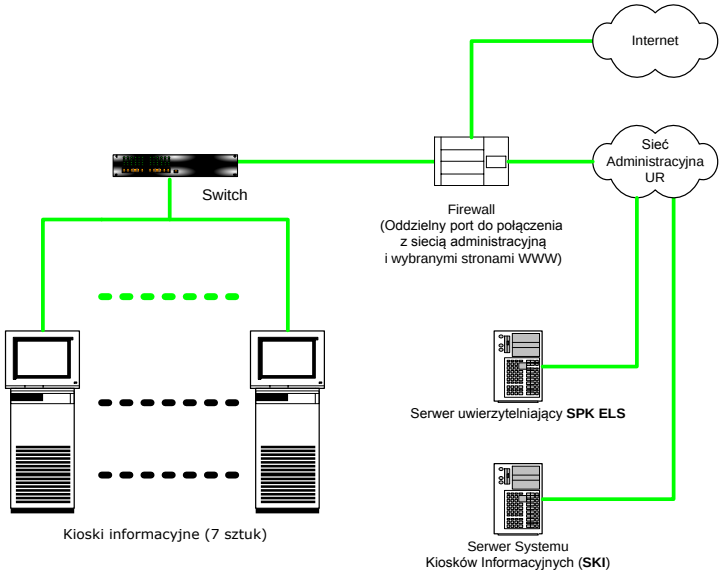
Dostarczone kioski informacyjne należy zintegrować z istniejącym i działającym u Zamawiającego Systemem Kiosków Informacyjnych o poniższych parametrach:

System Kiosków Informacyjnych – tzw. „Infomatów" – tworzą:

- serwer aplikacji zwany dalej serwerem Systemu Kiosków Informacyjnych (serwer SKI);
- kioski informacyjne

Serwer Systemu Kiosków Informacyjnych (SKI) znajduje się w chronionej sieci administracyjnej UR. Serwer SKI musi nawiązywać połączenia z serwerem uwierzytelniającym ELS (znajdującym się wewnątrz sieci administracyjnej UR) oraz z wybranymi witrynami zewnętrznymi(sieć Internet i Intranet). Infomaty znajdują się w odrębnej sieci Infomatów oddzielonej od sieci Administracyjnej poprzez firewall.
Kioski Informacyjne, które zostaną dostarczone muszą współpracować z posiadanym przez Zamawiającego Systemem Elektronicznej Legitymacji Studenckiej (SELS), Systemem Elektronicznej Legitymacji Doktoranta oraz Systemem Elektronicznej Karty Pracowniczej.

Dostarczone Kioski Informacyjne muszą umożliwiać zapis, odczyt, wykorzystanie kodu PIN zapisanego w strukturach funkcjonujących u Zamawiającego kart ELS, ELD, EKP do uwierzytelniania.
Oprogramowanie Kiosku musi przygotować ELS, ELD i EKP do obsługi PKI w kioskach informacyjnych.
Oprogramowanie Kiosku umożliwi zalogowanie się użytkownika przy pomocy certyfikatu (PKI).
Oprogramowanie Kiosku musi mieć możliwość obsługi Bezobsługowego Centrum Wydruku - BCW (m.in. ładowanie impulsów na karty ELS, ELD, EKP)



b) Oprogramowanie do nowych dostarczanych kiosków informacyjnych:

1	Kiosk informacyjny musi posiadać sterowniki do obsługi czytnika kart elektronicznych zgodnych z normą ISO/IEC 7816 lub równoważną oraz standardem PC/S.C. lub równoważnym, a w szczególności legitymacji ELS o specyfikacji zgodnej z rozporządzeniem Ministerstwa Szkolnictwa Wyższego - Dziennik Ustaw z dnia 8 grudnia 2006 r. (Nr 224, poz. 1634) Rozporządzenie wydano na podstawie art. 192 ust. 1 ustawy z dnia 27 lipca 2005 r. -Prawo o szkolnictwie wyższym.
2	Kiosk informacyjny musi autoryzować i uwierzytelniać użytkownika na podstawie danych zapisanych w specjalnej, przewidzianej do tego strukturze danych przechowywanej na legitymacji ELS lub przy pomocy logowania z hasłem, umożliwiające dostęp do stron zawierających dane osobiste, które mogą pochodzić z innych systemów uczelnianych (np. systemu dziekanatowego lub bibliotecznego).
3	Kiosk informacyjny musi obsługiwać procesorowe karty serwisowe, umożliwiające konfigurację serwisu informacyjnego kiosku przy pomocy stron WWW.
4	Powłoka użytkownika (shell) oprogramowania kiosku musi być wykonana w postaci aplikacji wykonanej w technologii „cienkiego klienta", współpracująca z dedykowaną bazą danych, umożliwiającą tworzenie kont użytkowników i zarządzanie ich uprawnieniami, przechowywanie indywidualnej konfiguracji kiosków, itp.
	Inne funkcje oprogramowania kiosku informacyjnego
5	Autoryzacja użytkownika musi odbywać się na podstawie legitymacji ELS z kodem PIN lub w oparciu o login i hasło. Niedopuszczalne jest autoryzowanie użytkownika na podstawie jedynie numeru numeru seryjnego karty ELS. W przypadku braku karty ELS w czytniku Infokiosku lub gdy użytkownik nie zalogował się za pośrednictwem Infokiosku wymagane jest ograniczenie dostępu użytkownika jedynie do: - strony głównej (wraz z podstronami); - rozkładów jazdy PKP, PKS, etc.; - innych witryn włączanych sukcesywnie przez administratora ze strony

	Zamawiającego do grupy witryn nie wymagających autoryzowanego dostępu. Oprogramowanie musi także mieć możliwość zastosowania struktury PKI (Infrastruktury Klucza Publicznego) do uwierzytelniania.
6	Kiosk informacyjny musi zapewnić automatyczne wylogowanie użytkownika (przejście do strony głównej systemu) w przypadku: - wyjęcia karty ELS z czytnika; - utraty połączenia z serwerem kiosków informacyjnych (wyświetlenie stosownego komunikatu dla użytkownika); - przekroczenia limitu czasu bezczynności (określanego przez administratora systemu w zakresie od 1 minuty do 60 minut z krokiem 1 minuta).
7	Kiosk informacyjny musi pozwalać na cykliczne odświeżanie konfiguracji programowej urządzenia, rozumiane jako zdalne załadowanie parametrów konfiguracyjnych dla przeglądarki internetowej działającej na kiosku w charakterze klienta.
8	Kiosk informacyjny musi pozwalać na ochronę kiosku poprzez restrykcje systemowe (blokowanie możliwości uruchamiania wskazanych aplikacji).
9	Kiosk informacyjny musi pozwalać na obsługę klawiatury ekranowej dostosowanej do ekranów dotykowych (duże przyciski), umożliwiającej jedynie wprowadzanie tekstów, z zablokowaną możliwością wykonywania funkcji sterujących (skrótów klawiszowych).
10	Kiosk informacyjny musi pozwalać na aktywowanie klawiatury ekranowej poprzez ustawienie kursora w polu edycji lub poprzez wywołanie dedykowanym przyciskiem.
11	Kiosk informacyjny musi pozwalać na obsługę modułów bezpieczeństwa
12	Kiosk informacyjny musi pozwalać na zapisywanie danych na kartach procesorowych, które są zabezpieczone kluczami 3DES (również kluczami zdywersyfikowanymi 3DES). Powinno także pozwalać na poszerzanie funkcjonalności karty poprzez tworzenie dodatkowych struktur danych na karcie.
13	Kiosk informacyjny musi pozwalać na przechowywanie kluczy 3DES w bezpiecznym magazynie chronionym.

System operacyjny infokiosku	
Platforma	Infokiosk musi mieć zainstalowany 64 bitowy system operacyjny. System operacyjny (klasy PC) musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; 1. 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; 2. Internetowa aktualizacja zapewniona w języku polskim; 3. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; 4. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; 5. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi) 6. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której

	podłączony jest komputer 7. 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. 8. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; 9. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 10. 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. 11. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych. 12. Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. 13. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika. 14. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 15. Wbudowany system pomocy w języku polskim; 16. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 17. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; 18. Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 19. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; 20. Wsparcie dla logowania przy pomocy smartcard; 21. Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; 22. System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; 23. Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; 24. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń; 25. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; 26. 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; 27. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację; 28. Graficzne środowisko instalacji i konfiguracji; 29. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; 30. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe 31. Udostępnianie modemu; 32. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;

	33. Możliwość przywracania plików systemowych; 34. 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.) 35. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).

Dostawa, instalacja, montaż, szkolenie:

W ramach dostawy należy:

- Wykonać montaż kiosków w miejscu wskazanym przez Zamawiającego
- Wykonać instalację urządzeń wraz z infrastrukturą potrzebną do ich uruchomienia (kable połączeniowe i zasilające, PEL)
- Wykonać instalację i konfigurację oprogramowania systemowego i oprogramowanie zarządzająco - sterującego
- Przeprowadzić bezpłatnie szkolenie w zakresie obsługi urządzenia i zainstalowanego oprogramowania dla administratorów
- Przygotować instrukcję obsługi dotyczącą eksploatacji kiosku i postępowania w przypadku awarii, instrukcja musi być wydana w języku polskim
- Przygotować instrukcję dotyczącą konfiguracji oprogramowania, instrukcja musi być wydana w języku polskim
- Umożliwić dokonywanie zmian konfiguracji przez Zamawiającego

Wymagane wsparcie techniczne/suport na urządzenie

W ramach dostawy należy zapewnić 12 miesięczny suport dla dostarczanego oprogramowania Kiosku informacyjnego.

Urządzenie przenośne do diagnostyki i konfiguracji sieci – szt. 1

Należy dostarczyć urządzenie przenośne do diagnostyki i konfiguracji sieci o parametrach:

Nazwa komponentu	Wymagane minimalne parametry techniczne
Procesor	Procesor osiągający w teście PassMark PerformanceTest co najmniej wynik min. 2500 punktów PassMark CPU Mark (wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net).
Płyta główna	Oparta na chipsecie rekomendowanym przez producenta procesora.
Matryca	Przekątna matrycy: min. 12,1" - max. 14,1"
Pamięć operacyjna	Zainstalowane min. 4 GB RAM, możliwość rozbudowy
Parametry pamięci masowej	Min. 500 GB
Sloty zewnętrzne	Czytnik kart pamięci min. SD i MMC
Połączenia i karty sieciowe	Port sieci LAN 10/100/1000 Ethernet RJ 45 zintegrowany z płytą główną oraz WLAN 802.11b/g/n, zintegrowany z płytą główną lub w postaci wewnętrznego modułu mini-PCI Express. Bluetooth
Wymagane zintegrowane złącza	Min. 2x USB; Min. 1 x VGA lub 1x HDMI; wyjście słuchawkowe; wejście mikrofonu; Min. 1 x sieć (RJ-45)
Bateria	Min. 4 cell Li-Ion zapewniająca pracę minimum przez 4h
System operacyjny	Zainstalowany system operacyjny w wersji polskiej. Dopuszczalny jest system operacyjny dla komputerów PC, spełniający następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; 2. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; 3. 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; 4. Internetowa aktualizacja zapewniona w języku polskim; 5. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; 6. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; 7. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi) 8. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer 9. 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. 10. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;

	11. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 12. 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. 13. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych. 14. Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. 15. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika. 16. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 17. Wbudowany system pomocy w języku polskim; 18. Certyfikat producenta oprogramowania na dostarczany sprzęt; 19. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 20. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; 21. Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; 22. Graficzne środowisko instalacji i konfiguracji; 23. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; 24. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe 25. Udostępnianie modemu; 26. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; 27. Możliwość przywracania plików systemowych; 28. 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.)
Dodatkowo	Przejściówka USB -> COM Torba do dostarczonego urządzenia: przegroda z pianki, pasek na ramię, kolor ciemny

Opis minimalnych wymagań dotyczących pozycji nr 2:

Opis minimalnych wymagań dotyczących pozycji nr 2:

1. Wykonawca w ramach realizacji przedmiotu zamówienia zobowiązany jest do wykonania koniecznych robót instalacyjnych w szczególności:

a) związanych z ułożeniem kabli strukturalnych

b) związanych z montażem gniazd RJ-45
2. Ułożeniu kabli strukturalnych i montażu gniazd mogą towarzyszyć roboty dodatkowe tj. przebicia przez ściany, ułożenie kanałów kablowych dwukomorowych umożliwiających zabudowę na nich gniazd RJ-45, wykonanie drobnych prac malarskich po wykonaniu robót budowlanych.
3. Należy przewidzieć ułożenie i zarobienie kabli oraz zamocowanie i przyłączenie do szaf dystrybucyjnych
4. Dodatkowe wymagania:
a) Załączony przedmiar stanowi materiał pomocniczy. Przed przystąpieniem do przetargu zaleca się wykonanie wizji lokalnej przez Wykonawcę.
b) Wykonawca opracuje dokumentację powykonawczą w 4 egzemplarzach.