GEOMAR SA
ul. Piotra Skargi 23, 70-487 Szczecin
tel. +48 91 432 49 00, fax +48 91 432 49 01
www.geomar.pl geomar@geomar.pl

Nr archiwalny: **GEO/WIM-271-5-229-2013/ZAMIENNY/2013**
Liczba egzemplarzy: **6**
Egz. nr:

PROJEKT WYKONAWCZY – CZĘŚĆ AKTYWNA

PROJEKT ZAMIENNY

Tytuł projektu: **ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA**

Lokalizacja: **miasto Dąbrowa Górnicza**

Branża: **Telekomunikacja**

Inwestor: **Gmina Dąbrowa Górnicza**
Ul. Graniczna 21
41-300 Dąbrowa Górnicza

Data wykonania: 2013r.

Zespół projektowy:		
Projektował:	**mgr inż. Wiktor Gabryliszyn** **ZAP/0169/POOT/06**	

DOKUMENTACJA PROJEKTOWA

CZĘŚCI AKTYWNEJ

WRAZ

ZE SPECYFIKACJĄ TECHNICZNĄ

ST – 02.00

w Dąbrowie Górniczej

Spis Rysunków

1 ZAŁOŻENIA

Dokument ten przedstawia projekt sieci metropolitarnej dla Dąbrowy Górniczej.

Założenia dotyczące budowy:

- lokalizacja węzłów: szkieletowych, agregujących oraz dystrybucyjnych została określona w niniejszym projekcie;

Węzły szkieletowe:

- Urząd Miejski, Komenda Straży Miejskiej ul. Graniczna 21
- Szkoła Podstawowa nr 11 Al. Piłsudskiego 103
- MZBM, Dyrekcja ul. Tysiąclecia 20
- Zespół Szkół Zawodowych „SZTYGARKA" ul. Legionów Polskich 69
- Miejska Biblioteka Publiczna (Dyrekcja) ul. Kościuszki 25
- Pałac Kultury Zagłębia Plac Wolności 1

Węzły agregujące:

- Zespół Szkól Ogólnokształcących nr 2 ul. Prusa 3
- Gimnazjum nr 9 ul. Zwycięstwa 44
- Miejska Biblioteka Publiczna filia nr 8 ul. Ofiar Katynia 93
- Miejska Biblioteka Publiczna filia nr 18 ul. Legionów Polskich 131
- Miejska Biblioteka Publiczna filia nr 1 ul. Wojska Polskiego 43
- Szkoła Podstawowa nr 10 ul. Reymonta 14

- Węzeł szkieletowy Urząd Miejski pełnić będzie także funkcję Centrum Zarządzania;

- połączenia w warstwie fizycznej zostaną zrealizowane w technologii światłowodowej;

- technologią warstwy drugiej jest Ethernet;

- Sieć szkieletowa, agregująca i dystrybucyjna została zrealizowana w technologii MPLS;

- dostęp dla użytkowników końcowych w technologii Ethernet;

W wyniku realizacji projektu zamawiający otrzyma skonfigurowaną, uruchomioną i przetestowaną kompletną sieć wraz z pakietem instruktaży stanowiskowych i wdrożenia obsługi oraz bezpłatny support i serwis w okresie 5 lat.

2 OPIS ROZWIĄZANIA

Sieć miejska została zaprojektowana w oparciu o wyżej wymienione założenia oraz ogólne zasady projektowania sieci MetroEthernet. Została opracowana w sposób hierarchiczny, gdzie możemy wyróżnić: rdzeń (szkielet), dystrybucję oraz dostęp. W zaprojektowanej sieci wszystkie urządzenia wspierają technologię MPLS. Sieć została zaprojektowana w sposób, który pozwoli na efektywne wykorzystanie zastosowanych urządzeń. Przełączniki przewidziane do węzłów agregujących i dystrybucyjnych posiadają zbliżoną funkcjonalność do urządzeń zastosowanych w szkielecie, jednak mają bardziej kompaktowe rozmiary.

Podstawowe zalety rozwiązania są następujące:

- Wszystkie urządzenia są klasy operatorskiej – tzn zarówno routery szkieletowe, przełączniki agregujące oraz dystrybucyjne wyposażone są w podwójne zasilacze z możliwością wymiany uszkodzonych elementów w trakcie pracy (OIR On line – Insertion – removal). Jest to szczególnie ważne w zdalnych lokalizacjach, gdzie dostęp do uszkodzonego urządzenia może być bardzo ograniczony. Dodatkowo routery szkieletowe są wyposażone w podwójne karty procesora, wentylatory i karty matrycy przełączającej. Modularny system operacyjny zapewnia instalację poprawek i nowych wersji oprogramowanie bez wpływu na działanie sieci i przesyłany ruch (ISSU – In Service Software Upgrade) Dodatkowo urządzenia agregujące i dystrybucyjnebędą wyposażone w styczniki alarmowe umożliwiające dopięcie alarmów zewnętrznych i podniesienie poziomu bezpieczeństwa fizycznego serwerowni i urządzeń.
- Modularna budowa kart liniowych zapewnia łatwą rozbudowę na zasadzie dodawania kolejnych portów małymi krokami. Istnieje możliwość przenoszenia interfejsów pomiędzy routerami co zapewnia ochronę już dokonanych inwestycji.
- Urządzenia charakteryzują się bardzo niskim zużyciem energii elektrycznej. W szczególności w przełącznikach agregacyjnych oraz dystrybucyjnych maksymalne zużycie energii nie będzie większe niż 230W, a w typowym zastosowaniu osiągnie jeszcze niższe wartości. Ma to szczególne znaczenie w warstwie dystrybucyjnej i agregacyjnej kiedy liczba zainstalowanych urządzeń jest duża co powoduje duże koszty za energię elektryczną

- Wszystkie proponowane urządzenia zapewniają wsparcie dla technologii MPLS. Dzięki temu możliwe jest rozciągnięcie usług oferowanych za pomocą protokołu MPLS również do warstwy agregacyjnej i dystrybucyjnej. Posiadanie MPLS w warstwie szkieletowej, dystrybucyjnej i agregującej zapewnia jednorodną obsługę wszystkich usług w sieci i znacząco obniża poziom skomplikowania sieci i koszty utrzymania systemu w kolejnych latach. . Poprawna implementacja usług opartych o MPLS musi być potwierdzona odpowiednią certyfikacją Metro Ethernet Forum - MEF9 i MEF14 oraz CE2.0 co najmniej w obszarach: E-Line, oraz E-LAN

- Urządzenia szkieletowe mogą być bardzo łatwo rozbudowywane do wyższych przepustowości 10/40/100GE oraz możliwe jest zastosowanie technologii IPoDWDM w celu uzyskania wyższej szybkości wykrywania awarii i jakości monitorowania łącza szkieletowego. Karta liniowa umożliwia ramkowanie zgodne ze standardem G.709 i

zapewnia korekcję błędów E-FEC lub Advanced FEC co poprawia niezawodność i jakość transmisji sygnału.

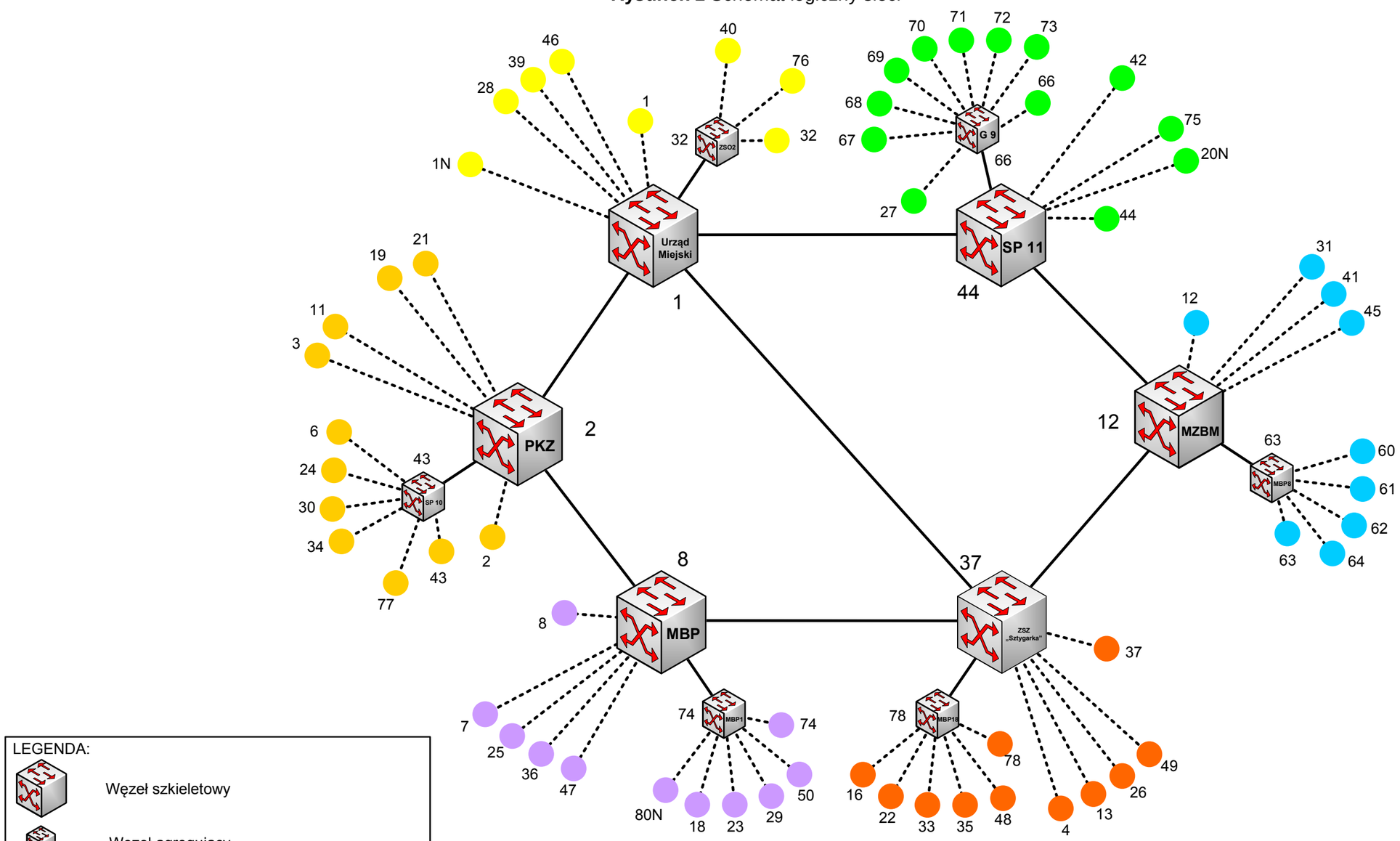
- Został wprowadzony czytelny podział na urządzenia szkieletowe, agregujące i dystrybucyjne. Każde z urządzeń wykonuje jasno określone funkcje, w szczególności:
  - Urządzenia szkieletowe mają za zadanie wydajne i niezawodne przełączanie pakietów
  - Urządzenia agregujące koncentrują ruch z bardziej oddalonych węzłów dystrybucyjnych oraz realizując bezpieczne usługi transportowe MPLS VPN oraz polityki jakości usług
  - Urządzenia dystrybucyjne dołączają bezpośrednio klientów końcowych i realizują dla nich bezpieczne usługi transportowe MPLS VPN oraz polityki jakości usług

  Dzięki temu możliwe jest efektywniejsze zarządzanie siecią i usługami, a co za tym idzie obniżenie kosztów utrzymania. Łatwiej też diagnozować ewentualne problemy oraz ograniczyć je do jednej tylko warstwy sieci, co podnosi niezawodność dostarczania usług w całej sieci oraz zwiększa bezpieczeństwo jej funkcjonowania.
  Urządzenia dostarczone przez wykonawcę muszą być fabrycznie nowe, o dacie produkcji nie starszej niż 6 miesięcy, pochodzące z najnowszej serii produkcyjnej.

2.1 SCHEMAT LOGICZNY

Logicznie schemat sieci składać się będzie ze szkieletu, który będzie realizować usługi transportowe za pomocą technologii MPLS. W sieci MPLS możemy wyróżnić dwa typy urządzeń: transportowe (P – Provider Router) oraz dystrybucyjne (PE – Provider Edge). Ze względu na modularność zaproponowanych urządzeń wszystkie węzły szkieletowe mogą pełnić zarówno funkcje transportowe (P) jak i brzegowe (PE). Ze względu na koszt portu najefektywniejszym rozwiązaniem jest terminowanie usługi klienta na urządzeniu dystrybucyjnym i dlatego najwięcej oszczędności przynosi logiczne odseparowanie funkcjonalność urządzenia szkieletowego i urządzenia brzegowego. Urządzenia szkieletowe pełnią więc w takim modelu wyłącznie funkcje transportowe (P). Połączenia pomiędzy urządzeniami szkieletowymi zostaną zrealizowane z prędkością 10 Gigabitów/sekundę. Również połączenia pomiędzy routerem szkieletowym, a przełącznikiem agregującym zrealizowane będą z prędkością 10Gbps. Natomiast każde połączenie od węzłów agregujących do dystrybucyjnych oferuje przepływność 1 lub 2 Gb/s. Poniższy rysunek przedstawia schemat logiczny sieci:

Rysunek 1 Schemat logiczny sieci



LEGENDA:

- Węzeł szkieletowy
- Węzeł agregujący
- Węzeł dystrybucyjny (zakończenie w budynku)
- Połączenie 10 GbE oraz nadmiarowe 1GbE
- Połączenie 1 GbE

GEOMAR S.A. Ul. Piotra Skargi 23 70-487 Szczecin			Podpis
	Opracował:	Mgr inż.. Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu: Dąbrowa Górnicza	Temat: ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA		
Rodzaj inwestycji: Liniowy			
Przedmiot rysunku: Schemat logiczny sieci			

2.2 SCHEMAT POŁĄCZEŃ POMIĘDZY WĘZŁAMI SIECI

W projektowanej sieci fizycznym medium transmisyjnym jest światłowód jednomodowy. Jest to obecnie najczęściej stosowane medium w nowo budowanych sieciach. Przyczyną takiej popularności jest bardzo duża przepływność, z możliwością jej łatwego zwiększania bez konieczności wymiany medium transmisyjnego oraz niska tłumienność. Przy zastosowaniu dodatkowych technik takich jak gęste zwielokrotnianie długości fali (DWDM) można uzyskiwać przepływności rządu Terabajtów na pojedynczej parze włókien. Dodatkową ich zaletą jest odporność na zakłócenia pochodzące z zewnątrz, znacznie wyższy poziom bezpieczeństwa transmitowanych danych w porównaniu do medium miedzianego oraz wysoka trwałość..

Do połączenia każdych dwóch urządzeń aktywnych sieci zostanie wykorzystana para włókien. Węzły szkieletowe zostaną połączone w pierścień, natomiast wszystkie węzły użytkownika w topologii gwiazdy dołączone do nadrzędnego dla nich węzła szkieletowego lub dystrybucyjnego. Przynależność węzłów użytkownika do poszczególnych węzłów szkieletowych przedstawia poniższa tabela:

Legenda:

Pogrubione + deseń – Węzeł szkieletowy,
Pogrubienie – Węzeł agregujący,
Cyfra w polu grupa – podłączenie do węzła szkieletowego,
Cyfra +"a" w polu grupa – podłączenie do węzła agregującego,

nr CPE	Nazwa CPE	Dzielnica	ADRES	TYP WĘZŁA	Grupa
1	**Urząd Miejski,**	**GOŁONÓG**	**Graniczna 21**	**Szkieletowy**	**1**
1N	Komenda Straży Miejskiej	GOŁONÓG	Graniczna 21		1
28	Techniczne Zakłady Naukowe	CENTRUM	Stanisława Łańcuckiego 10		1
32	**Zespół Szkół Ogólnokształcących nr 2**	**CENTRUM**	**Bolesława Prusa 3**	**Agregujący**	**1**
39	Zespół Szkół Ekonomicznych	GOŁONÓG	Al. Piłsudskiego 5		1
40	Zespół Szkół nr 3	GOŁONÓG	Morcinka		1a
46	Szkoła Podstawowa nr 18	GOŁONÓG	Al. Piłsudskiego 73		1
76	Miejska Biblioteka Publiczna filia nr 3	GOŁONÓG	Wybickiego 3		1a
42	Zespół Szkół nr 4	ŁĘKNICE	Łęknice 35		2
44	**Szkoła Podstawowa nr 11**	**GOŁONÓG**	**Al. Piłsudskiego 103**	**Szkieletowy**	**2**
66	**Gimnazjum nr 9**	**ZĄBKOWICE**	**Al. Zwycięstwa 44**	**Agregujący**	2
20N	Specjalny ośrodek szkolno-wychowawczy dla dzieci i młodzieży	ZĄBKOWICE	Swobodna 59		2
67	Szkoła Podstawowa nr 21	ZĄBKOWICE	Gospodarcza 1		2a
68	Szkoła Podstawowa nr 31	ZĄBKOWICE	Zwycięstwa		2a
73	DKZ - Dom Kultury Ząbkowice	ZĄBKOWICE	Chemiczna 2		2a
75	Miejska Biblioteka Publiczna filia nr 20	ŁĘKNICE	Topolowa 32		2

nr CPE	Nazwa CPE	Dzielnica	ADRES	TYP WĘZŁA	Grupa
72	Świetlica Środowiskowa	ANTONIÓW	Spacerowa 4		2a
70	Miejska Biblioteka Publiczna filia nr 2 (w DKZ)	ZĄBKOWICE	Chemiczna 2		2a
27	Wielofunkcyjna Placówka Opiekuńczo-Wychowawcza		Jasna 29		2a
69	Ochotnicza Straż Pożarna	ZĄBKOWICE	Szosowa 13		2a
71	Miejska Biblioteka Publiczna filia nr 10	ZĄBKOWICE	Al. Zwycięstwa 91		2a
12	**MZBM, Dyrekcja**	**GOŁONÓG**	**Tysiąclecia 20**	**Szkieletowy**	**3**
31	Zespół Szkół nr 2	CENTRUM	Al.Piłsudskiego 24		3
41	Zespół Szkół Plastycznych	GOŁONÓG	Kosmonautów 8		3
45	Szkoła Podstawowa nr 12	GOŁONÓG	Tysiąclecia 25		3
62	Szkoła Podstawowa nr 17	STRZEMIESZYCE	Ofiar Katynia 76		3a
60	Zespół Szkół Ogólnokształcących nr 3	STRZEMIESZYCE	Obrońców Pokoju 7		3a
61	Szkoła Podstawowa nr 5	STRZEMIESZYCE	Strzemieszycka 390		3a
63	**Miejska Biblioteka Publiczna filia nr 8**	**STRZEMIESZYCE**	**Ofiar Katynia 93**	**Agregujący**	**3**
64	Ochotnicza Straż Pożarna	STRZEMIESZYCE	Strzemieszycka 393a		3a
4	Miejskie Muzeum "Sztygarka"	CENTRUM	Legionów Polskich 69		4
13	Szpital Specjalistyczny im. Sz. Starkiewicza	CENTRUM	Szpitalna 13		4
16	Powiatowy Urząd Pracy	CENTRUM	Sobieskiego 12		4a
22	Zespół Szkół Muzycznych	CENTRUM	Dąbskiego 17		4a
26	Liceum - V Liceum Ogólnokształcące	CENTRUM	Kazimierza Czapińskiego 8		4
33	Przedszkole	CENTRUM	Mireckiego 28		4a
35	Zespół Szkół Sportowych	CENTRUM	Chopina 34		4a
37	**Zespół Szkół Zawodowych SZTYGARKA**	**CENTRUM**	**Legionów Polskich 39**	**Szkieletowy**	**4**
48	Szkoła Podstawowa nr 3	CENTRUM	Mireckiego 1		4a
49	Zespół Szkół nr 7	CENTRUM	Jaworowa 6		4
78	**Miejska Biblioteka Publiczna filia nr 18**	**CENTRUM**	**Legionów Polskich 131**	**Agregujący**	**4**
7	Centrum Sportu i Rekreacji - Hala Widowiskowo - Sportowa	CENTRUM	Al. Róż 3		5
8	**Miejska Biblioteka Publiczna (Dyrekcja)**	**CENTRUM**	**Kościuszki 25**	**Szkieletowy**	**5**
18	Dom Pomocy Społecznej	CENTRUM	Norwida 1		5a
23	Gimnazjum nr 4	CENTRUM	Wyspiańskiego 1		5a
25	Liceum - II Liceum Ogólnokształcące	CENTRUM	Górnicza 17		5
29	Miejski Ośrodek Pomocy Społecznej	CENTRUM	Wojska Polskiego 52		5a
36	Zespół Szkół Technicznych	CENTRUM	Królowej Jadwigi 12		5
nr	**Nazwa CPE**	**Dzielnica**	**ADRES**	**TYP WĘZŁA**	**Grupa**

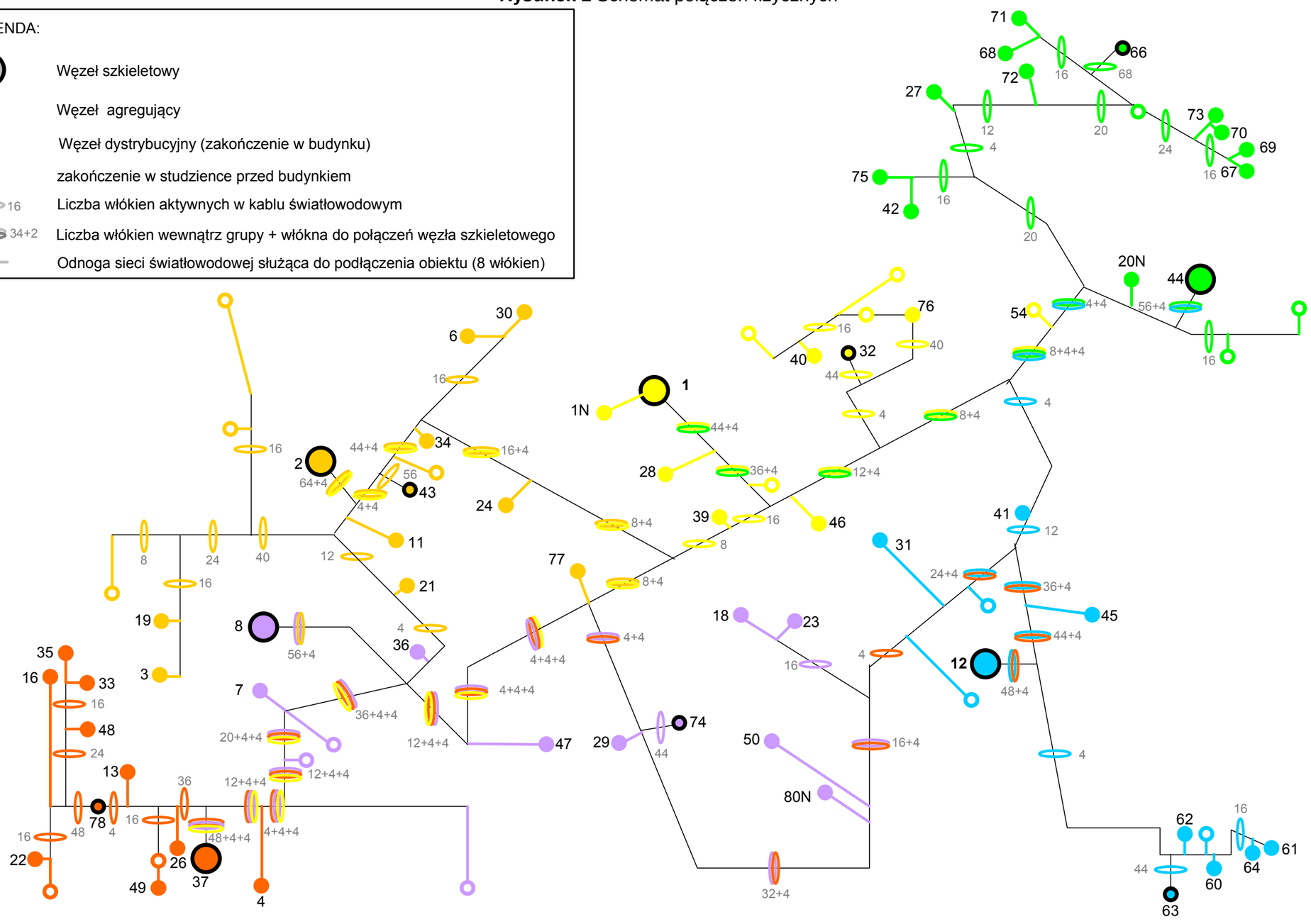
CPE					
47	Szkoła Podstawowa nr 20	CENTRUM	Adamieckiego 12		5
50	Szkoła Podstawowa nr 8	CENTRUM	Krasińskiego 34		5a
80N	Oddział Psychiatryczny Szpitala Specjalistycznego im. Starkiewicza	CENTRUM	Krasińskiego 43		5
74	**Miejska Biblioteka Publiczna filia nr 1**	**CENTRUM**	**Wojska Polskiego 43**	**Agregujący**	**5**
2	**Pałac Kultury Zagłębia**	**CENTRUM**	**Plac Wolności 1**	**Szkieletowy**	**6**
3	Młodzieżowy Ośrodek Pracy Twórczej	CENTRUM	3-go Maja 30		6
6	Centrum Sportu i Rekreacji	CENTRUM	Konopnickiej 29		6a
11	Miejski Ośrodek Pomocy Społecznej	CENTRUM	Skibińskiego 1		6
19	Poradnia Psychologiczno-Pedagogiczna	CENTRUM	3-go Maja 22		6
21	Gimnazjum nr 1	CENTRUM	Królowej Jadwigi 11		6
24	Liceum - I Liceum Ogólnokształcące	CENTRUM	Kopernika 40		6a
30	Zespół Szkół nr 1	CENTRUM	Konopnickiej 56		6a
34	Zespół Szkół Specjalnych nr 6	CENTRUM	Konopnickiej 36		6a
43	**Szkoła Podstawowa nr 10**	**CENTRUM**	**Górników Redenu 4**	**Agregujący**	**6**
77	Miejska Biblioteka Publiczna filia nr 4	CENTRUM	Reymonta 14		6a

Tabela wykaz węzłów szkieletowych i agregujących z podziałem na grupy

Rysunek 2 Schemat połączeń fizycznych

LEGENDA:

- Węzeł szkieletowy
- Węzeł agregujący
- Węzeł dystrybucyjny (zakończenie w budynku)
- zakończenie w studzience przed budynkiem
- 16 — Liczba włókien aktywnych w kablu światłowodowym
- 34+2 — Liczba włókien wewnątrz grupy + włókna do połączeń węzła szkieletowego
- Odnoga sieci światłowodowej służąca do podłączenia obiektu (8 włókien)



GEOMAR S.A. ul. Piotra Skargi 23 70-487 SZCZECIN			Podpis
	Opracował:	mgr inż. Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu: Dąbrowa Górnicza	Temat: ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM – DĄBROWA GÓRNICZA		
Rodzaj inwestycji: Liniowy			
Przedmiot rysunku: Schemat połączeń fizycznych			

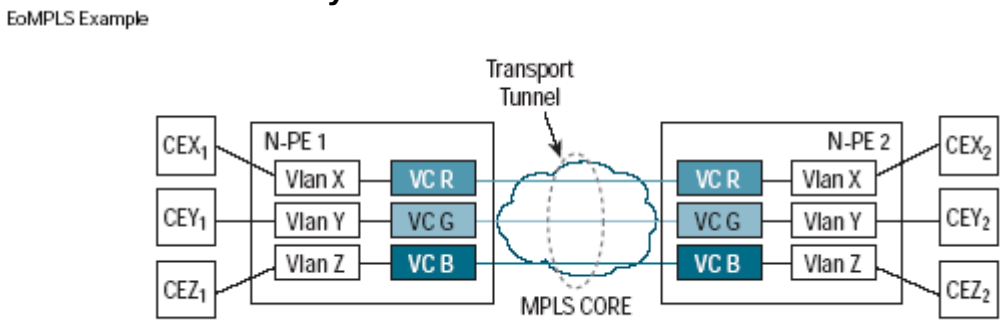
2.3 ARCHITEKTURA SIECI – TECHNOLOGIA

Sieć miejska został zaprojektowana w oparciu o routery i przełączniki MPLS. Technologia ta została wybrana ponieważ wykorzystuje pełną gamę mechanizmów, zarówno przenoszenia warstwy 2 (w połączeniach poin-to-point, point-to-multipoint oraz mesh) jak i warstwy 3 tzw. VPN L3.

Transmisja danych w MPLS i jej rodzaje:

- **MPLS VLL** (Virtual Leased Line) używany do transmisji ramek Ethernet poprzez sieć MPLS w połączeniach punkt-punkt. Ramka Ethernet odebrana przez router brzegowy (PE) zostaje obudowana w pakiet MPLS i przetransmitowana poprzez sieć. Z transmisją tą związane są dwa rodzaje znaczników (labeli). Jeden reprezentuje tunel (tunnel label), który ma być użyty przez pakiet, drugi reprezentuje ścieżkę MPLS (VC label), przez którą ma nastąpić transmisja.

Rysunek 3 MPLS VLL

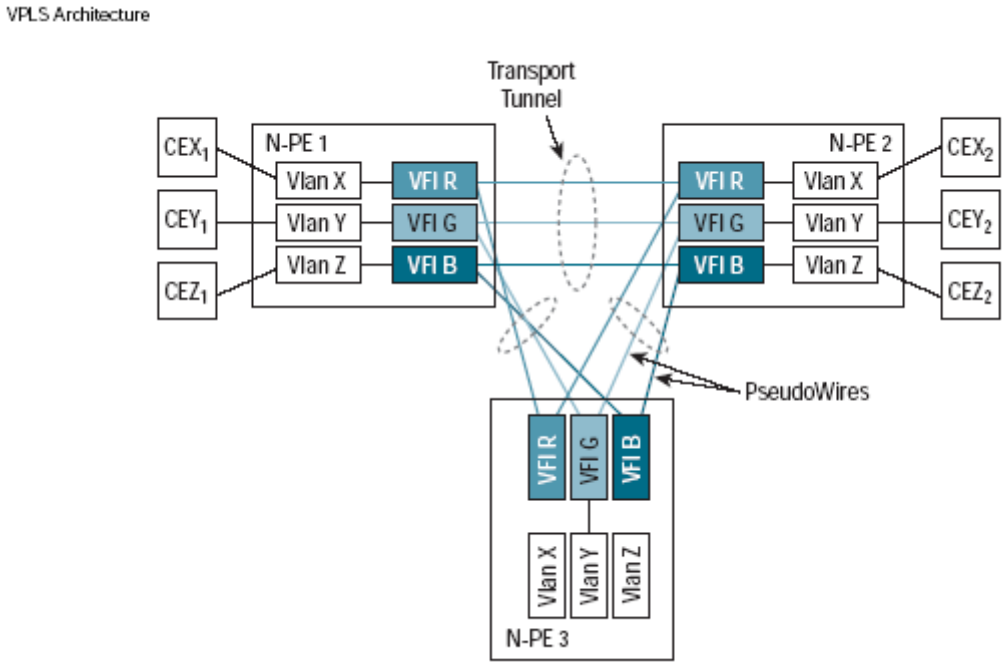


VLL - rodzaje transportu:

a) 802.1Q VLAN to 802.1Q VLAN (VLAN mode);
b) Port Ethernet do portu Ethernet (port mode);
c) 802.1Q do portu Ethernet;

- **VPLS** (Virtual Private LAN Service) zwiększa funkcjonalność VLL poprzez możliwość zestawiania tuneli punkt - wielopunkt poprzez sieć MPLS. Funkcjonalność VPLS umożliwia emulację sieci LAN oraz zestawianie połączeń typu każdy z każdym (full meshed), które są realizowana za pomocą wirtualnych kanałów (pseudo-wires).

Rysunek 4 MPLS VPLS



- **BGP/MPLS VPN** jest sposobem budowania sieci VPN opartych o routery PE VPN. Metoda BGP/MPLS, jest wykorzystywana do dystrybucji poprzez BGP informacji o osiągalności adresów IP pomiędzy oddziałami należącymi do tej samej sieci VPN. Każdy router PE posiada tabelę VRF (VPN Routing and Forwarding – routing i przekazywanie dla VPN) dla każdego VPN, do którego PE jest przyłączony. Każdy interfejs łączący klienta z dostawcą, czyli PE z CE, jest skojarzony z jedną tabelą VRF. Jeśli jakikolwiek pakiet przyjdzie od urządzenia klienta (nazywanego tu brzegiem klienta CE - Customer Edge), to jego adres przeznaczenia jest wyszukiwany w skojarzonej tabeli VRF, by określić jak pakiet ma byś routowany przez szkielet. Tabela VRF w routerze PE jest budowana na podstawie informacji o trasach nauczonych od urządzeń brzegu klienta CE. Metoda BGP/MPLS nie standaryzuje żadnej konkretnej metody nauki tras, PE może nauczyć się tras stosując zarówno protokół dynamiczny routingu, jakim jest np., BGP lub OSPF (Open Shortest Path First) albo przez konfigurację tras statycznych. PE muszą także nauczyć się tras od innych routerów PE w tym samym VPN.

Ze względu na upowszechnienie się rozwiązań opartych o MPLS, wszystkie urządzenia sieci miejskiej (szkieletowe, agregujące i dystrybucyjne) będą wspierać tą technologię, przy czym:
-urządzenia szkieletowe będą pełnić rolę urządzeń typu P czyli będą przełączać wydajnie i niezawodnie ruch MPLS
-urządzenia agregujące i dystrybucyjne będa pełnić rolę typu PE czyli będą terminować usługi VPN i mapować ruch z jednostek na poszczególne usługi.
Dzięki temu dostęp do nowoczesnych i bezpiecznych usług transporotwych będzie rozproszony po całym mieście co powoli łatwiej wdrażać kolejne usługi i realizować ideę „inteligentnych” miast.

2.4 PODSIECI I USŁUGI

Zaprojektowaną sieć musi cechować duża elastyczność i różnorodność oferowanych usług. Dzięki pełnej gamie mechanizmów MPLS można tworzyć połączenia w warstwie drugiej jak i trzeciej. W sieci miejskiej należy stworzyć wydzielone podsieci, które będą umożliwiały łączność dla różnego rodzaju usług oraz instytucji. Wymagane jest aby stworzone zostały następujące podsieci:

L.p.	Nazwa sieć	Zastosowanie	Dostępność
1	Internet	Zabezpieczony centralnie dostęp do Internetu	Wszystkie węzły
2	Monitoring	Monitoring wizyjny miasta	Wskazane węzły dystrybucyjne i agregujące
3	CZK	Sieć na potrzeby Centrum Zarządzania Kryzysowego	Wskazane węzły dystrybucyjne i agregujące
4	Zarządzanie	Zarządzanie urządzeniami aktywnymi sieci	Węzły szkieletowe dystrybucyjne oraz agregujące

Pozostałe sieci na potrzeby :

- wymiany informacji (połączenie sieci lokalnych) jednostek miasta, innych urzędów i placówek użyteczności publicznej,
- systemu komunikacji głosowej
- aplikacji związanych z systemem karty miejskiej (e-karta),
- aplikacji związanych z edukacją np. dostęp do zasobów bibliotek,
- zarządzania transportem i ruchem drogowym np. sterowanie sygnalizacją świetlną na skrzyżowaniach,
- dostępu do usług telemedycznych.

I ich osiągalność w poszczególnych węzłach zostanie ustalona na etapie projektu wykonawczego.

Węzeł szkieletowy umiejscowiony w Urzędzie Miejskim będzie pełnił także funkcje centrum zarządzania. Oprócz urządzenia szkieletowego zostaną tam zainstalowane serwery, które będą pełnić wyznaczone funkcje:

- Zarządzania siecią;

- Serwer WWW, DNS oraz FTP;

- Przechowywanie informacji o ruchu internetowym;

Centrum Zarządzania będzie także miejscem styku sieci z Internetem. W tej lokalizacji należy zainstalować urządzenie, które posiada funkcjonalność firewall i VPN. Pozwoli ono zabezpieczyć dostęp do Internetu oraz umożliwi archiwizacje na dedykowanym serwerze informacji o ruchu internetowym. Dzięki funkcjonalności VPN będzie możliwy zdalny, bezpieczny dostęp do zasobów wewnątrz sieci poprzez szyfrowany tunel.

2.5 WYMAGANIA

Jeżeli uruchomienie którejkolwiek z przedstawianych w projekcie funkcjonalności wymaga dodatkowej licencji wykonawca zobowiązany jest dostarczyć je wraz z oferowanym sprzętem. Zastosowane rozwiązanie sprzętowe nie może w żaden sposób oganiczać tych funkcjonalności.

2.5.1 WĘZŁY SZKIELETOWE

2.5.1.1 Wymagania techniczne dla pomieszczeń

- Pomieszczenie suche, o murowanych ścianach, stropie i posadzce, wolne od kurzu i pyłu. Preferowana lokalizacja w podziemiu budynku przy ścianie zewnętrznej, z nieutrudnionym dostępem umożliwiającym transport szaf teleinformatycznych i wyposażenia o gabarytach SxGxW 0.8x1.0x2.2m.
- Położenie pomieszczenia powinno być dogodne dla wprowadzenia podziemnych kabli sieci szkieletowej i dystrybucyjnej, jak i kabli dystrybucji transmisji w budynku, o ile zachodzi taka potrzeba.
- Wielkość pomieszczenia powinna umożliwiać instalację:
  - szafy teleinformatycznej 42U o wym. SxGxW 0.8x1.0x2.2m z pozostawieniem miejsca na swobodny dostęp dookoła, w tym min. 1 m od przodu,
  - baterii siłowni i UPS na stojakach,
  - zapasu kabli światłowodowych,
  - koryt kablowych ponad szafami.
- Jeżeli pomieszczenie posiada okna, muszą być one szczelne, sprawne i zabezpieczone przed wtargnięciem z zewnątrz.
- Temperatura w pomieszczeniu nie może spadać poniżej 0°C o żadnej porze roku, chyba że zastosowany zostanie klimatyzator z odwracaniem pracy.
- Musi istnieć możliwość zainstalowania stałego klimatyzatora z chłodnicą zewnętrzną przeznaczonego do pracy ciągłej, o wydajności chłodniczej min. 4.0 kW.
- Posadzka pomieszczenia powinna wytrzymywać obciążenie do 400 kG/m^2.
- Należy zaprojektować po dwa ciągi metalowych koryt kablowych podwieszonych pod sufitem umożliwiających niezależne prowadzenie przewodów zasilających i uziomów oraz sygnałowych.
- W pomieszczeniu powinien znajdować się punkt przyłączeniowy pozwalający na dołączenie uziemień z szaf teletechnicznych
- Do pomieszczenie powinna być doprowadzona sieć energetyczna 230/400V 50Hz, z rozdzielnicą umożliwiająca zasilanie z oddzielnych obwodów siłowni 48VDC, zasilacza UPS, oświetlenia górnego oraz kilku gniazd ściennych, z wyłącznikiem różnicowoprądowym tylko w tym ostatnim obwodzie. Przewidywaną moc potrzebną do zasilania projektowanych urządzeń należy założyć z co najmniej 35% rezerwą.
- W pomieszczeniu powinna zostać zainstalowana jedna szafa teleinformatyczna j/n, którą należy uziemić. Szafa ma pomieścić urządzenia siłowni i ew. UPS z pozostawieniem baterii na zewnątrz szafy.

Szafa teleinformatyczna	**1 szt.**
Wysokość	42 U
Głębokość	1000 mm
Szerokość	800 mm
Drzwi przednie	Szklane (szkło hartowane) z dwoma zamkami
Inne	Dach pełny
Inne	Trzy pary belek nośnych w rozstawie 19’
Inne	Szkielet na cokole z wysuwaną ramą wsporczą
Inne	Drzwi tylne blaszane pełne
Inne	Osłony boczne perforowane – demontowane
Inne	Listwa zasilająca 5-gniazd z bolcem 2P+Z, wyłącznik podświetlany, zabezpieczenie przepięciowe z filtrem sieciowym – **2 szt.**
Inne	Panel wentylacyjny mocowany na belkach nośnych sterowany za pomocą termostatu 2-wentylatory
Inne	Moduł zdalnej kontroli temperatury wraz z sygnalizacją otwarcia drzwi szafy.

- W instalowanej szafie od góry należy zamontować przełącznice optyczne za złączami LC/PC, duplex, z magazynami, na których mają być zakończone tory światłowodowe sieci szkieletowej i dystrybucyjnej.

2.5.1.2 Wymagania techniczne dla urządzeń

Router szkieletowy dla obiektów nr 1 oraz nr 37 musi być wyposażony w następujące interfejsy i moduły:

- min. 4 porty 10 Gigabit Ethernet dla wkładek optycznych XFP, SFP+ lub równoważnych - należy dostarczyć 4 moduły optyczne typu LR przeznaczone do pracy ze światłowodem jednomodowym na dystansie do 10km,
- min. 20 portów Gigabit Ethernet dla wkładek optycznych SFP lub równoważnych - należy dostarczyć 6 modułów optycznych przeznaczonych do pracy ze światłowodem jednomodowym na dystansie do 10km, 1 wkładka optyczna ze złączem RJ45 przeznaczonym do pracy z kablem miedzianym UTP 1000BASE-T
- dwa moduły zarządzająco-kontrolne,
- ilość matryc przełączających spełniającą wymogi specyfikacji technicznej (min. dwie),
- redundantne zasilacze i wentylatory
- urządzenie modularne – dostępne min. 6 slotów do instalacji kart zarządzających i liniowych.
- min. 2 wolne sloty do obsadzenia kartami liniowymi.
- obsługa interfejsów 1GE, 10GE, 40GE, 100GE,
- wsparcie dla interfejsów 100GE z optyką CFP LR4 oraz SR10

Wymagania techniczne dla routerów szkieletowych dla obiektów nr 1, 37:

1. Obudowa przeznaczona do instalacji w szafie telekomunikacyjnej rack 19”.
2. Architektura urządzenia:
    a. rozproszone przetwarzanie pakietów – logicznie lub fizycznie rozdzielone funkcje kontrolne (routing engine, control plane) od przełączania (forwarding engine, data plane) ruchu,
    b. karty liniowe muszą mieć możliwość autonomicznego przełączania ruchu, bez udziału warstwy zarządzającej,
    c. redundancja krytycznych elementów urządzenia (karty zarządzające, matryca przełączająca, zasilacze, wentylatory) – awaria któregokolwiek z nich nie może spowodować ograniczenia wydajności urządzenia (poniżej parametrów opisanych w punkcie trzecim), należy dostarczyć odpowiednią ilość poszczególnych elementów,
    d. wymiana wszystkich modułów w trakcie pracy urządzenia bez wpływu na inne komponenty (hot swap),
    e. zasilanie 230V AC.
    f. urządzenie modularne
3. Wydajność i niezawodność urządzenia:
    a. min. 200 Gbps (full duplex, lub 400Gbps half duplex) per slot – dostępne w dniu składania oferty, awaria jednej z matryc przełączających nie może powodować spadku wydajności poniżej 200 Gbps (full duplex, lub 400Gbps half duplex),
    b. możliwość obsługi min. 2 000 000 tras IPv4,
    c. min. 1 000 000 adresów MAC,
    d. możliwość transmisji pojedynczych strumieni IP (unicast lub multicast) z przepływnością na poziomie min. 10 Gbps per strumień,
    e. min. 6GB pamięci DRAM,
    f. min. 32GB nieulotnej pamięci flash rozdzielonej na 2 nośniki na podstawowy i zapasowy obraz systemu operacyjnego,
    g. wszystkie oferowane porty muszą pracować z pełną wydajnością łącza, w przypadku kart z nadsubskrybcją należy zaoferować odpowiednio większą liczbę portów.
4. Obsługiwane interfejsy:
    a. 100 Gigabit Ethernet LR4
    b. 40 Gigabit Ethernet LR4
    c. 10 Gigabit Ethernet LR, SR, ER, ZR,
    d. 10 Gigabit Ethernet DWDM, DWDM z laserem o zmiennej częstotliwości fal,
    e. 1 Gigabit Ethernet T, SX, LX, ZX, BX
    f. duża możliwa gęstość portów w ramach jednego routera:
        - możliwość podłączenia min. 8 portów 100GE line rate,

- możliwość podłączenia min. 96 interfejsów typu 10GE line rate,

g. wszystkie interfejsy liniowe muszą mieć styk definiowany przez moduły typu SFP, XFP, SFP+, CFP lub podobne.

5. Funkcjonalności przełączania MPLS dla urządzenia pracującego jako LSR (P):
   a. obsługa LDP, T-LDP,
   b. obsługa VPLS i H-VPLS,
   c. obsługa enkapsulacji VPWS / EoMPLS,
   d. MPLS TE (z mechanizmami ochrony ścieżki), RSVP,
   e. MPLS FRR, redundancja pseudowire,
6. Możliwość uruchomienia funkcjonalności:
   a) MPLS L3 VPN (IPv4 i IPv6),
   b) MVPN (MPLS multicast VPN),
   c) Carrier supporting Carrier (CsC).

   Zastosowane rozwiązanie sprzętowe nie może w żaden sposób oganiczać tych funkcjonalności i musi umożliwiać zakup odpowiednich licencji w przyszłej rozbudowie systemu.
7. Funkcjonalności routingu IP:
   a. obsługa IPv4 (statyczny, BGP, OSPF, IS-IS),
   b. obsługa IPv6 (statyczny, OSPFv3, BGP, IS-IS),
   c. multicast IPv4 (IGMPv2/3, PIM SM, SSM, MSDP),
   d. multicast IPv6 (MLD, PIM SM, SSM),
   e. BGP Prefix Independent Convergence
   f. obsługa Bidirectional Forwarding Detection (BFD) dla IPv4 oraz IPv6 min. dla OSPFv2, OSPFv3, BGP, MPLS-TE, IS-IS, PIM, tras statycznych
   g. obsługa NonStop Forwarding (lub równoważny umożliwiający przełączenie się na rezerwowy control plane" bez utraty połączeń z sąsiednimi węzłami)dla BGP, OSPF, IS-IS, LDP, multicast,
   h. obsługa VRRP (IPv4 i IPv6),
   i. obsługa IP Fast Reroute.
8. Funkcjonalności przełączania Ethernet:
   a. obsługa 802.1ah,
   b. obsługa 802.1ad, QinQ,
   c. obsługa 802.1Q,
   d. obsługa agregacji 802.3ad (LACP), także dla interfejsów umieszczonych w różnych urządzeniach (multi-chassis LAG lub równoważne),
   e. mapowanie (translacja) tagów 802.1Q – 1:1, 1:2, 2:1, 2:2,
   f. znaczniki VLAN muszą mieć znaczenie lokalne dla interfejsu (Local VLAN Significance),

g. możliwość ograniczania liczby adresów MAC per interfejs logiczny lub instancję usługową,

h. obsługa tunelowania protokołów warstwy drugiej,

i. obsługa ramek Jumbo (min. 9000B).

9. Funkcjonalności bezpieczeństwa sieciowego:

a. listy kontroli dostępu (ACL) L2 i L3 (IPv4 i IPv6) – wymagane liczniki pakietów obsługujące poszczególne wpisy list,

b. DHCP snooping, DHCP relay,

c. Unicast Reverse Path Forwarding (uRPF),

d. mechanizmy ochrony przed sztormami ruchu rozgłoszeniowego i multicast (broadcast/multicast storm),

e. mechanizmy bezpieczeństwa na bazie adresów MAC dla EVC,

f. mechanizmy ochrony warstwy kontrolnej urządzenia przed atakami kierowanymi do niego (ograniczanie ruchu kierowanego do urządzenia),

g. obsługa autoryzacji administratorów za pośrednictwem RADIUS.

10. funkcjonalności zapewnienia jakości ruchu (QoS):

a. obsługa mechanizmów QoS (klasyfikacja, kolejkowanie, oznaczanie, policing, shaping) per port/VLAN,

b. mechanizmy zarządzania jakością na poziomie matrycy przełączającej (zabezpieczenie przed wystąpieniem zjawiska HoLB i QoS oversubscription na poziomie matrycy, np. przez wewnętrzne kolejkowanie ruchu),

c. możliwość klasyfikacji ruchu w oparciu o: MPLS EXP, IP DSCP, VLAN (min. 2 poziomy zagnieżdżenia), adresy MAC i IP, protokół

d. min. 8 kolejek per port.

11. Funkcjonalności związane z zarządzaniem urządzeniem:

a. modularny system operacyjny:

- oddzielne procesy obsługujące poszczególne grupy funkcjonalne (protokoły routingu, zarządzania itp.) ,
- możliwość aktualizacji wybranych grup funkcjonalnych za pomocą poprawek (patch-y) dostępnych na stronie producenta bez przerw w działaniu urządzenia lub innych grup funkcjonalnych,
- możliwość restartu poszczególnych procesów, w szczególności poszczególne protokoły routingu muszą być obsługiwane przez niezależne procesy, awaria lub restart jednego z nich nie może wpływać na funkcjonowanie pozostałych,
- minimum dwustopniowe zatwierdzanie komend (wprowadzenie komendy, aktywacja konfiguracji),
- możliwość cofnięcia zmian konfiguracji,
- możliwość tworzenia punktów kontrolnych konfiguracji i ich odtwarzania,

- obsługa tworzenia i przywracania kopii zapasowych konfiguracji systemu,

b. obsługa E-OAM (802.1ag, 802.3ah, Y.1731 DMM),

c. obsługa krótkich pakietów E-OAM i BFD przez osobny, dedykowany układ sprzętowy na każdej karcie liniowej,

d. obsługa MPLS OAM (LSP ping, LSP traceroute),

e. możliwość kopiowania ruchu z określonego portu/VLANu na inny port/VLAN urządzenia (mirroring),

f. funkcjonalność monitorowania jakości usług na bazie aktywnych próbników ruchu – pomiar min. dostępności, opóźnienia, jego zmian, strat pakietów,

g. sprzętowa obsługa Jflow/ NetFlow lub równoważne dla IPv4, IPv6, MPLS – export min. 40 tysięcy flow'ów na sekundę per karta liniowa oraz lokalne składowanie min. 1.000.000 wpisów na karcie linowej (dopuszcza się realizację sprzętową na każdej karcie liniowej lub w postaci redundantnych kart usługowych),

h. interfejsy muszą obsługiwać funkcjonalność zdalnej diagnostyki połączeń optycznych (Digital Diagnostics Monitoring, Digital Optical Monitoring lub równoważne),

i. możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej - konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona,

j. możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów,

k. zarządzanie przez CLI (konsola szeregowa, SSHv2), SNMPv3, XML API,

l. obsługa syslog,

m. dedykowany port szeregowy na potrzeby dostępu do konsoli urządzenia lub zdalnego zarządzania (modem),

n. port Ethernet do celów zarządzania urządzeniem,

o. możliwość rozszerzenia funkcjonalności o obsługę monitorowania strumieni wideo (min. 1000 strumieni – straty pakietów, zmiany opóźnień, MDI MLR/DF zgodnie z RFC 4445),

12. Urządzenie musi posiadać certyfikaty Metro Ethernet Forum - MEF9 i MEF14 oraz CE2.0 co najmniej w obszarach: E-Line, oraz E-LAN.

Routery szkieletowe dla obiektów nr 2, 8,12, 44 muszą być wyposażone w następujące interfejsy:

- min. 4 porty 10 Gigabit Ethernet dla wkładek optycznych XFP, SFP+ lub równoważnych - należy dostarczyć 3 moduły optyczne typu LR przeznaczone do pracy ze światłowodem jednomodowym na dystansie do 10km,

- min. 20 portów Gigabit Ethernet dla wkładek optycznych SFP lub równoważnych - należy dostarczyć 6 modułów optycznych przeznaczone do pracy ze światłowodem jednomodowym na dystansie do 10km, 1 wkładka optyczna przeznaczona do pracy z kablem miedzianym UTP 1000BASE-T
- redundantne zasilacze i wentylatory
- min. 1 wolny slot do obsadzenia kartami liniowymi.
- obsługa interfejsów 1GE, 10GE, 40GE

Wymagania techniczne dla przełączników szkieletowych dla obiektów nr 2,8,12,44:

1. Obudowa przeznaczona do instalacji w szafie telekomunikacyjnej rack 19”.
2. Architektura urządzenia:
    a. rozproszone przetwarzanie pakietów – logicznie lub fizycznie rozdzielone funkcje kontrolne (routing engine, control plane) od przełączania (forwarding engine, data plane) ruchu,
    b. wymiana wszystkich modułów w trakcie pracy urządzenia bez wpływu na inne komponenty (hot swap),
    c. redundatne zasilanie 230V AC.
    d. urządzenie modularne
3. Wydajność i niezawodność urządzenia:
    a. min. 120 Gbps (full duplex, lub 240Gbps half duplex)
    b. możliwość obsługi min. 2 000 000 tras IPv4,
    c. min. 1 000 000 adresów MAC,
    d. możliwość transmisji pojedynczych strumieni IP (unicast lub multicast) z przepływnością na poziomie min. 10 Gbps per strumień,
    e. min. 6GB pamięci DRAM,
4. wszystkie oferowane porty muszą pracować z pełną wydajnością łącza,
5. Obsługiwane interfejsy:
    a. 40 Gigabit Ethernet LR4
    b. 10 Gigabit Ethernet LR, SR, ER, ZR,
    c. 10 Gigabit Ethernet DWDM, DWDM z laserem o zmiennej częstotliwości fal,
    d. 1 Gigabit Ethernet T, SX, LX, ZX, BX
    e. wszystkie interfejsy liniowe muszą mieć styk definiowany przez moduły typu SFP, XFP, SFP+, CFP lub podobne.
6. Funkcjonalności przełączania MPLS dla urządzenia pracującego jako LSR (P)::
    a. obsługa LDP, T-LDP,
    b. obsługa VPLS i H-VPLS,
    c. obsługa enkapsulacji VPWS / EoMPLS,

d. MPLS TE (z mechanizmami ochrony ścieżki), RSVP,
e. MPLS FRR, redundancja pseudowire,

7. Możliwość uruchomienia funkcjonalności:
   a) MPLS L3 VPN (IPv4 i IPv6),
   b) MVPN (MPLS multicast VPN),
   c) Carrier supporting Carrier (CsC).

   Zastosowane rozwiązanie sprzętowe nie może w żaden sposób oganiczać tych funkcjonalności i musi umożliwiać zakup odpowiednich licencji w przyszłej rozbudowie systemu.
8. Funkcjonalności routingu IP:
   a. obsługa IPv4 (statyczny, BGP, OSPF, IS-IS),
   b. obsługa IPv6 (statyczny, OSPFv3, BGP, IS-IS),
   c. multicast IPv4 (IGMPv2/3, PIM SM, SSM, MSDP),
   d. multicast IPv6 (MLD, PIM SM, SSM),
   e. BGP Prefix Independent Convergence
   f. obsługa Bidirectional Forwarding Detection (BFD) dla IPv4 oraz IPv6 min. dla OSPFv2, OSPFv3, BGP, MPLS-TE, IS-IS, PIM, tras statycznych
   g. obsługa NonStop Forwarding (lub równoważny umożliwiający przełączenie się na rezerwowy control plane" bez utraty połączeń z sąsiednimi węzłami) dla BGP, OSPF, IS-IS, LDP, multicast,
   h. obsługa VRRP (IPv4 i IPv6),
   i. obsługa IP Fast Reroute.
9. Funkcjonalności przełączania Ethernet:
   a. obsługa 802.1ah,
   b. obsługa 802.1ad, QinQ,
   c. obsługa 802.1Q,
   d. obsługa agregacji 802.3ad (LACP), także dla interfejsów umieszczonych w różnych urządzeniach (multi-chassis LAG lub równoważne),
   e. mapowanie (translacja) tagów 802.1Q – 1:1, 1:2, 2:1, 2:2,
   f. znaczniki VLAN muszą mieć znaczenie lokalne dla interfejsu (Local VLAN Significance),
   g. możliwość ograniczania liczby adresów MAC per interfejs logiczny lub instancję usługową,
   h. obsługa tunelowania protokołów warstwy drugiej,
   i. obsługa ramek Jumbo (min. 9000B).
10. Funkcjonalności bezpieczeństwa sieciowego:
   a. listy kontroli dostępu (ACL) L2 i L3 (IPv4 i IPv6) – wymagane liczniki pakietów obsługujące poszczególne wpisy list,

b. DHCP snooping, DHCP relay,
c. Unicast Reverse Path Forwarding (uRPF),
d. mechanizmy ochrony przed sztormami ruchu rozgłoszeniowego i multicast (broadcast/multicast storm),
e. mechanizmy bezpieczeństwa na bazie adresów MAC dla EVC,
f. mechanizmy ochrony warstwy kontrolnej urządzenia przed atakami kierowanymi do niego (ograniczanie ruchu kierowanego do urządzenia),
g. obsługa autoryzacji administratorów za pośrednictwem RADIUS.

11. funkcjonalności zapewnienia jakości ruchu (QoS):
    a. obsługa mechanizmów QoS (klasyfikacja, kolejkowanie, oznaczanie, policing, shaping) per port/VLAN,
    b. mechanizmy zarządzania jakością na poziomie matrycy przełączającej (zabezpieczenie przed wystąpieniem zjawiska HoLB i QoS oversubscription na poziomie matrycy, np. przez wewnętrzne kolejkowanie ruchu),
    c. możliwość klasyfikacji ruchu w oparciu o: MPLS EXP, IP DSCP, VLAN (min. 2 poziomy zagnieżdżenia), adresy MAC i IP, protokół
    d. min. 8 kolejek per port.
    e. Hierachiczny QoS na wszystkich portach
12. Funkcjonalności związane z zarządzaniem urządzeniem:
    a. modularny system operacyjny:
        - oddzielne procesy obsługujące poszczególne grupy funkcjonalne (protokoły routingu, zarządzania itp.) ,
        - możliwość aktualizacji wybranych grup funkcjonalnych za pomocą poprawek (patch-y) dostępnych na stronie producenta bez przerw w działaniu urządzenia lub innych grup funkcjonalnych,
        - możliwość restartu poszczególnych procesów, w szczególności poszczególne protokoły routingu muszą być obsługiwane przez niezależne procesy, awaria lub restart jednego z nich nie może wpływać na funkcjonowanie pozostałych,
        - minimum dwustopniowe zatwierdzanie komend (wprowadzenie komendy, aktywacja konfiguracji),
        - możliwość cofnięcia zmian konfiguracji,
        - możliwość tworzenia punktów kontrolnych konfiguracji i ich odtwarzania,
        - obsługa tworzenia i przywracania kopii zapasowych konfiguracji systemu,
    b. obsługa E-OAM (802.1ag, 802.3ah, Y.1731 DMM),
    c. obsługa krótkich pakietów E-OAM i BFD przez osobny, dedykowany układ sprzętowy na każdej karcie liniowej,
    d. obsługa MPLS OAM (LSP ping, LSP traceroute),

e. możliwość kopiowania ruchu z określonego portu/VLANu na inny port/VLAN urządzenia (mirroring),

f. funkcjonalność monitorowania jakości usług na bazie aktywnych próbników ruchu – pomiar min. dostępności, opóźnienia, jego zmian, strat pakietów,

g. sprzętowa obsługa Jflow/ NetFlow lub równoważne dla IPv4, IPv6, MPLS – export min. 40 tysięcy flow'ów na sekundę per system oraz lokalne składowanie min. 1.000.000 wpisów (dopuszcza się realizację zintegrowaną w urządzeniu lub w postaci karty usługowej),

h. interfejsy muszą obsługiwać funkcjonalność zdalnej diagnostyki połączeń optycznych (Digital Diagnostics Monitoring, Digital Optical Monitoring lub równoważne),

i. możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej - konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona,

j. możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów,

k. zarządzanie przez CLI (konsola szeregowa, SSHv2), SNMPv3, XML API,

l. obsługa syslog,

m. dedykowany port szeregowy na potrzeby dostępu do konsoli urządzenia lub zdalnego zarządzania (modem),

n. port Ethernet do celów zarządzania urządzeniem,

o. możliwość rozszerzenia funkcjonalności o obsługę monitorowania strumieni wideo (min. 1000 strumieni – straty pakietów, zmiany opóźnień, MDI MLR/DF zgodnie z RFC 4445),

13. Urządzenie musi posiadać certyfikaty Metro Ethernet Forum - MEF9 i MEF14 oraz CE2.0 co najmniej w obszarach: E-Line, oraz E-LAN.

2.5.2 WĘZŁY AGREGUJĄCE I DYSTRYBUCYJNE

2.5.2.1 Wymagania techniczne dla pomieszczeń agregujących

- Pomieszczenie suche, o murowanych ścianach, stropie i posadzce, wolne od kurzu i pyłu. Preferowana lokalizacja w podziemiu budynku przy ścianie zewnętrznej, z nieutrudnionym dostępem umożliwiającym transport szaf teleinformatycznych i wyposażenia o gabarytach SxGxW 0.6x0.6x1,5m.
- Położenie pomieszczenia powinno być dogodne dla wprowadzenia podziemnych kabli sieci szkieletowej i dystrybucyjnej, jak i kabli dystrybucji transmisji w budynku, o ile zachodzi taka potrzeba.
- Wielkość pomieszczenia powinna umożliwiać instalację:
  - szafy teleinformatycznej 21U o wym. SxGxW 0.6x0.6x1,5m z pozostawieniem miejsca na swobodny dostęp od przodu,

- Temperatura w pomieszczeniu nie może spadać poniżej 0°C o żadnej porze roku.
- Do pomieszczenie powinna być doprowadzona sieć energetyczna 230/400V 50Hz, z rozdzielnicą umożliwiająca zasilanie z oddzielnego obwodu, zasilacza UPS,
- W pomieszczeniu powinna zostać zainstalowana jedna szafa teleinformatyczna j/n, którą należy uziemić.

2.5.2.2 Wymagania techniczne dla urządzeń agregujących

1. Przełącznik modularny lub o zamkniętej konfiguracji, posiadający co najmniej 24 porty Gigabit Ethernet przeznaczone dla wkładek optycznych SFP lub równoważnych oraz co najmniej 2 porty uplink pozwalające na pracę jako porty 1 Gigabit Ethernet oraz jako 10Gigabit Ethernet oraz umożliwiające instalację wkładek SFP/SFP+ lub równoważnych.
2. Wszystkie gniazda typu SFP lub równoważne muszą pozwalać na instalację wkładek Gigabit Ethernet 1000BASE-T, 1000BASE-SX, 1000BASE-ZX, 1000BASE LX/LH, wkładek CWDM, DWDM, wkładek umożliwiających transmisję dwukierunkową na pojedynczym włóknie światłowodowym oraz wkładek z portami FastEthernet.
3. Wszystkie gniazda typu SFP+ lub równoważne muszą pozwalać na instalację wkładek 10 Gigabit Ethernet typu 10GBASE-LR, 10GBASE-SR, 10GBASE-ER, 10GBASE-ZR oraz wkładek 10Gigabit Ethernet DWDM.
4. Urządzenie musi być wyposażone w min. 1 wkładkę typu 10GBase-LR przeznaczoną do pracy na światłowodzie jednomodowym na dystansie 10km, 6 wkładek typu 1000Base-LX przeznaczone do pracy na światłowodzie jednomodowym na dystansie 10km oraz 1 wkładkę 1000Base-T.

2.5.2.3 Wymagania techniczne dla pomieszczeń dystrybucyjnych

- Pomieszczenie suche, o murowanych ścianach, stropie i posadzce, z nieutrudnionym dostępem umożliwiającym transport szaf teleinformatycznych i wyposażenia o gabarytach SxGxW 0.6x0.6x0.4m.
- Wielkość pomieszczenia powinna umożliwiać instalację:
  - szafy teleinformatycznej wiszącej 6U o wym. SxGxW 0.6x0.6x0.4m z pozostawieniem miejsca na swobodny dostęp od przodu, którą należy uziemić.
- Temperatura w pomieszczeniu nie może spadać poniżej 0°C o żadnej porze roku.
- Pomieszczenie powinno posiadać doprowadzoną sieć energetyczną 230V 50Hz, umożliwiające zasilenie urządzeń aktywnych w szafie 6U,

2.5.2.4 Wymagania techniczne dla urządzeń dystrybucyjnych

- Przełącznik modularny lub o zamkniętej konfiguracji, posiadający co najmniej 24 porty Gigabit Ethernet 1000Base-T RJ45 oraz co najmniej 2 porty uplink pozwalające na pracę jako porty Gigabit Ethernet oraz umożliwiające instalację wkładek SFPlub równoważnych. Porty uplink Gigabit Ethernet powinny umożliwiać rozbudowę do 10GigabitEthernet.Urządzenie musi być wyposażone w min. 1 wkładkę typu 1000Base-LX przeznaczoną do pracy na światłowodzie jednomodowym na dystansie 10km.

2.5.2.5 Wymagania techniczne wspólne dla przełączników agregujących i dystrybucyjnych

1. Dwa redundantne, wymienne zasilacze, nie dopuszcza się rozwiązań zewnętrznych w jakiekolwiek formie.
2. W dostarczonej wersji urządzenie musi być zasilane prądem przemiennym 230V.
3. Dostępne w przełączniku porty 10/100/1000 powinny spełniać funkcję Auto-MDIX oraz zapewniać diagnostykę kabli sieciowych (TDR).
4. Przełącznik musi posiadać wydajność przełączania przynajmniej 44Gbps full duplex/ 88Gbps halfduplex oraz 65Mpps.
5. Przełącznik musi zapewniać obsługę 16,000 adresów MAC, 4000 sieci VLAN, 24000 tras rutingowych i 1000 grup multicast.
6. Przełącznik powinien wpierać następujące protokoły routingu dynamicznego: IS-IS, OSPF, BGPv4, routing statyczny, ruting oparty o tzw. polityki (Policy Based Routing) oraz routing dla IPV6 w zakresi: routing statyczny oraz dynamiczny (min. OSPFv3).
7. Funkcjonalności związane z przełączaniem MPLS:

a. obsługa LDP, T-LDP
b. obsługa Ethernet over MPLS
c. obsługa VPLS
d. MPLS L3VPN
e. MPLS TE (z mechanizmami ochrony ścieżki)
f. MPLS FRR
g. możliwość konfiguracji min. 100 MPLS VPN

8. Przełącznik musi obsługiwać tzw. Jumbo Frames (9000 bajtów) na wszystkich portach.
9. Przełącznik musi wspierać funkcje DHCP Serwer, Klient, Relay.
10. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

a. IEEE 802.1s Rapid Spanning Tree
b. IEEE 802.1w Multi-Instance Spanning Tree
c. Protokół zapewniającym szybką zbieżność dla topologii pierścienia ITU-T G.8032 Ethernet Ring Protection Switching
d. możliwość grupowania portów zgodnie ze specyfikacją IEEE 802.3ad (LACP)
e. mechanizmy umożliwiające optymalne wykorzystanie łączy dla protokołów wartwy drugiej (np. shortest path bridging lub tworzenie topologii Spanning Tree niezależnie dla każdego VLAN-u)
f. możliwość zapewnienia redundancji interfejsów warstwy drugiej bez wykorzystania protokołów rodziny STP poprzez skonfigurowanie interfejsu zapasowego (Redundant Trunk Group, Flex-Link lub odpowiednik).
g. BFD dla protokołów RIP, OSPF, BGP
h. VRRP lub odpowiednik
i. MPLS TE/FRR

11. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. obsługa mechanizmów QoS (klasyfikacja, kolejkowanie, oznaczanie, policing, shaping) per port/VLAN
    b. Obsługa hierarchicznego QoS (H-QoS) na wszystkich portach równocześnie (nie dopuszcza się portów na urządzeniu niewspierających HQoS)

c. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: adres MAC, adres IP, port TCP, VLAN ID(min 2 poziomy zagnieżdżenia), MPLS EXP.
d. dynamiczna alokacja kolejek sprzętowych, dostępne min. 4000 kolejek
e. Implementacja algorytmu Round Robin (Shaped Round Robin) lub podobnego dla obsługi kolejek.
f. Możliwość obsługi jednej z kolejek z priorytetem w stosunku do innych. Mechanizm ograniczania ilości ruchu w kolejce priorytetowej.
g. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
h. Możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi(ingress policing, rate limiting).
i. Ingress Policing w oparciu o VLAN ID, DSCP, CoS, adres IP, adres MAC
j. Obsługa Weighted Tail Drop, WRED lub odpowiednika

12. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    a. Ograniczenie ilości obsługiwanych adresów MAC per port przełącznika lub per usługa zdefiniowana na porcie.
    b. Wiele poziomów dostępu administracyjnego poprzez konsolę.
    c. Możliwość uzyskania dostępu do urządzenia przez SNMPv3 .
    d. Możliwość uzyskania dostępu do urządzenia przez SSH.
    e. Obsługa protokołu RADIUS.
    f. Mechanizm ochrony drzewa Spanning-Tree .
    g. Możliwość zapobiegania sztormom broadcastów
    h. Możliwość tworzenia list kontroli dostępu w warstwach 2-4.
    i. Możliwość tworzenia list kontroli dostępu filtrujących ruch o podanym wzorcu w całym VLAN na przełączniku.
    j. Możliwość tworzenia list kontroli dostępu filtrujących ruch o podanym wzorcu na portach L2 przełącznika.
    k. Listy kontroli dostępu definiowane per port i per VLAN
    l. Listy kontroli dostępu z obsługą IPv4 oraz IPv6
    m. Mechanizmy ochrony warstwy zarządzającej urządzenia (Control Plane) przed atakami DDos oraz filtracja ruchu zarządzającego (np. poprzez policing ruchu kontrolnego)
    n. Mechanizm Dynamic ARP Inspection lub równoważny
13. Przełącznik musi zapewniać podstawową obsługę ruchu IP Multicast w zakresie:

a. IGMP v1/v2/v3
b. IGMP Snooping v1/v2/v3
c. PIM w trybach sparse mode, dense mode
d. Source Specific Multicast

14. Urządzenie musi dodatkowo wspierać następujące mechanizmy związane z usługami Metro Ethernet:
    a. Przełącznik musi obsługiwać protokół L2PT.
    b. Przełącznik musi obsługiwać funkcjonalność 802.1Q tunnelling (QinQ tunnelling).
    c. mapowanie (translacja) tagów 802.1Q – 1:1, 1:2, 2:1, 2:2
15. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem narzędzi zarządzania:
    a. Powinno umożliwiać zarządzanie poprzez interfejs CLI (konsolę).

b. Powinno umożliwiać zarządzanie poprzez SNMP v1, SNMP v2, SNMP v3.
c. Link Layer Discovery Protocol lub odpowiednik.
d. obsługa E-OAM (802.1ag, 802.3ah, E-LMI)
e. obsługa MPLS OAM (LSP ping, LSP traceroute)
f. interfejsy muszą obsługiwać funkcjonalność zdalnej diagnostyki połączeń optycznych zgodna z SFF-8472 (Digital Diagnostics Monitoring, Digital Optical Monitoring
g. Powinno posiadać funkcjonalność umożliwiającą podłączenie zewnętrznych źródeł sygnałów alarmowych (np. otwarcie drzwi do szafy, przekroczenie progowej temperatury w szafie) i wysłanie alarmu systemowego w przypadku wystąpienia takich alarmów.
h. ITU-T Y.1731 Performance Monitoring
i. ITU-T Synchronous Ethernet

16. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się restartów urządzenia po dokonaniu zmian.
17. Plik konfiguracyjny urządzenia powinien być zabezpieczony przed niepowołanym dostępem oraz zmianami – tylko osoby uwierzytelnione powinny posiadać dostęp do pliku konfiguracyjnego.
18. Urządzenie musi posiadać certyfikację Metro Ethernet Forum (MEF9 i MEF14), oraz CE2.0 co najmniej w obszarach: E-Line oraz E-LAN.
19. Praca w zakresie temperatur: 0-45C
20. Musi mieć możliwość montażu w szafie 19”.

2.5.3 CENTRUM ZARZĄDZANIA

2.5.3.1 Wymagania techniczne dla pomieszczeń

Pomieszczenie dla urządzeń aktywnych

- Pomieszczenie wyposażone w podłogę techniczną antystatyczną. W przypadku braku możliwości instalacji podłogi technicznej należy zaprojektować po dwa ciągi drabinek podwieszonych pod sufitem umożliwiających niezależne doprowadzenie przewodów zasilających oraz sygnałowych
- W pomieszczeniu powinien znajdować się punkt przyłączeniowy pozwalający na dołączenie uziemień z szaf teletechnicznych
- Do pomieszczenie powinno być doprowadzone zasilanie AC 230V z dwóch niezależnych źródeł o mocy zapewniającej poprawną pracę zainstalowanych urządzeń oraz posiadające zapas mocy. Szacowana moc potrzebna do zasilenia projektowanych urządzeń wraz z zapasem na potrzeby 20 kW
- Pomieszczenie powinno być wyposażone w klimatyzację pozwalające na utrzymanie temperatury w pomieszczeniu na zadanym poziomie z uwzględnieniem zainstalowanych urządzeń

- W pomieszczeniu powinny zostać zainstalowane szafy teleinformatyczne, które należy uziemić oraz doprowadzić zasilanie z dwóch niezależnych źródeł.

Szafa serwerowa	**1 szt.**
Wysokość	42 U
Głębokość	1000 mm
Szerokość	800 mm
Drzwi przednie	Szklane (szkło hartowane) z dwoma zamkami
Inne	Dach pełny
Inne	Trzy pary belek nośnych w rozstawie 19’
Inne	Szkielet na cokole z wysuwaną ramą wsporczą
Inne	Drzwi tylne blaszane pełne
Inne	Osłony boczne perforowane – demontowane
Inne	Listwa zasilająca 5-gniazd z bolcem 2P+Z, wyłącznik podświetlany, zabezpieczenie przepięciowe z filtrem sieciowym – 3 szt. zasilane z dostarczanego UPS 230VAC
Inne	Panel wentylacyjny mocowany na belkach nośnych sterowany za pomocą termostatu 2-wentylatory zasilane z dostarczanego UPS 230VAC
Inne	Moduł zdalnej kontroli temperatury wraz z sygnalizacją otwarcia drzwi szafy.

Szafa strukturalna	**1 szt.**
Wysokość	42 U
Głębokość	1000 mm
Szerokość	800 mm
Drzwi przednie	Szklane (szkło hartowane) z dwoma zamkami
Inne	Dach pełny
Inne	Trzy pary belek nośnych w rozstawie 19’
Inne	Szkielet na cokole z wysuwaną ramą wsporczą
Inne	Drzwi tylne blaszane pełne
Inne	Osłony boczne perforowane – demontowane
Inne	Listwa zasilająca 5-gniazd z bolcem 2P+Z, wyłącznik podświetlany, zabezpieczenie przepięciowe z filtrem sieciowym – **2 szt.** zasilane z dostarczanego UPS 230VAC
Inne	Moduł zdalnej kontroli temperatury wraz z sygnalizacją otwarcia drzwi szafy.

Szafa elementów aktywnych sieci	**1 szt.**
Wysokość	42 U
Głębokość	1000 mm
Szerokość	800 mm
Drzwi przednie	Szklane (szkło hartowane) z dwoma zamkami
Inne	Dach pełny
Inne	Trzy pary belek nośnych w rozstawie 19’
Inne	Szkielet na cokole z wysuwaną ramą wsporczą
Inne	Drzwi tylne blaszane pełne
Inne	Osłony boczne perforowane – demontowane
Inne	Panel wentylacyjny mocowany na belkach nośnych sterowany za pomocą termostatu 2-wentylatory zasilane z dostarczanej siłowni -48VDC lub 230V AC
Inne	Moduł zdalnej kontroli temperatury wraz z sygnalizacją otwarcia drzwi szafy.

- Wielkość pomieszczenia powinna być taka aby w przypadku przyszłej

rozbudowy możliwe było zainstalowanie kolejnych 2 szaf.

- Wszystkie kable światłowodowe dochodzące do budynku należy zakończyć w „szafie elementów aktywnych sieci”,
- W sąsiedztwie serwerowi należy zaadoptować pomieszczenie na potrzeby stanowiska nadzoru siecią.

Pomieszczenie na potrzeby nadzoru siecią

- Pomieszczanie powinno być na tyle duże aby umożliwiało swobodną pracę dwóch osób.
- Pomieszczenie należy wyposażyć w dwa stanowiska nadzoru (biurka), dodatkowo do każdego z nich należy zapewnić szafkę z szufladami zamykaną na klucz oraz ergonomiczne krzesło obrotowe z regulowaną wysokością i odchylanym oparciem. Na każdym z nich musi być możliwość umiejscowienia jednego monitora 24" oraz stacji operatorskiej (komputera przenośnego).
- Do każdego ze stanowisk należy doprowadzić minimum po 8 gniazd RJ-45 zakończonych w serwerowi w „szafie strukturalnej” oraz co najmniej po 4 gniazda zasilania gwarantowanego z UPSa Centrum Nadzoru i po 2 gniazda napięcia nie gwarantowanego,
- Każde ze stanowisk operatorskich powinno posiadać minimum po 2 gniazda telefoniczne podłączone do centrali,
- Na ścianie przed stanowiskami nadzoru, w miejscu wskazanym przez zamawiającego, należy zapewnić 2 monitory wielkoformatowe o przekątnej 56’’,
- Należy doprowadzić kable wideo od serwera video w pomieszczeniu serwerowni do w/w monitorów,
- Należy zapewnić jedno urządzenie wielofunkcyjne laserowe z możliwością podłączenia do sieci komputerowej, z funkcją kopiowania, skanowania, faksowania oraz drukowania w kolorze czarnym

2.5.3.2 Wymagania techniczne dla urządzeń – przełącznik dostępowy CZS – Centrum Zarządzania

1. Urządzenie o architekturze modularnej.
2. Wyposażony w min. 16 portów 10 GigabitEthernet dla wkładek typu SFP+ lub równoważne, z czego min. 4 porty obsadzone wkładkami typu 10GBase-SR oraz 6 portów obsadzonych wkładkami 1000BaseT.
3. Umożliwia rozbudowę min. o dodatkowe 8 portów 10GigabitEthernet.
4. Matryca przełączająca o wydajności min. 480 Gbps, wydajność przełączania przynajmniej 250 Mpps dla IPv4..
5. Obsługa min. 50 000 adresów MAC, 64 000 tras w tablicy routingu, 24 000 tras multicast, 64 tyś wpisów na potrzeby realizacji polityk QoS i bezpieczeństwa (listy kontroli dostępu), 4000 VLAN oraz identyfikatorów VLAN.
6. Obsługa ramek jumbo (min. 9000B).
7. Zintegrowane redundatne zasilacze i wentylatory.
8. Routing IPv4: trasy statyczne, RIPv2, OSPF, BGP. Przełącznik musi zapewniać sprzętowe wsparcie dla routingu IPv4.

9. Routing IPv6: trasy statyczne, RIPng, OSPFv3, BGP. Przełącznik musi zapewniać sprzętowe wsparcie dla routingu IPv6.
10. Obsługa ruchu IP Multicast: IGMP Snooping, IGMPv3, IGMP Filtering, MLDv2, MLD Snooping, PIM Sparse(IPv4 I IPv6), SSM (IPv4 I IPv6).
11. Obługa wirtualnych tablic routingu (VRF lub odpowiednik) oraz routing oparty o polityki.
12. Funkcjonalności DHCP: DHCP Server, Relay, snooping
13. Wsparcie dla GRE
14. Mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. IEEE 802.1s Multiple Spanning Trees
    b. IEEE 802.1w Rapid Spanning Tree
    c. możliwość grupowania portów zgodnie ze specyfikacją IEEE 802.3ad (LACP)
    d. mechanizmy redundancji bramy VRRP lub równoważny.
    e. umożliwia dołączanie zewnętrznych urządzeń (np. serwerów lub przełączników) do pary urządzeń będących przedmiotem specyfikacji poprzez zagregowany kanał (LACP, PortChannel) złożony z min. 2 fizycznych interfejsów w taki sposób, że jeden interfejs zewnętrznego przełącznika dołączony jest do jednego z urządzeń, drugi zaś do innego, niezależnego (tzw. Multichasis LAG, MultiChassis EtherChannel lub równoważne)
15. Mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, numer portu TCP
    b. implementacja co najmniej ośmiu kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Round Robin lub podobnego dla obsługi tych kolejek
    c. obsługa jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
    d. QoS per port oraz per VLAN
    e. możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
    f. możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi
16. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    a. autoryzacja użytkowników/portów w oparciu o IEEE 802.1x z możliwością przydziału listy kontroli dostępu (ACL) i VLANu, wsparciem dla MAC Authentication Bypass oraz dla Radius Change of Authorisation
    b. funkcjonalność prywatnego VLAN-u, czyli możliwości blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane)
    c. Mechanizmy kontroli adresów MAC na poziomie portu
    d. DHCP Snooping (ochrona przed wrogimi serwerami DHCP)
    e. IP Source Guard (ochrona przed podszyciem się pod adres IP)
    f. Ochrona SpanningTree, min. Root Guard, BPDU Filtering lub równoważne
    g. Dynamic ARP Inspection
    h. Unicast RPF dla Ipv4 oraz IPv6
    i. Ochrona warstwy kontrolnej urządzenia
    j. współpraca z systemami kontroli dostępu do sieci typu NAC, NAP lub równoważnym
    k. możliwość filtrowania ruchu na poziomie portu oraz VLANu w oparciu o adresy MAC, IP, porty TCP/UDP

l. listy kontroli dostępu także dla IPv6
m. Storm control

17. Funkcjonalności w zakresie zarządzania:
    a. Możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub poprzez określony VLAN
    b. Umożliwia stworzenie wirtualnego systemu złożonego z min. 2 urządzeń będącego przedmiotem opisu, zarządzanego jako całość. Urządzenia praacujące w takiej konfiguracji muszą umożliwiać połączenie w system z wykorzystaniem stadardowych portów 10GE Ethernet oraz modułów optycznych typu 10GBASE-LRM.
    c. dostęp do urządzenia przez:
        i. CLI (konsolę)
        ii. HTTP/HTTPS,
        iii. SNMPv3 (ang. Simple Network Management Protocol version 3)
        iv. SSHv2
    d. Powinno umożliwiać identyfikację i uwierzytelnianie administratorów w oparciu o serwer RADIUS.
    e. Posiada możliwość raportowania do systemów zarządzających z wykorzystaniem S-Flow lub odpowiednika (J-Flow lub NetFlow). Konieczna jest obsługa/buforowanie minimum 100 000 wpisów. Funkcjonalność ta musi być obsługiwana sprzętowo i wspierać IPv4 oraz IPv6
    f. Wsparcie dla DHCP
    g. synchronizacja czasu zgodnie z NTP
    h. Syslog over IPv6
    i. Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona.
    j. Urządzenie musi posiadać możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów.
18. Możliwość montażu w szafie 19”, maks. 2RU obudowa wykonana z metalu
19. Urządzenie ma być zasilane napięciem 230 V.

2.5.3.3 Wymagania techniczne dla urządzeń - Firewall – Centrum Zarządzania

1. System zabezpieczeń Firewall – Centrum Zarządzania ma być dostarczony jako dedykowane urządzenie lub zestaw maks. dwóch dedykowanych urządzeń bezpieczeństwa sieci połączonych w sposób nie ograniczających ich wydajności dodatkowymi interfejsami.
2. System zabezpieczeń musi zapewnić następujące funkcjonalności: zapora ogniowa (firewall), system filtracji web. Szczegółowe wymagania dla każdej z funkcjonalności są zdefiniowane poniżej.
3. Należy dostarczyć aplikację lub aplikacje umożliwiające zarządzanie opisanymi funkcjonalnościami z poziomu graficznego interfejsu użytkownika.

4. Brak ograniczeń licencyjnych na ilość jednocześnie pracujących użytkowników w sieci chronionej.
5. Co najmniej osiem portów 10/100/1000 Ethernet
6. Możliwość rozbudowy o dodatkowe 6 intefejsów 10/100/1000 Ethernet lub 6 interfejsów Gigabit Ethernet dla wkładek optycznych
7. Dedykowany port dla podłączenia konsoli oraz port USB.
8. System zabezpieczeń musi być wyposażony w redundatne zasilacze 230V oraz dyski SSD zapewniające redundancję na poziomie co najmniej odpowiednim do RAID1
9. Urządzenie powinno być zarządzalne zarówno poprzez linię komend jak i przy wykorzystaniu dedykowanej aplikacji umożliwiającej płynną (z użyciem kreatorów) konfigurację poszczególnych funkcji urządzenia. Należy dostarczyć aplikację lub zestaw aplikacji umożliwiajacy zarządzenie z graficznego interfejsu użytkownika opisywanymi funkcjonalnościami.
10. Dostęp do urządzeń i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).
11. W ramach zamówienia dostarczyć należy system wraz z opieką techniczną dla wszystkich dostarczanych komponentów oraz dostępem do nowych wersji oprogramowania, i bazy reputacji stron Web dla 5 letniego okresu trwałości projektu.
12. Urządzenie powinno być przystosowane do montażu w 19” szafie rackowej.

Funkcjonalności zapora ogniowa / VPN

13. Tryb pracy jako transparentna ściana ogniowa warstwy drugiej ISO OSI.
14. Terminowanie co najmniej 2000 jednoczesnych sesji VPN opartych o protokół IPSEC. Jeśli dla realizacji tej funkcjonalności wymagane są odpowiednie licencje, muszą one zostać dołączone.
15. Terminowanie co najmniej 2000 jednoczesnych sesji VPN opartych o protokół SSL. Jeśli dla realizacji tej funkcjonalności wymagane są odpowiednie licencje, muszą one zostać dołączone.
16. Obsługa co najmniej 750 000 jednoczesnych sesji/połączeń z prędkością min. 30 000 połączeń na sekundę.
17. Przepustowość maksymalna obsługiwana przez urządzenie nie mniejsza niż 3 Gbps i nie mniejsza niż 1.5 Gbps dla ruchu mieszanego.
18. Przepustowość 400 Mbps dla ruchu szyfrowanego symetrycznymi algorytmami 3DES/AES.
19. Możliwość realizacji redundantnego systemu typu active/active oraz active-stand-by.
20. Obsługa min 10 wirtualnych kontekstów firewall (dla każdego z nich musi być możliwość zdefiniowania różnych i niezależnych polityk bezpieczeństwa) z możliwością rozbudowy licencyjnej w celu obsługi do 50 wirtualnych instancji firewall .
21. Mechanizmy inspekcji aplikacyjnej i kontroli następujących usług:
    a. Hypertext Transfer Protocol (HTTP),
    b. File Transfer Protocol (FTP),

c. Simple Mail Transfer Protocol (SMTP),
d. Domain Name System (DNS),
e. H.323
f. Session Initiation Protocol (SIP)
g. Lightweight Directory Access Protocol (LDAP)
h. Internet Control Message Protocol (ICMP)
i. Network File System (NFS)

22. Blokowanie aplikacji tunelowanych z użyciem portu 80 w tym:
    a. blokowanie komunikatorów internetowych
    b. blokowanie aplikacji typu peer-to-peer
23. Protokoły routingu dynamicznego OSPF oraz RIPv2.
24. Wsparcie dla multicast poprzez
    a. protokoły routingu multicast (PIM Sparse Mode)
    b. IGMP,
    c. definiowanie list kontroli dostępu dla ruchu multicast.
25. Wsparcie dla IPv6 poprzez:
    a. pracę w sieci z adresacją IPv6
    b. definiowanie list kontroli dostępu dla ruchu IPv6
    c. zarządzanie urządzeniem poprzez SSHv2, HTTPS w sieci IPv6

Funkcjonalności filtracji web:

26. Wydajność co najmniej 1Gbps dla ruchu poddawanego filtracji.
27. Urządzenie musi zapewnieć ochronę przed nieznanymi (ang. zero-day) zagrożeniami i złośliwym oprogramowaniem użytkownikom w sieci wewnętrznej i użytkownikom łączącym się do sieci wewnętrznej zdalnie, w szczególności w oparciu o bazę reputacji stron web dostarczaną i aktualizowaną przez producenta rozwiązania
28. Urządzenie musi umożliwiać ochronę przed nieznanymi (ang. zero-day) zagrożeniami i złośliwym oprogramowaniem w trybie transparentnym (w warstwie drugiej modelu OSI) lub w trybie routera (w warstwie trzeciej modelu OSI).
29. Urządzenie musi rozpoznawać i umożliwiać filtrowanie conajmniej 500 aplikacji a w tym conajmniej następujące:
    a. Skype
    b. Dropbox
    c. eDonkey
    d. Bittorent
    e. Gnutella
    f. Google Docs
    g. Google Talk
    h. iCloud
    i. Megaupload

j. RapidShare
k. YouTube
l. Facebook
m. Google Plus
n. ssh
o. dns
p. http
q. ftp
r. sip
s. rtp

30. Urządzenie do rozpoznawania aplikacji musi wykorzystywać sygnatury, heurystykę i badanie treści umożliwiając rozpoznanie aplikacji również wtedy, gdy działają na portach niestandardowych.
31. Urządzenie w ramach rozpoznawanych aplikacji webowych musi umożliwiać rozpoznawanie tak zwanych mikroaplikacji w celu granularnego filtrowania czynności, które może wykonać użytkownik korzystający z rozpoznanej aplikacji webowej (np. dodawanie komentarzy lub wgrywanie zdjęć na portal społeczny).
32. Wymaga się, aby w stosunku do rozpoznawanych webowych aplikacji umożliwiających transfer i współdzielenie plików, urządzenie umożliwiało akcję zablokowania wgrywania plików na przestrzeń dyskową udostępnianą przez aplikację.
33. Urządzenie musi umożliwiać tworzenie reguł filtrowania aplikacji webowych w oparciu o typ urządzenia końcowego wykorzystywanego do nawiązania połączenia (np. wykrywanego na podstawie informacji z nagłówka HTTP).
34. Urządzenie musi umożliwiać tworzenie reguł filtrowania aplikacji webowych w oparciu o conajmniej 60 kategorii obejmujących co najmniej:
    a. Strony dla dorosłych
    b. Ogłoszenia
    c. Alkohol
    d. Aukcje
    e. Chaty i komunikatory
    f. Randkowanie
    g. Rozrywka
    h. Moda
    i. Serwisy transferu plików
    j. Oprogramowanie
    k. Serwery proxy
    l. Hazard
    m. Gry
    n. Hacking
    o. Nienawiść
    p. Pornografia
    q. Religia
    r. Nieruchomości
    s. Portale społecznościowe

t. Broń

35. Urządzenie musi umożliwiać tworzenie reguł filtrowania w oparciu o to czy użytkownik przebywa wewnątrz sieci czy łączy się do niej zdalnie.
36. Urządzenie musi umożliwiać tworzenie reguł filtrowania w opraciu o nazwę użytkownika lub nazwę grupy, do której należy użytkownik.
37. Informacje na temat użytkownika i grup, do których należy użytkownik urządzenie musi pobierać z Microsoft Active Directory lub z innych serwerów usług katalogowych dostępnych przy pomocy protokołu LDAP.
38. Urządzenie współpracując z Active Directory musi umożliwiać transparentną identyfikację użytkownika w sposób nie wymagając żadnych dodatkowych akcji ze strony użytkownika.
39. Urządzenie musi umożliwiać aktywną identyfikację użytkownika przy pomocy przeglądarki internetowej z wykorzystaniem protokołów NTLM lub Kerberos.
40. Urządzenie musi umożliwiać wykorzystanie aktywnej metody identyfikacji użytkownika w przypadku gdy metoda transparenta nie dostarczy informacji o tożsamości użytkownika.
41. Urządzenie musi dla wybranych kategorii aplikacji webowych umożliwiać inspekcję ruchu http szyfrowanego przy pomocy protokołów SSL/TLS.
42. Urządzenie musi wyświetlać komunikat w oknie przeglądarki użytkownika, jeśli dana strona webowa została zablokowana.
43. Urządzenie musi umożliwiać raportowanie aktywności użytkowników historycznie i na bieżąco.
44. Urządzenie musi umożliwiać zarządzanie przy pomocy webowego interfejsu użytkownika

2.5.3.4 Wymagania techniczne dla urządzeń - Aplikacja Zarządzająca

1. Oprogramowanie do zarządzania urządzeniami sieci LAN musi stanowić zintegrowany pakiet aplikacji do konfiguracji, administracji, monitoringu i diagnozowania sieci.
2. Funkcje te muszą być dostępne poprzez graficzny interfejs użytkownika poprzez przeglądarkę stron WWW.
3. Oprogramowanie musi umożliwiać definiowanie spersonalizowanego interfejsu prezentującego informacje o sieci.
4. Wymagany zakres funkcjonalności:
    a. wykrywanie błędów i problemów w czasie rzeczywistym,
    b. wykrywanie urządzeń i połączeń, szczegółowy podgląd topologii, śledzenie urządzeń końcowych (w oparciu o adresy MAC i adresy IP), analiza połączeń warstwy drugiej i trzeciej, zbieranie informacji o telefonach IP,
    c. narzędzia do zarządzania listą urządzeń (ang. inventory management), oprogramowaniem urządzeń i ich konfiguracją,

d. diagnozowanie stanu, wydajności i dostępności sieci, raportowanie w czasie rzeczywistym oraz w oparciu o dane historyczne,
e. generowanie szczegółowego opisu użytkowanych urządzeń i ich konfiguracji.

5. Oprogramowanie musi być dostarczone wraz z licencją na minimum 100 urządzeń oraz umożliwiać dalsze skalowanie do minimum 400 urządzeń sieciowych.
6. System zarządzania musi być dostarczony w postaci virtual appliance – musi być możliwość uruchomienia systemu w środowisku wirtualnym na module serwerowym TYPU A opisanym niżej.
7. System powinien zostać dostarczony w postaci virtual appliance – musi być możliwość uruchomienia systemu w środowisku wirtualnym na platformie serwerowej opisanej dalej.
8. Platforma sprzętowa, na której oprogramowanie będzie uruchomione, powinna być wyposażona w odpowiednią technologię wirtualizacji, zapewniającą odpowiedni poziomu niezawodności:
    a. systemu zarządzania siecią
    b. systemu uwierzytelniania, autoryzacji i rozliczeń
    c. systemu zarządzania tożsamością użytkowników sieci i dostępem gościnnym

Aplikacja powinna mieć możliwość dostępu w tym samym czasie co najmniej z obydwu terminali w Centrum Zarządzania, zdalnie lub lokalnie bez konieczności zakupu dodatkowych licencji.

2.5.3.5 Wymagania techniczne dla urządzeń - Stacja zarządzająca – serwer zarządzający

1) Modularny system serwerowy oparty o:
    a) obudowę serwerową (chassis) zawierającą gniazda rozszerzenia przewidziane do instalacji modułów serwerowych (blade)
    b) zespół przełączający przeznaczony do realizacji dostępu do sieci LAN/SAN
    c) centralne środowisko zarządzające
2) Obudowa serwerowa musi posiadać następujące cechy:
    a) Możliwość zainstalowania przynajmniej 8 modułów
    b) Zintegrowane w ramach chassis moduły zasilaczy i wentylatorów
    c) Każdy wykorzystany w chassis moduł komunikacyjny musi być sieciowym modułem dołączającym każdy moduł serwerowy dedykowanym, wewnętrznym interfejsem 10 GE (zgodnym ze standardami FCoE T11)
    d) Moduły zasilające zapewniające redundancję typu N+1
    e) Wszystkie komponenty obudowy muszą być oferowane w konfiguracji redundantnej
3) Zespół przełączający musi posiadać następujące cechy:
    a) Centralny zespół przełączający musi posiadać architekturę nieblokującą
    b) Dołączanie obudów serwerowych do systemu przełączania poprzez umieszczone w obudowach zintegrowane sieciowe moduły rozszerzające 10GE.

c) Możliwość dołączenia pojedynczej obudowy serwerowej poprzez min. 2 x 4 interfejsy 10GE (lub połączenie o równoważnej wydajności).
d) Dostęp do sieci LAN oraz do sieci SAN musi być realizowany na wspólnych portach, w oparciu o protokół FCoE (FibreChannel over Ethernet) zgodnie ze specyfikacją ANSI T11.
e) Obsługa IEEE Data Center Bridging (802.1Qbb PFC, 802.1AB, 802.1Qaz Enhanced Transmission Selection)
f) Centralny system przełączający musi być zaimplementowany w sposób redundantny tzn. m.in. na zdublowanych urządzeniach
g) Wszystkie wykorzystane urządzenia muszą mieć wbudowane minimum 32 porty FCoE
h) System musi pracować w przynajmniej w trybie zasilania N+1 z możliwością podniesienia do trybu N+N
i) Montaż w 19'' szafie Rack (zestaw montażowy dostarczony z urządzeniem)

4) Zespół zarządzający musi spełniać następujące wymagania

a) Zespół zarządzający może składać się z wielu komponentów oprogramowania. Jeśli oprogramowanie wymaga osobnych serwerów, należy dostarczyć je razem z odpowiednimi licencjami. W wypadku instalacji komponentów zarządzających na maszynach wirtualnych, należy dostarczyć osobno serwery pod te wirtualne maszyny wg zaleceń producenta oraz licencje na platformę wirtualizacyjną w wersji wymaganej przez oprogramowanie.
b) System zarządzania musi oferować graficznie następujące funkcjonalności:`
   i) Listę komponentów, z których składają się obudowy serwerowe
   ii) Wyświetlanie informacji o awariach i zdarzeniach
   iii) Automatyczne powiadamianie o awarii, email do administratora
   iv) Zarządzanie konfiguracjami za pomocą interfejsu graficznego oraz konsolowego
   v) Zarządzanie z uwzględnieniem roli użytkowników
   vi) Integrację ze środowiskiem wirtualizacji serwerów
   vii) Zarządzanie mocą całego środowiska poprzez podgląd maksymalnej i średniej wykorzystanej przez komponenty mocy
   viii) Zarządzanie chłodzeniem całego środowiska poprzez podgląd temperatur na poszczególnych komponentach środowiska
   ix) Wizualizację środowiska, pokazanie jego komponentów w sposób graficzny oraz umożliwienie ich konfiguracji poprzez wybranie ich za pomocą myszki
   x) Obsługę szablonów definiujących serwery - np. zapisanie wzorcowej konfiguracji serwera, a następnie tworzenie nowych konfiguracji z pierwotnie przygotowanego szablonu
   xi) Wsparcie scenariuszy disaster-recovery poprzez funkcje odtworzenia utraconej konfiguracji systemu za pomocą graficznego interfejsu GUI
   xii) Konfigurowanie serwerów oraz środowiska na podstawie puli wcześniej zdefiniowanych, dzielonych zasobów za pomocą szablonów
   xiii) Oprogramowanie musi wizualizować połączenia interfejsów fizycznych oraz warstwy wirtualizacyjnej serwerów

c) System musi umożliwiać wymianę serwera przy pomocy logicznego profilu obejmującego konfigurację serwera w zakresie sieci LAN i SAN. W zakres logicznego profilu serwerowego muszą wchodzić minimum następujące parametry:, adres MAC, adres WWNN/WWPN, sekwencja bootowania systemu, sposób konfiguracji oraz cechy adapterów NIC i HBA
d) System musi umożliwiać przeniesienie profilu serwera do dowolnego chassis środowiska (profil zdefiniowany wg punktów wyżej)
e) System musi umożliwiać automatyczne przeniesienie profilu z uszkodzonego serwera na zdefiniowany wcześniej przez administratora wolny serwer
f) Dopuszczalne jest zaoferowane rozwiązania, w którym funkcje wspólnego systemu przełączającego oraz wspólnego zarządzania chassis realizowane będą na tych samych urządzeniach

5) Moduł serwerowy TYP A musi posiadać następujące cechy:

a) Moduł serwerowy oparty o architekturę x86
b) Dwa gniazda dla procesorów umożliwiających osiągnięcie przez oferowane serwery wyników testu SPEC int_rate_base2006 na poziomie:
   i) dla procesorów 6-rdzeniowych – 400 pkt.
   ii) dla procesorów 8-rdzeniowych – 500 pkt.
c) Obsługa procesorów wspierających magistralę PCI Express 3.0
d) W oferowanej konfiguracji moduły serwerowe muszą być wyposażone w następujące komponenty:
   i) 2 procesory wyposażone w min. 6 rdzeni obliczeniowych każdy, minimum 15MB pamięci cache oraz katalogowym poborze mocy nie większym niż 95W, umożliwiające osiągnięcie przez serwer w teście SPECint_rate_base2006 wyniku na poziomie min. 350 pkt. (ilość ramu w testowanym serwerze może być różna)
   ii) Min. 48 GB pamięci RAM z możliwością rozbudowy do 128GB
   iii) Min. 2 dyski twarde SAS 6G o pojemności 300G 10k rpm
   iv) Min. jeden dwuportowy adapter sieciowy 10 GE typu CNA (Converged Network Adapter) z implementacją FCoE i możliwością sprzętowej wirtualizacji interfejsów Ethernet.

6) Moduł serwerowy TYP B musi posiadać następujące cechy:

a) Moduł serwerowy oparty o architekturę x86
b) Dwa gniazda dla procesorów umożliwiających osiągnięcie przez oferowane serwery wyników testu SPEC int_rate_base2006 na poziomie:
   i) dla procesorów 6-rdzeniowych – 400 pkt.
   ii) dla procesorów 8-rdzeniowych – 500 pkt.
c) Obsługa procesorów wspierających magistralę PCI Express 3.0
d) W oferowanej konfiguracji moduły serwerowe muszą być wyposażone w następujące komponenty:
   i) 2 procesory wyposażone w min. 6 rdzeni obliczeniowych każdy, minimum 15MB pamięci cache oraz katalogowym poborze mocy nie większym niż 95W,

umożliwiające osiągnięcie przez serwer w teście SPECint_rate_base2006 wyniku na poziomie min. 350 pkt. (ilość ramu w testowanym serwerze może być różna)

ii) Min. 128 GB pamięci RAM z możliwością rozbudowy do 192GB
iii) Min. 2 dyski twarde SAS 6G o pojemności 300G 15k rpm
iv) Min. jeden dwuportowy adapter sieciowy 10 GE typu CNA (Converged Network Adapter) z implementacją FCoE i możliwością sprzętowej wirtualizacji interfejsów Ethernet.

7) W ramach postępowania wymagane jest dostarczenie środowiska serwerowego:
a. Redundantny zespół przełączający, redundantne oprogramowanie zarządzające, chassis
b. 2 moduły serwerowe wg specyfikacji TYP A oraz 2 moduły serwerowe według specyfikacji TYP B
c. 4 porty 10GE/FCoE (2x2) obsadzone wkładkami SFP/SFP+ lub równoważnymi typu 10GBASE-SR dla dołączenia do zewnętrznej sieci LAN
d. Redundantny system zarządzania modularnym systemem serwerowym
e. Minimum jedna szafka na serwery wyposażona wg. specyfikacji
f. Kable połączeniowe
g. Licencje niezbędne do uruchomienia opisanej funkcjonalności

2.5.3.6 Wymagania techniczne dla urządzeń - System uwierzytelniania, autoryzacji i rozliczeń

1. Musi stanowić dedykowany system do uwierzytelnienia, autoryzacji oraz billingu (ang. accounting – rozliczenia, rozumiane jako system statystyk obrazujący wykorzystanie sieci przez wskazane podmioty) użytkowników. Nie dopuszcza się stosowania pakietów darmowych lub wersji testowych (ang. trial) oprogramowania komercyjnego ze względu na brak odpowiedniego wsparcia serwisowego dla takich produktów.
2. Musi komunikować się z urządzeniami sieciowymi z wykorzystaniem protokołów RADIUS.
3. Musi umożliwiać współpracę z routerami, przełącznikami sieciowymi, punktami dostępu bezprzewodowego, urządzeniami z funkcjonalnością firewall/VPN, rozwiązaniami VoIP, w szczególności tymi opisanymi w innych punktach.
4. Musi umożliwiać autoryzację użytkowników z wykorzystaniem protokołu 802.1x.
5. Musi wpierać następujące protokoły uwierzytelniające: PAP, CHAP, MS-CHAP, EAP-TLS, EAP-GTC.
6. Musi umożliwiać autoryzację użytkowników w oparciu o hasła stałe, jednorazowe (przy współpracy z serwerem tokenowym) oraz z wykorzystaniem infrastruktury klucza publicznego PKI.
7. Musi zapewniać szereg elastycznych mechanizmów kreowania polityki dostępu:
    a. przypisanie użytkowników do VLAN'u na podstawie uwierzytelnienia i autoryzacji,
    b. przypisanie listy kontroli dostępu per użytkownik,
    c. przypisanie ograniczeń czasowych i per ilość sesji dla danego użytkownika.

8. Musi stanowić centralny punkt decyzyjny w strukturach typu Network Access Protection lub typu Network Admission Control.
9. Musi zapewniać mechanizmy kontroli dostępu do systemu przez administratorów:
    a. ograniczenia działań dla wskazanych kont administratorów,
    b. wymuszenia polityki dotyczącej haseł administracyjnych,
    c. ograniczenia adresów IP, z których można uzyskać dostęp do systemu.
10. Musi wspierać, przechowywać dane historyczne komend wydawanych przez administratorów oraz rozliczenia sesji RADIUS
11. Musi wspierać protokół LDAP (ang. Lightweight Directory Access Protocol), Active Directory oraz ODBC (Open Database Connectivity) do współpracy z systemami zewnętrznymi.
12. Musi pracować w trybie przeglądarkowym pozwalając administratorowi na dostęp z dowolnego (po uzyskaniu odpowiednich uprawnień) miejsca w sieci.
13. Musi umożliwiać tworzenie grup użytkowników i definiowanie polityk per grupa użytkowników.
14. Musi mieć możliwość pracy w trybie redundantnym.
15. Oprogramowanie musi być dostarczone wraz z licencją na minimum 300 urządzeń oraz umożliwiać dalsze skalowanie do minimum 500 urządzeń sieciowych.
16. System powinien zostać dostarczony w postaci virtual appliance – musi być możliwość uruchomienia systemu w środowisku wirtualnym na module serwerowym TYPU A opisanym wyżej.

17. Platforma sprzętowa, na której system będzie uruchomiony, powinna być wyposażona w odpowiednią technologię wirtualizacji, zapewniającą odpowiedni poziomu niezawodności:
    a. systemu zarządzania siecią
    b. systemu uwierzytelniania, autoryzacji i rozliczeń
    c. systemu zarządzania bezpieczeństwem dostępu do sieci

2.5.3.7 Wymagania techniczne dla urządzeń - System zarządzania bezpieczeństwem dostępu do sieci

System zarządzania bezpieczeństwem dostępu do sieci ma zapewnić metody uwierzytelnienia i autoryzacji użytkowników i urządzeń sieci LAN, sieci bezprzewodowej, dostępu gościnnego, wykrywania urządzeń końcowych oraz oceny stanu urządzeń końcowych.

System zarządzania bezpieczeństwem dostępu do sieci musi spełniać co najmniej poniższe wymagania:

1. System musi wspierać następujące protokoły uwierzytelnienia i standardy:
    a. RADIUS, zgodnie z dokumentami:
        - RFC 2138 — Remote Authentication Dial In User Service (RADIUS)
        - RFC 2139 — RADIUS Accounting
        - RFC 2865 — Remote Authentication Dial In User Service (RADIUS)

- RFC 2866 — RADIUS Accounting
- RFC 2867 — RADIUS Accounting for Tunnel Protocol Support
- RFC 2868 — RADIUS Attributes for Tunnel Protocol Support
- RFC 2869 — RADIUS Extensions

b. RADIUS Proxy dla zewnętrznego serwera RADIUS

2. System musi umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych i w ten sposób umożliwiać skalowanie rozwiąznaia.
3. System musi umożliwiać realizację wysokiej dostępności wszystkich elementów funkcjonalnych, co najmniej 1:1
4. System musi wspierać integrację z Windows Active Directory, w tym conajmniej Microsoft Windows Active Directory 2003 32/64bit, Microsoft Windows Active Directory 2008 32/64-bit.
5. System musi wspierać protokół Lightweight Directory Access Protocol (LDAP).
6. System musi umożliwiać zarządzanie za pomocą interfejsu graficznego przez przeglądarkę internetową, w tym co najmniej: Google Chrome, Microsoft IE, Mozilla Firefox
7. System musi co najmniej wspierać następujące protokoły uwierzytelniania:
   a. Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
   b. Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:
      - EAP-MS-CHAPv2
      - EAP-GTC
      - EAP-TLS
   c. System musi umożliwiać aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym, serwerze TFTP/FTP/SFTP, udziale NFS, dysku CDROM
8. System musi umożliwiać zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).
9. System musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled).
10. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.
11. System musi umożliwiać wymuszenie reguł złożoności haseł dla administratorów.
12. System musi umożliwiać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora.
13. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP.
14. System musi umożliwiać generowanie przynajmniej następujących raportów:
   a. raportów dla protokołów AAA:
      - trendów uwierzytelnienia 802.1X
      - accountingu RADIUS
      - uwierzytelniania RADIUS
   b. raportów dozwolonych protokołów
   c. raportów dla stacji końcowych, w tym:
      - uwierzytelnień typu MAC Authentication
      - Top N uwierzytelnień per adres MAC stacji
      - Top N uwierzytelnień per maszyna
      - Top N uwierzytelnień per RADIUS Calling Station ID
   d. raportów dla błędów, w tym:
      - sumarycznych przyczyn nieudanych uwierzytelnień

- Top N uwierzytelnień per rodzaj błędu

e. raportów dla urządzeń sieciowych:
   - sumarycznych uwierzytelnień dla urządzeń sieciowych
   - Top N uwierzytelnień per urzadzenie sieciowe

f. raportów użytkowników:
   - sumarycznych uwierzytelnień użytkowników
   - Top N uwierzytelnień per użytkownik
   - stanu provisioningu agenta Posture na stacjach końcowych
   - sesji uzytkowników gościnnych
   - aktywności użytkowników gościnnych
   - uwierzytelnień per unikalny użytkownik

g. raportów sesji RADIUS
   - aktywnych sesji RADIUS
   - historii sesji RADIUS

h. raportów dla głębokiej analizy stacji końcowej (Posture):
   - trendów głębokiej analizy (Posture) per skonfigurowana polityka Posture
   - szczegółowych wyników posture assessment per użytkownik

15. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą
    a. wiadomości e-mail
    b. syslog
16. System musi posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
    a. badanie łączności IP za pomocą ping, nslookup, traceroute
    b. wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
       - nazwy użytkownika
       - adresu MAC
       - Audit Session ID
       - adresu IP NAS
       - numeru portu NAS
       - statusu uwierzytelnienia (udana lub nieudana)
       - powodu, jeżeli uwierzytelnienie nieudane
       - zakresu czasowego co do dnia, godziny i minuty
    c. ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem:
    d. rozwiązywanie problemów głębokiej analizy stanu stacji końcowej (Posture Assessment)
    e. wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu
17. System musi umożliwiać równoczesną obsługę co najmniej 2000 urządzeń końcowych (endpoints) przewodowych i bezprzewodowych dla funkcjonalności uwierzytelnienia, autoryzacji oraz dostępu gościnnego
18. System musi umożliwiać elastyczne dodawanie licencji w ramach wzrostu liczby obsługiwanych stacji końcowych.
19. System musi umożliwiać uwierzytelenienie i kontrolę dostępu:
    a. kablowego w sieci LAN
    b. bezprzewodowego w sieci WLAN
    c. zdalnego VPN
20. System musi umożliwiać inkrementalą skalowalność do przynajmniej 5,000 równocześnie obsługiwanych urządzeń końcowych (endpoints) poprzez dodawanie kolejnych serwerów do istniejącego wdrożenia.

21. System musi umożliwiać instalację na maszynie wirtualnej (VM) lub maszynie fizycznej, w tym:
    a. na hypervisorze VMWare ESX 4.x
    b. na hypervisorze VMWare ESXi 4.x i 5.x
    c. na serwerach fizycznych wspieranych przez producenta
22. System musi wspierać implementację 802.1X z przynajmniej następującymi suplikantami:
    a. wbudowanym klientem 802.1X dla Windows XP
    b. wbudowanym klientem 802.1X dla Windows Vista
    c. wbudowanym klientem 802.1X dla Windows 7
    d. Apple Mac OS X Supplicant
    e. Cisco AnyConnect 3.x
    f. Juniper Odyssey 5.x
23. System musi umożliwiać tworzenie polityk uwierzytelniania 802.1X opartych złożone o reguły (rule-based).
24. System musi umożliwiać uwierzytelnianie 802.1X maszyn i użytkowników.
25. System musi umożliwiać tworzenie polityk kontroli dostępu (authorization) 802.1X opartych złożone o reguły.
26. System musi posiadać lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV.
27. System musi posiadać lokalną bazę stacji końcowych. Lokalną bazę stacji końcowych można tworzyć per stacja końcowa na podstawie unikalnego adresu MAC.
28. System musi wspierać uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC za pomocą mechanizmu MAB (MAC Authentication Bypass) lub równoważnego.

29. System musi umożliwiać realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym co najmniej:
    a. Microsoft Windows 7, Vista, XP (Microsoft IE, Mozilla Firefox, Google Chrome)
    b. Apple Mac OS X (Mozilla Firefox, Safari, Google Chrome)
30. System musi umożliwiać dodawanie kont gościnnych przez wybrane osoby (sponsorów).
31. Uwierzytelnienie sponsora musi się odbywać sekwencyjnie w oparciu o:
    a. wewnętrzną bazę użytkowników
    b. zewnętrzne repozytorium użytkowników
32. System musi umożliwiać konfigurację uprawnień sponsora, w tym uprawnienia do:
    a. logowania się do systemu
    b. tworzenia pojedynczego konta gościnnego
    c. tworzenia wielu kont gościnnych
    d. tworzenia kont losowych
    e. importowania kont gościnnych z pliku CSV
    f. wysyłania wiadomości e-mail po utworzeniu konta gościnnego
    g. wysyłania wiadomości SMS po utworzeniu konta gościnnego
    h. wyświetlenia hasła konta gościnnego
    i. wydrukowania danych konta gościnnego
    j. wyświetlenia danych stworzonych kont gościnnych
    k. zawieszenia (suspend) i reinicjacji kont gościnnych
33. System musi umożliwiać konfigurację wyglądu portalu sponsora i gościa, w tym:
    a. zmianę logo strony logowania
    b. zmianę obrazu tła strony logowania

c. zmianę logo bannera
d. zmianę obrazu tła bannera
e. zmianę koloru tła strony logowania
f. zmianę koloru tła strony bannera
g. zmianę koloru tła strony z treścią
h. zresetowanie ustawień do konfiguracji fabrycznej producenta

34. System musi umożliwiać zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym:
    a. portu HTTP
    b. portu HTTPS
35. System musi umożliwiać automatyczne kasowanie wygasłych kont gościnnych:
    a. na żądanie
    b. okresowo co zadaną liczbę dni i o określonej godzinie
36. System musi posiadać wzorce językowe lub umożliwiać ich dodanie dla stron sponsora i gościa, w tym w językach:
    a. polskim
    b. angielskim
    c. francuskim
    d. niemieckim
37. System musi umożliwiać stworzenie własnego wzorca językowego dla stron sponsora i gościa.
38. System musi umożliwiać specyfikację opcjonalną lub obowiązkową następujących danych gościa w trakcie kreacji konta przez sponsora:
    a. imienia
    b. nazwiska
    c. firmy
    d. adresu e-mail
    e. numeru telefonu
    f. danych opcjonalnych takich jak PESEL (nie mniej niż 5 dodatkowych pól)
39. System musi umożliwiać konfigurację dla użytkowników gościnnych:
    a. wyświetlenia im informacji o polityce akceptowalnego użycia sieci
    b. zezwolenia gościom na zmianę hasła
    c. wymogu zmiany hasła gościa przed wygaszeniem
    d. wymogu ściągnięcia i instalacji klienta głębokiej analizy stacji (posture) przez gościa
    e. samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora
    f. samorejestracji urządzenia końcowego dla dostępu gościnnego
40. System musi umożliwiać konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego
41. System musi umożliwiać konfigurację maksymalnej liczby urządzeń per konto gościnne
42. System musi umożliwiać konfigurację czasu ważności hasła w zadanym przedziale w dniach.
43. System musi umożliwiać kreację profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego.
44. System musi umożliwiać konfigurację polityki złożoności haseł użytkowników gościnnych:
    a. znaków alfabetu, które mogą występować w haśle
    b. minimalnej ilości znaków alfabetu w haśle
    c. znaków numerycznych, które mogą występować w haśle

d. minimalnej ilości znaków numerycznych w haśle
e. znaków specjalnych, które mogą występować w haśle
f. minimalnej ilości znaków specjalnych w haśle

45. System musi umożliwiać konfigurację polityki nazwy (login) użytkownika gościnnego:
    a. tworzenie nazwy użytkownika z adresu e-mail
    b. minimalnej długości nazwy użytkownika
    c. znaków alfabetu, które mogą występować w nazwie użytkownika
    d. minimalnej ilości znaków alfabetu w nazwie użytkownika
    e. znaków numerycznych, które mogą występować w nazwie użytkownika
    f. minimalnej ilości znaków numerycznych w nazwie użytkownika
    g. znaków specjalnych, które mogą występować w nazwie użytkownika
    h. minimalnej ilości znaków specjalnych w nazwie użytkownika

46. System musi umożliwiać rozbudowę licencyjną o funkcjonalność profilowania (profiling) stacji końcowej i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu.
47. System musi umożliwiać dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzacych z nastepujących źródeł:
    a. DHCP
    b. HTTP
    c. RADIUS
    d. Network Scan (NMAP)
    e. DNS
    f. SNMP
48. System musi umożliwiać wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176 po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji.
49. System musi umożliwiać dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy.
50. System musi posiadać dostarczony przez producenta zestaw profili urządzeń, w tym dla:
    a. Android
    b. Apple (MacBook, iPad, iPhone, iPod)
    c. BlackBerry
    d. Stacji roboczych z systemami operacyjnymi (FreeBSD, Linux, OS-X, Windows Vista, Windows 7, Windows XP, OpenBSD, Sun)

51. System musi umożliwiać rozbudowę licencyjną o głęboką analizę stacji końcowej.

52. System musi umożliwiać głęboką analizę stacji końcowej Windows pod kątem plików w tym:
    a. istnienia pliku na stacji końcowej
    b. wersji pliku na stacji końcowej (równa, wcześniejsza niż, późniejsza niż)
    c. daty utworzenia i modyfikacji pliku na stacji końcowej (równa, wcześniej niż, później niż)
53. System musi umożliwiać głęboką analizę stacji końcowej z systemem Windows XP, Windows Vista, Windows 7 pod kątem wpisów w rejestrze, w tym kluczy rejestru z kluczem root: HKLM, HKCC, HKCU, HKU, HKCR z zadanym podkluczem pod kątem:
    a. istnienia lub nieistnienia klucza
    b. wartości klucza rejestru

c. istnienia i wartości domyślnej wartości klucza rejestru typu Number, String, Version

54. System musi umożliwiać głęboką analizę stacji końcowej z systemem Windows XP, Windows Vista, Windows 7 pod kątem uruchomionych aplikacji (Application Condition), w tym:
    a. nazwy uruchomionego lub nie uruchomionego procesu
55. System musi umożliwiać głęboką analizę stacji końcowej z systemem Windows XP, Windows Vista, Windows 7 pod kątem uruchomionych usług systemowych (Service Condition), w tym:
    a. nazwy uruchomionego lub nie uruchomionego procesu
56. System musi umożliwiać tworzenie słownika prostych i złożonych warunków dla głębokiej analizy stacji końcowej za pomocą wyrażeń logicznych AND, OR, NOT
57. System musi umożliwiać głęboką analizę stacji końcowej z systemem Windows XP, Windows Vista, Windows 7, Mac OS-X pod kątem zainstalowanych aplikacji Antywirusowych w tym:
    a. stwierdzenia czy system AV jest obecny na stacji
    b. stwierdzenia czy definicje sygnatur AV są nie starsze niż zadana ilość dni od:
        - daty ostatniego pliku definicji
        - aktualnego czasu systemowego
58. System musi umożliwiać głęboką analizę stacji końcowej z systemem Windows XP, Windows Vista, Windows 7, Mac OS-X pod kątem zainstalowanych aplikacji AntiSpyware w tym:
    a. stwierdzenia czy system AS jest obecny na stacji
    b. stwierdzenia czy definicje sygnatur AS są nie starsze niż zadana ilość dni od:
        - daty ostatniego pliku definicji
        - aktualnego czasu systemowego

59. System powinien zostać dostarczony w postaci virtual appliance – musi być możliwość uruchomienia systemu w środowisku wirtualnym na module serwerowym TYPU A opisanym wyżej.

60. Dopuszcza się zrealizowanie powyższych wymagań w postaci zintegrowanej w jednej aplikacji lub w postaci zespołu aplikacji. W przypadku zespołu aplikacji należy zintegrować poszczególne elementy ze sobą, tak by umożliwiały tworzenie spójnych polityk bezpieczeństwa, zarządzanych centralnie, należy szczegółowo opisać architketurę rozwiązania i udokumnetować w jaki sposób realizowane są poszczególne funkcje i jakie informacje i w jaki sposób są wymieniana poprzez poszczeólne aplikacje. Wszystkie użyte komponenty muszą stanowić rozwiązania komercyjne z gwarantowanym wsparciem technicznym producenta. Należy dołączyć oświadczenia producentów o wzajemnej kompatybilności aplikacji oraz o wsparciu proponowanej architektury.

2.5.3.8 Wymagania techniczne dla urządzeń – System centralnego zarządzania domeną Active Directory

Zamawiający oczekuje migracji aktualnie posiadanego system centralnego zarządzania domeną Active Direktory o 500 użytkowników z zachowaniem pełnej funkcjonalności wraz z licencją Microsoft Server 2012. Dostarczony system powinien zostac zainstalowany na module serwerowym TYPU B opisanym wyżej.

2.5.3.9 Wymagania techniczne dla urządzeń – urządzenie brzegowe do peeringu BGP z funkcją firewall

1. Urządzenie wyposażone w co najmniej 4 porty Gigabit Ethernet przeznaczone dla modułow optycznych typu SFP lub równoważnych, w dostarczonej wersji urządzenie musi posiadać zainstalowane 4 konwertery z portem 1000BASE LX/LH.
2. Możliwość rozszerzenia o przynajmniej:
   a) port 10GigabitEthernet
   b) 4 porty Gigabit Ethernet
   c) interfejs ATM STM1 lub STM4
3. Zapewnia wydajność systemu na poziomie 5Gbps i 7Mpps
4. Min. 8 GB pamięci RAM
5. Obsługuje co najmniej 1 000 000 prefiksów w tablicach rutingu IPv4
6. Obsługuje co najmniej 1 000 000 prefiksów w tablicach rutingu IPv6
7. Obsługuje co najmniej 64 000 tras multicast
8. Obsługuje ruting dynamiczny dla IPv4: OSPF, ISIS, BGP
9. Obsługuje ruting dynamiczny dla IPv6: OSPFv3, ISIS, BGP
10. Wspiera multicast w szczególności: PIM sparse/dense/SSM, IGMP, MLD, Multicast VPN
11. Funkcjonalności związane z niezawodnością pracy
    a) posiada system modularny umożliwiający aktualizację poszczególnych modułów programowych niezależnie od siebie
    b) zapewnia redundancję procesów rutingowych poprzez redundancję modułów zarządzających lub poprzez uruchomienie dwóch kopii systemu operacyjnego.
    c) obsługuje BFD dla OSPF, BGP, ISIS
    d) obsługuje BGP Prefix-Independent Convergence (PIC)
    e) obsługuje Graceful Restart dla OSPF, BGP, ISIS, LDP, RSVP
    f) funkcjonalność VRRP lub odpowiednika
    g) urządzenie wyposażone w redundantne zasilacze 230V
    h) umożliwia wymianę modułów w trakcie pracy (ang. hot swap)
12. Wspiera MPLS, w szczególności
    a) LDP
    b) EoMPLS, VPLS
    c) MPLS L3 VPN
    d) MPLS TE
    e) MPLS FRR w trybach protekcji łącza oraz węzła
13. Obsługuje co najmniej 4000 instancji wirtualnych tablic rutingu
14. Obsługuje mechnizmy jakości usług (QoS):
    a. obsługa mechanizmów QoS (klasyfikacja, kolejkowanie, oznaczanie, policing, shaping) per port/VLAN zarówno dla IPv4 jak i IPv6
    b. obsługa hierarchicznego QoS (H-QoS)
    c. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: adres MAC, adres IP, port TCP, VLAN ID, MPLS EXP, 802.1p (CoS), IP ToS/DSCP.
    d. dynamiczna alokacja kolejek sprzętowych, dostępne min. 16 000 kolejek
    e. implementacja algorytmu Round Robin (Shaped Round Robin) lub podobnego dla obsługi kolejek.
    f. możliwość obsługi jednej z kolejek z priorytetem w stosunku do innych. Mechanizm ograniczania ilości ruchu w kolejce priorytetowej.

g. możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
h. możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi(ingress policing, rate limiting).
i. obsługa WRED lub odpowiednika

15. Posiada funkcjonalności bezpieczeństwa o następujących parametrach:
    a) sprzętowa ochrona warstwy zarządzającej (Control Plane Policing), min. ze wsparciem dla list kontroli dostępu
    b) obsługuje RPF (Reverse Path Forwarding)
    c) min. 25 000 wpisów na listach kontroli dostępu (ACL), min. 4 000 list kontroli dostępu (ACL)
    d) zapora ogniowa typu statefull (ang. statefull firewall), z możliwością konfiguracji polityk per wirtualna tablica routingu, przepustowość 5Gbps dla funkcjonalności Firewall z obsługą 250 000 równoczesnych sesji
    e) sprzętowa obsługa szyfrowania - 1.5 Gbps dla VPN (AES256) z obsługą co najmniej 2 000 tuneli Ipsec. Dopuszcza się zakup dodatkowej licencji w celu uruchomienia tej funkcjonalności

    Dopuszcza zrealizowanie tych funkcjonalności na zintegrowanym module sprzętowym lub na zewnętrznym specjalizowanym urządzeniu. Urządzenie zewnętrzne musi być podłączone za pomocą dedykowanej karty liniowej z interfejsami nieograniczającymi w żaden sposób opisanych powyżej parametrów wydajnościowych oraz posiadać redundantne zasilanie.
16. Obsługuje tunele GRE (1000 tuneli).
17. W ramach funkcjonalności zarządzania:
    a) Umożliwia zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3
    b) Porty umożliwiające zarządzanie: port konsoli, port Ethernet.
    c) Obsługuje Ethernet OAM (IEEE 802.3ah, IEEE 802.1ag, ITU-T Y.1731)
    d) Obsługuje MPLS OAM
    e) Możliwość pisania skryptów konfiguracyjnych
    f) Obsługuje Sflow lub odpowiednik (Open-Flow, Net-Flow)
    g) Wbudowane narzędzia umożliwiające pomiar parametrów jakościowych łącza (np. opóźnienie, jitter, straty pakietów)
    h) Wsparcie dla Radius.

18. Redudatne zasilacze AC 230V
19. Możliwość montażu w szafie 19”

2.5.3.10Wymagania techniczne dla urządzeń – terminale centrum zarządzania sieci (stanowiska operatorskie)

Każde z dwóch stanowisk operatorskich powinno być wyposażone w komputer przenośny o parametrach nie gorszych niż:

Opis wymagań (**minimum**)	
Ekran	TFT 15.6” LED HD o rozdzielczości min 1920x1080, z powłoką matową, nie dopuszcza się matryc typu "glare".

Opis wymagań (**minimum**)	
Procesor	Procesor uzyskujący wynik co najmniej 6000 punktów w teście Passmark - CPU Mark według wyników testów opublikowanych na stronie http://www.cpubenchmark.net/laptop.html
Chipset	Zaprojektowany i wykonany do pracy w komputerach przenośnych rekomendowany przez producenta procesora.
Obudowa	Dopuszczalne kolory - czarny, srebrny, grafitowy, szary lub ich kombinacje.
Pamięć RAM	8GB.
Dysk twardy	250 GB SSD
Karta graficzna	uzyskujący wynik co najmniej 850 punktów w teście Passmark G3D Mark według wyników testów opublikowanych na stronie http://www.videocardbenchmark.net/high_end_gpus.html
Karta dźwiękowa	Karta dźwiękowa zgodna z HD Audio, wbudowane dwa głośniki stereo oraz mikrofon
Połączenia i karty sieciowe	- Port sieci LAN 10/100/1000 Ethernet RJ 45. - Zintegrowana karta sieci WLAN obsługująca łącznie standardy IEEE 802.11 a/b/g/n. - Modem 3G (WWAN)
Porty/złącza (wbudowane, ilość minimalna)	1 x Złącze RJ-45 (podłączenie sieci lokalnej) 1 x Czytnik Kart pamięci 5 w 1 (SD™, MMC, MS, MS PRO, xD) 2 x USB 2.0 1x USB 3.0 1 x VGA (D-Sub), 1 x Gniazdo mikrofonowe 1 x Gniazdo słuchawkowe 1 x HDMI 1 x zasilanie DC-in 1 x Display Port
Klawiatura	Podświetlana, w układzie US-QWERTY, polskie znaki zgodne z układem MS Windows "polski programisty", klawiatura musi być wyposażona w 2 klawisze ALT (prawy i lewy). Klawiatura odporna na zalanie.
Urządzenie wskazujące	1. Touch Pad (płytka dotykowa) z minimum dwoma niezależnymi klawiszami wyboru, 2. Mysz optyczna z dwoma klawiszami i funkcją przewijania

Opis wymagań (**minimum**)	
Czytnik linii papilarnych	Tak
Kamera	Wbudowana kamera o rozdzielczości min 2,0 Mpix,
Napęd optyczny	DVD +/- RW wewnętrzny (z oprogramowaniem do nagrywania płyt DVD oraz odtwarzania płyt DVD Video).
Bateria	zapewniająca min. 5 godzin pracy, plus dodatkowa bateria umożliwiająca pracę w czasie niemniejszym niż bateria oryginalna
Zasilacz	Zewnętrzny, pracujący w sieci elektrycznej 230V 50/60Hz,
Stacja Dokująca	Tak , wraz z dodatkowym zasilaczem
Złącze stacji dokującej	TAK
Gwarancja	5 letnia gwarancja na cały zestaw
System operacyjny	System operacyjny musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: System operacyjny przeznaczony dla komputerów opartych na architekturze x86-64 bit, w wersji aktualnej, to jest wydanej nie wcześniej niż 1.6.2012 . Polska wersja językowa. . Wymagana jest pełna zgodność z posiadanym przez Zamawiającego systemem centralnego zarządzania domeną Active Directory (MS Windows serwer – 2003), w tym miedzy innymi możliwość zdalnej instalacji oprogramowania z poziomu kontrolera domeny, możliwość zastosowania grupowych polityk bezpieczeństwa w pełnym wymiarze ich funkcjonalności.
Oprogramowanie biurowe	Zintegrowany pakiet aplikacji biurowych musi zawierać co najmniej: - edytor tekstów - arkusz kalkulacyjny - narzędzie do przygotowywania i prowadzenia prezentacji - narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) - zainstalowanie na jednym komputerze produktów, pochodzących od różnych producentów, nie jest uznane za ofertę zintegrowanego w aktualnej wersji handlowej Pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. Pakiet biurowy powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim. Dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach od 8-19 – cena połączenia nie większa niż cena połączenia lokalnego.
Certyfikaty i standardy	- Certyfikat ISO 9001:2000 dla producenta sprzętu - Certyfikat ISO 14001 dla producenta sprzętu

Opis wymagań (**minimum**)	
	- Oferowany model notebooka musi być zgodny z normą Energy Star 5.0 - Deklaracja zgodności CE
Torba	Torba dostosowana do wymiarów notebooka.
Mysz	Bezprzewodowa dedykowana do urządzeń przenośnych

2.5.3.11 Wymagania techniczne dla urządzeń – Monitory dla stanowisk operatorskich

Typ matrycy	LED, E-IPS
Przekątna ekranu	24"
Format ekranu	16:10
Rozdzielczość	1920 x 1200
Wielkość plamki	0,27 mm
Jasność	Nie mniej niż 300 cd/m2
Kontrast statyczny	Nie mniej niż 1000:1
Kontrast dynamiczny	2 000 000:1
Kąt widzenia w poziome	178 stopni
Kąt widzenia w pionie	178 stopni
Czas reakcji	8 ms (gtg)
Liczba wyświetlanych kolorów	16,7 mln
Rodzaje wyjść / wejść	DC-in (wejście zasilania) - 1 szt.
	VGA (D-sub) - 1 szt.
	DVI-D - 1 szt.
	DisplayPort - 1 szt
Pobór mocy podczas pracy	Nie więcej niż 38 W
Dodatkowe informacje	Regulacja pochylenia
	Obrotowy ekran (pivot)
	Gwarancja 5 lat
Dołączone akcesoria	Kabel VGA
	Kabel Display Port
	Kabel zasilający

2.5.3.12 Wymagania techniczne dla urządzeń – Serwer video

Możliwość zainstalowania w szafie rack 19''	
Procesor	Procesor uzyskujący wynik co najmniej 6000 punktów w teście Passmark - CPU Mark według wyników testów opublikowanych na stronie http://www.cpubenchmark.net/
Pamięć RAM	8GB.
Karty sieciowe	LAN 10/100/1000 Ethernet RJ 45.
Dysk twardy	1000 GB
Gwarancja	5 letnia gwarancja na cały zestaw
2 karty video zaopatrzone w wyjścia:	VGA (D-sub) - 1 szt.
	DVI-D - 1 szt.
	HDMI - 1 szt

Serwer video powinien być dostarczony wraz z systemem operacyjnym oraz rozwiązaniem programowym umożliwiającym wyświetlanie na jednym z monitorów wielkoformatowych w Pomieszczeniu Zarządzania Siecią informacji z aplikacji zarządzania siecią, a na drugim monitorze wielkoformatowym w tym samym czasie informacji z systemu zarządzania bezpieczeństwem dostępu do sieci lub z systemu paszportyzacji.

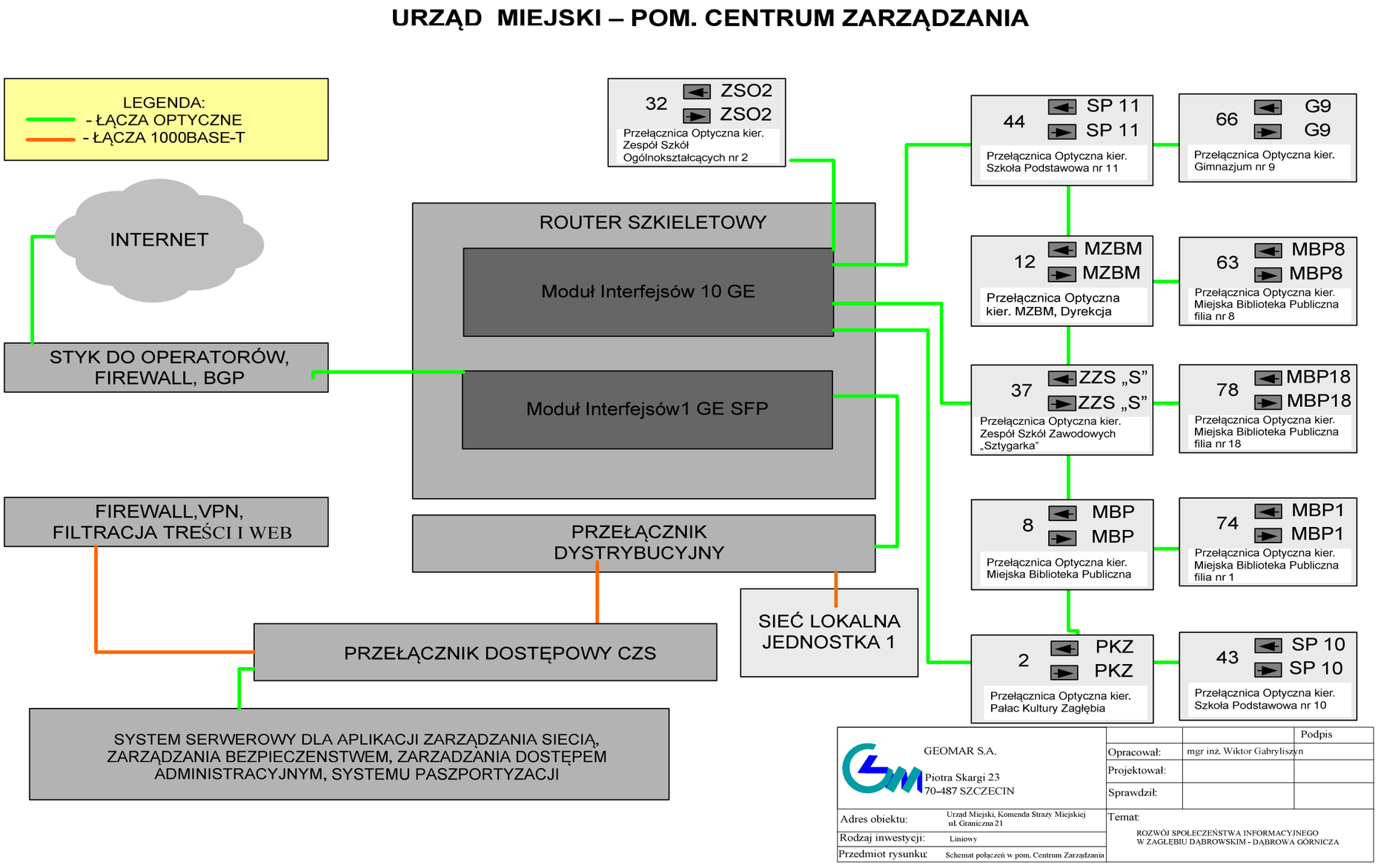
3 SCHEMATY I PLANY WĘZŁÓW SIECI

3.1 WĘZŁY SZKIELETOWE

3.1.1 URZĄD MIEJSKI,– POZ.1

3.1.1.1 Schemat połączeń

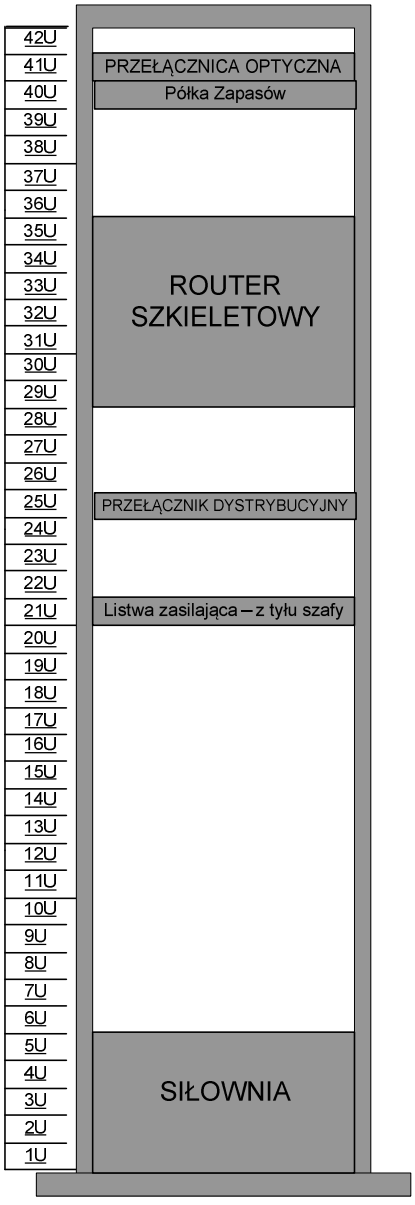
Rysunek 5 Urząd Miejski (CZ) - schemat połączeń



3.1.1.2 Rozmieszczenie urządzeń

Rysunek 6 Urząd Miejski - piętro (CZ) - rozmieszczenie urządzeń (szafa szkieletowa)

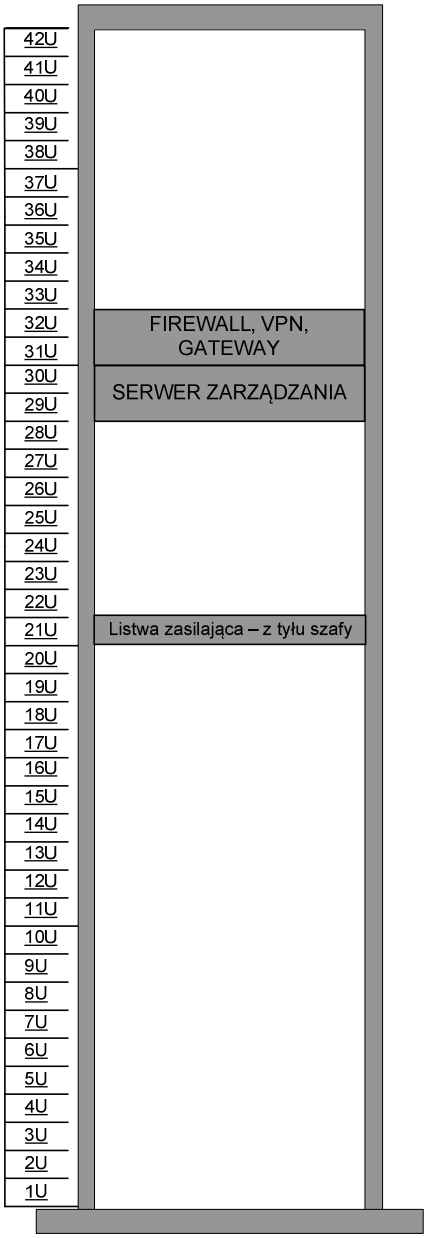
CENTRUM ZARZĄDZANIA – szafa szkieletowa



			Podpis
GEOMAR S.A. ul. Piotra Skargi 23 70-487 SZCZECIN	Opracował:	mgr inż. Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu: Urząd Miejski ul. Graniczna 21 Rodzaj inwestycji: Liniowy Przedmiot rysunku: Szafa szkieletowa w pomieszczeniu Centrum Zarządzania	Temat: ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA		

Rysunek 7 Urząd Miejski - piętro(CZ)
- rozmieszczenie urządzeń (szafa serwerowa)

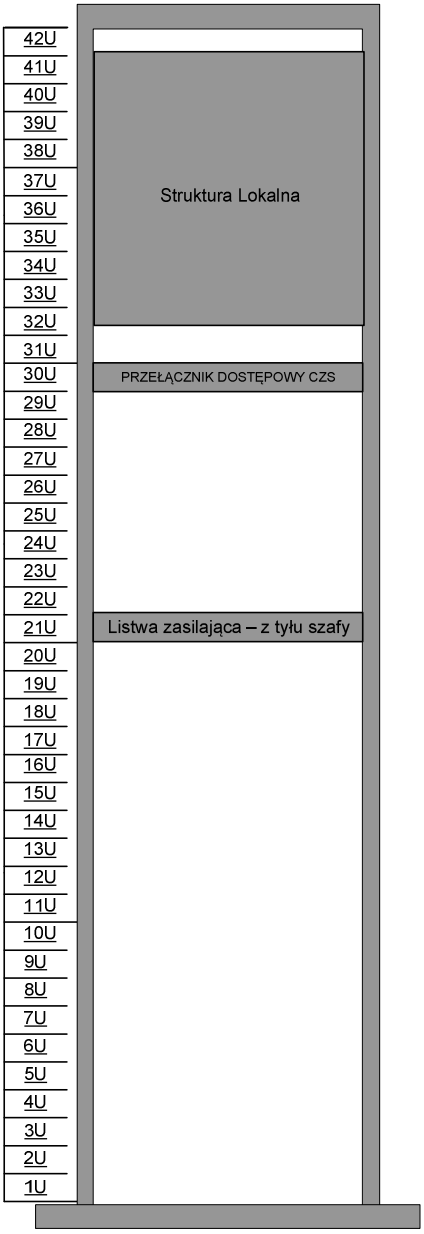
CENTRUM ZARZĄDZANIA – szafa serwerowa



GEOMAR S.A. ul. Piotra Skargi 23 70-487 SZCZECIN			Podpis
	Opracował:	mgr inż.Wiktor Gabryliszyni	
	Projektował:		
	Sprawdził:		
Adres obiektu:	Urząd Miejski ul. Graniczna 21	Temat:	
Rodzaj inwestycji:	Liniowy	ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Przedmiot rysunku:	Szafa serwerowa w pomieszczeniu Centrum Zarządzania		

Rysunek 8 Urząd Miasta - piętro(CZ)
- rozmieszczenie urządzeń (szafa dystrybucyjna)

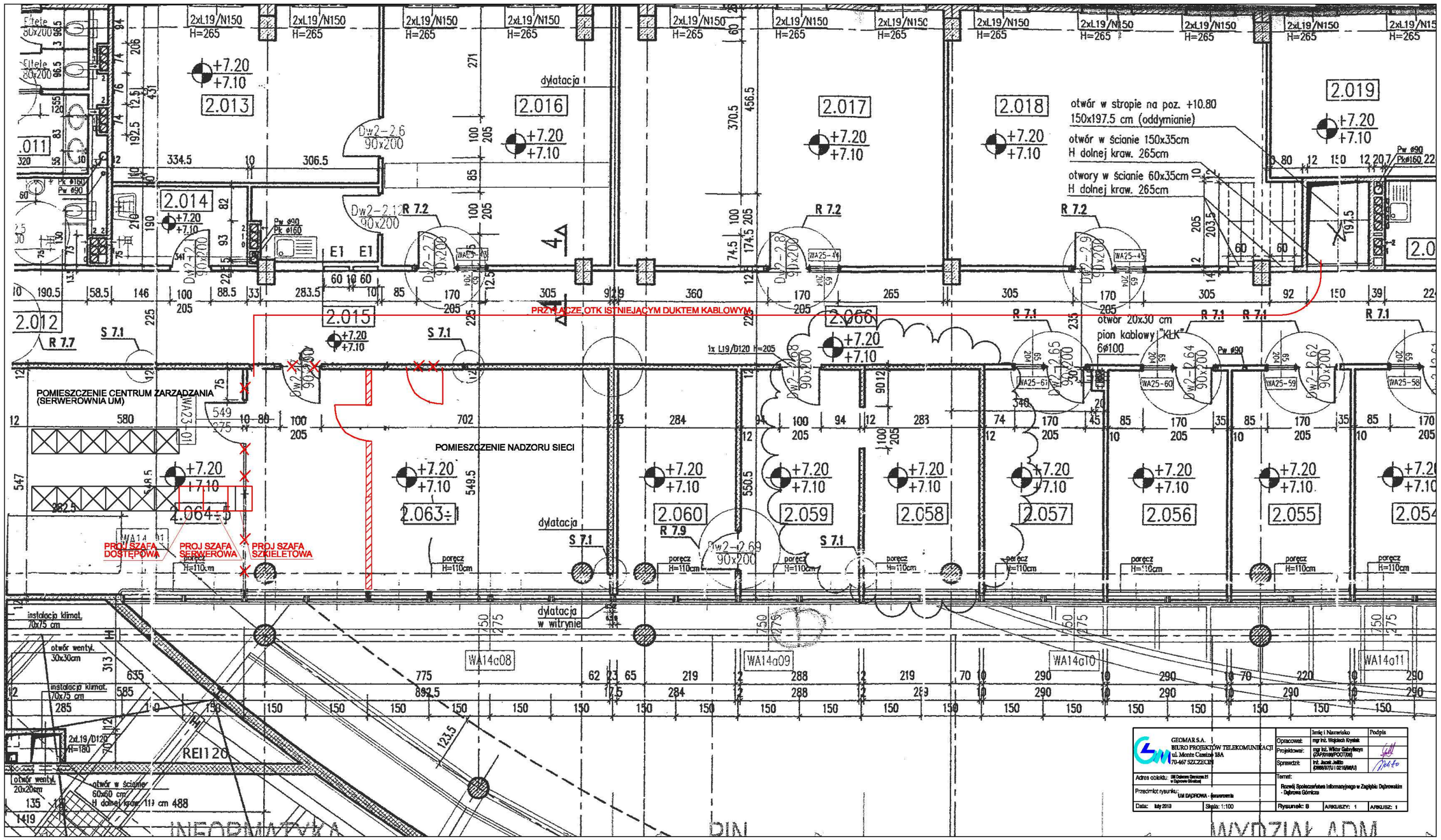
CENTRUM ZARZĄDZANIA – szafa dostępowa



GEOMAR S.A. ul. Piotra Skargi 23 70-487 SZCZECIN			Podpis
	Opracował:	mgr inż. Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu:	Urząd Miejski ul. Graniczna 21	Temat:	
Rodzaj inwestycji:	Liniowy	ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Przedmiot rysunku:	Szafa dostępowa w pomieszczeniu Centrum Zarządzania		

3.1.1.3 Rzut pomieszczenia

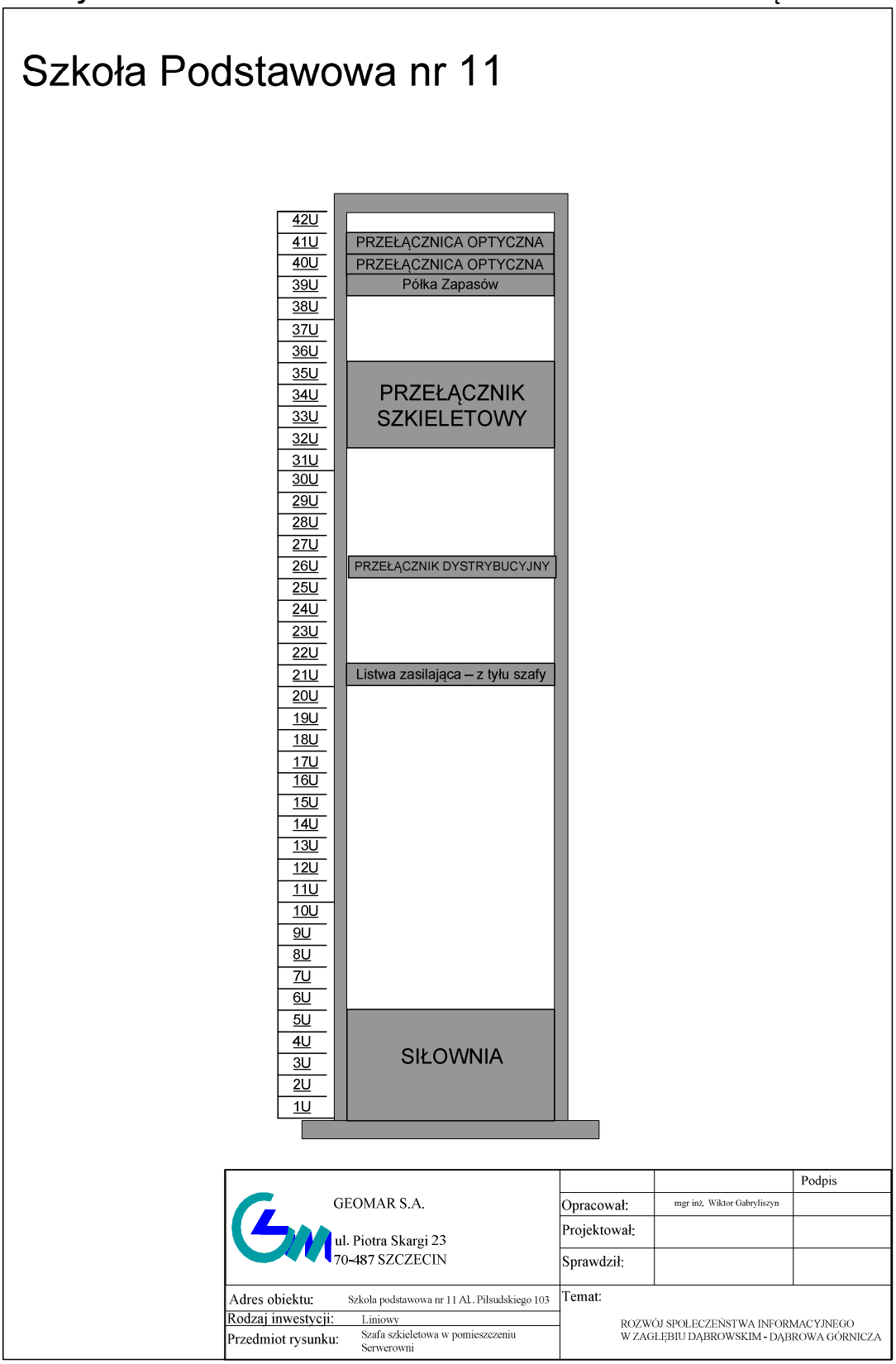
Rysunek 9 Urząd Miejski– piętro (CZ) - rzut pomieszczenia



3.1.2 SZKOŁA PODSTAWOWA NR 11 – POZ.44

3.1.2.1 Rozmieszczenie urządzeń

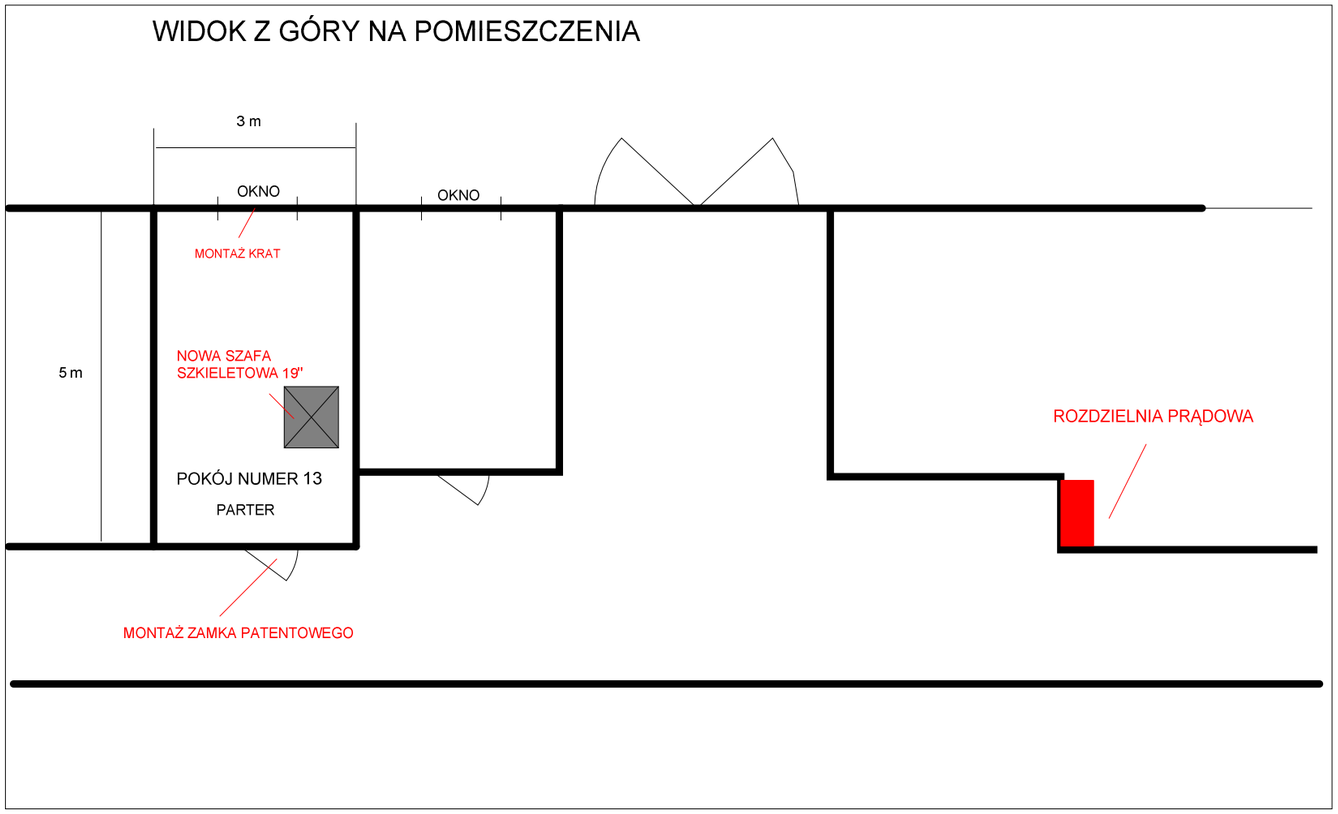
Rysunek 10 Szkoła Podstawowa nr 11 - rozmieszczenie urządzeń



3.1.2.2 Rzut pomieszczenia

Rysunek 11 Szkoła Podstawowa nr 11 - rzut pomieszczenia

SZKOŁA PODSTAWOWA NR 11 Al. Piłsudskiego 103

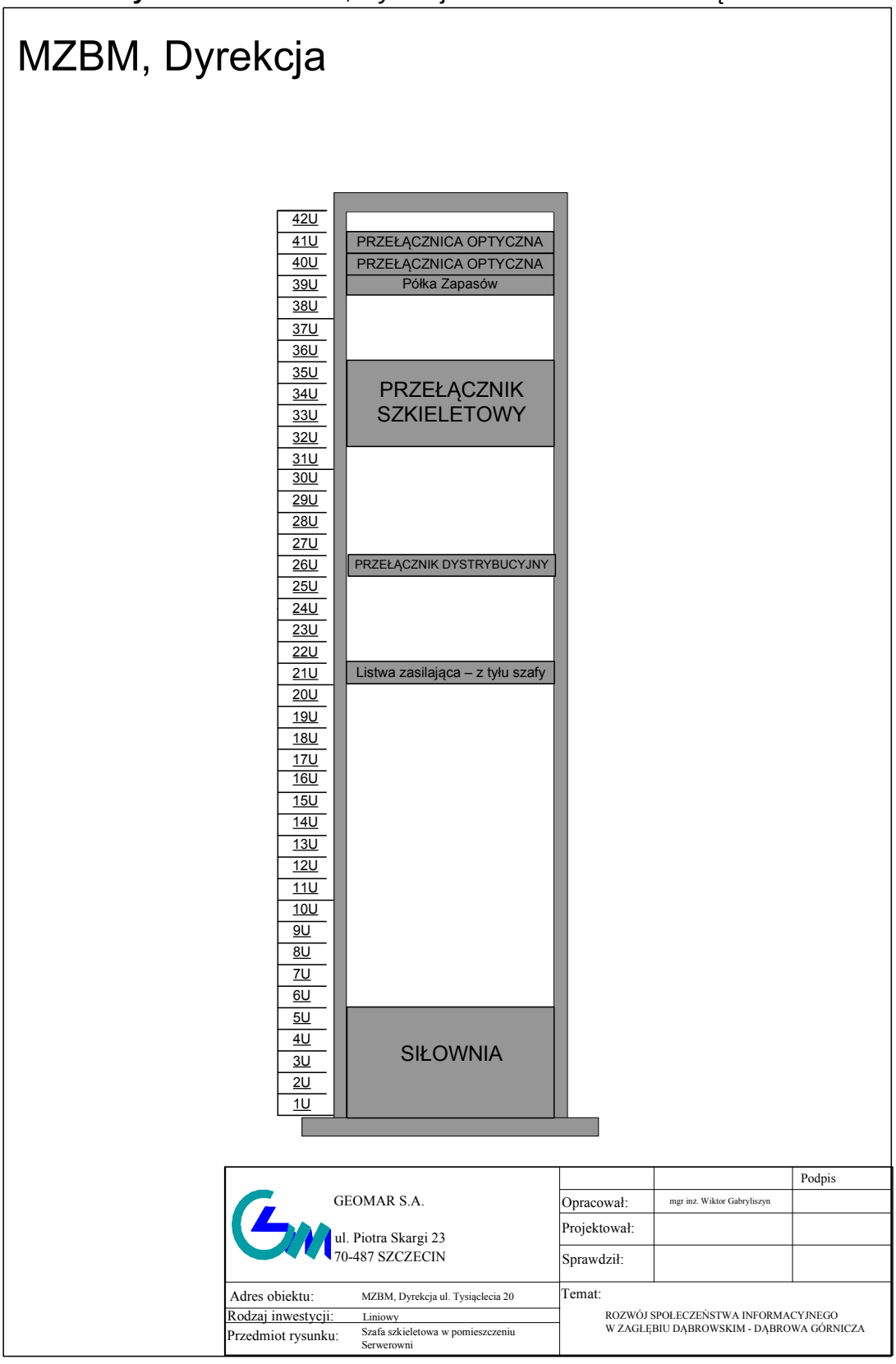


GEOMAR S.A. ul. Piotra Skargi 23 70-487 SZCZECIN			Podpis
	Opracował:	mgr inż. Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu:	Szkoła Podstawowa nr 11 Al. Piłsudskiego 103	Temat:	
Rodzaj inwestycji:	Liniowy	ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Przedmiot rysunku:	Rozmieszczenie urządzeń w pom. Serwerowni		

3.1.3 MZBM, DYREKCJA – POZ.12

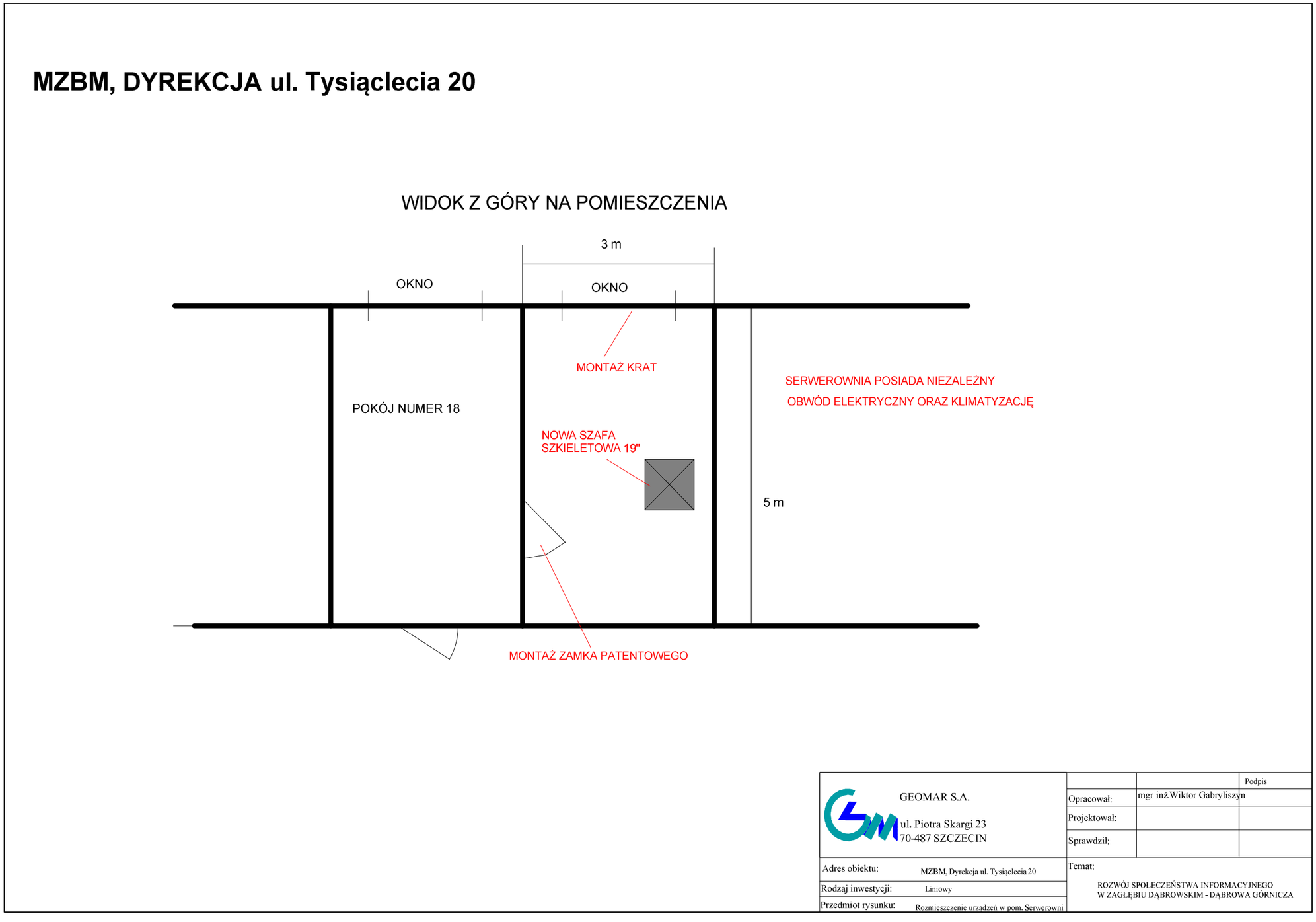
3.1.3.1 Rozmieszczenie urządzeń

Rysunek 12 MZBM, Dyrekcja - rozmieszczenie urządzeń



3.1.3.2 Rzut pomieszczenia

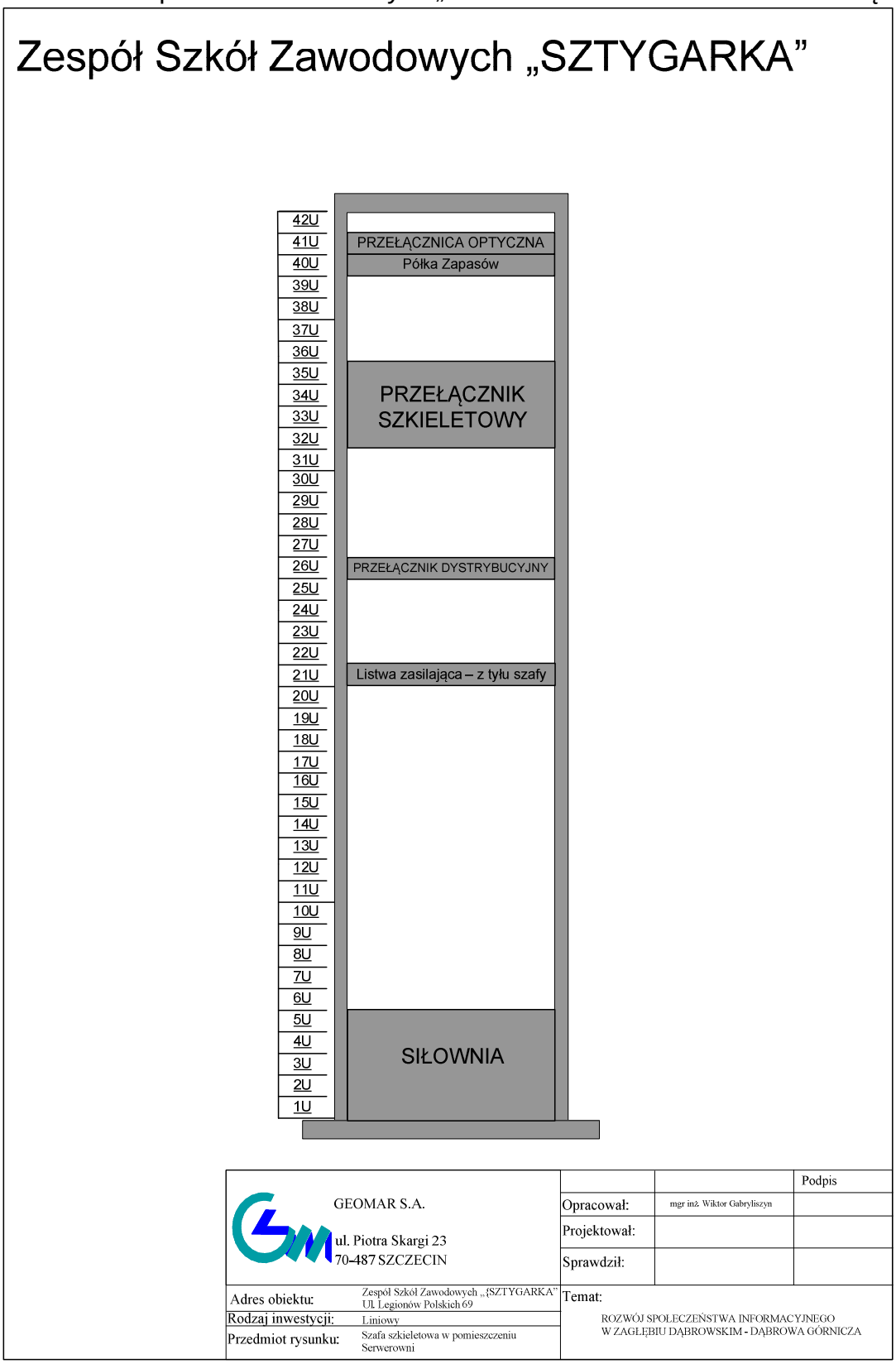
Rysunek 13 MZBM, Dyrekcja - rzut pomieszczenia



3.1.4 ZESPÓŁ SZKÓŁ ZAWODOWYCH „SZTYGARKA” – POZ.37

3.1.4.1 Rozmieszczenie urządzeń

Rysunek 14 Zespół Szkół Zawodowych „SZTYGARKA” - rozmieszczenie urządzeń

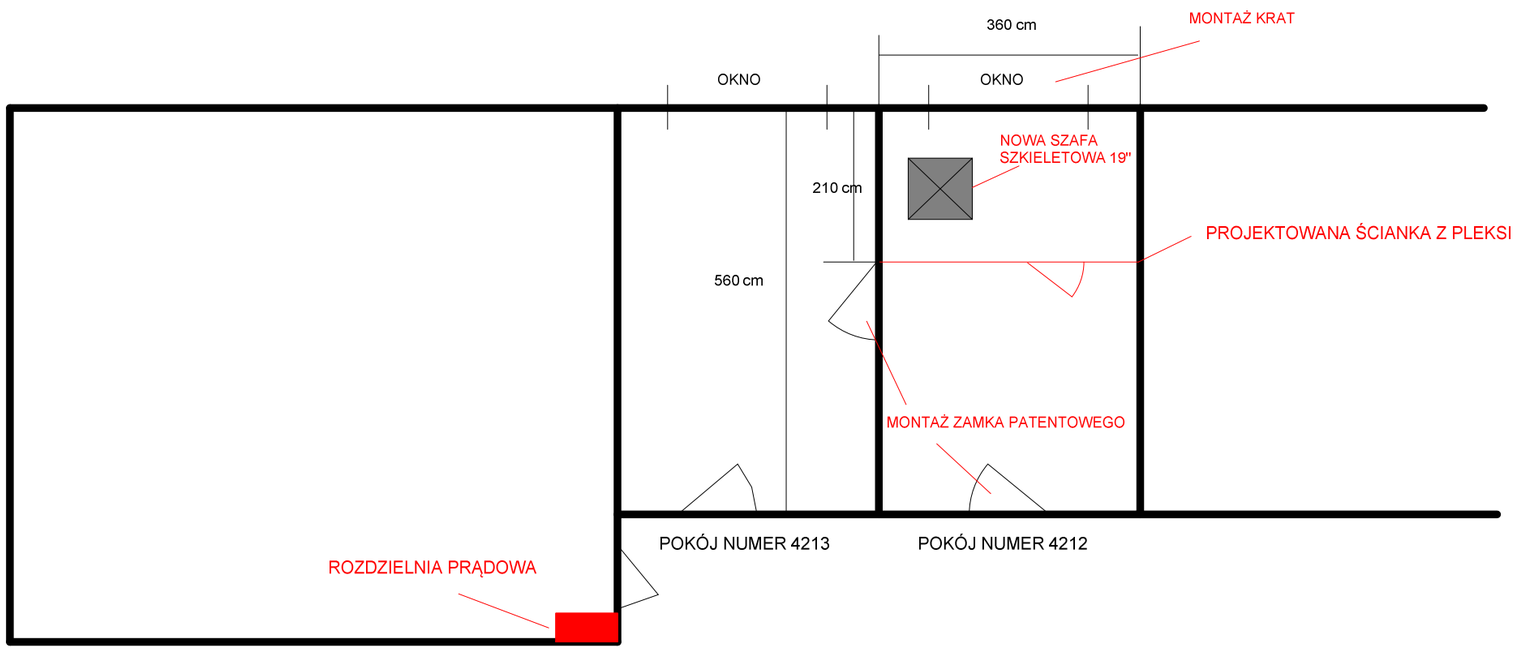


3.1.4.2 Rzut pomieszczenia

Rysunek 15 Zespół Szkół Zawodowych „SZTYGARKA” - rzut pomieszczenia

ZESPÓŁ SZKÓŁ ZAWODOWYCH „SZTYGARKA” ul. Legionów Polskich 131

WIDOK POMIESZCZEŃ Z GÓRY

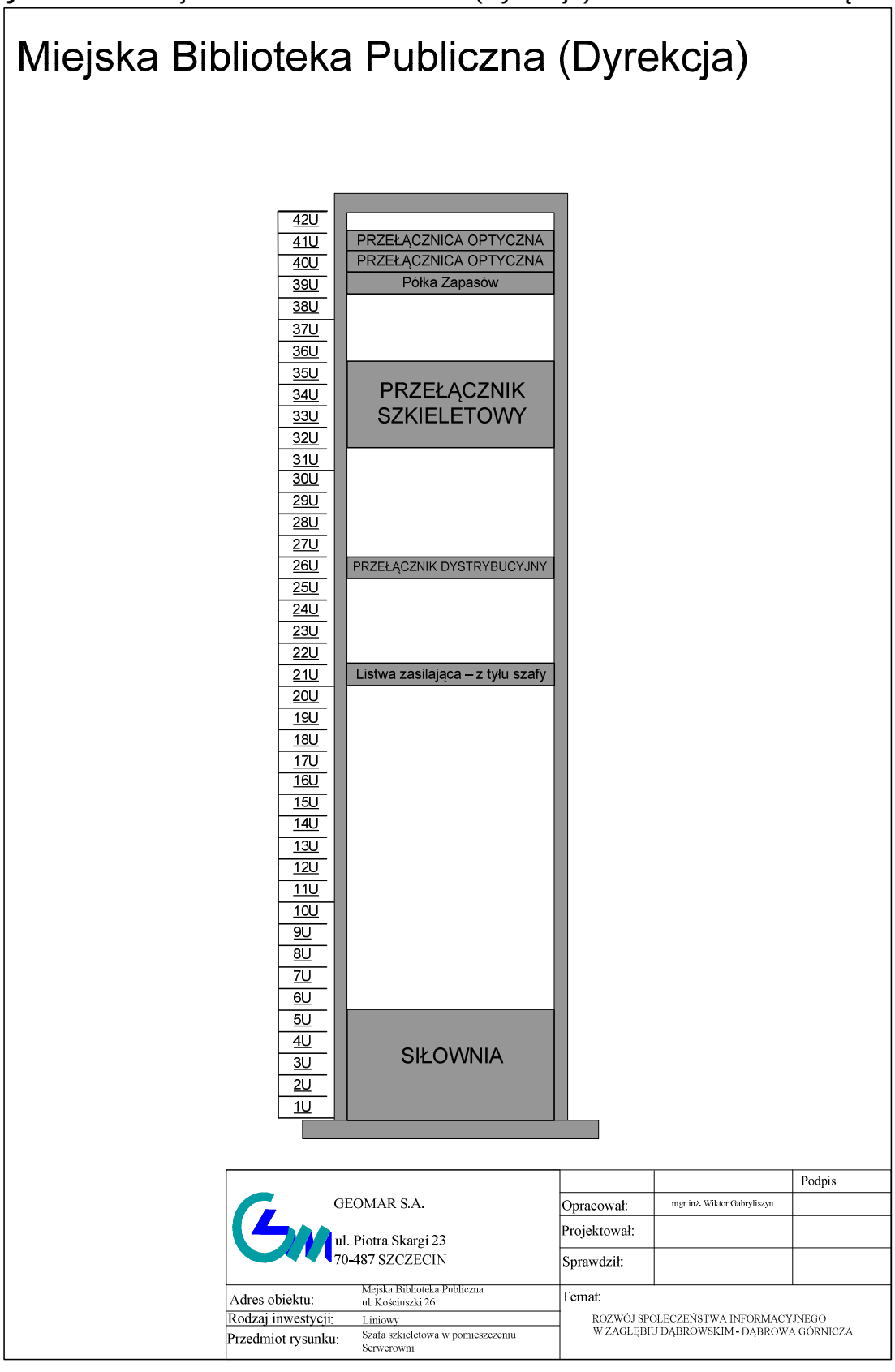


GEOMAR S.A. ul. Piotra Skargi 23 70-487 SZCZECIN			Podpis
	Opracował:		
	Projektował:	Mgr inż.. Wiktor Gabryliszyn	
	Sprawdził:		
Adres obiektu: Zespol Szkól Zawodowych SZTYGARKA Ul. Legionów Polskich 131A	Temat: ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA		
Rodzaj inwestycji: Liniowy			
Przedmiot rysunku: Rozmieszczenie urządzeń w pom. Serwerowni			

3.1.5 MIEJSKA BIBLIOTEKA PUBLICZNA (DYREKCJA) – POZ.8

3.1.5.1 Rozmieszczenie urządzeń

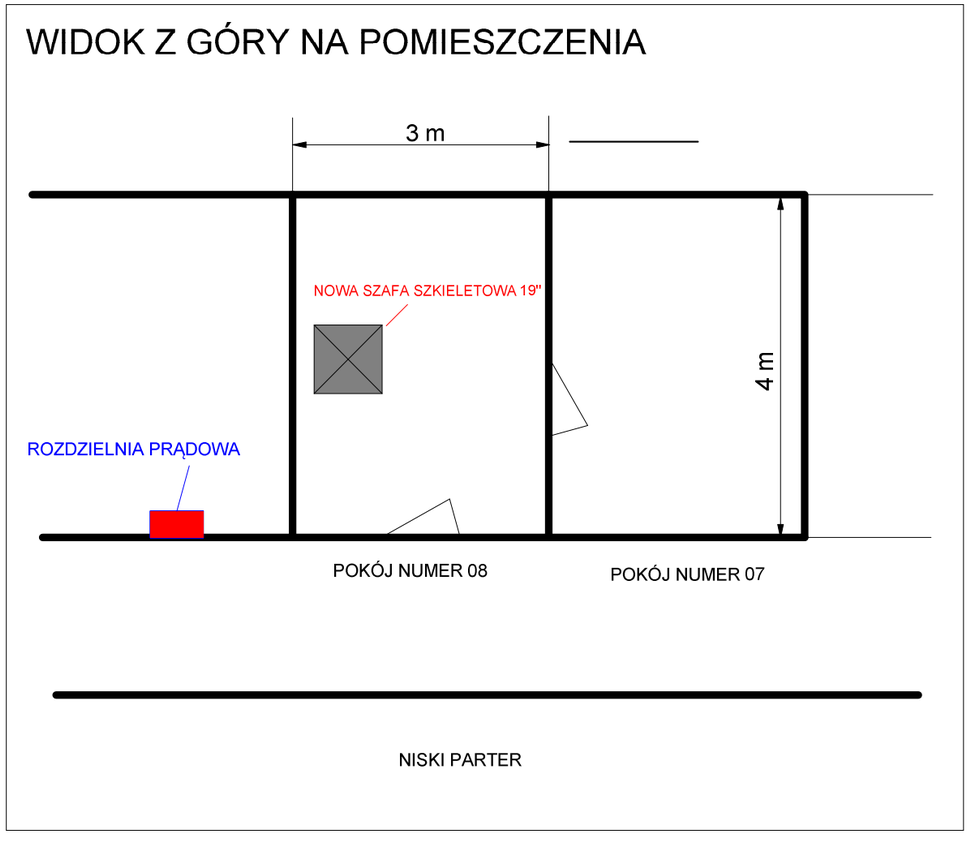
Rysunek 16 Miejska Biblioteka Publiczna (Dyrekcja) - rozmieszczenie urządzeń



3.1.5.2 Rzut pomieszczenia

Rysunek 17 Miejska Biblioteka Publiczna (Dyrekcja) - rzut pomieszczenia

MIEJSKA BIBLIOTEKA PUBLICZNA – DYREKCJA ul. Kościuszki 25

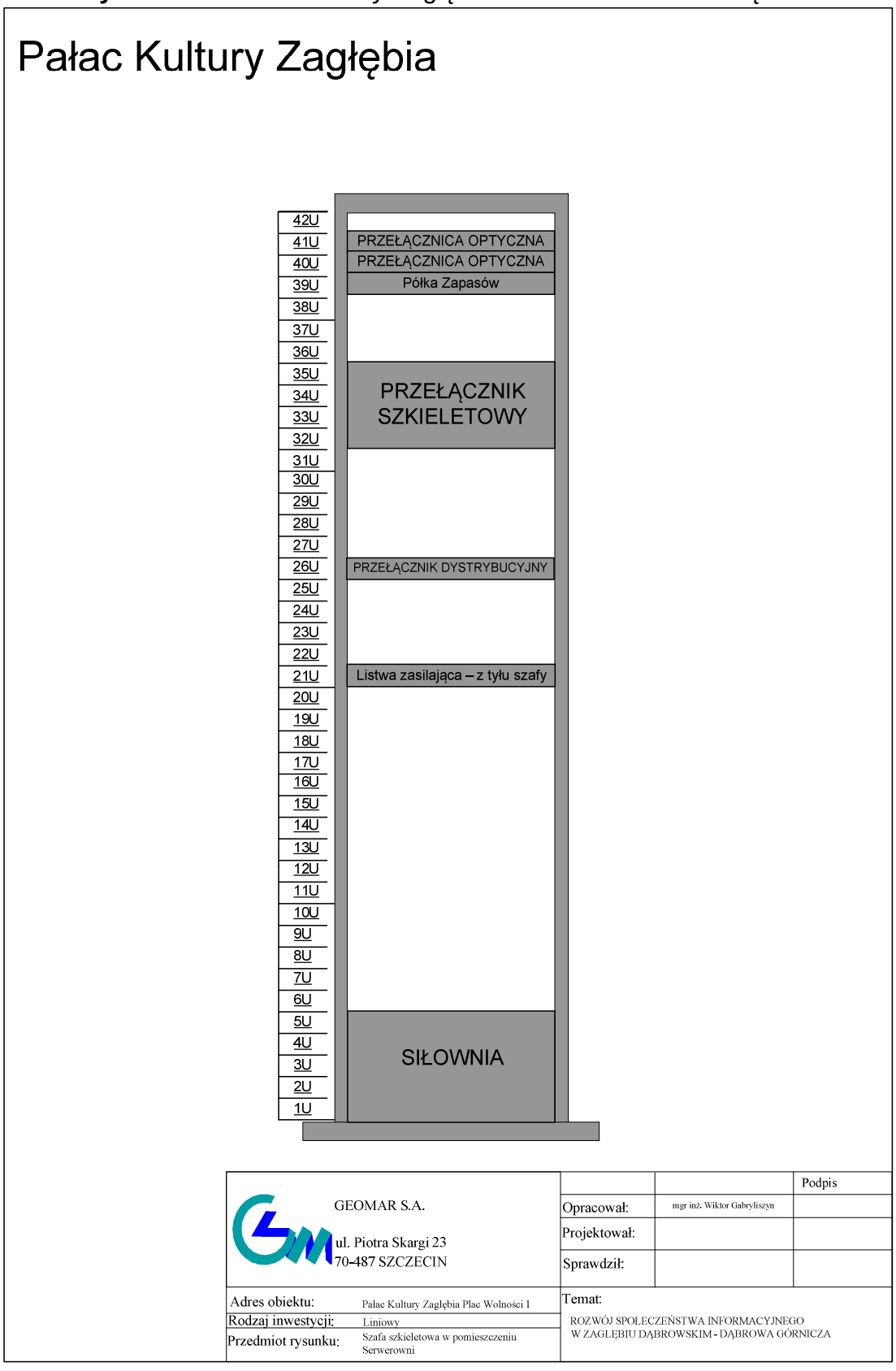


GEOMAR S.A. ul. Piotra Skargi 23 70-487 SZCZECIN			Podpis
	Opracował:	Mgr inż.. Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu:	Miejska Biblioteka Publiczna, Dyrekcja Ul. Kosciuszki 25	Temat: ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Rodzaj inwestycji:	Liniowy		
Przedmiot rysunku:	Rozmieszczenie urządzeń w pom. Serwerowni		

3.1.6 PAŁAC KULTURY ZAGŁĘBIA – POZ.2

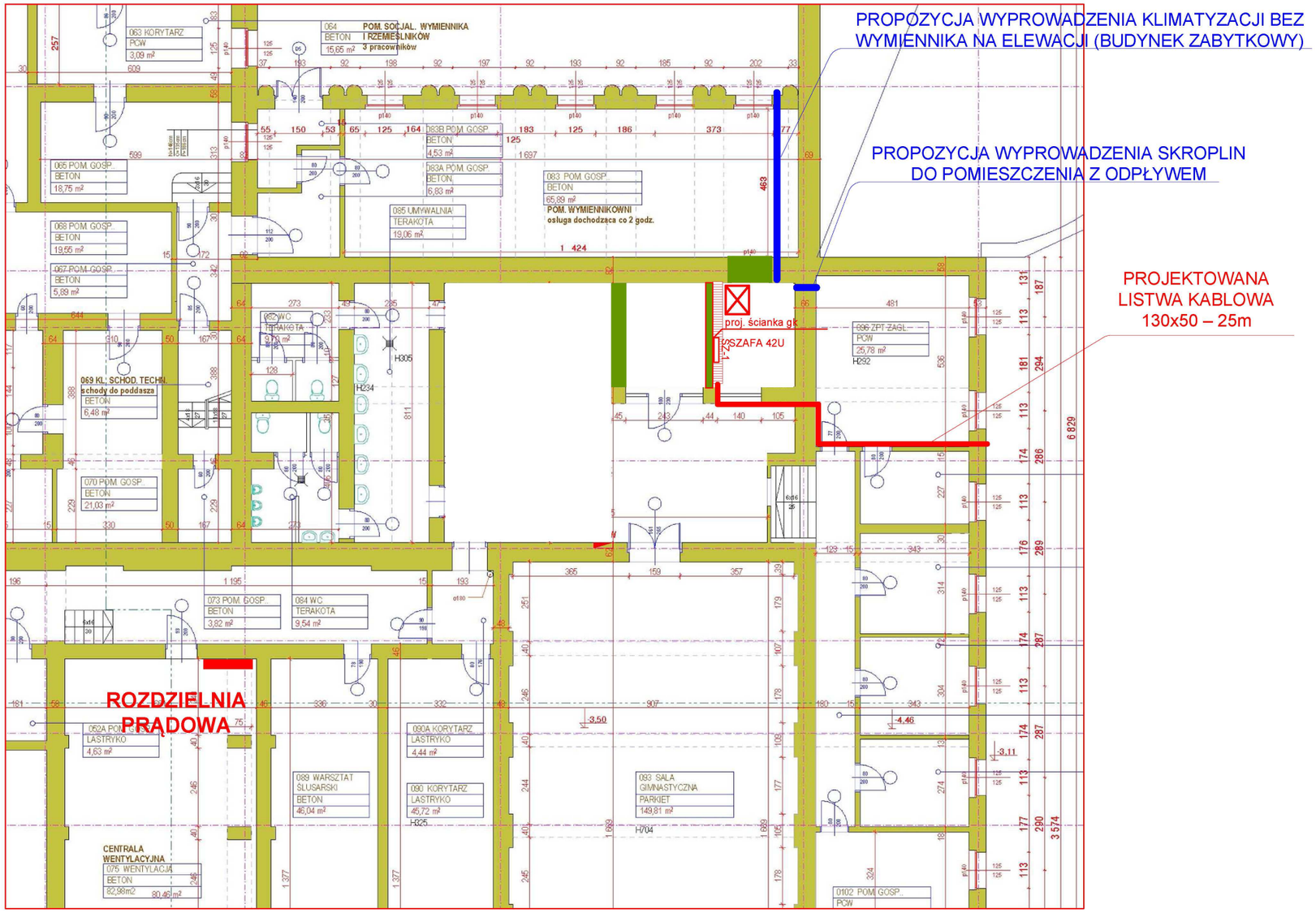
3.1.6.1 Rozmieszczenie urządzeń

Rysunek 18 Pałac Kultury Zagłębia - rozmieszczenie urządzeń



3.1.6.2 Rzut pomieszczenia

Rysunek 19 Pałac Kultury Zagłębia - rzut pomieszczenia



	Podpis	
Opracował:	inż. Marek Ligowski	
Opracował:	mgr inż. Wiktor Gabryliszyn (ZAP/0169/POOT/06)	
Projektował:	mgr inż. Wiktor Gabryliszyn (ZAP/0169/POOT/06)	
Temat:	BUDOWA MIEJSKIEJ SIECI SZEROKOPASMOWEJ DLA MIASTA JASTRZĘBIE ZDRÓJ	
	RYS.: 9	Arkusz: 1 Arkuszy: 1

GEOMAR S.A.
ul. Piotra Skargi 23
70-487 SZCZECIN

Przedmiot rysunku:	Pałac Kultury Zagłębia
Adres obiektu:	Plac Wolności 1, Dąbrowa Górnicza
Rodzaj inwestycji:	Liniowy

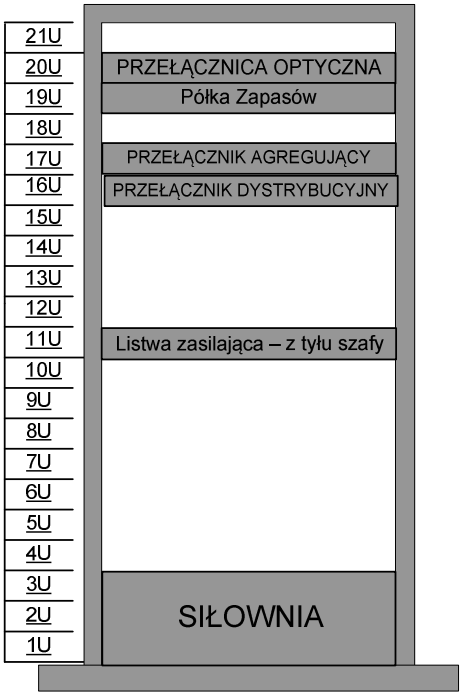
3.2 WĘZŁY AGREGUJĄCE

3.2.1 ZESPÓŁ SZKÓŁ OGÓLNOKSZTAŁCĄCYCH NR 2– POZ. 32 (DOŁĄCZONY DO POZ 1)

3.2.1.1 Rozmieszczenie urządzeń

Rysunek 20 Zespół Szkół Ogólnokształcących nr 2 – rozmieszczenie urządzeń

Zespół Szkół Ogólnokształcących nr 2

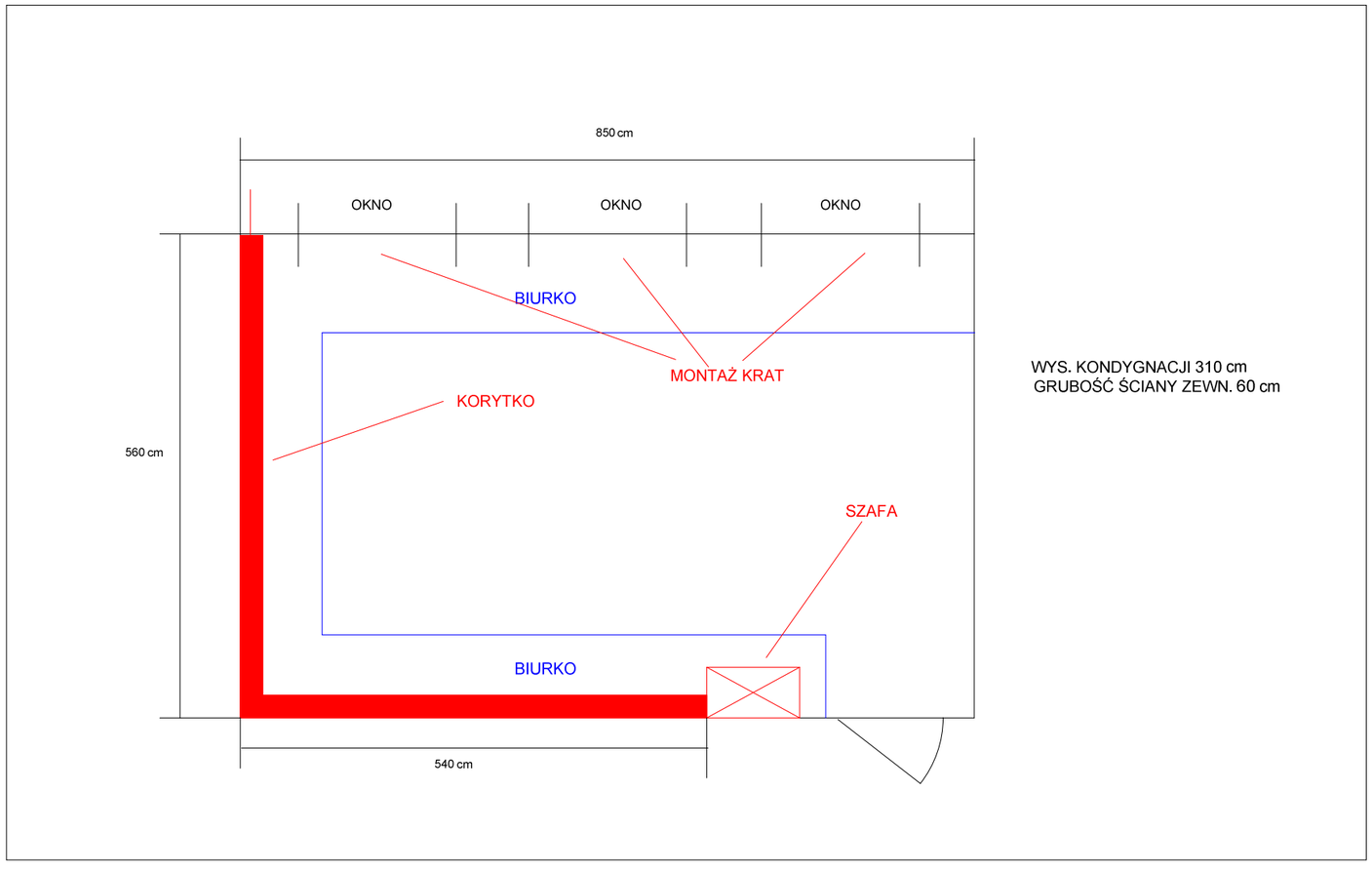


GEOMAR S.A. ul. Piotra Skargi 23 70-487 SZCZECIN			Podpis
	Opracował:	mgr inż. Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu: Zespół Szkół Ogólnokształcących nr 2 Ul. Prusa 3	Temat: ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA		
Rodzaj inwestycji: Liniowy			
Przedmiot rysunku: Szafa węzła w pomieszczeniu Serwerowni			

3.2.1.2 Rzut pomieszczenia

Rysunek 21 Zespół Szkół Ogólnokształcących nr 2 - rzut pomieszczenia

ZESPÓŁ SZKÓŁ OGÓLNOKSZTAŁCĄCYCH NR 2 ul. Prusa 3



WIDOK POMIESZCZENIA Z GÓRY - I PIĘTRO, NUMER POKOJU 20

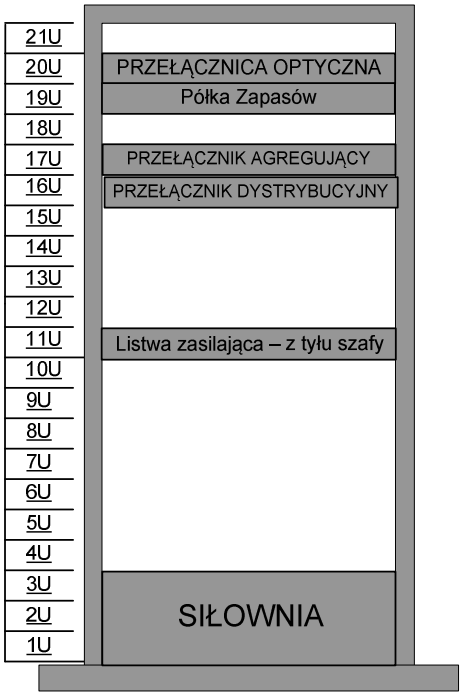
GEOMAR S.A. Ul. Piotra Skargi 23 70-487 SZCZECIN		..	Podpis
	Opracował:		
	Projektował:	Mgr inż. Wiktor Gabryliszyn	
	Sprawdził:		
Adres obiektu: Zespół Szkół Ogólnokształcących nr 2 Ul. Prusa 3	Temat: ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA		
Rodzaj inwestycji: Liniowy			
Przedmiot rysunku: Rozmieszczenie urządzeń w pom. Serwerowni			

3.2.2 GIMNAZJUM NR 9 – POZ. 66 (DOŁĄCZONY DO POZ 44)

3.2.2.1 Rozmieszczenie urządzeń

Rysunek 22 Gimnazjum nr 9 – rozmieszczenie urządzeń

Gimnazjum nr 9

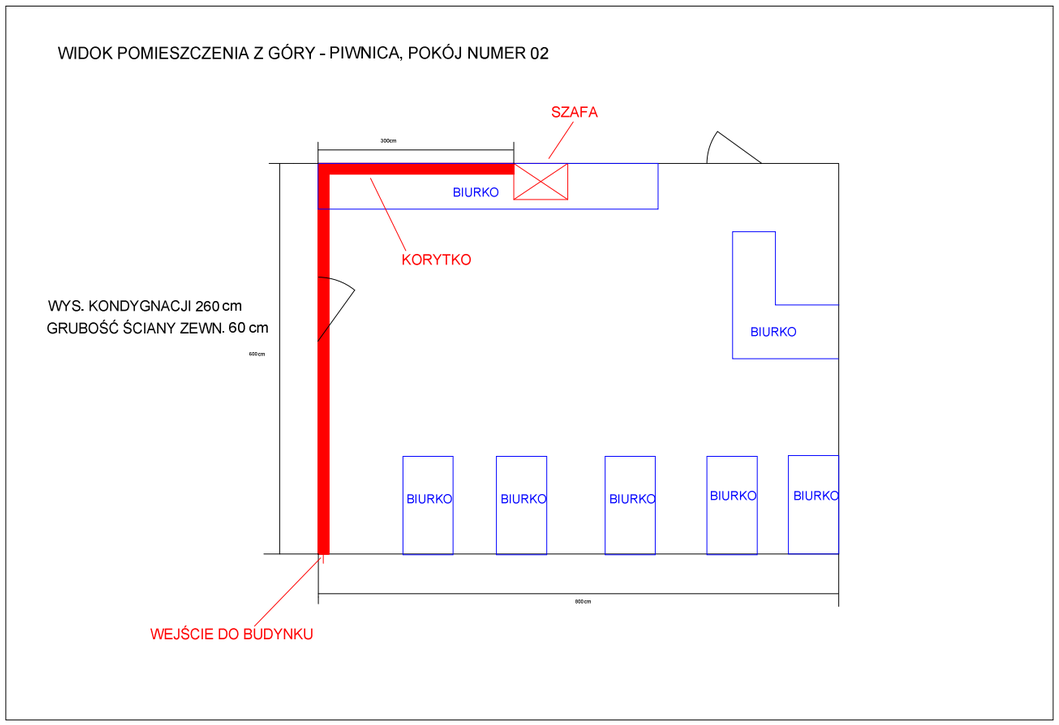


GEOMAR S.A. ul. Piotra Skargi 23 70-487 SZCZECIN			Podpis
	Opracował:	mgr inż. Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu:	Gimnazjum nr 6 ul. Zwycięstwa 44	Temat:	
Rodzaj inwestycji:	Liniowy	ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Przedmiot rysunku:	Szafa węzła w pomieszczeniu Serwerowni		

3.2.2.2 Rzut pomieszczenia

Rysunek 23 Gimnazjum nr 9 - rzut pomieszczenia

GIMNAZJUM NR 9 ul. Zwycięstwa 44



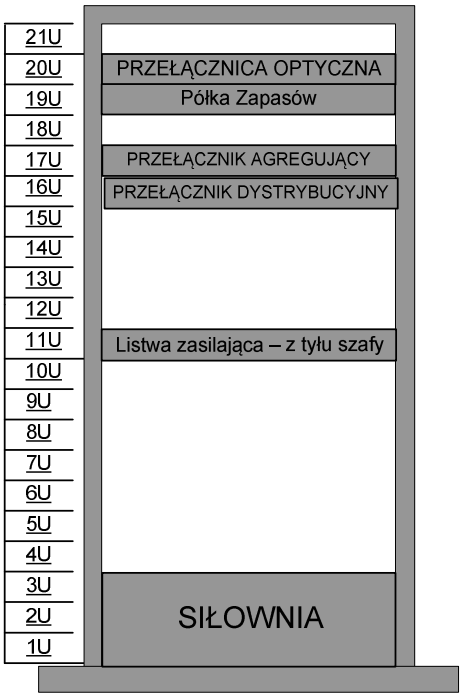
GEOMAR S.A. Ul. Piotra Skargi 23 70-487 Szczecin			Podpis
	Opracował:	Mgr inż.. Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu: Gimnazjum nr 9 ul. Zwycięstwa 44	Temat: ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA		
Rodzaj inwestycji: Liniowy			
Przedmiot rysunku: Rozmieszczenie urządzeń w pom. Serwerowni			

3.2.3 MIEJSKA BIBLIOTEKA PUBLICZNA FILIA NR 8– POZ. 63 (DOŁĄCZONY DO POZ 12)

3.2.3.1 Rozmieszczenie urządzeń

Rysunek 24 Miejska Biblioteka Publiczna filia nr 8 – rozmieszczenie urządzeń

Miejska Biblioteka Publiczna filia nr 8



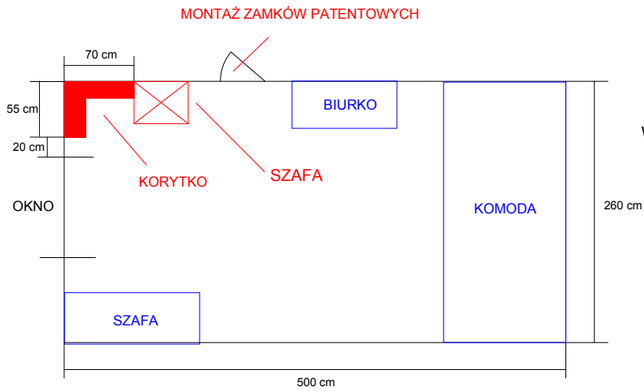
GEOMAR S.A. ul. Piotra Skargi 23 70-487 SZCZECIN			Podpis
	Opracował:	Mgr inż., Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu:	Miejska Biblioteka Publiczna filia nr 8 ul. Ofiar Katynia 93	Temat:	
Rodzaj inwestycji:	Liniowy	ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Przedmiot rysunku:	Szafa węzła w pomieszczeniu Serwerowni		

3.2.3.2 Rzut pomieszczenia

Rysunek 25 Miejska Biblioteka Publiczna filia nr 8- rzut pomieszczenia

MIEJSKA BIBLIOTEKA PUBLICZNA FILIA NR 8 ul. Ofiar Katynia 93

WIDOK POMIESZCZENIA Z GÓRY - PARTER, POMIESZCZENIE SŁUŻBOWE



WYS. KONDYGNACJI 350 cm
GRUBOŚĆ ŚCIANY ZEWN. 60 cm

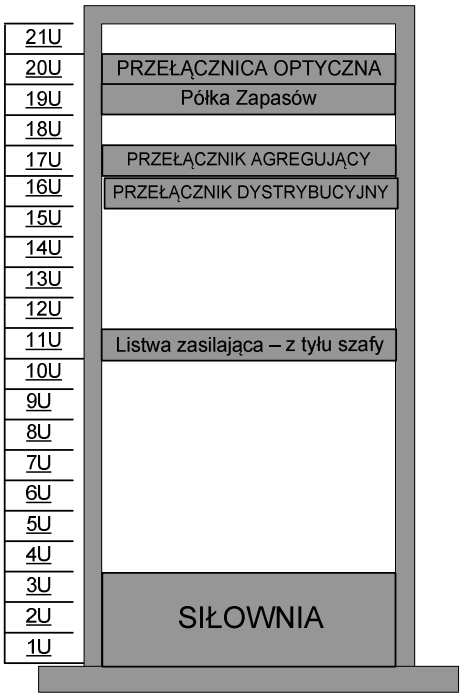
GEOMAR S.A. Ul. Piotra Skargi 23 70-487 Szczecin			Podpis
	Opracował:	Mgr inż.. Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu:	Miejska Biblioteka Publiczna filia nr 8 Ul. Ofiar katynia 93	Temat:	
Rodzaj inwestycji:	Liniowy	ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Przedmiot rysunku:	Rozmieszczenie urządzeń w pom. Serwerowni		

3.2.4 MIEJSKA BIBLIOTEKA PUBLICZNA FILIA NR 18– POZ. 78 (DOŁĄCZONY DO POZ 37)

3.2.4.1 Rozmieszczenie urządzeń

Rysunek 26 Miejska Biblioteka Publiczna filia nr 18 – rozmieszczenie urządzeń

Miejska Biblioteka Publiczna filia nr 18



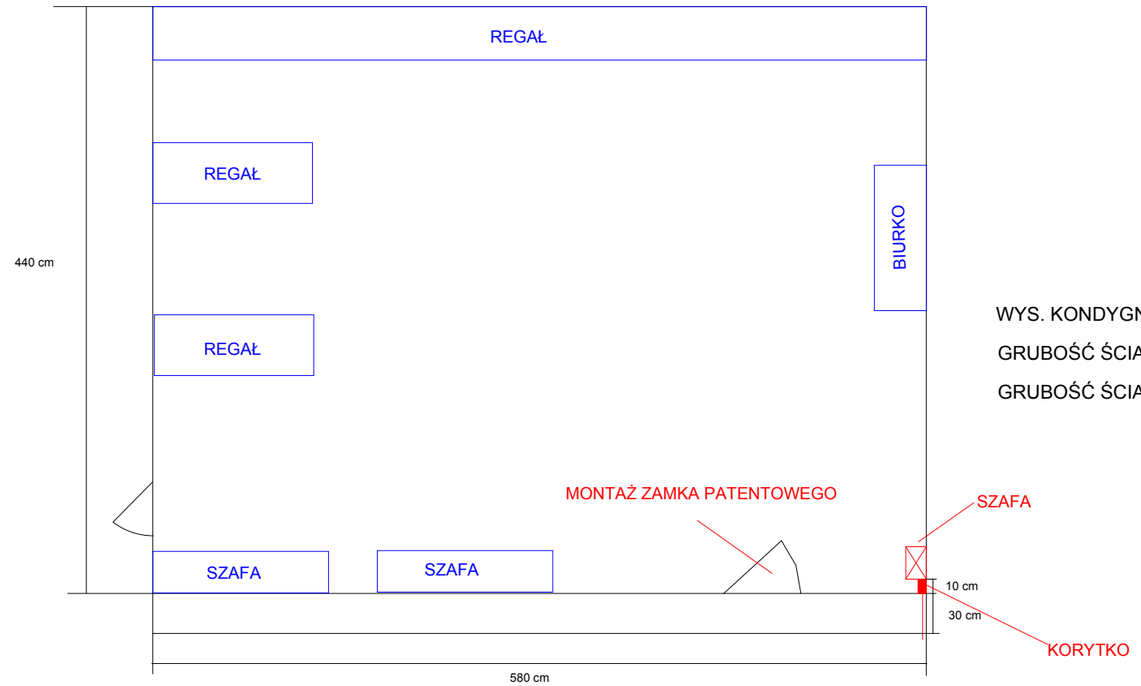
GEOMAR S.A. ul. Piotra Skargi 23 70-487 SZCZECIN			Podpis
	Opracował:	mgr inż. Wiktor Gabryliszyni	
	Projektował:		
	Sprawdził:		
Adres obiektu:	Miejska Biblioteka Publiczna filia nr 18 ul. Legionów Polskich 131	Temat:	
Rodzaj inwestycji:	Liniowy	ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Przedmiot rysunku:	Szafa węzła w pomieszczeniu Serwerowni		

3.2.4.2 Rzut pomieszczenia

Rysunek 27 Miejska Biblioteka Publiczna filia nr 18 - rzut pomieszczenia

MIEJSKA BIBLIOTEKA PUBLICZNA FILIA NR 18 ul. Legionów Polskich 131

RZUT POMIESZCZENIA Z GÓRY - PARTER,
POMIESZCZENIE SŁUŻBOWE



WYS. KONDYGNACJI 300 cm

GRUBOŚĆ ŚCIANY ZEWN. 30 cm

GRUBOŚĆ ŚCIANY WEWN. 30 cm

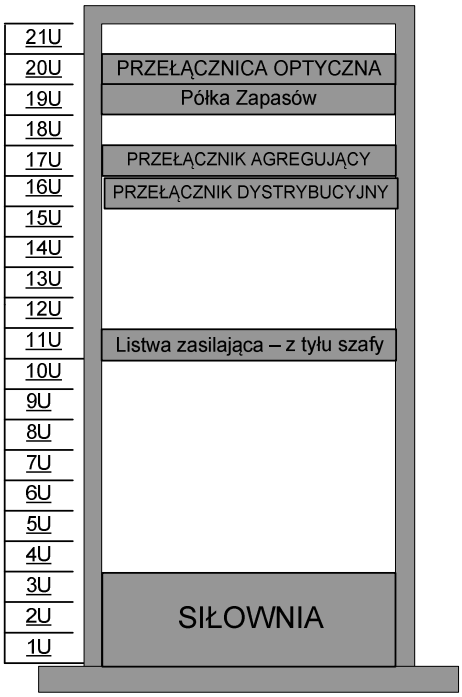
GEOMAR S.A. Ul. Piotra Skargi 23 70-487 SZCZECIN			Podpis
	Opracował:	Mgr inż.. Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu:	Miejska Biblioteka Publiczna filia nr 18 Ul. Legionów Polskich 131	Temat:	
Rodzaj inwestycji:	Liniowy	ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Przedmiot rysunku:	Rozmieszczenie urządzeń w pom. Serwerowni		

3.2.5 MIEJSKA BIBLIOTEKA PUBLICZNA FILIA NR 1– POZ. 74 (DOŁĄCZONY DO POZ 8)

3.2.5.1 Rozmieszczenie urządzeń

Rysunek 28 Miejska Biblioteka Publiczna filia nr 1 – rozmieszczenie urządzeń

Miejska Biblioteka Publiczna filia nr 1



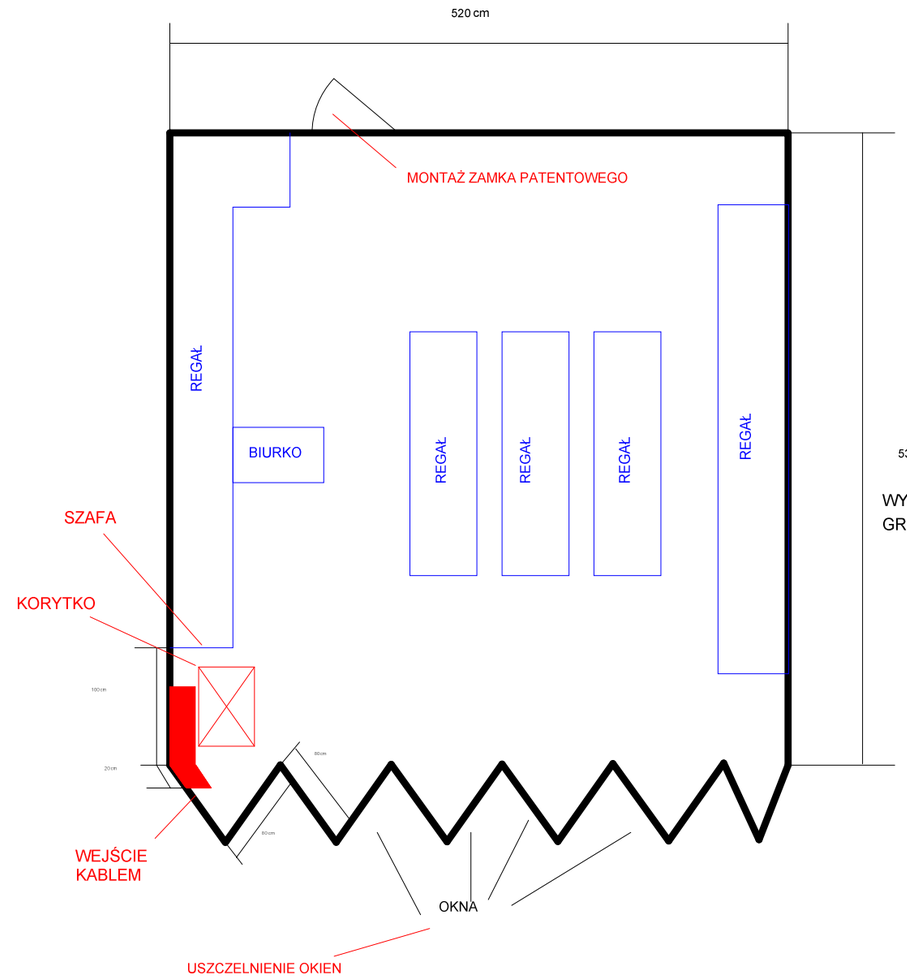
GEOMAR S.A. ul. Piotra Skargi 23 70-487 SZCZECIN			Podpis
	Opracował:	mgr inż. Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu:	Miejska Biblioteka Publiczna filia nr 1 ul. Wojska Polskiego 43	Temat:	
Rodzaj inwestycji:	Liniowy	ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Przedmiot rysunku:	Szafa węzła w pomieszczeniu Serwerowni		

3.2.5.2 Rzut pomieszczenia

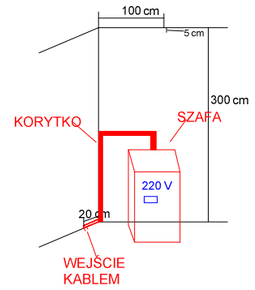
Rysunek 29 Miejska Biblioteka Publiczna filia nr 1 - rzut pomieszczenia

MIEJSKA BIBLIOTEKA PUBLICZNA FILIA NR 1 ul. Wojska Polskiego 43

WIDOK POMIESZCZENIA Z GÓRY - PARTER, POKÓJ NUMER 5



WIDOK POMIESZCZENIA W 3D



WYS. KONDYGNACJI 300 cm
GRUBOŚĆ STROPU 20 cm

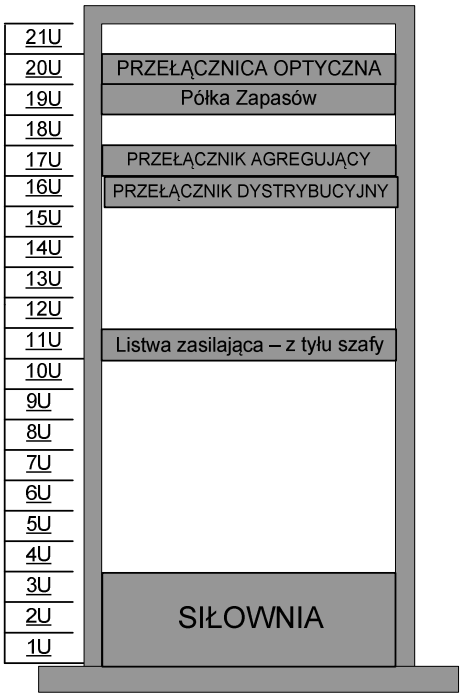
GEOMAR S.A. Ul. Piotra Skargi 23 70-487 Szczecin			Podpis
	Opracował:	Mgr inż. Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu:	Miejska Biblioteka Publiczna filia nr 1 Ul. Wojska Polskiego 43	Temat:	
Rodzaj inwestycji:	Liniowy	ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Przedmiot rysunku:	Rozmieszczenie urządzeń w pom. Serwerowni		

3.2.6 SZKOŁA PODSTAWOWA NR 10– POZ. 43 (DOŁĄCZONY DO POZ 2)

3.2.6.1 Rozmieszczenie urządzeń

Rysunek 30 Szkoła Podstawowa nr 10 – rozmieszczenie urządzeń

Szkoła Podstawowa nr 10



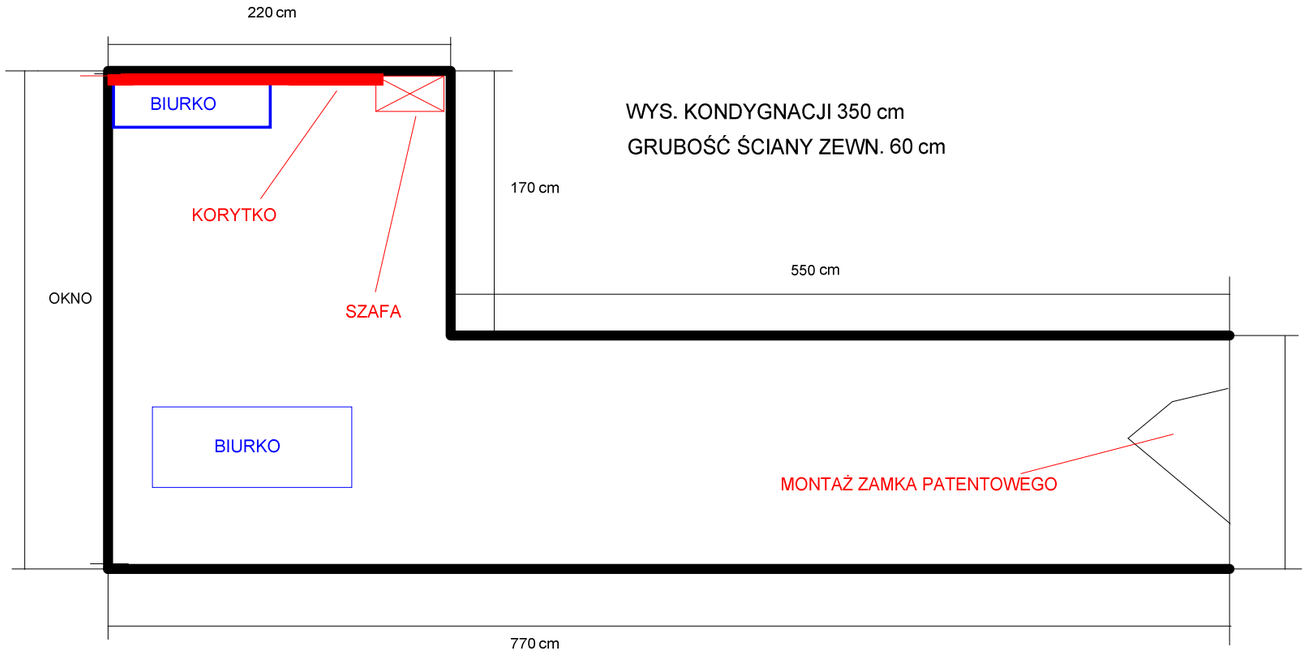
GEOMAR S.A. ul. Piotra Skargi 23 70-487 SZCZECIN			Podpis
	Opracował:	Mgr inż., Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu:	Szkoła Podstawowa nr 10 ul. Górników Redenu 4	Temat:	
Rodzaj inwestycji:	Liniowy	ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Przedmiot rysunku:	Szafa węzła w pomieszczeniu Serwerowni		

3.2.6.2 Rzut pomieszczenia

Rysunek 31 Szkoła Podstawowa nr 10 - rzut pomieszczenia

SZKOŁA PODSTAWOWA NR 10 ul. Górników Redenu 4

WIDOK POMIESZCZENIA Z GÓRY - PARTER, KSIĘGOWOŚĆ



GEOMAR S.A. Ul. Piotra Skargi 23 70-487 SZCZECIN			Podpis
	Opracował:	Mgr inż., Wiktor Gabryliszyn	
	Projektował:		
	Sprawdził:		
Adres obiektu: Szkoła Podstawowa nr 10 Ul. Górników Redenu 4	Temat:		
Rodzaj inwestycji: Liniowy	ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA		
Przedmiot rysunku: Rozmieszczenie urządzeń w pom. Serwerowni			

4 KLIMATYZACJA

W pomieszczeniach serwerowni w węzłach szkieletowych oraz w pomieszczeniach Centrum Zarządzania zostały zaprojektowane urządzenia do klimatyzacji wraz z instalacją freonową i odprowadzenia skroplin. Powyższe urządzenia, wg obowiązującego prawa budowlanego, powinny posiadać dopuszczenie na rynek polski w postaci europejskiego znaku bezpieczeństwa CE.

Proponuje się, aby proces chłodzenia pomieszczeń odbywał się za pomocą indywidualnych systemów klimatyzacyjnych typu SPLIT (jeden agregat sprężarkowo-skraplający obsługujący jedną jednostkę wewnętrzną-parownik), tylko chłodzących. Agregaty zewnętrzne wyposażone w sprężarkę ze zmienną prędkością obrotową, umożliwiającą płynną regulację wydajności chłodniczej klimatyzatorów. Urządzenia działają na zasadzie bezpośredniego odparowania zmiennej ilości czynnika chłodniczego (freon R410A) w urządzeniach klimatyzacyjnych wewnętrznych (czynnik chłodniczy do odparowania pobiera ciepło z pomieszczenia klimatyzowanego). Parowniki w wykonaniu ściennym recyrkulują powietrze wewnętrzne. Sterowanie odbywa się za pomocą bezprzewodowego sterownika (pilota).
Instalacja łącząca agregaty zewnętrzne z jednostkami wewnętrznymi, wykonana z rur miedzianych izolowanych. Odprowadzenie skroplin z jednostek wewn. grawitacyjne lub pompowe.
Czynnikiem roboczym jest ekologiczny czynnik chłodniczy R410A, posiadający atest na stosowanie w unii europejskiej.
Klimatyzatory pracują w następujących przedziałach temp. powietrza zewnętrznego: w trybie chłodzenia od -10 ^{o}C do +46 ^{o}C.
W przypadku Pałacu Kultury Zagłębia klimatyzator musi być jednostką samodzielną z wyrzutem powietrza rurą wentylacyjną (min 6mb) na zewnątrz budynku.

Rysunek 32 Typy klimatyzatorów w pomieszczeniach węzłów szkieletowych

Lp	Nazwa obiektu	Nazwa	Ilość Szt.
1	Urząd Miejski ul. Graniczna 21 Centrum Zarządzania	Agregat zewnętrzny	1
		Jednostka wewnętrzna	1
2	Szkoła Podstawowa nr 11 Al. Piłsudskiego 103	Agregat zewnętrzny	1
		Jednostka wewnętrzna	1
3	MZB, Dyrekcja ul. Tysiąclecia 20	Agregat zewnętrzny	1
		Jednostka wewnętrzna	1
4	Zespół Szkół Zawodowych „SZTYGARKA” Ul. Legionów Polskich 131	Agregat zewnętrzny	1
		Jednostka wewnętrzna	1
5	Miejska Biblioteka Publiczna, Dyrekcja ul. Kościuszki 25	Agregat zewnętrzny	1
		Jednostka wewnętrzna	1

6	Pałac Kultury Zagłębia Plac Wolności 1	Jednostka wewnętrzna z wyrzutem powietrza na zewnątrz	1

Rysunek 33 Parametry minimalne klimatyzatorów

Chłodzenie	wydajność	nominalna	kW	2.5
		min. - max	kw	0.9-3.0
	pobór mocy	klasa energetyczna		A
	wydatek powietrza	jedn.wew.	m3/min	4.1-9.6
Grzanie	wydajność	nominalna	kW	3.2
		min. - max	kw	0.9-4.5
	pobór mocy	klasa energetyczna		A
	wydatek powietrza	jedn.wew.	m3/min	4.6-10.0
Max pobór prądu				A
Zasilanie			V/Hz	230/50
Orurowanie chłodnicze	średnica		mm	6.35-9.52
	maks. dł/maks.różnica poziomów		m	20-gru
Zakres temp pracy jednostki zewn	chłodzenie		C	-10 +46
	grzanie		C	-15 +24

5 ZASILANIE WĘZŁÓW SZKIELETOWYCH

5.1 PRZEDMIOT OPRACOWANIA

Przedmiotem opracowania jest wykonanie instalacji elektrycznej zasilania gwarantowanego oraz częściowo zasilania dedykowanego w pomieszczeniach węzłów szkieletowych sieci szerokopasmowej w Dąbrowie Górniczej.

5.2 ZAKRES OPRACOWANIA

- Przebieg tras zasilania Rozdzielni w węzłach szkieletowych,
- Ogólne schematy Rozdzielni zasilających

5.3 PODSTAWA OPRACOWANIA

Instalację węzłów szkieletowych opracowano na podstawie:

-przekazanych przez Inwestora informacji i dokumentów

- oględzin istniejących instalacji w obiekcie
- wizji lokalnej i inwentaryzacji
- uzgodnień branżowych
- obowiązujących aktualnie norm i przepisów

Normy i przepisy

- PN-IEC 60364-5-523 (Obciążalność prądowa długotrwała przewodów)
- PN-IEC 60364-5-54 (uziemienia i przewody ochronne)
- PN-IEC 60364-4-473 (Środki ochrony przed prądem przetężeniowym)
- PN-IEC 60364-4-443 (Ochrona przed przepięciami atmosferycznymi lub łączeniowymi
- PN-IEC 60364-6-61 (Sprawdzanie odbiorcze)
- PN-IEC 60364-4-41 (Ochrona przeciwporażeniowa)
- PN-IEC 60364-4-482 (Ochrona przeciwpożarowa)
- PN-IEC 60364-5-548 (Układy uziemiające i połączenia wyrównawcze instalacji informatycznych)
- „Prawo budowlane”

5.4 ROZDZIELNIE RK-L I RK-CZ

Schematy ideowe nowej rozdzielnicy RK-L oraz Schematu Zasilania CZ jako propozycje podano na załączonych rysynkach.
Całość instalacji należy wykonać przewodami YDY 3x2,5 układanymi w ciągach kanałów kablowych PCV. W serwerowni nad szafami kable będą ułożone w nowych kanałach metalowych siatkowych np. typu CABLOFIL lub podobnych .

5.5 ZASILANIE CENTRUM ZARZĄDZANIA

Celem zapewnienia niezawodności zasilania Centrum Zarządzania w budynku Urzędu Miejskiego w Dąbrowie Górniczej po dokonaniu wstępnych uzgodnień przyjęto koncepcję:
-UPS redundantny o mocy około 10 kVA , wersja 3 fazy we / 3 fazy wy. będzie zasilany poprzez SZR (Samoczynne Załączanie Rezerwy) przy jednoczesnym podłączeniu dwustronnym zasilania UM.
UPS dodatkowo zostanie wyposażony w zewnętrzny przełącznik serwisowy (bypass) umożliwiający całkowite odłączenie UPS-a celem naprawy lub wymiany.
UPS zostanie zainstalowany w istniejącym pomieszczeniu energetycznym na parterze.
Zasilanie Centrum Zarządzania zostanie zrealizowane poprzez WLZ (Wewnętrzna Linia Zasilająca) z pomieszczenia energetycznego na parterze poprzez dwa obwody zasilające:
- obwód zasilania ogólnego z SZR-a
- obwód zasilania gwarantowanego z UPS-a

Urządzenia aktywne oraz gniazdka w pomieszczeniu obsługi oraz oświetlenie zasilane będą z obwodów UPS-a.
Gniazdka zasilania ogólnego oraz Klimatyzacja zasilana będzie z obwodu zasilania ogólnego poprzez SZR.
Obwody zasilające gniazdka należy wykonać w listwach PCV.
W Serwerowi zasilanie szaf z urządzeniami aktywnymi wykonać w korytkach metalowych siatkowych.
Do poprowadzenia obwodów elektrycznych należy maksymalnie wykorzystać przestrzeń nad sufitem podwieszonym.
Zejście WLZ-tów z I Piętra wykonać pionem technicznym. Na parterze maksymalnie wykorzystać istniejące trasy korytek metalowych oraz istniejące przepusty.
Przejścia przez strefy ogniowe zabezpieczyć masą ogniochronną.
Wszystkie Rozdzielnie (po uzgodnieniu) w wykonaniu natynkowym.
.

5.6 PARAMETRY UPS

UPS redundantny o mocy około 10 kVA

Parametry	Wymagania minimalne
Moc pozorna	10kVA
Moc rzeczywista	10kW
Możliwość skalowania mocy w ramach urządzenia bez konieczności dokładania dodatkowych modułów	max do 20kVA/16kW
Topologia	VFI-SS-111

Urządzenie fabrycznie nowe tj. data ich produkcji nie może być wcześniejsza niż 3 miesiące przed datą dostawy	wymagane
Napięcie wejściowe	~173 – 485V rms +/-2%
Częstotliwość napięcia	45 – 55Hz +/- 1Hz
Napięcie wyjściowe	~400V rms +/-2%
Sprawność całkowita dla Pmax (dla VFI)	<94%
Sprawność całkowita dla Pmax (dla ECO)	>98%
Współczynnik mocy PF	>0,99
Moc bierna pojemnościowa	0 VAR
THDi nominalne	3%
Zniekształcenia napięcia wyjściowego THDu	<1,2% dla Pmax (liniowe) <5% (nieliniowe wg PN=EN 62040-3)
Przeciążalność	130% - 10min 160% - 1min 300% - 10ms
Prąd zwarcia	> 5 In
Współczynnik szczytu CF	6:1
Akumulatory	Szczelne bezobsługowe o projektowanej żywotności 6-9 lat, Minimum 64szt 12V9Ah zamontowane wewnątrz UPSa, gwarantujące minimum 19min podtrzymania dla obciążenia 10kW
Komunikacja	RS232, USB Karta SNMP/http umożliwiająca zdalne zarządzanie (przegląd parametrów, kondycja ogniw, reset, test) Wbudowane bezpotencjałowe wyjścia programowalne (min. 4) oraz Wejścia sterujące (min. 5) Sygnalizacja awarii
Sygnalizacja optyczna	Otwierany panel LCD z możliwością ustawienia pod różnym kątem oraz 3 diody LED sygnalizujące tryb pracy, załączenie linii bypass, tryb awaryjny
Oprogramowanie	W języku polskim pod systemy Windows i Linux umożliwiające bezpieczne zamknięcie systemu; możliwość zarządzania komputerami w sieci LAN (min. 30 stanowisk)
Wbudowany w UPS czujnik temperatury i wilgotności	Odczyt parametrów na wyświetlaczu LCD
Redundancja	Minimum praca w systemie tzw. „gorącej rezerwy” opisana w normie PN-EN 62040-3:2011
Zimny start	wymagane
Ilość wydzielanego ciepła dla nominalnych warunków pracy	< 2600 BTU
Certyfikaty / oświadczenia	CE
	ISO 9001:2008 obejmujące projektowanie, produkcję, sprzedaż, serwis, doradztwo i instalowanie systemów zasilania
	Karta katalogowa oferowanego rozwiązania
	Oświadczenie producenta iż dostarczane urządzenie będzie fabrycznie nowe, wyprodukowane nie wcześniej, niż na 2 miesiące przed ich dostarczeniem
	w przypadku nie wywiązania się z obowiązków gwarancyjnych przez wykonawcę, producent przejmie na siebie zobowiązania związane z gwarancją
	Oświadczenie producenta iż sprzęt i oprogramowanie będzie pochodzić z autoryzowanego kanału sprzedaży

	Okres gwarancji minimum 5lat uwzględniający baterie, także w zakresie ich naturalnego eksploatacyjnego zużycia przed terminem 5lat.

UPS redundantny o mocy około 3 kVA

Parametry	**Wymagania minimalne**
Moc pozorna	3 kVA
Moc rzeczywista	2,4 kW
Topologia	VFI
Obudowa	Rack/Tower max wysokość w wersji Rack - 2U max głębokość 660mm (dla szaf agregujących - max głębokość pozwalająca na montaż w szafie 60x60)
Zakres napięcia wejściowego (zależnie od obciążenia)	140-275VAC
Częstotliwość napięcia	50Hz +/-5%
Napięcie wyjściowe	~230V +/-2%
Zniekształcenia harmoniczne (odbiornik liniowy/nieliniowy)	≤4% / ≤6%
Przeciążalność	<110% - ostrzeżenie 111 - 135% - 12sekund (UPS w tryb bypass) >135% - 1,5sekundy (UPS wyłączony)
Zabezpieczenie zwarciowe	Wymagane
Akumulatory	Szczelne bezobsługowe, Minimum 6szt 12V9Ah zamontowane wewnątrz UPSa, gwarantujące minimum 10min podtrzymania dla 50% obciążenia
Możliwość podpięcia modułów bateryjnych	Tak, max 4szt Automatyczne wykrywanie dodatkowych modułów
Komunikacja	RS232, USB Karta SNMP/http umożliwiająca zdalne zarządzanie (przegląd parametrów, kondycja ogniw, reset, test), sygnalizacja awarii
Sygnalizacja optyczna	Wyświetlacz LCD z menu w języku polskim oraz 3 diody LED sygnalizujące tryb pracy sieciowej, tryb bypass/Eco, błąd
Oprogramowanie	W języku polskim pod systemy Windows i Linux umożliwiające bezpieczne zamknięcie systemu;
Zabezpieczenia	Przeciążeniowe, przeciwzwarciowe, przepięciowe, termiczne, akumulatorów
Certyfikaty / oświadczenia	CE
	ISO 9001:2008 obejmujące projektowanie, produkcję, sprzedaż, serwis, doradztwo i instalowanie systemów zasilania
	Karta katalogowa oferowanego rozwiązania
	w przypadku nie wywiązania się z obowiązków gwarancyjnych przez wykonawcę, producent przejmie na siebie zobowiązania związane z gwarancją
	Oświadczenie producenta iż sprzęt i oprogramowanie będzie pochodzić z autoryzowanego kanału sprzedaży
	Okres gwarancji minimum 5lat uwzględniający baterie, także w zakresie ich naturalnego eksploatacyjnego zużycia przed terminem 5lat.

5.7 INSTALACJA OŚWIETLENIOWA

W remontowanch i adaptowanych pomieszczeniach przewidziano instalację oświetleniową odpowiednią dla charakteru pomieszczeń. W Centrum Zarządzania część opraw będzie z modułem podtrzymania awaryjnego. Szczegółowe rozwiązania zostaną podane w Projekcie Wykonawczym.

5.8 INSTALACJA ELEKTRYCZNA KLIMATYZATORA

Wszystkie obwody związane z szafami klimatyzacyjnymi zsilane będą z sieci napięcia dedykowanego.

5.9 POŁĄCZENIA WYRÓWNAWCZE

W celu wyrównania potencjału sieci logicznych połączono listwę zasilającą urządzenia komputerowe z przewodem PE jak również połączono korytka metalowe oraz szafy logiczne z przewodem PE linką LgY 6mm.

5.10 OCHRONA OD PORAŻEŃ

Dla ochrony przed dotykiem pośrednim należy zastosować szybkie wyłączenie zasilania w układzie TN-S. Ochrona realizowana jest przez zastosowanie wyłączników instalacyjnych nadmiarowoprądowych oraz wyłączników przeciwporażeniowych różnicowoprądowych o czułości 30 mA
Po wykonaniu instalacji należy przeprowadzić pomiary skuteczności zabezpieczeń ze względu na szybkie wyłączenie, poprawności działania wyłączników różnicowoprądowych oraz pomiary stanu izolacji przewodów.

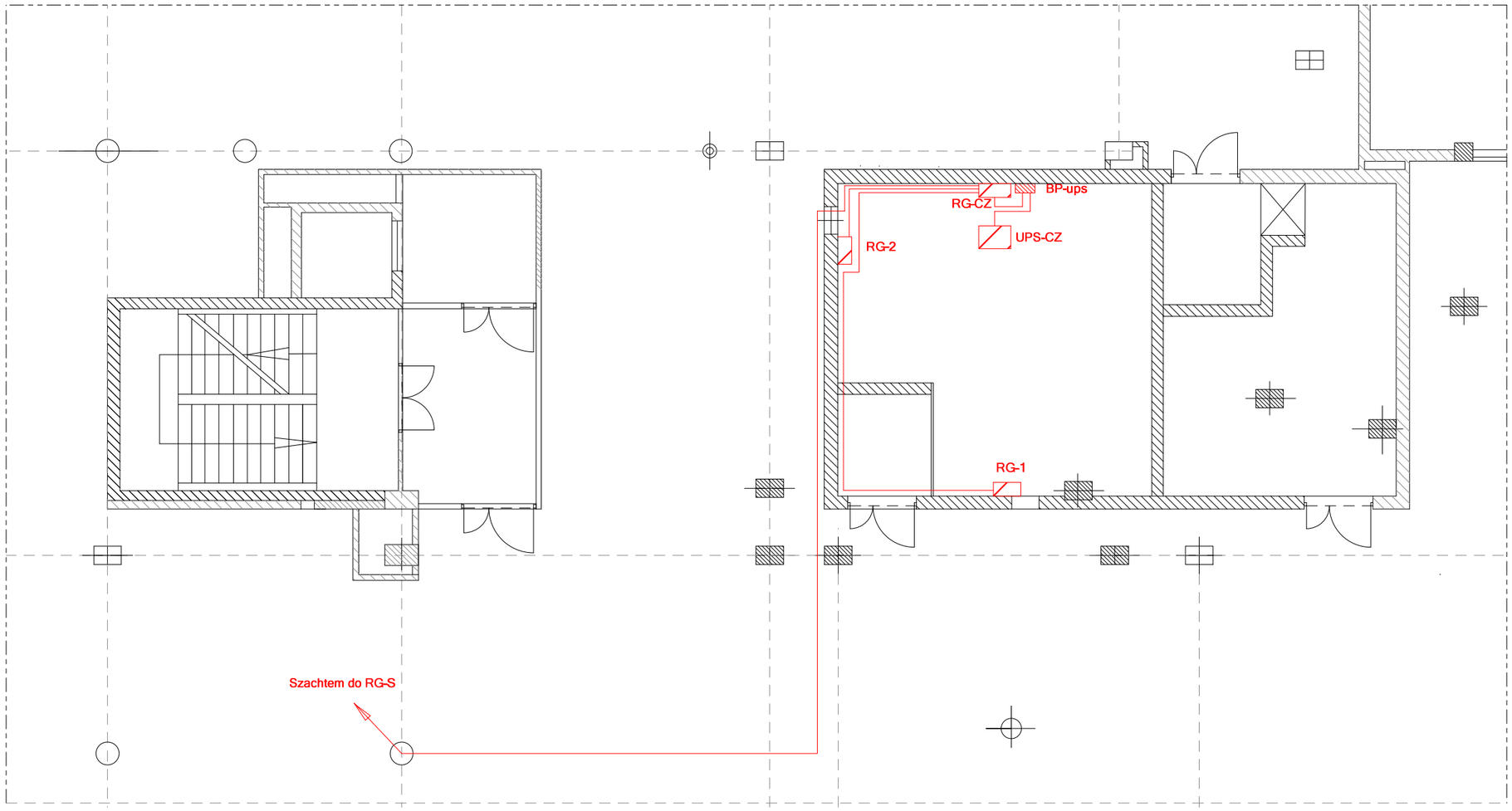
5.11 ZASILANIE URZĄDZEŃ AKTYWNYCH WĘZŁÓW DYSTRYBUCYJNYCH

W instalacji urządzeń aktywnych węzłów dystrybucyjnych zapewnia się ochronę przeciwporażeniową podstawową i dodatkową zgodnie z wymaganiami pakietu norm PN-IEC 60364-4 i PN-IEC 60364-5. Ochronę podstawową przed dotykiem bezpośednim spełnić przez stosowanie urządzeń izolowanych posiadających atest i odpowiedni stopień ochrony. Podczas montażu w szafie 6U urządzenie należy podłączyć kablem zasilającym do gniazdka sieciowego w pomieszczeniu a obudowę szafy 6U do przewodu ochronnego PE instalacji elektrycznej. W celu weryfikacji instalacji pod kątem spełniania norm należy uzyskać od administratora aktualne zaświadczenie z przeglądu instalacji elektrycznej w budynku. W przypadku braku dokumentów należy bezzwłocznie zgłosić ten fakt zamawiającemu. Po wykonaniu robót elektrycznych objętych niniejszym projektem należy dokonać pomiarów, zgodnie z obowiązującymi przepisami i zaleceniami PN-IEC 60364-4. Wszystkie prace należy wykonywać zgodnie z obowiązującymi przepisami i normami branżowymi. Po zakończeniu prac, należy doprowadzić obszar objęty robotami do stanu pierwotnego.

Rysunek 34 Urząd Miejski – poziom parkingu - zasilanie urządzeń

URZĄD MIEJSKI, KOMENDA STRAŻY MIEJSKIEJ ul. Graniczna 21

PARTER

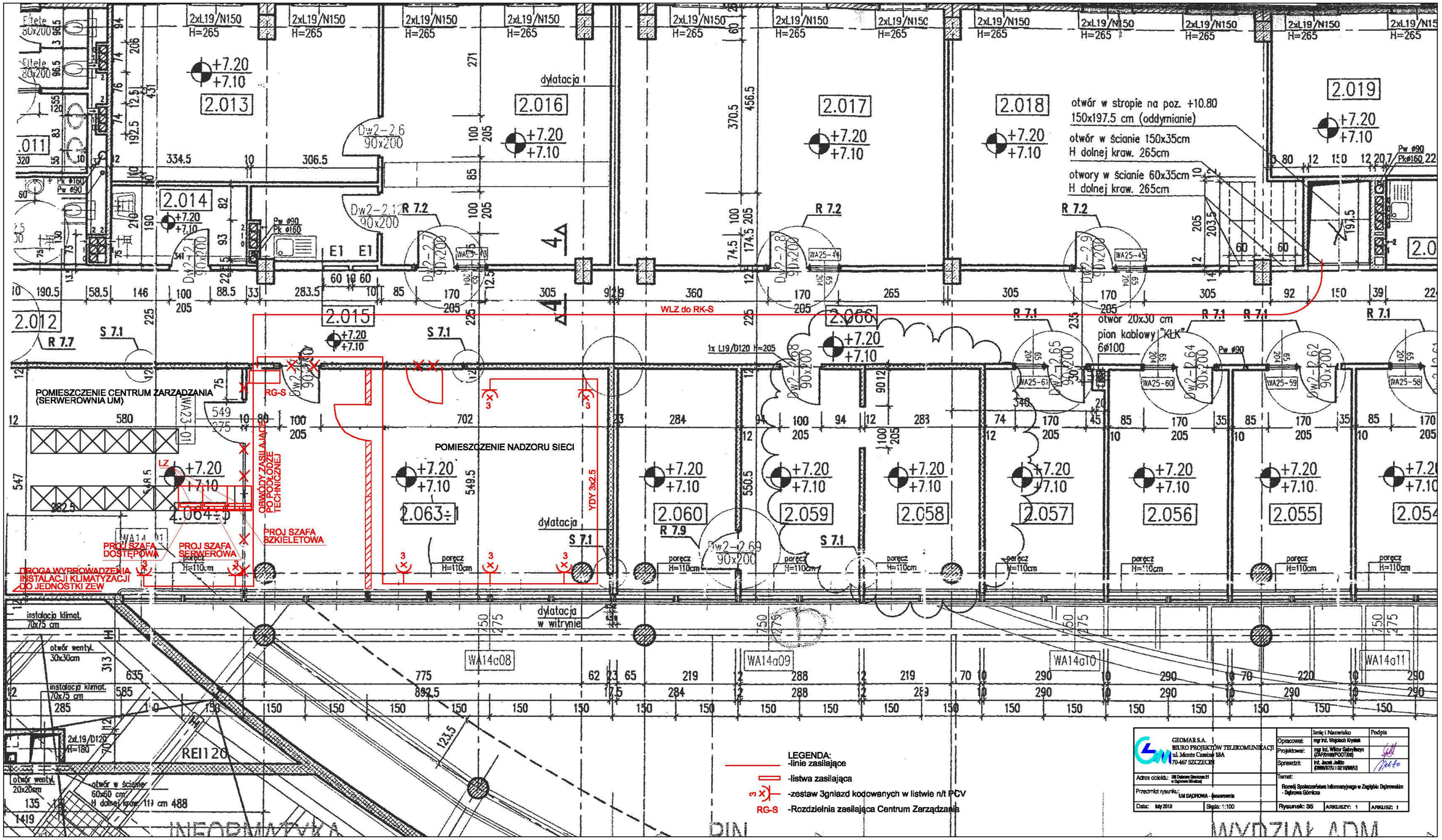


LEGENDA

	linie zasilające
RG-1	Rozdzielnia Główna UM zasilanie kierunek Nr1
RG-2	Rozdzielnia Główna zasilająca Centrum Zarządzania
RG-CZ	Rozdzielnia Główna zasilająca Centrum Zarządzania
UPS-CZ	Zasilacz awaryjny 10 kVA 3/3 fazowy zasilający Centrum Zarządzania
BP-UPS	Przełącznik serwisowy (bypass UPS-a)

GEOMAR S.A.			Podpis
ul. Monte Cassino 18A 70-467 SZCZECIN	Opracował:		
	Projektował:	Mgr inż,. Wiktor Gabryliszyn	
	Sprawdził:		
Adres obiektu:	Urząd Miejski, Komenda Straży Miejskiej Ul. Graniczna 21	Temat:	
Rodzaj inwestycji:	Liniowy	ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Przedmiot rysunku:	Zasilanie urządzeń w Centrum Zarządzania		

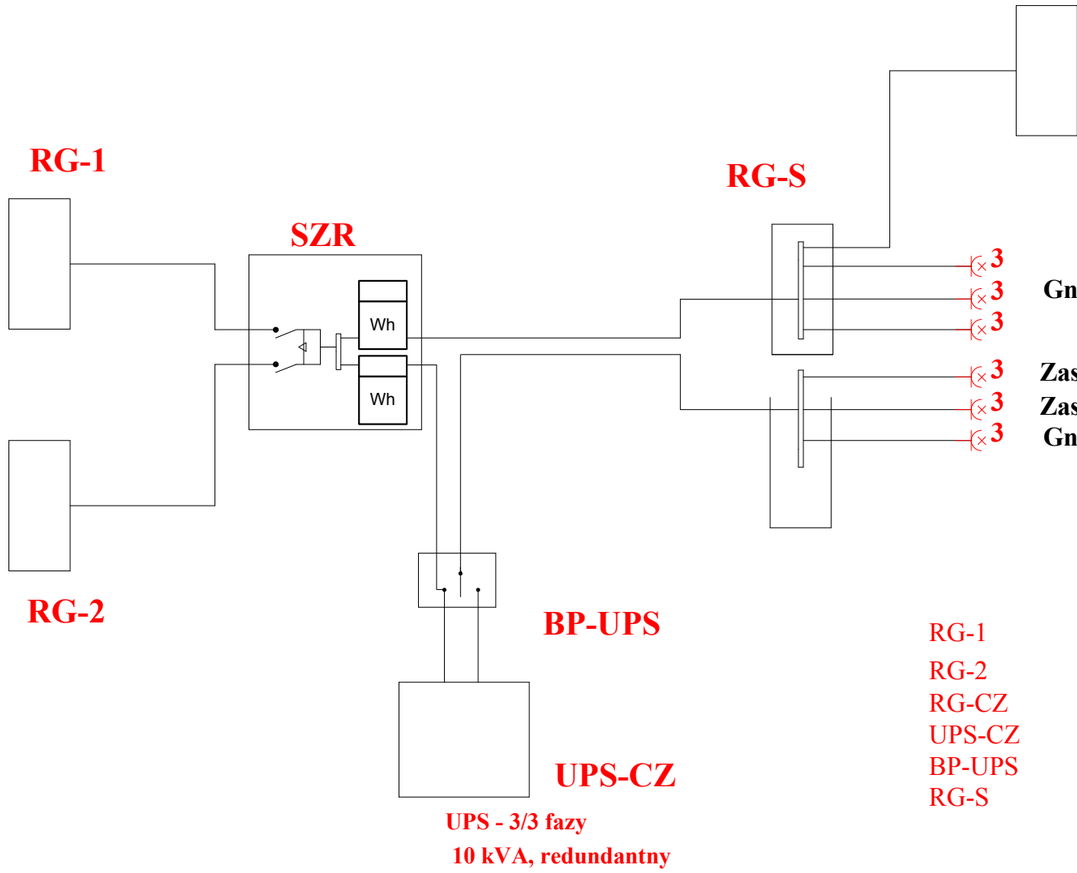
Rysunek 35 Urząd Miejski - II piętro- zasilanie urządzeń



Rysunek 36 Schemat zasilania w Urzędzie Miejskim (CZ)

URZĄD MIEJSKI ul. Graniczna 21

SCHEMAT ZASILANIA CENTRUM ZARZĄDZANIA

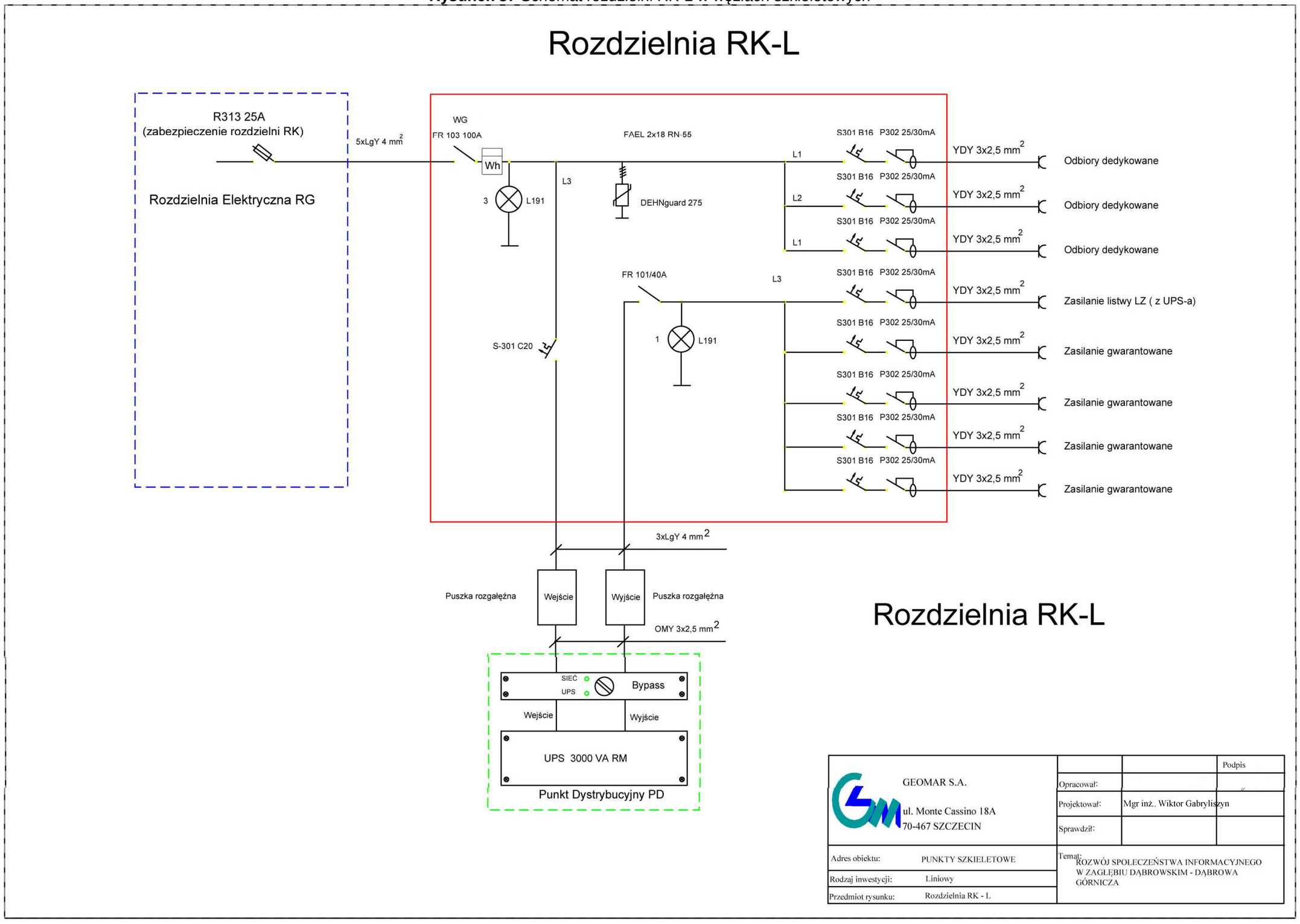


LEGENDA

RG-1	Rozdzielnia Główna UM zasilanie kierunek Nr1
RG-2	Rozdzielnia Główna UM zasilanie kierunek Nr2
RG-CZ	Rozdzielnia Główna zasilająca Centrum Zarządzania
UPS-CZ	UPS redundantny 10 kVA 3/3 fazowy zasilający Centrum Zarządzania
BP-UPS	Przełącznik serwisowy (bypass UPS-a)
RG-S	Rozdzielnia Główna Serwerowni

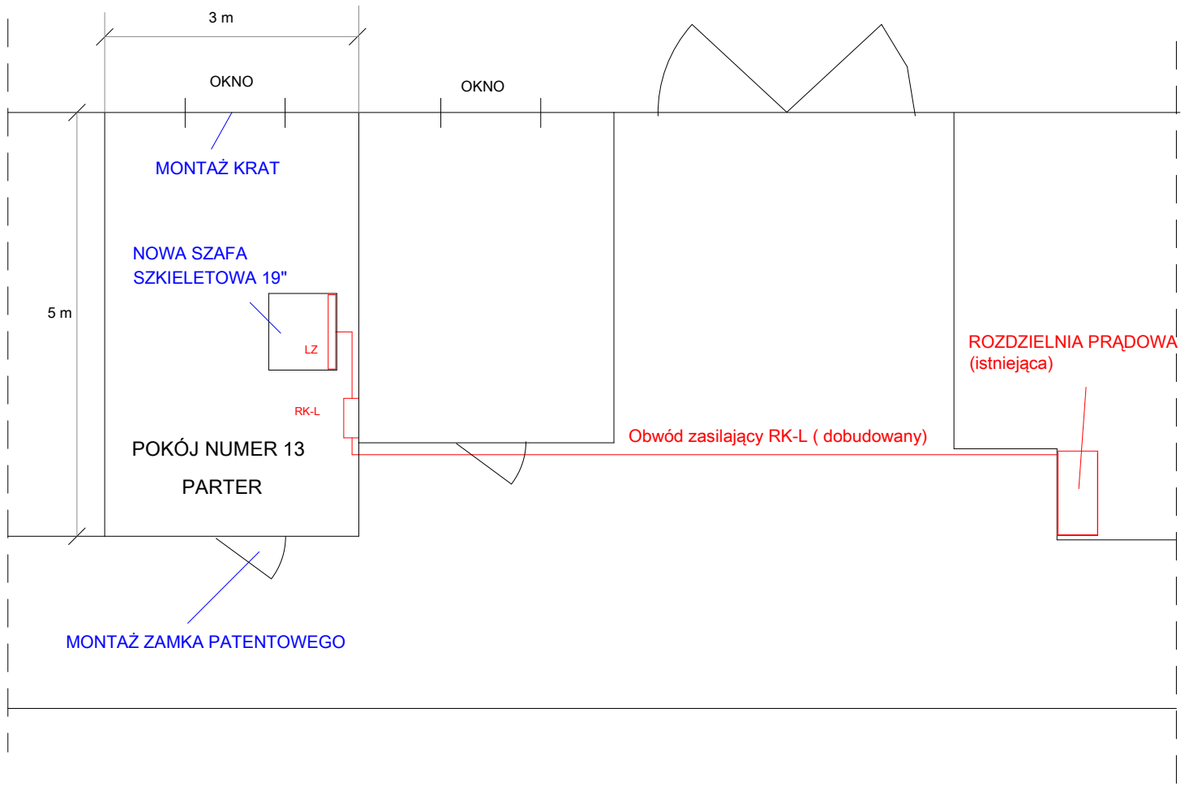
GEOMAR S.A. ul. Monte Cassino 18A 70-467 SZCZECIN			Podpis
	Opracował:		
	Projektował:	Mgr inż. Wiktor Gabryliszyn	
	Sprawdził:		
Adres obiektu:	Urząd Miejski, Komenda Straży Miejskiej Ul. Graniczna 21	Temat: ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Rodzaj inwestycji:	Liniowy		
Przedmiot rysunku:	Zasilanie urządzeń w Centrum Zarządzania		

Rysunek 37 Schemat rozdzielni RK-L w węzłach szkieletowych



Rysunek 38 Szkoła Podstawowa nr 11 – zasilanie urządzeń

SZKOŁA PODSTAWOWA NR 11 Al. Piłsudskiego 103



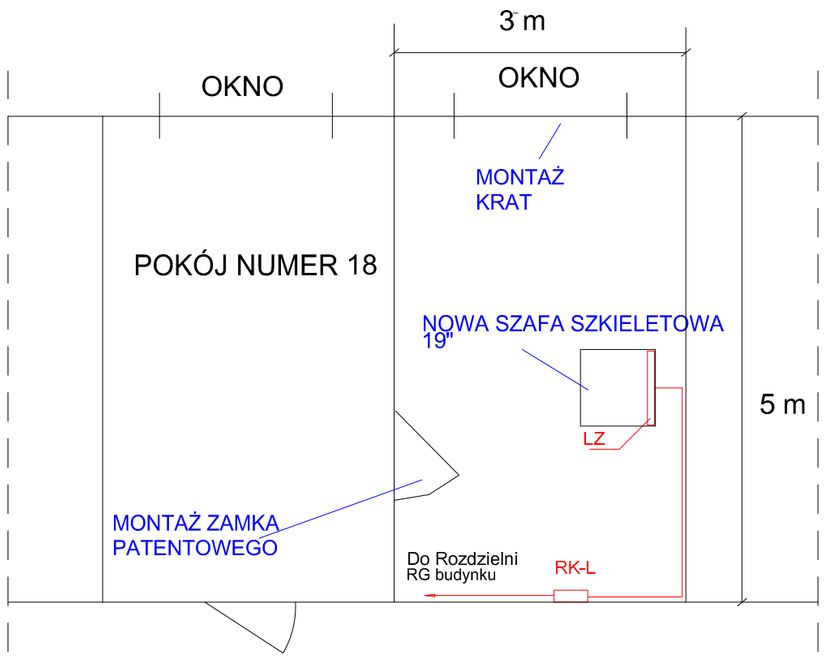
LEGENDA

	Zasilanie RK-L
LZ	Listwa Zasilająca 19" urządzenia
RK-L	Rozdzielnia Liniowa Węzłą Szkieletowego

GEOMAR S.A. ul. Monte Cassino 18A 70-467 SZCZECIN			Podpis
	Opracował:		
	Projektował:	Mgr inż. Wiktor Gabryliszyn	
	Sprawdził:		
Adres obiektu:	Szkoła Podstawowa nr 11 Al. Piłsudskiego 103	Temat: ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Rodzaj inwestycji:	Liniowy		
Przedmiot rysunku:	Zasilanie urządzeń w pom. Serwerowni		

Rysunek 39 MZBM, Dyrekcja – zasilanie urządzeń

MZBM, DYREKCJA ul. Tysiąclecia 20



LEGENDA

———	Zasilanie RK-L
LZ	Listwa Zasilająca 19" urządzenia
RK-L	Rozdzielnia Liniowa Węzłą Szkieletowego

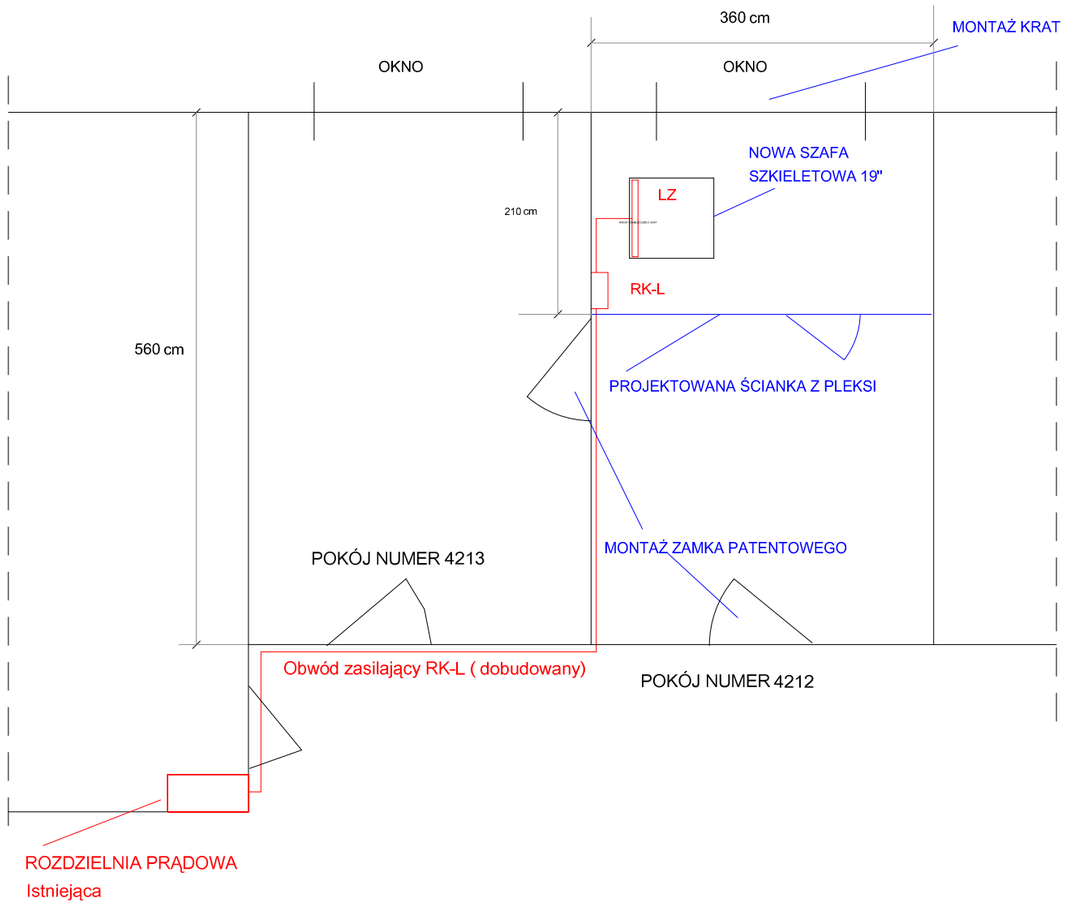
SERWEROWNIA POSIADA NIEZALEŻNY
OBWÓD ELEKTRYCZNY ORAZ KLIMATYZACJĘ

GEOMAR S.A. ul. Monte Cassino 18A 70-467 SZCZECIN			
	Opracował:	·	
	Projektował:	Mgr inż.. Wiktor Gabryliszyn	
	Sprawdził:		
Adres obiektu: MZBM, Dyrekcjaul. Tysiąclecia 20	Temat: ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA		
Rodzaj inwestycji: Liniowy			
Przedmiot rysunku: Zasilanie urządzeń w pom. Serwerowni			

Rysunek 40 Zespół Szkół Zawodowych „SZTYGARKA” – zasilanie urządzeń

ZESPÓŁ SZKÓŁ ZAWODOWYCH „SZTYGARKA” ul. Legionów Polskich 131

WIDOK POMIESZCZENIA Z GÓRY



LEGENDA

Zasilanie RK-L

LZ Listwa Zasilająca 19" urządzenia

RK-L Rozdzielnia Liniowa Węzłą Szkieletowego

GEOMAR S.A. ul. Monte Cassino 18A 70-467 SZCZECIN			Podpis
	Opracował:	·	
	Projektował:	Mgr inż. . Wiktor Gabryliszyn	
	Sprawdził:		
Adres obiektu:	Zespol Szkół Zawodowych SZTYGARKA Ul. Legionów Polskich 131A	Temat: ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Rodzaj inwestycji:	Liniowy		
Przedmiot rysunku:	Zasilanie urządzeń w pom. Serwerowni		

Rysunek 41 Miejska Biblioteka Publiczna (Dyrekcja) – zasilanie urządzeń

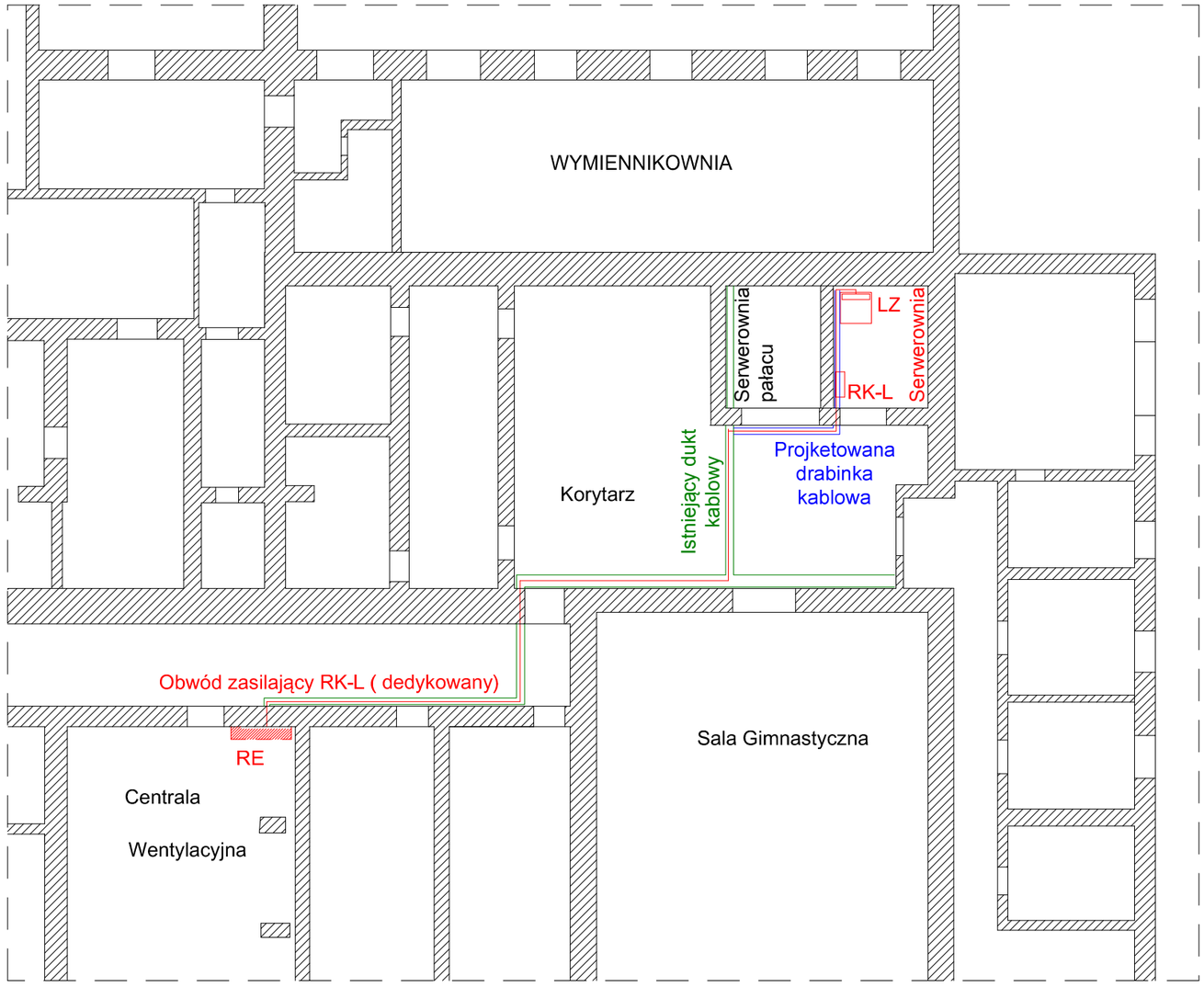
MIEJSKA BIBLIOTEKA PUBLICZNA – DYREKCJA ul. Kościuszki 25

LEGENDA

———	Zasilanie RK-L
LZ	Listwa Zasilająca 19" urządzenia
RK-L	Rozdzielnia Liniowa Węzłą Szkieletowego

GEOMAR S.A. ul. Monte Cassino 18A 70-467 SZCZECIN			Podpis
	Opracował:		
	Projektował:	Mgr inż.. Wiktor Gabryliszyn	
	Sprawdził:		
Adres obiektu:	Miejska Biblioteka Publiczna, Dyrekcja Ul. Kościuszki 25	Temat: ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA	
Rodzaj inwestycji:	Liniowy		
Przedmiot rysunku:	Zasilanie urządzeń w pom. Serwerowni		

Rysunek 42 Pałac Kultury Zagłębia – zasilanie urządzeń

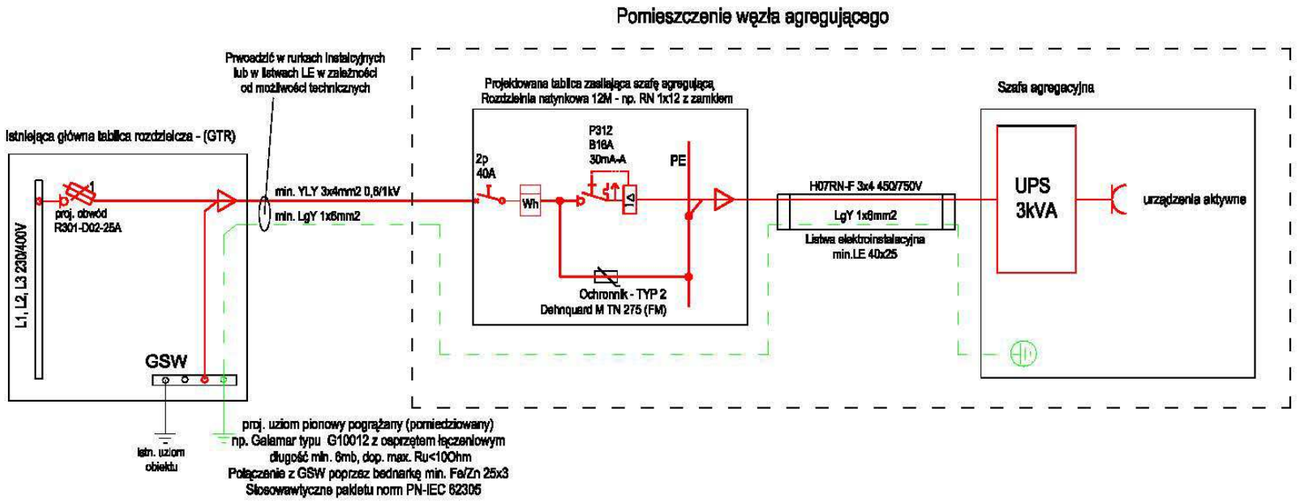


LEGENDA

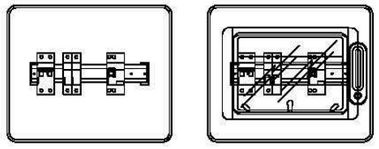
Zasilanie RK-L	
LZ	Listwa Zasilająca 19" urządzenia
RK-L	Rozdzielnia Liniowa Węzłą Szkieletowego

GEOMAR S.A. ul. Piotra Skargi 23 70-487 SZCZECIN			
	Opracował:		
	Projektował:	Mgr inż.. Wiktor Gabryliszyn	
	Sprawdził:		
Adres obiektu:	Pałac Kultury Zagłębia ul. Plac Wolności 1	Temat:	ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA
Rodzaj inwestycji:	Liniowy		
Przedmiot rysunku:	Zasilanie urządzeń w pom. Serwerowni		

Rysunek 43 Węzeł agregujący – zasilanie urządzeń



Ochrona dodatkowa przed dotykiem pośrednim SAMOCZYNNE WYŁĄCZENIE ZASILANIA wg PN-IEC 60346-4-41
UKŁAD SIECI TN-C / TN-C-S



Projektowaną tablicę zasilania węzła agregującego wykonać jako rozdzielnicę natynkową. Wysokość montażu, 1,8m licząc od posadzki do dolnej krawędzi rozdzielni. Tablica z drzwiczkami transparentnymi wyposanymi w zamek na klucz. Tablice wyposażyć w osprzęt jak na schemacie. Montaż aparatury na szynach TH35. Przyktdowo do celów projektowych wykorzystano tablice typu RN-12. Orientacyjne min. wymiary rozdzielnicy 280x340x141mm (wys. x szer. x g).

Całość instalacji wnętrzowej wykonać przewodami miedzianym o przekrojach jak na schemacie jednokreskowym o izolacji 450/750V dla przewodów, a dla kabli 0,6/1kV. Instalację wykonać jako natynkową chowaną w listwach elektroinstalacyjnych. W przypadku prowadzenia przewodów pod zabudowami regipsowym lub innymi wprowadzić przewody w rurki ochronne peszla o odpowiednim przekroju. Stosować wyłącznie rurki ochronne i listwy elektroinstalacyjne samogasnące. Wszystkie przebicia rurami ochronnymi i inne powstałe na skutek rozprowadzania instalacji, zaślepić odpowiednimi masami, zgodnie z wymaganiami pożarowymi i przyjętą technologia dla stref pożarowych obiektu. Po wykonaniu robót objętych niniejszym projektem należy dokonać pomiarów, zgodnie z obowiązującymi przepisami i zaleceniami PN-IEC 60364-4. Wszystkie prace należy wykonywać zgodnie z obowiązującymi przepisami i normami branżowymi. Po zakończeniu prac, należy doprowadzić obszar objęty robotami do stanu pierwotnego.

W projektowanej instalacji zapewnia się ochronę przeciwporażeniową podstawową i dodatkową zgodnie z wymaganiami pakietu norm PN-IEC 60364-4 i PN-IEC 60364-5. Ochronę podstawową przed dotykiem bezpośrednim spełnić przez stosowanie urządzeń izolowanych posiadających atest i odpowiedni stopień ochrony. Uzupełnienie w/w ochrony spełniać także będą wyłączniki różnicowoprądowe.

W przypadku układu zasilania dla istniejącej instalacji w układzie TN-C, należy w istn. głównej tablicy rozdzielczej obiektu (GTR), dokonać rozdzielenia przewodu PEN na przewód neutralny N i przewód ochronny PE. Tablica zasilająca węzeł agregujący, zostanie zasilona w układzie TN-C-S. Projektowany uzlom pionowy pogrążany, doprowadzić bednarką Fe/Zn 25x3 do GTR i przyłączyć do głównej szyny wyrównawczej (GSW), uziemiając punkt rozdziału sieci.

W przypadku układu zasilania dla istniejącej instalacji w układzie TN-S, należy podłączyć zasilanie tablicy zasilającej węzeł agregujący pod właściwe zaciski L1, N, i PE w istn. głównej tablicy rozdzielczej obiektu (GTR). Dodatkowo wykonać projektowany uzlom pionowy pogrążany, doprowadzić bednarkę Fe/Zn 25x3 do GTR i przyłączyć do głównej szyny wyrównawczej (GSW).

LP.	MATERIAŁ	ILOŚĆ
1	Uzlom pionowy pomiedziowany , np. Galmar G10012	4 szt.
2	Głowica , np. Galmar G10402	3 szt.
3	Grot , np. Galmar G10602	1 szt.
4	Bednarka ocynkowana Fe/Zn 25x3	
5	Przewód LgY 1x6mm2	
6	Przewód YLY 3x4mm2 0,6/1kV	
7	Przewód H07RN-F 3x4 450/750kV	
8	Rozdzielnia natynkowa IP55, z drzwiami transparentnymi i zamkiem na klucz, np. RN-12	1 szt.
9	Rozłącznik bezpiecznikowy z wkładką DO2/25A, np. R301 D02-25A	1 szt.
10	Rozłącznik izolacyjny 2-polowy 40A, np FR302-40A	1 szt.
11	Wyłącznik różnicowoprądowy 2-polowy , 30mA o charak. typu A, z członem nadmiarowy 16A o charak. B, np. P312-B16-30mA-A	1 szt.
12	Ochronnik przepięciowy 2-polowy , typ 2,. np. Dehnguard M TN 275(FM)	1 szt.
13	Licznik zużycia energii elektrycznej na szynę TH35	1 szt.

BIURO PROJEKTÓW TELEKOMUNIKACJI GEOMAR S.A. ul. Piotra Skargi 23 70–487 SZCZECIN		Imię i Nazwisko	Podpis
	Opracował:	mgr inż. Wiktor Gabryliszyn	
	Projektował:	mgr inż. Wiktor Gabryliszyn (ZAP/0169/POOT/05)	
Przedmiot rysunku: Zasilanie węzła agregującego	Temat: ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W ZAGŁĘBIU DĄBROWSKIM - DĄBROWA GÓRNICZA		
Data: marzec 2013 / Skala: –	Rysunek: 43	ARKUSZY: 1	ARKUSZ: 1

6 PASZPORTYZACJA

System ma służyć do ewidencji elementów infrastruktury kabli światłowodowych i elementów sieci, jak również kanalizacji teletechnicznej w której układane są kable.
System ma mieć następujące cechy:

- Powinien inwentaryzować zasoby fizyczne takie jak:
    - Zasoby infrastruktury (budynki, pomieszczenia, szafki, itp.)
    - Studnie kanalizacja teletechniczna,
    - Kable optyczne
- Ma umożliwiać prezentację następujących parametrów:
    - zasobów sieci na mapie cyfrowej
    - połączeń zestawionych w sieci na mapie
    - topologii sieci i połączeń w węzłach sieci na dynamicznie generowanych schematach
    - widoków pomieszczeń
    - widoków i struktury urządzeń
- Umożliwiać wprowadzanie informacji o zasobach sieci i umożliwiać modyfikację ich parametrów
- Pozwalać na definiowanie połączeń w węzłach sieci na poziomie włókien
- Umożliwiać zestawianie połączeń w sieci (ręczne i automatyczne) na poziomie włókien
- Pozwalać na wprowadzaniu informacji o rozmieszczeniu kabli w zasobach kanalizacji
- Pozwalać na kojarzenie zewnętrznych plików z inwentaryzowanymi zasobami
- Pozwalać na inwentaryzację awarii zasobów kablowych optycznych
- Pozwalać na wyznaczanie skutków awarii zasobów kablowych optycznych
- Umożliwiać wprowadzanie informacji o położeniu obiektów (przynależność terytorialna – powiat, gmina, dzielnica, itp.)
- Możliwość wprowadzania adresów lokalizacji w oparciu o słowniki TERYT
- Umożliwiać wprowadzanie informacji z katastru: numery działek, stan prawny działek, informacje o właścicielach
- Przechowywać informacje o
    - certyfikatach i homologacjach obiektów
    - terminach przeglądów i gwarancji
    - osobach odpowiedzialnych za utrzymanie obiektów
    - wyniki pomiarów

- specyfikacje techniczne
- instrukcje użytkownika
- szkice i mapki dojazdu
- zdjęcia obiektów
- linki do kamer WEB monitorujących obiekty,
- zgody
- pozwolenia, itp.

- Umożliwiać przechowywanie informacji o przypisaniu obiektów ewidencjonowanej infrastruktury do środków trwałych
- System musi mieć możliwość pracy z wieloma układami współrzędnych geodezyjnych (WGS84, 1965, 1992, 2000, układy lokalne)
- System będzie posiadał funkcje analizujące topologię sieci- śledzenia.
- GUI systemu umożliwi pracę w wielu oknach z widokiem mapy lub schematu sieci, a także w przypadku pracy na stanowiskach wielomonitorowych z więcej niż jedną otwartą instancją aplikacji Systemu.
- System musi mieć możliwość wykonywania raportów wymaganych przez UKE.

System powinien przechowywać pełną historię edycji obiektów, w szczególności: Rejestrowane powinny być informacje Logowanie o zmianach wartości poszczególnych atrybutów, jak również zdarzenia związane z usunięciem obiektu. Usunięte obiekty powinny być nadal przechowywane w bazie danych na potrzeby raportowania. Każdemu logowanemu zdarzeniu powinien towarzyszyć stosowny zapis zawierający takie informacje jak:

- Identyfikator modyfikowanego obiektu,
- data wykonanej zmiany
- poprzednia wartość modyfikowanego atrybutu,
- wartość obecna,
- nazwa użytkownika dokonującego zmiany.

Aplikacja powinna mieć możliwość dostępu w tym samym czasie z obydwu terminali w Centrum Zarządzania, zdalnie lub lokalnie bez konieczności zakupu dodatkowych licencji i obsługiwać 5 użytkowników.

6.1 SPECYFIKACJA SYSTEMU PASZPORTYZACJI

Parametr / Funkcjonalność	Podstawowe parametry nie gorsze niż..
Funkcjonalność systemu	System ma służyć do ewidencji elementów infrastruktury, kabli światłowodowych i elementów sieci FO, jak również kanalizacji teletechnicznej w której układane są kable. **ZAKRES FUNKCJONALNY** System ma spełniać następujące parametry: • Powinien inwentaryzować zasoby fizyczne takie jak: o Zasoby infrastruktury (budynki, pomieszczenia, szafki, itp.) o Studnie kanalizacja teletechniczna, o Kable optyczne • Ma umożliwiać prezentację następujących parametrów: o zasobów sieci na mapie cyfrowej o połączeń zestawionych w sieci na mapie o topologii sieci i połączeń w węzłach sieci na dynamicznie generowanych schematach o widoków pomieszczeń o widoków i struktury urządzeń • Umożliwiać wprowadzanie informacji o zasobach sieci i umożliwiać modyfikację ich parametrów • Pozwalać na definiowanie połączeń w węzłach sieci na poziomie włókien • Umożliwiać zestawianie połączeń w sieci (ręczne i automatyczne) na poziomie włókien • Pozwalać na wprowadzaniu informacji o rozmieszczeniu kabli w zasobach kanalizacji • Pozwalać na kojarzenie zewnętrznych plików z inwentaryzowanymi zasobami • Pozwalać na inwentaryzację awarii zasobów kablowych optycznych • Pozwalać na wyznaczanie skutków awarii zasobów kablowych optycznych • Zapewniać narzędzia do rozbudowy modelu informacyjnego zasobów sieci i tworzenia własnych bibliotek • Umożliwiać wprowadzanie informacji o położeniu obiektów (przynależność terytorialna – powiat,

Parametr / Funkcjonalność	Podstawowe parametry nie gorsze niż..
	gmina, dzielnica, itp.) • Możliwość wprowadzania adresów lokalizacji w oparciu o słowniki TERYT • Umożliwiać wprowadzanie informacji z katastru: numery działek, stan prawny działek, informacje o właścicielach • Przechowywać informacje o o certyfikatach i homologacjach obiektów o terminach przeglądów i gwarancji o osobach odpowiedzialnych za utrzymanie obiektów • Umożliwiać przechowywanie informacji o przypisaniu obiektów ewidencjonowanej infrastruktury do środków trwałych • System musi mieć możliwość pracy z wieloma układami współrzędnych geodezyjnych (WGS84, 1965, 1992, 2000, układy lokalne) • System umożliwi pracę na tle map rastrowych i wektorowych pochodzących z serwera systemu lub ze źródeł WMS i/lub WFS serwowanych w dowolnym układzie współrzędnych i transformowanych „w locie” • System będzie posiadał system podpowiedzi dla operatora dotyczący aktualnie realizowanej funkcji • System będzie posiadał funkcje analizujące topologię sieci- śledzenia. • GUI systemu umożliwi pracę w wielu oknach z widokiem mapy lub schematu sieci, a także w przypadku pracy na stanowiskach wielomonitorowych z więcej niż jedną otwartą instancją aplikacji Systemu. • Pozwalać na przygotowanie raportów do UKE. System powinien umożliwiać także zaimportowanie zewnętrznych dokumentów w postaci elektronicznej, zawierających przykładowo: wyniki pomiarów, specyfikacje techniczne, instrukcje użytkownika, szkice i mapki dojazdu do obiektów, zdjęcia obiektów, linki do kamer WEB monitorujących obiekty, zgody, pozwolenia, itp. Zaimportowane pliki mają być dołączone do istniejących obiektów.

Parametr / Funkcjonalność	Podstawowe parametry nie gorsze niż..
Logowanie zmian	System powinien przechowywać pełną historię zmian obiektów, w szczególności: Rejestrowane powinny być informacje Logowanie o zmianach wartości poszczególnych atrybutów, jak również zdarzenia związane z usunięciem obiektu. Usunięte obiekty powinny być nadal przechowywane w bazie danych na potrzeby raportowania. Każdemu logowanemu zdarzeniu powinien towarzyszyć stosowny zapis zawierający takie informacje jak: • Identyfikator modyfikowanego obiektu, • data wykonanej zmiany • poprzednia wartość modyfikowanego atrybutu, • wartość obecna, • nazwa użytkownika dokonującego zmiany, • nazwa i adres stacji roboczej z której ta zmiana została wykonana,
Minimalne wymagania oprogramowania dla serwera bazy danych i aplikacji	• Linux Red Hat Enterprise 6 lub równoważny • Oracle 11g Standard lub równoważny Serwer powinien wykorzystywać system operacyjny Linux Red Hat Enterprise 6 lub równoważny, o nie gorszej funkcjonalności. System powinien wykorzystywać silnik bazy danych zbudowany w oparciu o Oracle 11g Standard lub równoważny o nie gorszej funkcjonalności. • Do edycji i obrazowania zasobów budowanej sieci oraz realizacji wymaganych funkcji System powinien wykorzystywać aplikacje internetową uruchamianą przez przeglądarkę internetową IE, FireFox lub równoważną. • Informacje opisowe o obiektach o sieci, geometrie i położenie obiektów oraz topologia sieci będą zgromadzone w bazie danych.
Podział na grupy użytkowników	System powinien umożliwiać podział na następujące grupy użytkowników: • Administrator Systemu • Użytkownik.
Założenia dotyczące wdrożenia	System ma być zainstalowany przez Wykonawcę w jednej centralnej lokalizacji (lokalizację wskaże Zamawiający).System powinien być dostarczony wraz z niezbędną platformą sprzętową (serwer) i software'ową (system operacyjny, silnik bazy danych, oprogramowanie serwera aplikacji) umożliwiającą pracę 4 użytkowników i 1 administratora. Dostęp do serwera aplikacji realizowany będzie po przez WAN lub LAN protokołem HTTP lub HTTPS.

Parametr / Funkcjonalność	**Podstawowe parametry nie gorsze niż..**
	Stacje robocze zapewni Zamawiający. Wykonawca dostarczy podstawowe biblioteki urządzeń i model danych umożliwiające funkcjonowanie systemu. W bibliotekach tych mają znaleźć się definicje następujących typów obiektów: **Infrastruktura :** • Budynek • Pomieszczenie • Studnia • Szafa • Maszt • Szafka • Dukt (odcinek kanalizacji) **Kable:** • Kabel optyczny. **Elementy sieci:** • Przełącznica optyczna • Złącze kablowe • Kamera • Zapas kabla. Administrator systemu w oparciu o dostarczone narzędzia powinien mieć możliwość samodzielnego modelowania urządzeń i ich parametrów bez konieczności ingerowania w kod aplikacji/systemu. Dla wyspecyfikowanych wyżej klas zasobów Wykonawca ma przygotować symbole graficzne reprezentujące te zasoby na mapie cyfrowej. Uprawnieni użytkownicy systemu ze strony Zamawiającego mają mieć możliwość samodzielnego przygotowywania symbolów graficznych dla nowo dodanych definicji. System powinien być przygotowany do zestawiania połączeń światłowodowych w zakresie kabli i włókien. Połączenia będą prezentowane na mapie oraz schemacie logicznym. W ramach wdrożenia Wykonawca ma włączyć do systemu dostarczoną przez Zamawiającego mapę wektorową w jednym ze wskazanych układów współrzędnych: PUWG2000 lub PUWG1992. Wykonawca w ramach wdrożenia opracuje procedurę kalibracji map do wykorzystania przez personel Zamawiającego.

Parametr / Funkcjonalność	**Podstawowe parametry nie gorsze niż..**
	Wykonawca ma zdefiniować następujące typy awarii: • planowane odłączenie • awaria rzeczywista W stan awarii będą mogły być wprowadzane urządzenia sieci kablowej oraz kable W wyniku wprowadzenia awarii dotyczącej sieci optycznej system ma wyznaczyć listę połączeń (optycznych), które przechodzą przez uszkodzony zasób. Po instalacji systemu Wykonawca przeprowadzi 3-dniowy instruktaż stanowiskowy dla max.5 użytkowników z następującego zakresu obsługi systemu: **Wprowadzanie danych:** • Umieszczanie elementów sieci na mapie • Wykonywanie połączeń • Krosowanie włókien/par miedzianych w węzłach sieci • Tworzenie instalacji budynkowych • Przygotowywanie widoków urządzeń • Wprowadzanie kabli do zasobów kanalizacji • Kojarzenie zewnętrznych plików z inwentaryzowanymi zasobami • Wprowadzanie danych o awariach. **Administracja – dane:** • Definiowanie modelu danych o Klasy o Atrybuty o Składnie o Wzorce urządzeń o Widoki urządzeń o Symbole urządzeń o Słowniki o Konfiguracja warstw mapy. **Administracja – utrzymanie:** • Organizacja systemu • Struktura bazy danych • Struktura katalogów • Procedury utrzymaniowe.
Wsparcie	Wykonawca zapewni Zamawiającemu bezpłatne wsparcie serwisowe na okres min 3 miesięcy od daty podpisania protokołu odbioru systemu.
Gwarancja	Wykonawca zapewni min 5 lata gwarancji na system.

6.2 SPECYFIKACJA SERWERA PASZPORTYZACJI

Minimalne wymagania sprzętowe

LP	Cecha	szt
1	Procesor uzyskujący wynik co najmniej 8000 punktów w teście Passmark - CPU Mark według wyników testów opublikowanych na stronie http://www.cpubenchmark.net/	1
2	8GB (1x8GB) DDR3 1600/1333 MHz ECC RDIMM	4
3	600 GB SAS 6G 10k obr/min 2,5" Hot Plug	2
4	3000 GB SATA 7,2k obr/min 2,5" Hot Plug	2
5	Kontroler SATA z Raid 0,1,10	1
6	2-port GbE Server Adapter	1
7	2-port 10 GbE Server Adapter (SFP)	1
8	Karta Zdalnego zarządzania (pełna wersja z KVM over LAN i oprogramowaniem	1
9	Napęd DVD-RW	1
10	Zasilacz redundantny	1
11	Możliwość instalacji w szafie rack 19"	

Serwer paszportyzacji powinien być wyposażony w system operacyjny umożliwiający pełnienie roli serwera zapasowego dla Active Directory w przypadku awarii serwera blade.

7 HARMONOGRAM PRAC

	Zadanie/Tydzień	1	2	3	5	6	7	8	9	10	11	12	13	14	15	16
1	Podpisanie umowy po potwierdzeniu wszystkich pozwoleń na budowę i otrzymanie rysunków wszystkich pomieszczeń															
2	Dokumentacja projektowa na instalację urządzeń we wszystkich punktach szkieletowych, agregacyjnych i dystrybucyjnych															
3	Dostawa szaf i UPS															
4	Dostawa klimatyzacji															
5	Instalacja szaf, zasilania i klimatyzacji															
6	Dostawa urządzeń sieciowych															
7	Instalacja urządzeń sieciowych															
8	Integracja urządzeń sieciowych															
9	Testy urządzeń sieciowych															
10	Wykonanie dokumentacji powykonawczej instalacji urządzeń sieciowych															
11	Odbiory															