

Szpital Pomorski Sp. z o.o.
DZIAŁ INFORMATYKI I INFORMATYZACJI
ul. Powstania Styczniowego 1
81-519 Gdynia, tel. 58/72-60-327,160
REGON 190141612, NIP 586-22-86-770

Wymagania techniczne budowy sieci LAN SZPITALA POMORSKIE Sp. z o.o.

Szpital Pomorski Sp. z o.o.

mf

Opracowanie:	Data:	Podpisy:
Wojciech Wrześniewski – Kierownik Działu Informatyki	20.11.20	KIEROWNIK Dział Informatyki i Informatyzacji <i>Wojciech Wrześniewski</i> Wojciech Wrześniewski

Zatwierdzenie:	Data:	Podpisy:
Beata Martyn-Mrozowska - Dyrektor ds. Zamówień Publicznych i IT		DYREKTOR DS. ZAMÓWIEN PUBLICZNYCH I IT <i>Beata Martyn-Mrozowska</i> mgr Beata Martyn-Mrozowska DYREKTOR ds. Administracyjno-Technicznych
Daria Mietlewska-Dura - Dyrektor ds. Administracyjno-Technicznych	20.11.20	<i>Daria Mietlewska-Dura</i> Daria Mietlewska-Dura
Dariusz Nałęcz – Wiceprezes Zarządu	20.11.2020	WICEPREZES ZARZĄDU <i>Dariusz Nałęcz</i> Dariusz Nałęcz
Jolanta Sobierańska-Grenda – Prezes Zarządu	22.11.2020	PREZES ZARZĄDU <i>Jolanta Sobierańska-Grenda</i> Jolanta Sobierańska-Grenda



my

Zmiany dokumentu:

Lp.	Data	Imię i nazwisko	Wersja	Opis i referencja do poprzedniej wersji
1	2020.02.07	Wojciech Wrzeźniewski	4.2	Opracowanie
2	2020.10.01	Wojciech Wrzeźniewski	4.3	Doprecyzowanie zapisów punktu 8.2 i 8.3
3	2022.12.13	Wojciech Wrzeźniewski	4.4	Rozszerzenie zapisów punktu 1
4				
5				

SPIS TREŚCI

1. PRZEDMIOT OPRACOWANIA
 - 1.1. KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA - OPERATOR USŁUGI KLUCZOWEJ
 - 1.2. KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA - REGULACJE PRAWNE
2. ZAŁOŻENIA TECHNICZNE
 - 2.1. NORMY I WYMAGANIA DOTYCZĄCE KOMPLETNOŚCI WYKONANIA
 - 2.1.1. PRZEPISY PRAWNE I NORMY ZWIĄZANE Z PROJEKTOWANIEM I WYKONANIEM ZAMIERZENIA BUDOWLANEGO
 - 2.2. ZAKRES PRAC DO WYKONANIA
 - 2.3. WYMAGANIA OGÓLNE
 - 2.4. WYMAGANIA GWARANCYJNE
3. OKABLOWANIE STRUKTURALNE
 - 3.1. OKABLOWANIE STRUKTURALNE POZIOME I PIONOWE BUDYNKOWE, INSTALACJA ELEKTRYCZNA, INSTALACJE TELETECHNICZNE
 - 3.2. WYMAGANIA I CECHY OKABLOWANIA STRUKTURALNEGO
 - 3.2.1. GNIAZDA I MODUŁY
 - 3.2.1.1. WYMAGANE MINIMALNE PARAMETRY MODUŁU
 - 3.2.2. PANELE KROSUJĄCE MIEDZIANE
 - 3.2.3. KABELE MIEDZIANE
 - 3.2.3.1. WYMAGANE MINIMALNE PARAMETRY KABLA
 - 3.2.4. OKABLOWANIE ŚWIATŁOWODOWE
 - 3.2.4.1. PANELE KROSUJĄCE ŚWIATŁOWODOWE
 - 3.2.4.2. ADAPTERY/INTERFEJSY ŚWIATŁOWODOWE
 - 3.2.4.3. KABELE KROSOWE ŚWIATŁOWODOWE
 - 3.3. WYMAGANIA DLA TRAS KABLOWYCH
 - 3.4. WYMAGANIA DLA PEL I/LUB AP
 - 3.5. WYMAGANIA DLA POŚREDNICH PUNKTÓW DYSTRYBUCYJNYCH (PPD)
 - 3.5.1. DRZWI DLA POMIESZCZEŃ PPD
 - 3.5.2. KLIMATYZATOR TYPU SPLIT DLA POMIESZCZEŃ PPD
 - 3.5.3. SIEĆ ZASILANIA GWARANTOWANEGO I ZASILACZE NAPIĘCIA GWARANTOWANEGO UPS
 - 3.5.3.1. UPS TYPU RACK
 - 3.5.3.2. UPS TYPU WOLNOSTOJĄCY
 - 3.5.4. SYSTEM KONTROLI DOSTĘPU (KD)
 - 3.6. WYMAGANIA DLA KANALIZACJI TELETECHNICZNEJ
 - 3.7. WYMAGANIA DOTYCZĄCE KOMPLETNOŚCI WYKONANIA
 - 3.8. WARUNKI WYKONANIA I ODBIORU ROBÓT
 - 3.9. OGÓLNE WARUNKI WYKONANIA I ODBIORU ROBÓT - PRACE BUDOWLANE
 - 3.10. MOŻLIWE DO WYSTĄPIENIA UTRUDNIENIA W WYKONYWANIU PRAC:
 - 3.11. WYMAGANIA DOTYCZĄCE MATERIAŁÓW
 - 3.12. DODATKOWE WYTTCZNE INWESTORSKIE I UWARUNKOWANIA ZWIĄZANE Z BUDOWĄ I JEJ PRZEPROWADZENIEM
4. SYSTEM OZNACZEŃ (PASZPORTYZACJA)
 - 4.1. OZNACZENIE GNIAZD
 - 4.2. OZNACZENIE PANELU KROSOWEGO
 - 4.3. OZNACZENIE RELACJI ŚWIATŁOWODOWYCH
 - 4.3.1. W GPD
 - 4.3.2. W PPD
 - 4.3.2.1. RELACJA DO GPD
 - 4.3.2.2. W PPD RELACJA DO INNEGO PPD
 - 4.4. OZNACZENIE PEL POD AP (WLAN)
 - 4.5. OZNACZENIE SZAF
5. SPRZĘT AKTYWNY SIECIOWY
6. POMIARY
7. DOKUMENTACJA POWYKONAWCZA
8. WYMAGANIA NA ETAPIE PLANOWANIA, PROJEKTOWANIA I REALIZACJI INNYCH PRAC BUDOWLANEYCH ORAZ REMONTOWYCH W ZAKRESIE UTRZYMANIA TRWAŁOŚCI PROJEKTOWEJ DLA SIECI TELETECHNICZNEJ ORAZ WYDZIELONEJ SIECI ZASILANIA GWARANTOWANEGO ZREALIZOWANEJ W RAMACH WSPARCIA FINANSOWEGO REGIONALNEGO PROGRAMU OPERACYJNEGO WOJEWÓDZTWA POMORSKIEGO DLA PROJEKTU "POMORSKIE E-ZDROWIE"
 - 8.1. WARIANT I - PRZEJĘCIE ODPOWIEDZIALNOŚCI PRZEZ WYKONAWCĘ
 - 8.2. WARIANT II - WYKONANIE PRAC PRZEZ WYKONAWCĘ E-ZDROWIE NA KOSZT WYKONAWCY I UTRZYMANIE ODPOWIEDZIALNOŚCI WYKONAWCY E-ZDROWIE

- 8.3. WARIANT III - WYKONANIE PRAC PRZEZ WYKONAWCĘ I UTRZYMANIE ODPOWIEDZIALNOŚCI WYKONAWCĘ E-ZDROWIE W PRZYPADKU AKCEPTACJI PRAC
- 9. WARUNKI I PARAMETRY DOSTĘPU ZDALNEGO DO WEWNĘTRZNYCH SIECI I STRUKTUR INFORMATYCZNYCH SPÓŁKI
 - 9.1. PRZYJĘTY I OBOWIĄZUJĄCY STANDARD POŁĄCZENIA VPN W SZPITALACH POMORSKICH SP. Z O.O.
- 10. SPRZĘT SERWEROWY I MACIERZOWY WYKORZYSTYWANY W SPÓŁCE
 - 10.1. MACIERZE DYSKOWE
 - 10.2. 10.2. SERWERY

1. PRZEDMIOT OPRACOWANIA

Celem opracowania jest określenie jednolitego sposobu budowy sieci okablowania strukturalnego i wydzielonej sieci zasilania gwarantowanego, stanowiącego wytyczne i zalecenia dla prac projektowych, wykonawczych i utrzymaniowych na terenie placówek wchodzących w skład Szpitali Pomorskich Sp. z o.o. (dalej zwaną Spółką lub OUK). Dokument wskazuje szczegółowe opisanie danych technologii, rozwiązań technicznych, specyfikacji produktowych, procedur konfiguracyjnych oraz procedur testowych dla elementu objętego niniejszym opracowaniem.

Dokument zawiera wytyczne dla przygotowania i realizacji inwestycji remontowych oraz budowlanych, począwszy od przygotowywania Specyfikacji Istotnych Warunków Zamówienia (SWZ) i Opisu Przedmiotu Zamówienia (OPZ) na etapie planowania inwestycji przez komórki organizacyjne Szpitali Pomorskich Sp. z o.o. zajmujące się tym planowaniem, poprzez opracowywanie projektów wykonawczych dla przygotowywanych inwestycji przez projektantów oraz przy przebiegu samego procesu inwestycyjnego realizowanego przez wykonawców.

1.1. KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA - OPERATOR USŁUGI KLUCZOWEJ

Szpitale Pomorskie Sp. z o.o. w dniu 30 kwietnia 2021 roku decyzją Ministra Zdrowia został uznany na podstawie art.104 §1 i art.107 ustawy z dnia 14 czerwca 1960 roku Kodeksu postępowania administracyjnego w związku z art.5 ust.2, art.41 pkt 6 oraz art.42 ust.1 pkt 2 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (UKSC lub ustawa KSC) za **Operatora Usługi Kluczowej (OUK) w sektorze ochrony zdrowia.**



DECYZJA

Na podstawie art. 104 § 1 i art. 107 ustawy z dnia 14 czerwca 1960 r. Kodeksu postępowania administracyjnego (Dz.U. z 2020 r. poz. 256, z późn. zm.), zwanej dalej „KPA” w związku z art. 5 ust. 2, art. 41 pkt 6 oraz art. 42 ust. 1 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369), zwanej dalej „UKSC”

UZNAJĘ

Szpitale Pomorskie Sp. z o.o. zarejestrowaną w rejestrze przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Gdańsk-Północ w Gdańsku, VIII Wydział Gospodarczy KRS pod numerem: 0000492201, NIP: 5862286770, REGON: 190141612,

za operatora usługi kluczowej w sektorze ochrony zdrowia, polegającej na:

1. udzielaniu świadczeń opieki zdrowotnej przez podmiot leczniczy,
2. obrocie i dystrybucji produktów leczniczych.

UZASADNIENIE

Pismem z dnia 19 października 2018 roku, znak FZP.163.216.2018.MS organ zawiadomił Szpitale Pomorskie Sp. z o.o. o wszczęciu postępowania w sprawie uznania za operatora usługi kluczowej. W zawiadomieniu wskazano, że Stronie przysługuje

prawo do czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji możliwość wypowiedzenia się co do zebranych dowodów i materiałów oraz zgłoszonych żądań. Strona nie wniosła żadnych pism. Pismem z dnia 19 listopada 2018 roku organ zawiadomił Stronę o zakończeniu postępowania administracyjnego, a w związku z tym o możliwości zapoznania się z aktami sprawy. Strona nie skorzystała z prawa wglądu w akta sprawy.

Pismem z dnia 18 marca 2020 r. organ zawiadomił Stronę o kontynuacji postępowania administracyjnego oraz wezwał do udzielenia dodatkowych wyjaśnień w przedmiocie świadczenia przez Szpitale Pomorskie Sp. z o.o. usług kluczowych.

Pismem z dnia 20 kwietnia 2020 r. Strona w odpowiedzi na w.w. pismo wskazała, że „Szpitale Pomorskie Sp. z o.o. udziela świadczeń opieki zdrowotnej za pośrednictwem systemów teleinformatycznych i systemów łączności. Szpitale Pomorskie Sp. z o.o. posiadają umowę przewidującą dokonywanie dla Spółki przez podmiot zewnętrzny opisów badań z zakresu diagnostyki obrazowej za pośrednictwem systemów teleinformatycznych lub systemów łączności. Obecnie spółka udziela również świadczeń za pośrednictwem tych systemów pacjentom (tzw. telemedycyna), w zakresie świadczeń, których udzielenie możliwe jest bez osobistego kontaktu z pacjentem, realizując wytyczne Państwowej Inspekcji Sanitarnej oraz Narodowego Funduszu Zdrowia w przedmiocie sposobu postępowania w okresie stanu epidemii.”

Pismem z dnia 3 lutego 2021 r. organ zawiadomił Stronę o zakończeniu postępowania administracyjnego, a w związku z tym o możliwości zapoznania się z aktami sprawy. Strona nie skorzystała z prawa wglądu w akta sprawy.

Organ zważył co następuje

Zgodnie z art. 5 ust. 2 UKSC organ właściwy wydaje decyzję o uznaniu podmiotu za operatora usługi kluczowej, jeżeli:

- 1) podmiot świadczy usługę kluczową,
- 2) świadczenie tej usługi zależy od systemów informacyjnych,
- 3) incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora.

W załączniku nr 1 do UKSC określone zostały sektory, podsektory oraz rodzaje podmiotów, które mogą być uznane za operatorów usług kluczowych. Przez usługę kluczową, stosownie do art. 2 pkt 16 UKSC, należy rozumieć usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej i została wymieniona w wykazie usług kluczowych. Wykaz usług kluczowych określa

rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. poz. 1806), zwane dalej „rozporządzeniem”. Istotność skutku zakłócającego incydentu dla świadczenia usługi kluczowej określona jest na podstawie progów istotności skutku zakłócającego, które zostały określone w rozporządzeniu.

Organ zgromadził w sprawie następujący materiał dowodowy:

- 1) pismo Zastępcy Prezesa ds. Operacyjnych Narodowego Funduszu Zdrowia z dnia 6.08.2018 r.,
- 2) zawiadomienie o wszczęciu postępowania,
- 3) aktualny odpis z Krajowego Rejestru Sądowego,
- 4) zawiadomienie o zakończeniu postępowania z dnia 19 listopada 2018 roku,
- 5) zawiadomienie o kontynuacji postępowania administracyjnego oraz wezwanie do udzielenia dodatkowych wyjaśnień z dnia 18 marca 2020 r.
- 6) pismo Strony z dnia 20 kwietnia 2020 r.
- 7) zawiadomienie o zakończeniu postępowania z dnia 3 lutego 2021 roku.

Mając na uwadze przywołane powyżej przepisy prawa oraz zgromadzony w sprawie materiał dowodowy organ ustalił, że:

- 1) Strona - Szpital Pomorskie Sp. z o.o. świadczy usługi kluczowe, o których mowa w załączniku do rozporządzenia „Wykaz usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych” polegające na udzielaniu świadczeń opieki zdrowotnej przez podmiot leczniczy oraz obrocie i dystrybucji produktów leczniczych.
- 2) Incydent miałby istotny skutek zakłócający dla świadczenia powyższej usługi kluczowej przez operatora. Zgodnie z rozporządzeniem przy określaniu progu istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej polegającej na udzielaniu świadczenia opieki zdrowotnej przez podmiot leczniczy należy wziąć pod uwagę, czy świadczeniodawca zakwalifikowany jest do systemu podstawowego szpitalnego zabezpieczenia świadczeń opieki zdrowotnej w ramach tzw. „sieci szpitali” oraz czy posiada Szpitalny Oddział Ratunkowy. W toku postępowania ustalono, że Strona jako świadczeniodawca zakwalifikowany jest do systemu podstawowego szpitalnego zabezpieczenia świadczeń opieki zdrowotnej w ramach tzw. „sieci szpitali”, a także posiada w swojej strukturze szpitalny oddział ratunkowy.
- 3) Świadczenie powyższej usługi kluczowej zależy od systemów informacyjnych.

3

POUCZENIE

Stosownie do art. 127 § 3 i art. 129 § 2 KPA, Strona niezadowolona z decyzji może w terminie 14 dni od dnia jej doręczenia wystąpić do Ministra Zdrowia z wnioskiem o ponowne rozpatrzenie sprawy. W trakcie biegu terminu do wniesienia ww. wniosku Strona może, na podstawie art. 127a w zw. z art. 127 § 3 KPA, zrzec się prawa do wystąpienia z wnioskiem o ponowne rozpatrzenie sprawy. Wówczas decyzja staje się ostateczna i prawomocna i brak jest możliwości zaskarżenia decyzji do Wojewódzkiego Sądu Administracyjnego. Alternatywnie, Strona może, na podstawie art. 52 § 3 w zw. z art. 3 § 2 pkt 1, art. 53 § 1 i art. 54 § 1 ustawy z dnia 30 sierpnia 2002 r. - Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2019 r. poz. 2325, z późn. zm.), skierować do Wojewódzkiego Sądu Administracyjnego w Warszawie, za pośrednictwem Ministra Zdrowia, skargę na decyzję w terminie 30 dni od dnia jej doręczenia, bez korzystania z prawa skierowania wniosku o ponowne rozpatrzenie sprawy. Wpis od skargi wynosi 200 zł (§ 2 ust. 1 pkt 2 rozporządzenia Rady Ministrów z dnia 16 grudnia 2003 r. w sprawie wysokości oraz szczegółowych zasad pobierania wpisu w postępowaniu przed sądami administracyjnymi (tj. Dz. U. z 2021 r. poz. 535)). Istnieje możliwość ubiegania się przez Stronę o zwolnienie od kosztów albo przyznanie prawa pomocy w trybie i na zasadach określonych w art. 243-263 ustawy z dnia 30 sierpnia 2002 r. - Prawo o postępowaniu przed sądami administracyjnymi oraz na podstawie rozporządzenia Rady Ministrów z dnia 19 sierpnia 2015 r. w sprawie określenia wzoru i sposobu udostępniania urzędowego formularza wniosku o przyznanie prawa pomocy w postępowaniu przed sądami administracyjnymi oraz sposobu dokumentowania stanu majątkowego, dochodów lub stanu rodzinnego wnioskodawcy (Dz. U. 1257, z późn. zm.).

Hubert Zyciński
Zastępca Dyrektora

(dokument podpisany elektronicznie)

5

Spółka posiada również wydany aktywny certyfikat zgodności wdrożonego Zintegrowanego Systemu Zarządzania w skład którego wchodzi System Zarządzania Jakością, System Zarządzania Środowiskowego, System Zarządzania Bezpieczeństwem i Higieną Pracy oraz System Zarządzania Bezpieczeństwem Informacji, z normami ISO 9001:2015, ISO 14001:2015, PN-N-18001:2004, ISO 45001:2018 i ISO/IEC 27001:2013.



Nr Certyfikatu
NC-1500

CERTYFIKAT

Przyznany Organizacji:

Szpital Pomorskie Sp. z o.o.
Szpital Morski im. PCK
ul. Powstania Styczniowego 1
81-519 Gdynia

Biuro Certyfikacji Systemów Zarządzania Polskiego Rejestru Sądowego S.A., ul. gen. Józefa Hallera 126, 80-416 Gdańsk, zawiadacza, iż Zintegrowany System Zarządzania obejmujący System Zarządzania Jakością, System Zarządzania Środowiskowego, System Zarządzania Bezpieczeństwem i Higieną Pracy oraz System Zarządzania Bezpieczeństwem Informacji wyżej wymienionej organizacji został oceniony i stwierdzono jego zgodność z wymaganiami:

ISO 9001:2015
ISO 14001:2015
PN-N-18001:2004
ISO 45001:2018
ISO/IEC 27001:2013

Zakres certyfikacji:

UDZIELANIE ŚWIADCZEŃ ZDROWOTNYCH SŁUŻĄCYCH UTRZYMANIU, PRZYWRACANIU I POPRAWIE ZDROWIA, PROFILAKTYKA ZDROWIA W ZAKRESIE DZIAŁALNOŚCI LECZENICZEJ SZPITALI POMORSKICH SP. Z O.O.
SZCZEGÓLOWY ZAKRES CERTYFIKACJI OKREŚLA ZAŁĄCZNIK DO NINIEJSZEGO CERTYFIKATU
W OBSZARZE ISMS CERTYFIKAT OBOWIĄZUJE ŁĄCZNIE Z DEKLARACJĄ STOSOWANIA ED. Z DNIA 01.03.2019

Certyfikat QMS, EMS, HSMS i ISMS jest ważny do:	15.02.2024	Niniejszy Certyfikat antykorupcyjny (rozporządzenie 6046/NC-1500/1) do:	13.12.2020
Certyfikat BHP jest ważny do:	30.09.2021		

Gdańsk, 16.02.2021



AC 014
QMS, EMS, BHP, HSMS, ISMS
Porozumienie IAF/MLA dotyczy QMS i EMS

Dyrektor Biura Certyfikacji
Michał Chudziński

Załącznik do certyfikatu nr NC-1500
wydanego przez Biuro Certyfikacji Systemów Zarządzania Polskiego Rejestru Sądowego S.A.

Przyznany Organizacji:

Szpital Pomorskie Sp. z o.o.
Szpital Morski im. PCK
ul. Powstania Styczniowego 1
81-519 Gdynia

ul. Powstania Styczniowego 1
81-519 Gdynia

ul. Huzarska 1
81-518 Gdynia

Zakres certyfikacji:

ODDZIAŁ CHIRURGII DZIECIĘCIEJ, ODDZIAŁ PEDIATRYCZNY, ODDZIAŁ PULMONOLOGICZNY, ODDZIAŁ CHOROŃ WEWNĘTRZNYCH I LECZENIA SCHOROŃ ENDOKRYNOLOGICZNYCH, ODDZIAŁ ANESTEZJOLOGI I INTENSywNEJ TERAPII, ODDZIAŁ NEONATOLOGICZNY I INTENSywNEJ TERAPII NOWORODKA, ODDZIAŁ GINEKOLOGII ONKOLOGICZNEJ, ODDZIAŁ CHIRURGII ONKOLOGICZNEJ Z PODODZIAŁEM CHIRURGII NOWOTWORÓW PIERSI, SKRYTA I TRANSEK WĘKRZYCH, ODDZIAŁ ONKOLOGII I RADIOTERAPII, ODDZIAŁ OKULISTYCZNY, ODDZIAŁ HEMATOLOGII I TRANSPORTU SZPIKU, APTEKA SZPITALNA, IZBA PRZYJĘĆ OGÓLNA, IZBA PRZYJĘĆ INTERNISTYCZNA, BLOK OPERACYJNY, ODDZIAŁ NEFROLOGICZNY, ODDZIAŁ UROLOGII, UROLOGII ONKOLOGICZNEJ I ANDROLOGII, PORADNIA MEDYCZYNY PRACY, PORADNIA REHABILITACYJNA, PORADNIA ONKOLOGICZNA, PORADNIA PROFILAKTYKI CHOROŃ PIERSI, PORADNIA PEDIATRYCZNA, PORADNIA CHEMOTERAPII, PORADNIA CHIRURGII ONKOLOGICZNEJ, PORADNIA OKULISTYCZNA, ZAKŁAD PATOMORFOLOGII, PRACOWNIA HISTOPATOLOGICZNA BADAŃ SRÓDOPERACYJNYCH GGO, PRACOWNIA ENDOSKOPII, PRACOWNIA KOLPOSKOPII, ZAKŁAD MEDYCZYNY NUKLEARNEJ, ZAKŁAD MEDYCZYNY MEDYCZNEJ, PORADNIA RADIOTERAPII, PORADNIA PODSTAWOWEJ OPIEKI ZDROWOTNEJ REJONOWO, SZKOŁA RODZINNA, PORADNIA HEMATOLOGICZNA, ZAKŁAD DIAGNOSTYKI OBRAZOWEJ – RTG, BANK KRWI, ZAKŁAD DIAGNOSTYKI OBRAZOWEJ – USG, ZAKŁAD DIAGNOSTYKI OBRAZOWEJ – TK, ZAKŁAD DIAGNOSTYKI OBRAZOWEJ – MM, PORADNIA MIĘDZ REJONOWO, PORADNIA GENETYCZNA, PORADNIA NEONATOLOGICZNA, PORADNIA CHIRURGII DZIECIĘCIEJ, BANK MLEKA KOBIECIEGO, FARMAKOTERAPEUTYCZNY OŚRODEK KONSULTACYJNY, PORADNIA DOMOWEGO LECZENIA TLENEM, PORADNIA CHOROŃ WEWNĘTRZNYCH

Gdańsk, 16.02.2021

Dyrektor Biura Certyfikacji
Michał Chudziński

Wobec powyższego niezbędne jest by wewnętrzna struktura Spółki posiadała i utrzymywała System Zarządzania

Bezpieczeństwem Informacji spełniający wymagania normy ISO 27001 (Zarządzanie Bezpieczeństwem Informacji), a także zapewniały ciągłość działania usłudze reagowania na incydenty zgodnie z ISO 22301 (Zarządzanie Ciągłością Działania) oraz dysponowały odpowiednimi środkami umożliwiającymi skuteczną i bezpieczną realizację działań związanych z cyberbezpieczeństwem. Szczegółowe wymagania w tym obszarze znajdują się w rozporządzeniu Ministra Cyfryzacji z dnia 10 września 2018r. Drugim kluczowym aspektem efektywnego wdrożenia Ustawy jest podobnie jak w przypadku RODO, wdrożenie systemu szacowania ryzyka wystąpienia incydentu oraz zarządzania tym ryzykiem (gdzie ryzyko należy rozumieć jako zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo). Przy ustanawianiu procesu zarządzania ryzykiem są również brane pod uwagę zasady i wytyczne określone w ISO 31000 (Zarządzanie Ryzykiem) oraz ISO 27005 (Zarządzanie Ryzykiem w Bezpieczeństwie Informacji). Spółka, jako OUK posiada ustanowione i wdrożone procesy oraz narzędzia IT umożliwiające wykrywanie, zarządzanie i zgłaszanie incydentów w zależności od ich klasyfikacji do odpowiednich organów.

W odniesieniu normatywnym wiążące są więc dla obsługiwanych procesów, wewnętrznych struktur organizacyjnych, struktur sieci informatycznych oraz systemów i usług wskazane powyżej normy, wymienione poniżej ustawy i rozporządzenia, a także przyjęte w tym opracowaniu wytyczne.

Oznacza to ścisłe i bezwzględne stosowanie się każdej osoby fizycznej (pracownika, wykonawcy), czy też zewnętrznego podmiotu współpracującego ze Spółką z zawartymi w tym opracowaniu wymaganiami.

1.2. KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA - REGULACJE PRAWNE

W zakresie regulacji prawnych Spółkę oraz osoby/podmioty zewnętrzne współpracujące ze Spółką obowiązują:

1. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE.L. z 2016r. poz.119.1)
3. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. UE.L. z 2016r. poz.194.1)
4. Ustawa z dnia 5 lipca 2018r. o Krajowym Systemie Cyberbezpieczeństwa (tekst jedn.: Dz.U. z 2020r. poz.1369, z późn. zm.)
5. Ustawa z dnia 28 kwietnia 2011r. o systemie informacji w ochronie zdrowia (Dz.U. z 2021r., poz. 666, z późn. zm.)
6. Ustawa z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021r., poz.2070, z późn. zm.)
7. Ustawa z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020r. poz.344, z późn. zm.)
8. Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. z 2019r. poz.1781, z późn. zm.)
9. Ustawa z dnia 14 lipca 1983r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2020r. poz.164, z późn. zm.)
10. Ustawa z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (Dz.U. z 2019r. poz.742, z późn. zm.)
11. Ustawa z dnia 5 września 2016r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2021r. poz.1797, z późn. zm.)
12. Rozporządzenie Rady Ministrów z dnia 31 października 2018r. w sprawie progów uznania incydentu za poważny (Dz.U. z 2018r. poz.2180, z późn. zm.)
13. Rozporządzenie Rady Ministrów z dnia 16 października 2018r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz.U. z 2018r. poz.2080, z późn. zm.)
14. Rozporządzenie Rady Ministrów z dnia 11 września 2018r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz.U. z 2018r. poz.1806, z późn. zm.)
15. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017r. poz.2247, z późn. zm.)

16. Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. z 2019r. poz.2479, z późn. zm.)
17. Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018r. poz.1999, z późn. zm.)
18. Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018r. wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług (Dz.U. z 2018r. poz.1831, z późn. zm.)
19. Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług (Dz.U. z 2018r. poz.1830, z późn. zm.)
20. Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018r. poz.1999, z późn. zm.)
21. Norma PN ISO/IEC 27000:2014-11 "Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Przegląd i terminologia"
22. Norma PN ISO/IEC 27001:2014-12 "Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania"
23. Norma PN ISO/IEC 27002:2014-12 "Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczania informacji"
24. Norma PN-EN ISO/IEC 27037:2016-12 „Technika informatyczna - Techniki bezpieczeństwa - Wytyczne do identyfikacji, gromadzenia, pozyskiwania i zachowania cyfrowych śladów dowodowych”
25. Norma PN-EN ISO/IEC 27038:2016-12 “Technika informatyczna - Techniki bezpieczeństwa - Specyfikacja metod cyfrowych trwałego usuwania”
26. Norma PN-EN ISO/IEC 27040: 2016-12 “Technika informatyczna - Techniki bezpieczeństwa - Bezpieczeństwo pamięci masowych”
27. Norma PN-EN ISO/IEC 27041:2016-12 “Technika informatyczna - Techniki bezpieczeństwa - Wytyczne do zapewnienia stosowności i adekwatności metody dochodzeniowej w związku z incydemem”
28. Norma PN-EN ISO/IEC 27042:2016-12 “Technika informatyczna - Techniki bezpieczeństwa - Wytyczne do analizy i interpretacji cyfrowego śladu dowodowego”
29. Norma PN-EN ISO/IEC 27043:2016-12 "Technika informatyczna - Techniki bezpieczeństwa - Pryncypia i procesy w dochodzeniach związanych z incydentami"
30. Norma PN-EN ISO/IEC 30121:2016-12 "Technika informatyczna - Nadzór nad strukturą ryzyka związanego z informatyką śledczą"
31. Norma PN-ISO/IEC 15408-1:2016-10 "ISO/IEC 15408-1 Technika informatyczna - Techniki bezpieczeństwa - Kryteria oceny zabezpieczeń informatycznych - Część 1: Wprowadzenie i model ogólny"
32. Norma PN-ISO/IEC 15408-2:2016-10 "ISO/IEC 15408-1 Technika informatyczna - Techniki bezpieczeństwa - Kryteria oceny zabezpieczeń informatycznych - Część 2: Komponenty funkcjonalne zabezpieczeń"
33. Norma PN-ISO/IEC 15408-3:2016-10 "Technika informatyczna - Techniki bezpieczeństwa - Kryteria oceny zabezpieczeń informatycznych - Część 3: Komponenty uzasadnienia zaufania do zabezpieczeń"
34. Norma PN-ISO/IEC 18045:2016-10 "Technika informatyczna - Techniki bezpieczeństwa - Metodyka oceny zabezpieczeń informatycznych"
35. Norma ISO/IEC TR 15443:2012 "A framework for IT security assurance / Ramy dla uzasadnionego zaufania do bezpieczeństwa informatycznego"
36. Norma ISO/IEC TR 15446:2009 "Guide for the production of Protection Profiles and Security Targets / Przewodnik do tworzenia profili zabezpieczeń oraz przedmiotów oceny"
37. Norma ISO/IEC 19608 "Guidance for developing security and privacy functional requirements based on ISO/IEC 15408"
38. Norma ISO/IEC TR 20004:2015 "Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045 / Doprecyzowanie analizy podatności oprogramowania zgodnie z ISO/IEC 15408 oraz ISO/IEC 18045"
39. Norma ISO/IEC TS 30104:2015 "Physical security attacks, mitigation techniques and security requirements / Ataki na bezpieczeństwo fizyczne. Techniki ograniczania oraz wymagania bezpieczeństwa"
40. Norma ISO/IEC 19790:2012 "Security requirements for cryptographic modules / Wymagania bezpieczeństwa dla modułów kryptograficznych"
41. Norma ISO/IEC 19792:2009 "Security evaluation of biometrics / Ocena bezpieczeństwa dla biometrii"

42. Norma ISO/IEC 17825:2016 "Testing methods for the mitigation of non-invasive attack classes against cryptographic modules / Metody testowania w celu ograniczenia klas nieinwazyjnych ataków na moduły kryptograficzne"
43. Norma ISO/IEC 18367:2016 "Cryptographic algorithms and security conformance testing / Algorytmy kryptograficzne i testowanie zgodności bezpieczeństwa"
44. Norma ISO/IEC 24759:2015 "Test requirements for cryptographic modules / Wymagania testowania dla modułów kryptograficznych"
45. Norma ISO/IEC 29128:2011 "Verification of cryptographic protocols / Weryfikacja protokołów kryptograficznych"
46. Norma ISO/IEC 29147:2014 "Vulnerability Disclosure / Ujawnienie podatności"
47. Norma ISO/IEC 30111:2011 "Vulnerability handling processes / Procesy postępowania z podatnościami"
48. Norma PN-EN 419211-1:2014 "Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu. Część 1: Przegląd"
49. Norma PN-EN 419211-2:2014 "Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu. Część 2: Urządzenie z generowaniem kluczy"
50. Norma PN-EN 419211-3:2014 "Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu. Część 3: Urządzenie z importem kluczy"
51. Norma PN-EN 419211-4:2014 "Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu. Część 4: Rozszerzenie dla urządzenia z generowaniem kluczy i bezpiecznym kanałem z aplikacją generującą certyfikaty"
52. Norma PN-EN 419211-5:2014 "Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu. Część 5: Rozszerzenie dla urządzenia z generowaniem kluczy i bezpiecznym kanałem z aplikacją podpisującą"
53. Norma PN-EN 419211-6:2014 "Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu. Część 6: Rozszerzenie dla urządzenia z importem kluczy i bezpiecznym kanałem z aplikacją podpisującą"
54. Norma PN-EN 419212-1:2015 "Interfejs aplikacyjny dla kart elektronicznych stosowanych jako bezpieczne urządzenia do składania podpisu elektronicznego. Część 1: Usługi podstawowe"
55. Norma PN-EN 419212-2:2015 "Interfejs aplikacyjny dla kart elektronicznych stosowanych jako bezpieczne urządzenia do składania podpisu elektronicznego. Część 2: Usługi dodatkowe"
56. Norma PN-EN 419251-1:2013 "Wymagania bezpieczeństwa dla urządzenia do uwierzytelniania. Część 1: Profil zabezpieczeń dla funkcjonalności podstawowej"
57. Norma PN-EN 419251-2:2013 "Wymagania bezpieczeństwa dla urządzenia do uwierzytelniania. Część 2: Profil zabezpieczeń dla rozszerzenia o wiarygodny kanał komunikacyjny z aplikacją generującą certyfikaty"
58. Norma PN-EN 419251-3:2013 "Wymagania bezpieczeństwa dla urządzenia do uwierzytelniania. Część 3: Dodatkowa funkcjonalność dla zadań zabezpieczeń*"

2. ZAŁOŻENIA TECHNICZNE

2.1. NORMY I WYMAGANIA DOTYCZĄCE KOMPLETNOŚCI WYKONANIA

Projekt oraz instalację systemu okablowania należy wykonać na podstawie:

- a. Ustaleń z przyszłym użytkownikiem;
- b. Ustaleń z przedstawicielem Działu Informatyki;
- c. Wizji lokalnej na terenie obiektów;
- d. Wytycznych zawartych w niniejszej specyfikacji;
- e. Obowiązujących norm europejskich i międzynarodowych, dotyczących wymagań ogólnych oraz specyficznych dla środowiska biurowego.
- f. Wykonawca musi posiadać odpowiedni status np. Licencjonowanego Przedsiębiorstwa do Projektowania i Instalacji, nadany bezpośrednio przez Producenta okablowania, potwierdzony umową, regulującą warunki udzielania gwarancji systemowej przez producenta.
- g. Dodatkowo wykonawca ma dysponować osobami posiadającymi imienne dyplomy potwierdzające ukończenie kursów kwalifikacyjnych w zakresie: instalacji, pomiarów, nadzoru, wykrywania oraz eliminacji uszkodzeń, projektowania okablowania strukturalnego, zgodnie z normami międzynarodowymi oraz procedurami instalacyjnymi producenta okablowania.
- h. Oferowany system okablowania strukturalnego musi być objęty programem minimum 25 letniej gwarancji systemowej.
- i. Wszystkie elementy systemu okablowania miedzianego i światłowodowego powinny być opracowane (tj. zaprojektowane, wykonane i wdrożone do oferty rynkowej), jako kompletne rozwiązania, celem uzyskania maksymalnych zapasów transmisyjnych oraz zapewnić uzyskanie certyfikatu producenta okablowania.
- j. Wymaga się, aby wszystkie elementy okablowania (w szczególności: panele krosowe, gniazda, kabel, kable krosowe, płyty czotowe gniazd, prowadnice kablowe) spełniały warunek zapewnienia uzyskania certyfikatu producenta okablowania.
- k. System okablowania strukturalnego musi obejmować kompletne rozwiązanie dla techniki miedzianej i światłowodowej, telekomunikacyjnej oraz szaf teleinformatycznych wraz z osprzętem. Elementy systemu okablowania powinny szczególnie być nastawione na uniwersalność, skalowalność, łatwość w montażu oraz prostotę i przejrzystość całości rozwiązań.
- l. Wszystkie komponenty systemu okablowania muszą być zgodne z wymaganiami obowiązujących norm: ISO/IEC 11801 2 Ed. oraz EN 50173 2.Ed, co musi być potwierdzone odpowiednimi certyfikatami. Należy zapewnić również certyfikat z niezależnego laboratorium posiadającego odpowiednią akredytację potwierdzającą zgodność łącza klasy EA z normą ANSI/TIA-568-C.2 (2009-08) w zakresie testu łącza 2 konektorowego Permanent Link.

2.1.1. PRZEPISY PRAWNE I NORMY ZWIĄZANE Z PROJEKTOWANIEM I WYKONANIEM ZAMIERZENIA BUDOWLANEGO

Dokumentacja projektowa oraz przeprowadzone prace muszą spełniać obowiązujące przepisy Prawa Budowlanego, przepisy techniczno-budowlane, przepisy związane i obowiązujące normy tj. w szczególności:

1. Rozporządzenia Ministra Infrastruktury w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego (Dz.U. 2013 poz. 1129).
2. Rozporządzenie (WE) Parlamentu Europejskiego i Rady nr 2195/2002 z dnia 5 listopada 2002 roku w sprawie Wspólnego Słownika Zamówień (Dz. Urz. WE L 340 z 16.12.2002, z późn. zm.).
3. Rozporządzenie Ministra Infrastruktury z dnia 18 maja 2004 roku w sprawie określenia metod i podstaw sporządzenia kosztorysu inwestorskiego, obliczania planowanych kosztów prac projektowych oraz planowanych kosztów robót budowlanych określonych w programie funkcjonalno-użytkowym (Dz.U. 2004 nr 130 poz. 1389).
4. Ustawa Prawo Budowlane (Dz.U. 2016 poz. 290 z późn. zm.) oraz wydanych na jej podstawie rozporządzeń.
5. Ustawa z dnia 30 sierpnia 2002 roku o systemie oceny zgodności (Dz.U. 2016 poz. 655 z późn. zm.).

6. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2011 nr 159 poz. 948).
7. Rozporządzenie Ministra Pracy i Polityki Socjalnej z 1 grudnia 1998 roku w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (Dz.U. 1998 nr 148 poz. 973).
8. Ustawa z 16 lipca 2004 roku Prawo Telekomunikacyjne (Dz.U. 2016 poz. 1489 z późn. zm.).
9. Ustawa z dnia 30 maja 2014r. o prawach konsumenta (Dz.U. 2014 poz. 827 z późn. zm.).
10. Ustawa z dnia 29 stycznia 2004 roku Prawo Zamówień Publicznych (Dz. U. 2015 poz. 2164 z późn. zm.).
11. Rozporządzenie Ministra Infrastruktury z dnia 23 czerwca 2003 roku w sprawie informacji dotyczącej zdrowia oraz planu bezpieczeństwa i ochrony zdrowia (Dz.U. 2003 nr 120 poz. 1126).
12. Rozporządzenie Ministra Infrastruktury z dnia 6 lutego 2003 roku w sprawie bezpieczeństwa i higieny pracy podczas wykonywania robót budowlanych (Dz.U. 2003 nr 47 poz. 401).
13. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 24 lipca 2009 roku w sprawie przeciwpożarowego zaopatrzenia w wodę oraz dróg pożarowych (Dz.U. 2009 nr 124 poz. 1030).
14. Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 roku w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy (Dz.U. 2003 nr 169 poz. 1650 z późn. zm.).
15. Rozporządzenie Ministra Infrastruktury z dnia 26 czerwca 2002 roku w sprawie dziennika budowy, montażu i rozbiórki, tablicy informacyjnej oraz ogłoszenia zawierającego dane dotyczące bezpieczeństwa pracy i ochrony zdrowia (Dz.U. 2002 nr 108 poz. 953 z późn. zm.).
16. Normy europejskie - oznaczają normy przyjęte przez Europejski Komitet Standaryzacji (CEN) oraz Europejski Komitet Standaryzacji Elektrotechnicznej (CENELEC) jako „Standardy europejskie (EN) ” lub dokumenty „harmonizacyjne (HD)” zgodnie z ogólnymi zasadami działania tych organizacji.
17. Warunki techniczne wykonania i odbioru robót budowlano-montażowych (część I Roboty ogólnobudowlane ITB, wyd. II).
18. Warunki techniczne wykonania i odbioru robót budowlano-montażowych. Instalacje elektryczne. Wydawnictwo "Arkady" 1990.
19. PN-IEC 60364:2000 Instalacje elektryczne w obiektach budowlanych.
20. PN-EN 50174-1: 2002 Technika informatyczna. Instalacja okablowania. Specyfikacja i zapewnienie jakości.
21. PN-EN 55022: 2002 Kompatybilność elektromagnetyczna. Dopuszczalny poziom i metody zakłóceń radioelektrycznych wytwarzanych przez urządzenia informatyczne.
22. PN-EN 50082-1: 2002 Kompatybilność elektromagnetyczna. Wymagania ogólne dotyczące odporności na zaburzenia.
23. PN-EN 50081-2: 2002 Kompatybilność elektromagnetyczna. Wymagania ogólne dotyczące emisyjności.
24. PN-EN 50310: 2002 Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym.
25. PN-EN 50364: 2003 Technika informatyczna. Instalacja okablowania. Testowanie zainstalowanego okablowania.
26. PN-79/T-052 10: 1979 Antenowe instalacje zbiorowe. Ogólne wymagania i badania.
27. BN-8984-05 Kanalizacja kablowa. Ogólne badania i wymagania.
28. PN-T-01003 Słownictwo telekomunikacyjne. Telefonii. Nazwy i określenia..
29. PN-T-06700 Bezpieczeństwo pracy przy promieniu emitowanym przez urządzenia laserowe. Klasyfikacja sprzętu. Wymagania i wytyczne dla użytkownika.
30. BN-3233-13 Telekomunikacyjne linie kablowe. Opaski oznaczeniowe.
31. BN-6353-03 Folia kalendrowana techniczna z uplastycznionego polichlorku winylu.
32. ZN-TP S.A.-002 Telekomunikacyjne linie kablowe dalekosiężne. Linie optotelekomunikacyjne. Ogólne wymagania techniczne.
33. ZN-TP S.A.-005 Kable optotelekomunikacyjne. Wymagania i badania.
34. ZN-TP S.A.-006 Złącza spajane światłowodów jednomodowych. Wymagania i badania.
35. ZN-TP S.A.-007 Złączki światłowodowe i kable stacyjne. Wymagania i badania.
36. ZN-TP S.A.-008 Osłony złączkowe. Wymagania i badania.
37. ZN-TP S.A.-011 Telekomunikacyjna kanalizacja kablowa. Ogólne wymagania techniczne.
38. ZN-TP S.A.-012 Kanalizacja pierwotna. Wymagania i badania.
39. ZN-TP S.A.-013 Kanalizacja wtórna i rurociągi kablowe. Wymagania i badania.
40. ZN-TP S.A.-017 Rury kanalizacji wtórnej i rurociągu kablowego (RHDPE). Wymagania i badania.
41. ZN-TP S.A.-018 Rury polietylenowe (RHDPEp) przepustowe.
42. ZN-TP S.A.-020 Złączki rur. Wymagania i badania.
43. ZN-TP S.A.-021 Uszczelki kodów rur. Wymagania i badania.

44. ZN-TP S.A.-024 Zasobniki złączowe. Wymagania i badania.
45. ZN-TP S.A.-025 Taśmy ostrzegawczo-lokalizacyjne. Wymagania i badania.
46. WTE-ZDBŁ-22 Wymagania techniczno-eksploatacyjne na kable optotelekomunikacyjne jednomodowe, ZDBŁ, Warszawa.
47. Instrukcja TP S.A. T-01. Odbiór i utrzymanie kablowych linii optotelekomunikacyjnych.
48. DT-ZDBŁ-43 Pomiar tłumienności, lokalizacja niejednorodności i uszkodzeń telekomunikacyjnych kabli światłowodowych reflektometrem, ZDBŁ, Warszawa.
49. DT-ZDBŁ-45 Wstępna technologia wykonywania złączy kabli światłowodowych z wykorzystaniem mufy MS. CzDDrjZDBŁ, Warszawa.
50. DT-ZDBŁ-47 jak wyżej, CzD DD, ZDBŁ, Warszawa.
51. DT-ZDBŁ-51 jak wyżej, CzD DII, ZDBŁ, Warszawa.
52. DT-ZDBŁ-57 Technologia pneumatycznego zaciągania (z wpychaniem) kabli światłowodowych do kanalizacji, ZDBŁ, Warszawa.
53. IT-ZDBŁ-52 Wstępna instrukcja zacinania kabli światłowodowych do kanalizacji kablowej oraz budowy kanalizacji wtórnej, ZDBŁ, Warszawa
54. IT-ZDBŁ-55 Wstępna instrukcja układania kabli światłowodowych w ziemi i w wodzie, ZDBŁ, Warszawa.
55. IT-ZDBŁ-60 Instrukcja układania kabli światłowodowych kanałowych, ZDBŁ.
56. Załącznik do Zarządzenia nr 83 Dyrektora Pionu Sieci Tadeusza Gracy z dnia 12 maja 2003r. – Instrukcja oznaczenia elementów stosowanych w sieci telekomunikacyjnej TP SA.
57. ISO/IEC 11801 Information technology. Generic cabling for customer premises.
58. EN 50173-1 Information technology. Generic cabling systems Part 1: "General requirements".
59. ANSI/TIA/EIA 568-B.2 Commercial Building Telecommunications Cabling Standards Part 2.
60. PN-EN 50173-1 Technika informatyczna. Systemy okablowania strukturalnego. Część 1: Wymagania ogólne.
61. PN-EN 50173-2 Technika informatyczna. Systemy okablowania strukturalnego. Część 2: Pomieszczenia biurowe.
62. PN-EN 50173-1 Technika informatyczna. Systemy okablowania strukturalnego. Część 1: Wymagania ogólne.
63. PN-EN 50173-5:2009/A1:2011+A2:2013 Technika informatyczna. Systemy okablowania strukturalnego. Część 5: Centra danych.
64. PN-EN 50173-6:2014 Technika informatyczna. Systemy okablowania strukturalnego. Część 6: Rozproszone usługi budynkowe.
65. PN-EN 50174-1:2010/A1:2011+A2:2015 Technika informatyczna. Instalacja okablowania – Część 1 – Specyfikacja i zapewnienie jakości.
66. PN-EN 50174-2:2010/A1:2011+A2:2015 Technika informatyczna. Instalacja okablowania – Część 2 – Planowanie i wykonawstwo instalacji wewnątrz budynków.
67. PN-EN 50174-3:2014 Technika informatyczna. Instalacja okablowania – Część 3 – Planowanie i wykonawstwo instalacji na zewnątrz budynków.
68. PN-EN 50575:2015 Kable i przewody elektroenergetyczne, sterownicze i telekomunikacyjne – Kable i przewody do zastosowań ogólnych w obiektach budowlanych o określonej klasie odporności pożarowej.
69. IEC 61935-1:2015 Specification form the testing of balanced and coaxial information technology cabling – Part 1: Installed balanced cabling as specified in ISO/IEC 11801 and related standards.
70. ISO/IEC 14763-3:2014 Implementation and operation of customer premises cabling – Part 3 – Testing of optical fibre cabling.
71. ISO/IEC TS 29125:2017 – Information technology – Telecommunications cabling requirements for remote powering of terminal equipment.
72. Rozporządzenie Delegowane Komisji (UE) 2016/364 z dnia 1 lipca 2015r. w sprawie klasyfikacji reakcji na ogień wyrobów budowlanych na podstawie rozporządzenia Parlamentu Europejskiego I Rady (UE) nr 305/2011.

UWAGA:

W przypadku powołań normatywnych niedatowanych obowiązuje zawsze najnowsze wydanie cytowanej normy. Wykonawca ma obowiązek wykonać instalację okablowania zgodnie z wymaganiami norm obowiązujących w czasie realizacji zadania, przy uwzględnieniu wymagań minimalnych opisanych w dokumentacji projektowej, a zdefiniowane przez dokumenty wskazane powyżej. System okablowania oraz wydajność komponentów musi

pozostać w zgodzie z wymaganiami norm PN-EN 50173-1: 2011 i ISO/IEC11801:2011, a także w zgodzie z dyrektywą CPR o klasie reakcji ogniowej nie gorszej niż B2ca-s1b, d1, a1.

UWAGA:

W PRZYPADKU POJAWIENIA SIĘ ZBIEŻNOŚCI REALIZOWANYCH PRAC BUDOWLANYCH ORAZ INSTALACYJNYCH MOGĄCYCH INGEROWAĆ FIZYCZNIE BĄDŹ LOGICZNIE W STRUKTURY SIECI TELEINFORMATYCZNEJ ORAZ WYDZIELONEJ SIECI ZASILANIA GWARANTOWANEGO OBECNEJ I UŻYTKOWANEJ JUŻ W PLACÓWKACH WCHODZĄCYCH W SKŁAD SZPITALI POMORSKICH SP. Z O.O., A ZREALIZOWANEJ W RAMACH ZADANIA „BUDOWY I DOSTOSOWANIA INFRASTRUKTURY PASYWNEJ (W TYM SERWEROWNIE), DOSTOSOWANIE I ROZBUDOWA SIECI TELEINFORMATYCZNYCH I SIECI ZASILANIA GWARANTOWANEGO WRAZ Z DOSTAWĄ BUDYNKOWYCH (CENTRALNYCH) ZASILACZY UPS” PROJEKTU „POMORSKIE E-ZDROWIE” (WSPÓŁFINANSOWANEGO ZE ŚRODKÓW UNII EUROPEJSKIEJ W RAMACH REGIONALNEGO PROGRAMU OPERACYJNEGO WOJEWÓDZTWA POMORSKIEGO), NALEŻY W PIERWSZEJ KOLEJNOŚCI PRZESTRZEGAĆ ZASAD TZW. TRWAŁOŚCI PROJEKTOWEJ (WYNIKAJĄCEJ ZE ZOBOWIĄZAŃ PODPISANYCH UMÓW O WSPÓŁFINANSOWANIE), A NASTĘPNIE ZASAD WYNIKAJĄCYCH Z WIAŻĄCEGO USTANOWIENIA OKRESU GWARANCYJNEGO I SERWISOWEGO Z GENERALNYM WYKONAWCĄ TEJŻE SIECI (FIRMA ATEM-POLSKA SP. Z O.O.).

SZCZEGÓŁOWE WARIANTY MOŻLIWOŚCI ODTWORZENIOWYCH DLA TYCH SIECI, W PRZYPADKU KONIECZNOŚCI INGERENCJI W ICH STRUKTURĘ ZAWARTO W ROZDZIALE 8.

2.2. ZAKRES PRAC DO WYKONANIA

A. Dla nowych potrzeb, czyli rozbudowy istniejących struktur sieciowych:

1. Wykonać projekty sieci LAN.
2. Wykonać projekty wydzielonej gwarantowanej instalacji zasilającej 230V sieć LAN.
3. Wykonać projekty sieci bezprzewodowej WLAN wraz z symulowanymi mapami pokrycia siecią poszczególnych pomieszczeń i pięter. Docelowy system sieci bezprzewodowej WLAN musi mieć możliwość zapewnienia równego czasu antenowego dla wszystkich klientów w środowiskach, w których wspólnie występują technologie 802.11a/b/g/n oraz 802.11ac oraz zapewnić funkcjonalność roamingu urządzeń bezprzewodowych pomiędzy Access Pointami.
4. Wykonać pomiary propagacji sygnału sieci bezprzewodowej dla standardów 802.11 g/n i ac w zakresie częstotliwości 2.4GHz oraz 5GHz (tzw. „Site Survey”), który będzie podstawą do rozmieszczenia i instalacji urządzeń Access Point w obszarach pomieszczeń, gdzie Zamawiający wymaga zapewnienia zasięgu sygnału sieci bezprzewodowej. Na etapie projektu Wykonawca uzgodni te obszary z Zamawiającym z uwzględnieniem załączonych przez Wykonawcę planów pomieszczeń z rozmieszczeniem urządzeń Access Point. W ramach pomiarów należy przeprowadzić analizę:
 - 1) Rozmieszczenia punktów dostępowych z pokryciem sygnału (min. Parametry siły sygnału odbieranego -60dBm do -70dBm),
 - 2) Parametru sygnał/szum (parametr sygnał/szum – min. 27dB, zalecane 35dB),
 - 3) Zasięgu dla poszczególnych punktów dostępowych (zasięgi poszczególnych Access Point muszą się nakładać w min. 15%, tak aby zapewnić funkcjonalność roamingu),
 - 4) Zajętości kanałów dla obu pasm,
 - 5) Widma częstotliwości 2,4GHz i 5GHz (w celu wykrycia potencjalnych zakłóceń/kolizji generowanych przez inne urządzenia),
 - 6) Propozycję przydziału kanałów do punktów dostępowych,
 - 7) Inne zalecenia techniczne i obserwacje powstałe w czasie pomiarów.
5. Na podstawie pomiarów opisanych powyżej wykonać Dokumentację Projektową sieci WLAN wraz z mapami pokrycia siecią poszczególnych pięter i pomieszczeń budynków.
6. Wykonać okablowanie strukturalne miedziane do zaprojektowanych lokalizacji (miejsc instalacji urządzeń Access Point) i zakończyć je gniazdem z interfejsem RJ45, z drugiej strony zakończyć je na panelu krosowym w najbliższym punkcie dystrybucyjnym (PPD), gdzie będą się znajdować przełączniki z funkcjonalnością PoE. Po stronie gniazda RJ45 pozostawić zapas okablowania około 3 m.
7. Wykonać okablowanie strukturalne – tzn. PEL w budynkach oraz ich pomieszczeniach. Instalację w korytarzach układać nad sufitem podwieszanym lub gdy go brak natynkowo, a magistrale prowadzić w

taki sposób, aby droga ich prowadzenia przebiegała poza miejscami ogólnodostępnymi lub na wysokości min. 2,5m od podłogi. W pomieszczeniach typowo biurowych lub nie wymagających zachowania specjalistycznego reżimu w zakresie ochrony epidemiologicznej, preferowanym modelem układania instalacji jest model instalacji układanej natynkowo (w listwach i kanałach). W pomieszczeniach sterylnych (np. sale zabiegowe lub operacyjne) dopuszcza się projektowanie i wykonanie instalacji podtynkowych (z wykorzystaniem osłonowych rur instalacyjnych umieszczonych podtynkowo) lub też natynkowo (z wykorzystaniem elementów okablowania systemowego przeznaczonego wyłącznie do wykorzystania w zakresie budowy sieci dla placówek medycznych, m.in. specjalnych paneli naściennych, kolumn pionowych, gniazd systemowych w specjalizacji medycznej).

8. Ostateczną lokalizację punktu PEL oraz AP na ścianie uzgodnić z Zamawiającym na etapie prac projektowych i potwierdzić na etapie prac instalacyjnych. Średnią długość drogi kablowej od PPD do punktu PEL należy przyjąć jako 80 mb.
9. Wykonać instalację zasilania gwarantowanego punktów PEL i PPD.
10. Rozdzielnice wydzielonej instalacji zasilic z rozdzielnic głównych budynkowych. Gniazda zasilające powinny być gniazdami z blokadą – klucz przyklejany do wtyczki. Wykonawca dostarczyć ma klucze do gniazd zasilających w ilości co najmniej odpowiadającej ilości zainstalowanych gniazd sieciowych.
11. Projektowanie infrastruktury sieciowej i wydzielonej sieci zasilania oprócz o zaprojektowanie wydzielonych pomieszczeń kondygnacyjnych, w których zlokalizowane będą piętrowe pośrednie punkty dystrybucyjne (dalej zwane PPD).
12. Każde z PPD musi być wyposażone w zintegrowany system kontroli dostępu (KD) oparty o karty kodowe i ich czytniki. System ten powinien być wspomagany przez odpowiednie zaprojektowanie i wykonanie konstrukcji drzwi wejściowych do takiego PPD, pozwalający na co najmniej zabezpieczenie drzwi dwoma zamkami – jeden zamek współdziałający z systemem KD (w chwili zaniku zasilania w tym systemie automatycznie zwalniający ten zamek i pozwalający otworzyć drzwi), drugi zamek odblokowywany kluczem. System ten należy po uzgodnieniu z Zamawiającym, zintegrować z posiadanym przez Zamawiającego systemem KD w pozostałych budynkach szpitala. System powinien umożliwiać zarządzanie nim z jednej konsoli i powinien być zintegrowany z użytkowanym w szpitalu systemem tego samego rodzaju.
13. Każde pomieszczenie/punkt PPD wyposażone powinno być w szafę teletechniczną, rozdzielnię zasilania gwarantowanego RD wraz z urządzeniem UPS o wymaganej mocy (obliczonych na podstawie bilansu mocy dla obsługiwanych gniazd PEL).
14. Każde wydzielone pomieszczenie PPD wyposażone powinno być w system wentylacji grawitacyjnej lub wymuszonej oraz system klimatyzacji, zapewniającej wymagane parametry środowiskowe dla zainstalowanego tam sprzętu aktywnego sieci oraz urządzeń UPS.
15. Każde pomieszczenie PPD wyposażone powinno być w system monitoringu infrastruktury i parametrów środowiskowych. System monitoringu środowiska powinien mierzyć parametry środowiskowe, poprzez zastosowanie odpowiednich czujników: zasilania, dymu oraz temperatury. Pozwoli to na zabezpieczenie znajdujących się w szafach teletechnicznych urządzeń, a także pozwoli dobrać optymalne warunki ich pracy. System powinien umożliwiać zarządzanie nim z jednej konsoli i powinien być zintegrowany z użytkowanym w szpitalu systemem tego samego rodzaju. System powinien być wyposażony i skonfigurowany w elementy pozwalające na komunikację z nim i przekazywanie przez niego komunikatów o stanach alarmowych po sieci LAN oraz GSM.
16. Każda z szaf teletechnicznych zainstalowana w projektowanych i wybudowanych pomieszczeniach PPD powinna posiadać połączenie światłowodowe (FO) do głównej serwerowni szpitala (GPD). Wszystkie połączenia należy wykonać co najmniej jednym torem światłowodowym jednomodowym SM 24J-E (kategorii OS2) [preferowane połączenie dwutorowe] oraz jednym torem światłowodowym wielomodowym MM 24J-E (kategorii OM4) [dla potrzeb m.in. połączeń SAN]. Każda z szaf teletechnicznych zainstalowanych w projektowanych i wybudowanych pomieszczeniach PPD powinna posiadać połączenia światłowodowe pomiędzy nimi wykonane torem światłowodowym jednomodowym SM 24J-E (kategorii OS2). Dodatkowo, w celu unieważnienia zaprojektowanej i wybudowanej infrastruktury na potencjalne uszkodzenia kabli światłowodowych międzyszafowych, należy pomiędzy wszystkimi szafami teletechnicznymi GPD - PPD zaprojektować i wykonać po cztery linie okablowania miedzianego (jeśli pozwalają na to warunki techniczne w zakresie np. odległości, w takim wypadku należy połączyć dwie najbliższe szafy PPD). Zakończyć te kable na panelach krosowych (międzyszafowych).

B. DLA PRAC ZWIĄZANYCH Z INGERENCJĄ W OBECNIE UŻYTKOWANE STRUKTURY SIECIOWE (REMONTY I MODERNIZACJE) – NALEŻY WYBRAĆ JEDEN Z WARIANTÓW OPISANY W PUNKCIE 8.

2.3. WYMAGANIA OGÓLNE

1. Wykonawca dostarczy Zamawiającemu komplet Dokumentacji Projektowej (Wykonawczej) i Dokumentacji Powykonawczej.
 - 1) Dokumentacja projektowa musi zawierać informacje ogólne (temat projektu, jego zakres, uwagi), ogólną koncepcję rozwiązań technicznych i funkcjonalnych, opis parametrów technicznych urządzeń, materiałów i oprogramowania, szczegóły rozwiązań technicznych, karty katalogowe zaproponowanych materiałów i urządzeń, stosowne certyfikaty, wykaz testów adaptacyjnych, wykaz urządzeń, materiałów, schematy instalacyjne, elektryczne i logiczne.
 - 2) Dokumentacja Powykonawcza musi zawierać opis faktycznego stanu rzeczy wraz z protokołami pomiarów wszystkich torów łączności oraz testami zabezpieczenia nadmiarowo-prądowego, przepięciowego, różnicowo-prądowego, oporności uziomu ochronnego itp. W części Dokumentacji Powykonawczej, dotyczącej sieci bezprzewodowej, Wykonawca umieści wyniki z przeprowadzonych pomiarów propagacji sygnału sieci bezprzewodowej 802.11 w zakresie częstotliwości 2.4 i 5GHz wraz z naniesionymi punktami na planach gdzie zamontowana zostaną urządzenia Access Point oraz schematami połączeń (okablowanie) prowadzących do najbliższych punktów PPD.
2. Zamawiający wymaga dostarczenia dokumentacji w formie wydruku (co najmniej 2 egzemplarze) i wersji na nośniku elektronicznym (co najmniej 2 egzemplarze). Część opisowa dokumentacji w postaci plików z edytora tekstu i PDF; trasy kablowe na podkładach budowlanych w formacie .DWG (lub zgodnym) i PDF. W przypadku braku dostarczonych przez Zamawiającego podkładów architektonicznych w formacie edytowalnym (np. DWG), Wykonawca musi dokonać inwentaryzacji architektonicznej i sporządzić taki podkład. Również podkłady architektoniczne dostarczone przez Zamawiającego, które z różnych innych przyczyn, mogą być nieaktualne i nie odzwierciedlać rzeczywistych układów architektonicznych pomieszczeń, muszą być przez Wykonawcę zaktualizowane, tak aby Dokumentacja Projektowa (Wykonawcza) i Dokumentacja Powykonawcza odpowiadały rzeczywistemu układowi architektonicznemu pomieszczeń.
3. Wszelkie uzasadnione zmiany, które Wykonawca chciałby wprowadzić do projektu (na etapie wykonawstwa) muszą być uzgodnione z autorem projektu i Zamawiającym. Wszelkie prace budowlano-montażowe związane z realizacją niniejszego zadania należy wykonać zgodnie z obowiązującymi normami oraz wytycznymi technicznymi, a w szczególności przestrzegać przepisów BHP. Wszelkie wykonywane prace oraz proponowane materiały winny odpowiadać Polskim Normom i posiadać stosowną deklarację zgodności lub posiadać znak CE i deklarację zgodności z normami zharmonizowanymi oraz posiadać niezbędne atesty tak aby spełniać obowiązujące przepisy, Wykonawca jest obowiązany do uzyskania odpowiedniego rezultatu końcowego. Wszelkie niezgodności, ewentualne braki lub niezgodności interpretacyjne dokumentacji w zakresie instalacji słaboprądowych należy uzgadniać z Zamawiającym oraz Projektantem.
4. Wyroby budowlane (instalacyjne) użyte do wykonania robót, mają spełniać wymagania polskich przepisów, a Wykonawca będzie posiadał dokumenty potwierdzające, że zostały one wprowadzone do obrotu zgodnie z regulacjami Ustawy o wyrobach budowlanych i posiadają wymagane parametry. Dokumenty te Wykonawca dołączy do dokumentacji powykonawczej. Zamawiający przewiduje bieżącą kontrolę wykonywanych robót budowlanych. Wykonawca jest odpowiedzialny za pełną kontrolę robót, jakość materiałów i elementów oraz zapewni odpowiedni system kontroli jakości.
5. Elementy okablowania strukturalnego oraz sieci elektrycznej mają zostać oznaczone zgodnie z wytycznymi Zamawiającego (paszportyzacja).
6. Należy zapewnić objęcie wykonanej instalacji gwarancją systemową producenta tego okablowania, gdzie okres gwarancji udzielony przez producenta nie może być krótszy niż 25 lat (Zamawiający wymaga certyfikatu producenta okablowania udzielonego bezpośrednio użytkownikowi końcowemu i stanowiącego 25-letnie zobowiązanie gwarancyjne producenta wszystkich elementów całego systemu okablowania dotrzymania parametrów jakościowych i materiałowych).

7. Okres gwarancji ma być standardowo udzielany przez producenta okablowania, tzn. na warunkach oficjalnych, ogólnie znanych, dostępnych i opublikowanych. Tym samym oświadczenia o specjalnie wydłużonych okresach gwarancji wystawione przez producentów, dostawców, dystrybutorów, pośredników, wykonawców lub innych nie będą uznawane za wiarygodne i spowodują bezwzględne odrzucenie oferty. Okres gwarancji liczony jest od dnia, w którym podpisano protokół końcowy odbioru prac i producent okablowania wystawił certyfikat gwarancyjny.
8. Wszystkie produkty muszą być fabrycznie nowe.
9. Celem idealnego dopasowania komponentów, wszystkie produkty okablowania muszą pochodzić z oferty jednego producenta i być oznaczone jego nazwą lub logo.
10. Należy użyć szaf 19" tego samego producenta, co pozostała część okablowania strukturalnego i oznaczonych jego nazwą lub logo.
11. Należy zastosować renomowany i sprawdzony w wielu instalacjach, nie tylko w Polsce, ale i w innych krajach Unii Europejskiej, system okablowania strukturalnego. Należy zastosować przetestowany system, którego producent ma, co najmniej 15-letnie doświadczenie w produkcji okablowania strukturalnego. Zakres jego działalności w całym tym okresie musi obejmować produkcję okablowania miedzianego (kable skrętkowych, paneli 19", złączy RJ45), światłowodowego oraz szaf dystrybucyjnych 19".
12. W celu wspierania rodzimych firm z Unii Europejskiej, należy zastosować system okablowania, którego producent ma swoją główną siedzibę w jednym z krajów Unii Europejskiej.
13. Producent okablowania strukturalnego musi spełniać wymagania międzynarodowej normy odnośnie standardów jakości ISO 9001, należy przedłożyć odpowiedni certyfikat.
14. Producent okablowania musi objąć zainstalowany system bezpłatną, 25-letnią systemową gwarancją niezawodności, która obejmie tory transmisyjne miedziane i światłowodowe w zakresie łącza Channel (kable instalacyjne, panele 19", złącza, kable krosowe i przyłączeniowe). Gwarancja musi być trójstronną umową podpisaną pomiędzy Użytkownikiem, Wykonawcą okablowania oraz Producentem.
15. Producent okablowania jest zobligowany do reasekuracji zobowiązań gwarancyjnych Wykonawcy, w przypadku niemożności wywiązania się Wykonawcy z tych zobowiązań. Reasekuracja obejmuje okres, na jaki została udzielona gwarancja.
16. Warunkiem udzielenia systemowej gwarancji niezawodności jest wykonanie instalacji zgodnie z obowiązującymi normami okablowania strukturalnego oraz zgodnie z zaleceniami producenta. Instalacja musi być wykonana przez Certyfikowanego Instalatora systemu okablowania.
17. Celem profesjonalnego wykonania instalacji okablowania strukturalnego, na najwyższym poziomie jakości i wydajności, wszystkich czynności instalacyjnych musi dokonać wykwalifikowany Wykonawca spełniająca poniższe wymagania:
 - 1) Wykonawca musi zatrudniać pracowników – Certyfikowanych Instalatorów posiadających ważne uprawnienia i certyfikat wydany przez producenta okablowania przyjętego w tym projekcie.
 - 2) Certyfikat Instalatora musi być wydany po odbyciu szkolenia, w którym każdy Instalator zdobędzie wszystkie niezbędne umiejętności praktyczne i teoretyczne, uprawniające do instalowania, serwisowania, tworzenia dokumentacji powykonawczej oraz wykonywania pomiarów certyfikacyjnych sieci.
 - 3) Certyfikat Instalatora, który posiadają osoby wykonujące instalację musi być dokumentem terminowym wydawanym na okres jednego roku. Po tym czasie instalator musi go przedłużyć na kolejny rok, uczestnicząc w szkoleniu realizowanym przez producenta lub dystrybutora okablowania.
 - 4) Wykonawca autoryzujący system okablowania strukturalnego musi posiadać uprawnienia do objęcia zainstalowanego systemu 25-letnią systemową gwarancją niezawodności.

2.4. WYMAGANIA GWARANCYJNE

Wymagana gwarancja musi być bezpłatną usługą serwisową oferowaną przez producenta okablowania. Musi obejmować swoim zakresem całość systemu okablowania od punktu dystrybucyjnego do gniazda końcowego dla części logicznej sieci.

Należy zapewnić objęcie wykonanej instalacji gwarancją systemową producenta, gdzie okres gwarancji udzielonej bezpośrednio przez producenta nie może być krótszy niż 25 lat (wymagany certyfikat gwarancyjny

producenta okablowania udzielony bezpośrednio Użytkownikowi końcowemu i stanowiący 25-letnie zobowiązanie gwarancyjne producenta w zakresie dotrzymania parametrów wydajnościowych, jakościowych, funkcjonalnych i użytkowych wszystkich elementów oddzielnie i całego systemu okablowania). Oświadczenia o specjalnie wydłużonych okresach gwarancji wystawione przez producentów, dostawców, dystrybutorów, pośredników, wykonawców lub inne osoby nie będą równoważne względem powyższych wymagań.

25 letnia gwarancja systemowa producenta ma obejmować:

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

3. OKABLOWANIE STRUKTURALNE

3.1. OKABLOWANIE STRUKTURALNE POZIOME I PIONOWE BUDYNKOWE, INSTALACJA ELEKTRYCZNA, INSTALACJE TELETECHNICZNE

- a) Zamawiający posiada i rozbudowuje swoją sieć strukturalną w oparciu o wytyczne podane w tym opracowaniu. Dlatego też oczekuje zachowania w nowej części budynkowej i w pomieszczeniach poddawanych remontom zastosowania systemów okablowania i wyposażenia sieci identycznych z aktualnie użytkowanym. Na etapie projektowania i wykonawstwa należy zachować identyczne parametry i wymagania w tym zakresie opisywane tym dokumentem.
- b) Okablowanie należy rozbudować o Punkty Elektryczno-Logiczne (PEL) zdefiniowane jako minimum 2xRJ45 +2x230Vdata, kategoria okablowania co najmniej 6A. Zamawiający w obecnej infrastrukturze bazuje na produktach firmy Reichle & De-Massari AG (R&M) - w tym na okablowaniu miedzianym R&M freenet F/FTP cat.7 [650MHz].
- c) Punkty dostępowe sieci bezprzewodowej WLAN AP należy montować w korytarzach na sufitach właściwych lub podwieszanych, zasilane AP wykonać po skrętce z PoE, kategoria okablowania co najmniej 6A (Zamawiający bazuje na produktach firmy Reichle & De-Massari AG (R&M) - w tym na okablowaniu miedzianym R&M freenet F/FTP cat.7 [650MHz]).
- d) W zakresie koryt i listew kablowych podstawą projektowania są systemy listew i wyposażenia firmy Legrand oraz koryt metalowych (siatkowych) firmy BAKS.
- e) W przypadku rozbudowy, modernizacji lub naprawy istniejącego w budynku systemu okablowania strukturalnego należy dostarczyć komponenty zgodne (kategoria, producent) z wcześniej zainstalowanym systemem, bądź zamienne – po wcześniejszym uzgodnieniu tego faktu z Działem Informatyki.
- f) W każdym projekcie należy uwzględnić okablowanie strukturalne dla sieci bezprzewodowej, tj. urządzeń Access Point (AP) montowane na suficie lub nad kasetonami. Miejsce i sposób doprowadzenia okablowania wydzielonego dla urządzeń sieci bezprzewodowej każdorazowo należy uzgodnić z Działem Informatyki.
- g) Połączenia między punktami PPD należy wykonać zawsze dwoma sposobami, tzn. zaprojektować i wykonać połączenie światłowodowe oraz połączenie kablowe miedziane (o ile pozwalają na to uwarunkowania techniczne w zakresie maksymalnego dystansu łącza pomiędzy szafami teletechnicznymi). Połączenie kablowe wykonane wg specyfikacji powyżej powinny być zakończone na dodatkowym panelu krosowym lub po zaakceptowaniu przez Dział Informatyki panelu krosowym już obecnym w szafie.
- h) Każdy remont/inwestycję/projekt/zmianę w zakresie okablowania strukturalnego należy uzgodnić z Działem Informatyki oraz użytkownikiem danego działu/oddziału.

3.2. WYMAGANIA I CECHY OKABLOWANIA STRUKTURALNEGO

3.2.1. GNIAZDA I MODUŁY

1. W płyty czołowe kątowe należy zamontować jeden lub dwa ekranowane dwuelementowe moduły gniazda RJ45 w kategorii co najmniej 6A.
2. Ze względu na konieczność zapewnienia przestrzeni pod zakończenia do innych zastosowań należy zastosować moduł RJ45 o wymiarach nie większych niż: 14,48x20,62x31,82mm.
3. Moduł gniazda RJ45 ma posiadać pełne ekranowanie i konstrukcję dwuelementową z ekranem uchwytem ekranu 360° kabla ekranowanego na całym obwodzie kabla.
4. Konstrukcja modułu ma podczas montażu składać się w szczelną całość, tworząc zintegrowaną i szczelną klatkę Faradaya, zabezpieczoną konstrukcyjnie nawet przed zakłóceniami pochodzącymi od modułów gniazd zainstalowanych w jednym rzędzie.
5. Konstrukcja modułu i uchwyty ekranu nie może zniekształcać konstrukcji kabla, ma również zapewniać maksymalną łatwość instalacji oraz gwarantować najwyższe parametry transmisyjne.
6. Wymaga się, aby każdy moduł gniazda RJ45 posiadał możliwość uniwersalnego terminowania kabli, tj. w sekwencji T568A lub T568B.
7. Każdy moduł ma być zarabiany narzędziami dedykowanymi, uniwersalnymi lub też beznarzędziowo.

8. Zalecane jest, wykorzystanie do montażu takich narzędzi, które poprzez jeden ruch narzędzia, zapewniają krótkie rozploty par – max. 6 mm (a przez to najlepsze możliwe osiągi transmisyjne) oraz dużą powtarzalność i szybkość zarabiania.
9. Moduły ekranowane gniazd RJ45, mają umożliwiać terminację drutu miedzianego o średnicy od 0,51 do 0,65mm (24 – 22 AWG).

3.2.1.1. WYMAGANE MINIMALNE PARAMETRY MODUŁU

1. Moduł Keystone RJ45 - ekranowany, dwuelementowy w kategorii co najmniej 6A
2. Styk ekranu – Stal nierdzewna
3. Schemat T568A & T568B nadrukowany na pokrywie IDC
4. Ilość cykli połączeniowych - minimum 750 cykli
5. Średnica przewodnika – drut 24-22 AWG
6. Temperatura pracy: -40°C do +70°C
7. Charakterystyka transmisyjna modułu gniazda RJ45 ma być potwierdzona przez certyfikaty wystawione przez niezależne akredytowane laboratorium z testów przeprowadzonych w paśmie częstotliwości do minimum 500MHz, zgodnie z wymaganiami transmisyjnymi norm specyfikujących Klasę EA/Kategorię 6A. Pod uwagę będą brane jedynie dokumenty zawierające konkretne numery produktów poddane procesowi certyfikacji.
8. W celu potwierdzenia utrzymania parametrów elektrycznych gniazd podczas długotrwałego użytkowania łącznie z PoE+ producent powinien przedstawić raport z testów wg normy IEC 60512-99-001 Connectors used in twisted pair communication cabling with remote power.

3.2.2. PANELE KROSUJĄCE MIEDZIANE

1. Kable należy zakończyć na 24 lub 48 – portowym modułowym panelu krosowym o wysokości montażowej 1U, posiadającym moduły RJ45 w kategorii minimum 6A, montowane indywidualnie w płycie czołowej panelu, co zapewnia zwartą konstrukcję, łatwy montaż, terminowanie kabli oraz uniwersalne rozszycie kabla w sekwencji T568A lub T568B.
2. Panele proste lub kątowe.
3. Panel ma zawierać tylną prowadnicę kabla.
4. W celu łatwego wyprowadzenia wpiętych kabli krosowych, panel musi posiadać zintegrowane boczne prowadnice kabli.
5. Skuteczne podtrzymanie kabli krosowych muszą zapewnić uchwyty kablów zamontowane na płycie frontowej panela.
6. Uchwyty kablów muszą mieć solidną, metalową konstrukcję zapewniającą utrzymanie do 24 kabli krosowych.
7. Panel ma zawierać zacisk uziemiający.
8. W tylnej części panela musi znajdować się metalowa prowadnica kabla, dająca możliwość trwałego przytwierdzenia skrętkowych kabli instalacyjnych.
9. Kable instalacyjne, zakańczane na panelu, należy – w celu zapewnienia optymalnego prowadzenia – wesprzeć na prowadnicy kabli, montując je za pomocą opasek kablów (należy zwrócić uwagę, aby zbyt mocno nie zaciskać opasek, mają one tylko lekko utrzymać kabel na prowadnicy).
10. Na przedniej płycie musi znajdować się pole umożliwiające umieszczenie etykiet opisujących porty.
11. Należy rozdzielić na osobnych panelach gniazda komputerowe i telefoniczne.

3.2.3. KABLE MIEDZIANE

1. W celu zapewnienia bezpieczeństwa technologicznego inwestycji, instalacja kablów ma być wykonana przy użyciu podwójnie ekranowanego kabla konstrukcji F/FTP lub S/FTP (PiMF) w kategorii minimum 6A (wymagane oznaczenie na kablu) z osłoną zewnętrzną trudnopalną (LSZH).
2. Zgodnie z wymaganiami norm każdy 4 - parowy kabel ma być w całości ekranowany - wszystkie pary, F/FTP lub S/FTP (PiMF) i trwale zakończony na 8-pozycyjnym złączu modułowym - w tym przypadku na ekranowanym module Keystone kategorii minimum 6A.

3.2.3.1. WYMAGANE MINIMALNE PARAMETRY KABLA

1. Kabel F/FTP lub S/FTP (PiMF) LSZH minimum w kategorii 6A.
2. Budowa:
 - 1) Każda para indywidualnie ekranowana folią aluminiową
 - 2) Kabel ekranowany plecionką miedzianą, cynowaną lub folią aluminiową
 - 3) Jednorodna żyła miedziana drut (AWG 23)
 - 4) Średnica zewnętrzna kabla 7,0 - 7,8 mm
 - 5) Powłoka LSZH zgodnie z normą IEC 60332-1
3. Parametry mechaniczne:
 - 1) Minimalny promień gięcia zgodnie z instrukcją montażową producenta
 - 2) Zakres temperatury pracy: -20°C do +60°C
 - 3) Zakres temperatury podczas instalacji: 0°C do +50°C
4. Zgodność z wymaganiami zawartymi w normach:
 - 1) ISO/IEC 11801:2002 wyd. II
 - 2) ISO/IEC 61156-5
 - 3) EN 50173-1
 - 4) EN 50288-10-1
5. Wydajność kabla oraz spełnienie powyższych wymagań powinno być potwierdzone certyfikatem wydanym przez niezależne akredytowane laboratorium. Pod uwagę należy brać jedynie dokumenty zawierające konkretne numery produktów poddane procesowi weryfikacji i certyfikacji zgodnie z ww. normami.
6. Wszystkie kable instalacyjne wewnątrz budynków mają być sklasyfikowane ze względu na palność zgodnie z przepisami zawartymi w Rozporządzeniu Delegowanym Komisji (EU) 2016/364 z dnia 1 lipca 2015r.

3.2.4. OKABLOWANIE ŚWIATŁOWODOWE

1. Okablowanie szkieletowe światłowodowe łączące punkty dystrybucyjne (PPD) jest zrealizowane kablem światłowodowym jednomodowym – dla torów transmisji danych typu DATA lub kablem światłowodowym wielomodowym – dla torów transmisji danych typu SAN (wielowłóknowe kable światłowodowe w osłonie o określonej klasie odporności na ogień, z włóknami o rdzeniu 9/125µm lub 50/125µm). Ilość, rodzaj i typ okablowania na etapie projektowania oraz wykonania uzgodnić z Zamawiającym. Kable mają mieć określoną klasę odporności na ogień, zgodnie z klasyfikacją z EN 13501-6, co ma być potwierdzone przez producenta Deklaracją Zgodności Producenta, w której sklasyfikowano ich charakterystyki zgodnie z EN50575:2014+A1:2016. Powłoka kabla ma posiadać nowe oznaczenia zgodne z dyrektywą CPR i posiadać oznaczenia euroklasy wg nowej Dyrektywy. Klasa nie niższa niż ECA.
2. Aby zapewnić możliwość przesyłania nie tylko aktualnie stosowanych protokołów transmisyjnych, ale również długi okres działania sieci z odpowiednim zapasem pasma przenoszenia jako medium transmisyjne należy zastosować kabel światłowodowy z włóknami kategorii OS2 zalecanymi do transmisji 10-Gigabitowych oraz 40-Gigabitowych.

Minimalne wymagania dla kable (włókna) światłowodowego OS2

OPIS:	ŚWIATŁOWÓD JEDNOMODOWY Z WŁÓKNAMI 9/125µM - KATEGORIA OS2					
1. Zgodność z normami:	IEC 60332 część 1 i 3 (palność) IEC 60754 część 1 i 2 (emisja gazów kwaśnych) IEC 61034 część 1 i 2 (emisja dymu)					
2. Konstrukcja:	4,8,12 lub 24 włókien 9/125µm w buforze 250µm w luźnej tubie					
3. Właściwości mechaniczne:	Liczba włókien	Średnica zewnętrzna (mm)	Ciężar (nom. kg/km)	Naprężenia podczas instalacji (N)	Odporność na zgniecenia (N/10cm)	Min. promień zgięcia podczas instalacji (mm)
	4/8/12/24	6,4	48	1250	100	140
4. Parametry optyczne:	Tłumienie (dB/km)	1310nm	Tłumienie (dB/km)	1550nm	Długość fali odcięcia (nm)	

OPIS:	ŚWIATŁOWÓD JEDNOMODOWY Z WŁÓKNAMI 9/125µM - KATEGORIA OS2		
	< 0,34	< 0,22	<1260
5. Temperatura pracy (°C):	-20° do +60°		
6. Osłona zewnętrzna:	Kable mają mieć określoną klasę odporności na ogień, zgodnie z klasyfikacją z EN 13501-6, co ma być potwierdzone przez producenta Deklaracją Zgodności Producenta, w której sklasyfikowano ich charakterystyki zgodnie z EN50575:2014+A1:2016. Powłoka kabla ma posiadać nowe oznaczenia zgodne z dyrektywą CPR i posiadać oznaczenia euroklasy wg nowej Dyrektywy. Klasa nie niższa niż ECA.		

OPIS:	ŚWIATŁOWÓD WIELOMODOWY Z WŁÓKNAMI 50/125µM - KATEGORIA OM3					
1. Zgodność z normami:	IEC 60332 - część 1 i 3 (palność) IEC 60754 - część 1 i 2 (emisja gazów kwaśnych) IEC 61034 - część 1 i 2 (emisja dymu)					
2. Konstrukcja:	12 włókien 50/125µm w buforze 250µm w luźnej tubie					
3. Właściwości mechaniczne:	Liczba włókien/tub	Średnica zewnętrzna (mm)	Ciężar (nom. kg/km)	Naprężenia podczas instalacji (N)	Odporność na zgniecenia (N)	Min. promień zgięcia podczas instalacji (mm)
	12/1	6.4	48	1250	1000	140
4. Parametry optyczne:	Tłumienie 850nm (dB/km)	Tłumienie optyczne: 1300nm (dB/km)	Szerokość pasma przenoszenia przy fali 850nm (MHz*km)	Szerokość pasma przenoszenia przy fali 1300nm (MHz*km)		
	< 2,7	< 0,7	> 1500	> 500		
5. Temperatura pracy (°C):	-20° do +60°					
6. Osłona zewnętrzna:	Kable mają mieć określoną klasę odporności na ogień, zgodnie z klasyfikacją z EN 13501-6, co ma być potwierdzone przez producenta Deklaracją Zgodności Producenta, w której sklasyfikowano ich charakterystyki zgodnie z EN50575:2014+A1:2016. Powłoka kabla ma posiadać nowe oznaczenia zgodne z dyrektywą CPR i posiadać oznaczenia euroklasy wg nowej Dyrektywy. Klasa nie niższa niż ECA.					

OPIS:	ŚWIATŁOWÓD WIELOMODOWY Z WŁÓKNAMI 50/125µM - KATEGORIA OM4					
1. Zgodność z normami:	IEC 60332 - część 1 i 3 (palność) IEC 60754 - część 1 i 2 (emisja gazów kwaśnych) IEC 61034 - część 1 i 2 (emisja dymu)					
2. Konstrukcja:	12 włókien 50/125µm w buforze 250µm w luźnej tubie					
3. Właściwości mechaniczne:	Liczba włókien/tub	Średnica zewnętrzna (mm)	Ciężar (nom. kg/km)	Naprężenia podczas instalacji (N)	Odporność na zgniecenia (N)	Min. promień zgięcia podczas instalacji (mm)
	12/1	6.4	48	1250	1000	140
4. Parametry optyczne:	Tłumienie 850nm (dB/km)	Tłumienie optyczne: 1300nm (dB/km)	Szerokość pasma przenoszenia przy fali 850nm (MHz*km)	Szerokość pasma przenoszenia przy fali 1300nm (MHz*km)		

	< 2,4	< 0,6	> 3500	> 500	
5. Temperatura pracy (°C):	-20° do +60°				
6. Osłona zewnętrzna:	Kable mają mieć określoną klasę odporności na ogień, zgodnie z klasyfikacją z EN 13501-6, co ma być potwierdzone przez producenta Deklaracją Zgodności Producenta, w której sklasyfikowano ich charakterystyki zgodnie z EN50575:2014+A1:2016. Powłoka kabla ma posiadać nowe oznaczenia zgodne z dyrektywą CPR i posiadać oznaczenia euroklasy wg nowej Dyrektywy. Klasa nie niższa niż ECA.				

3. Kable światłowodowe zaprojektowane do stosowania w sieci szkieletowej mają się charakteryzować konstrukcją w luźnej tubie.
4. W celu łatwej identyfikacji wszystkie włókna światłowodowe mają być oznaczone przez producenta na całej długości różnymi kolorami, zaś osłona zewnętrzna powinna mieć kolor żółty.
5. Kable mają mieć określoną klasę odporności na ogień, zgodnie z klasyfikacją z EN 13501-6, co ma być potwierdzone przez producenta Deklaracją Zgodności Producenta, w której sklasyfikowano ich charakterystyki zgodnie z EN50575:2014+A1:2016. Powłoka kabla ma posiadać nowe oznaczenia zgodne z dyrektywą CPR i posiadać oznaczenia euroklasy wg nowej Dyrektywy. Klasa nie niższa niż ECA. Wszystkie kable instalacyjne wewnątrz budynków mają być sklasyfikowane ze względu na palność zgodnie z przepisami zawartymi w Rozporządzeniu Delegowanym Komisji (EU) 2016/364 z dnia 1 lipca 2015r.
6. Wymagane kolory – kolejność rozszycia i terminacji włókien kabla światłowodowego na panelu:
 1. niebieski
 2. pomarańczowy
 3. zielony
 4. brązowy
 5. szary
 6. biały
 7. czerwony
 8. czarny
 9. żółty
 10. fioletowy
 11. różowy
 12. błękitny

3.2.4.1. PANELE KROSUJĄCE ŚWIATŁOWODOWE

1. Uniwersalny panel krosowy w stelażu powinien posiadać wysuwaną, metalową i blokową szufladę, w celu umożliwienia łatwego dostępu przy montażu modułów zatraskowych i ewentualnej rekonfiguracji połączeń w komfortowej odległości od szafy kablowej.
2. Mechanizm zamykania szuflady ma być zatraskowy, nie powodujący konieczności posiadania żadnych narzędzi do otwarcia panela i wysunięcia szuflady montażowej.
3. Panel standardowo ma być wyposażony w elementy zapasu włókna (prowadnice – krzyżaki), dławiki do wprowadzania i utrzymania kabli.
4. Każdy panel krosowy musi być jednoznacznie oznaczony etykietą zawierającą co najmniej informacje o ilości włókien, typie kabla, sposobie instalacji, sposobie zakończenia.
5. Wszystkie włókna światłowodowe muszą mieć strukturę ciągłą od zakończenia na jednym końcu toru do zakończenia na drugim końcu toru, spawanie wzdłuż toru światłowodowego w ramach okablowania budynkowego jest niedozwolone.
6. Wszystkie włókna optyczne muszą być zakończone przy użyciu spawarki termicznej przeznaczonej dla danego typu włókna
7. Połączenie światłowodowe zakończone po obu stronach kasetą/skrzynką z zapasem oraz panelem światłowodowym. Włókna zakończone złączami typu duplex LC. Zmiana rodzaju okablowania lub zakończenia musi być zaakceptowana przez Dział Informatyki Zamawiającego.
8. Okablowanie światłowodowe poprowadzone w peszlu lub innej ochronnej otulinie.

3.2.4.2. ADAPTERY/INTERFEJSY ŚWIATŁOWODOWE

1. Interfejsy, na których powinno opierać się okablowanie światłowodowe to złącza LC/PC. Adaptery LC to złącza najczęściej obecnie występujące w urządzeniach aktywnych sieci komputerowej renomowanych producentów.

3.2.4.3. KABLE KROSOWE ŚWIATŁOWODOWE

1. Ekrany złączy na kablach krosowych powinny zapewnić pełną szczelność elektromagnetyczną z każdej strony złącza.

3.3. WYMAGANIA DLA TRAS KABLOWYCH

1. Wykonawca poprowadzi tory kablowe w zakresie całego projektu w taki sposób, aby droga ich prowadzenia przebiegała poza miejscami ogólnodostępnymi lub nad sufitem podwieszanym lub na wysokości min. 2,5m od podłogi.
2. Trasy kablowe muszą być ułożone w taki sposób, aby chronić kable przed bezpośrednim uszkodzeniem przez pracowników.
3. W przypadku traktów, gdzie kable sieci teleinformatycznej i zasilającej biegną razem i równolegle do siebie należy zachować odległość (rozdział) między instalacjami (szczególnie zasilającą i logiczną), co najmniej 100mm (w przypadku głównych ciągów kablowych) lub stosować metalowe przegrody oraz co najmniej 2mm dla gniazd końcowych. Wielkość separacji dla trasy kablowej jest obliczona dla przypadku kabli F/UTP o tłumieniu sprzężenia nie gorszym niż 80dB.
4. Preferowanym sposobem projektowania i układania instalacji teletechnicznej i wydzielonej sieci zasilania gwarantowanego jest metoda natynkowa (zgodna z technologią wykorzystywaną w obecnie użytkowanej sieci wybudowanej w ramach Projektu „Pomorskie e-Zdrowie”). Zamawiający dopuszcza wykorzystanie technologii podtynkowej w obiektach/pomieszczeniach o dużym reżimie ochrony epidemiologicznej (np. sale operacyjne lub specjalistyczne gabinety zabiegowe), jednak z zachowaniem podstawowych parametrów technicznych zawartych w tym opracowaniu.
5. Wszystkie kable muszą być umieszczone w sposób uporządkowany i zgodny z wytycznymi producenta tak, aby nie były narażone na nacisk i zgięcia wzdłuż drogi prowadzenia, przymocowane i zabezpieczone za pomocą opasek kablowych (tylko w punktach, gdzie nie ma zgięć i skręceń) i rzepowych, zachowując właściwy promień gięcia. Dopuszcza się następujące rozwiązania (szczegóły do uzgodnienia z Działem Informatyki):
 - a). Kanały i listwy instalacyjne (w przypadku instalacji układanej natynkowo) - zawierające przegrodę oddzielającą kable zasilające od kabli miedzianych do transmisji danych i głosu, specjalne uchwyty i puszki umożliwiające montaż gniazd zasilających oraz telekomunikacyjnych. Jeśli system kanałów zawiera już kable, należy dokonać ich przeglądu, aby upewnić się, czy jest wystarczająca ilość miejsca dla nowego systemu okablowania i czy kable zasilające nie są prowadzone w części przeznaczony dla kabli telekomunikacyjnych. Okablowanie układane w kanałach i listwach instalacyjnych nie może przekraczać 80% objętości przekroju poprzecznego kanału lub listwy instalacyjnej w której jest prowadzone.
 - b). Sufit podwieszany - kable muszą być prowadzone w przestrzeni międzysufitowej w kanale kablowym lub korycie siatkowym metalowym, który jest przymocowany bezpośrednio do sufitu właściwego. Jeśli sufit właściwy ma powłokę ognioodporną, nie powinien być nawiercany. Należy zwrócić szczególną uwagę, aby nie pozostawić zabrudzeń na demontowanych na potrzeby instalacji kasetonach. Okablowanie układane w kanałach kablowych nie może przekraczać 80% objętości przekroju poprzecznego kanału kablowego w której jest prowadzone.
 - c). Kanały podłogowe – kable muszą być prowadzone pod podłogą w kanałach instalacyjnych lub na drabinach kablowych. Podłoga podniesiona musi posiadać zainstalowane puszki podłogowe, służące do montażu standardowych gniazd abonenckich. Należy pozostawić zapas 3m kabla, zwinięty pod puszką podłogową. Okablowanie układane w kanałach i drabinach kablowych nie może przekraczać 80% objętości przekroju poprzecznego kanału lub drabiny kablowej w której jest prowadzone.
 - d). Kable skrętkowe i światłowodowe oraz wydzielonej sieci napięcia gwarantowanego okablowania poziomego instalowane pod tynkiem (w przypadku technologii podtynkowej) należy układać w rurach osłonowych z tworzywa sztucznego. Nie należy prowadzić kabli telekomunikacyjnych i zasilających w tej samej rurze osłonowej. W obu przypadkach należy zabezpieczyć stosowny zapas technologiczny w przestrzeni rury osłonowej – przyjmuje się 20% zapasu. Również dopuszczalne jest stosowanie technologii montażu podtynkowego instalacji teletechnicznej w m.in. salach operacyjnych oraz zabiegowych, w których wykorzystuje się elementy typu panele medyczne oraz kolumny i ramiona montażowe. Również w tym przypadku należy pamiętać o traktowaniu takich połączeń jako punktów PEL (czyli gniazdek logicznych i gniazdek wydzielonej sieci zasilania gwarantowanego).
6. Po wykonaniu przejścia należy dokonać wypełnienia ubytków w stropie oraz ścianach powstałych na skutek przewiertu bądź przekucia. W przypadku zapór ogniowych należy zabezpieczyć otwór oraz

elementy drogi kablowej odpowiednią powłoką ognioodporną (preferowane wyroby firmy HILTI) wraz z przywieszką identyfikacyjną (firma wykonująca, data wykonania, typ masy uszczelniającej, identyfikator przejścia). Niedopuszczalne jest zastosowanie (w celu zabezpieczenia powłoką ognioodporną zapory ogniowej) masy uszczelniającej innego typu niż wcześniej zastosowana (dotyczy przejść przez istniejące zapory ogniowe). Wszystkie miejsca i lokalizacje przejść uzupełnionych masą ognioodporną należy wskazać również na rysunkach i schematach dokumentacji powykonawczej (numery i oznaczenia przejść w dokumentacji powinny się pokrywać z numerami i oznaczeniami na przewieszkach identyfikacyjnych w obiekcie). Wszelkie uszkodzenia mechaniczne, w tym ubytki powstałe w wyniku przekuć i przewiertów oraz ubytki w malowaniu powierzchni ścian, Wykonawca jest zobowiązany uzupełnić w sposób nie gorszy niż przywracający poprzednią strukturę pomieszczeń i korytarzy.

7. Trasy pomiędzy pośrednimi punktami dystrybucyjnymi (PPD) muszą być oznaczone i opisane w sposób łatwy do identyfikacji.
8. Okablowanie poziome magistrale należy prowadzić w nowo projektowanych kanałach kablowych. Koryta kablowe przymocować do ścian lub stropu za pomocą kołków rozporowych lub metodą klejową zapobiegającą ich odklejeniu. Maksymalna odległość pomiędzy miejscami mocowania koryta do ściany nie powinna być większa niż 0,5m. W przypadku pomieszczeń w których zainstalowany jest sufit podwieszany, istnieje możliwość prowadzenia instalacji w przestrzeni międzysufitowej. Koryta kablowe należy podwieszać do stropu pomieszczenia z wykorzystaniem zawiesi. Dobór typu oraz odległości pomiędzy zawieszami, należy poprzedzić obliczeniami całkowitego obciążenia instalacji. W obu przypadkach Wykonawca powinien prowadzić koryta kablowe bezkolizyjnie z innymi instalacjami i urządzeniami. Przejścia przez ściany należy wykonać w rurach osłonowych, w celu dodatkowego zabezpieczenia kabli przed fizycznym uszkodzeniem.
9. Przejścia kabli pomiędzy piętrami należy wykonywać z wykorzystaniem drabinek kablowych zainstalowanych w projektowanych szachtach kablowych. W przypadku braku szachtów kablowych Wykonawca powinien wykonać przejścia w postaci otworów wierconych, w których powinien osadzić przepusty z winidurowych rur instalacyjnych.
10. Wszelkie przepusty wykonane pomiędzy strefami ogniowymi powinny zostać wypełnione barierami ogniowymi posiadającymi atest Narodowego Instytutu Zdrowia Publicznego oraz Instytutu Techniki i Budowlanej.
11. Wszędzie tam, gdzie to możliwe, należy instalować punkty PEL lub AP wybierając optymalną trasę kabli, łącząc następny punkt w sąsiednim pomieszczeniu przez wywiercony otwór w ścianie działowej. Wszystkie wykonane otwory w stropach i ścianach działowych powinny być zabezpieczone zgodnie z wymaganiami zabezpieczenia przeciwpożarowego.
12. W głównych trasach kablowych w korytach kablowych należy uwzględnić 20% zapas na dodatkowe kable.
13. Połączenia wykonywane na zewnątrz budynków należy realizować przy wykorzystaniu dedykowanej kanalizacji teletechnicznej.

3.4. WYMAGANIA DLA PEL I/LUB AP

1. Okablowanie należy wykonać w topologii gwiazdy, wszystkie kable należy doprowadzić do właściwego Pośredniego Punktu Dystrybucyjnego (PPD).
2. Gniazda w pomieszczeniach należy zamontować na wysokości nie mniejszej niż 30 cm od podłogi, w puszkach natynkowych lub bezpośrednio w korycie kablowym, w miejscach wskazanych przez Zamawiającego.
3. Wykonawca powinien ograniczyć ilość skrzyżowań kabli teleinformatycznych z przewodami elektrycznymi, a w przypadku konieczności poprowadzenia kabli sieciowych i prądowych równolegle odseparować je z wykorzystaniem przegród kablowych.
4. Punkt Elektryczno-Logiczny (PEL) powinien składać się minimum z 2 gniazd RJ45 (ramka biała, puszka potrójna (natynkowa, podtynkowa), support potrójny) kategorii minimum 6A lub wyższej oraz dwóch gniazd elektrycznych (ramka biała, puszka podwójna (natynkowa, podtynkowa), support podwójny) z blokadą uniemożliwiającą podłączenie nieuprawnionych odbiorników. Każdorazowo ilość punktów przyłączeniowych oraz sposób instalacji należy uzgodnić z przedstawicielem Działu Informatyki.
5. W przypadku skrętki miedzianej należy bezwzględnie przestrzegać wynikającego z normy ograniczenia związanego z maksymalną długością łącza sieciowego.

6. Wszystkie kable telekomunikacyjne jak i elektryczne muszą być opisane zgodnie z Rozporządzeniem UE 305/2011. Producent kabla musi przedstawić deklarację właściwości użytkowych zgodnie z Rozporządzeniem UE 305/2011.
7. Wszystkie kable sieciowe należy oznakować w czytelny sposób, w odległości ok. 0,3m od ich końców.
8. Odpowiednie oznakowania muszą znaleźć się także na gniazdach w pomieszczeniach oraz na panelach krosowych w PPD.
9. Kable powinny być zgodne z oznaczeniami punktów abonenckich zgodnie ze standardem przyjętym w danym budynku (paszportyzacja), w uzgodnieniu z Zamawiającym.
10. Kable należy zakończyć w gniazdach oraz w panelach krosowych zainstalowanych w PPD, zgodnie z standardem 568B EIA/TIA.
11. Panele krosowe oraz gniazda należy opisać w jednolity sposób, zgodnie z przyjętym standardem uzgodnionym z Zamawiającym.
12. W punktach PEL lub AP moduły RJ45 muszą być wykonane w standardzie Keystone Jack; co pozwala na ich montaż w każdym dostępnym osprzęcie.
13. Moduł RJ45 powinien zapewnić uniwersalność rozwiązania (taki sam moduł po stronie gniazda i po stronie panelu krosowego/modularnego).
14. Moduł RJ45 musi być wielokrotnego użytku - pozwalać na demontaż z kabla skrętkowego a następnie powtórne zaterminowanie.
15. Prowadzenie kabla w pomieszczeniach, do gniazda końcowego - w kanałach natynkowych (należy zastosować osprzęt z uchwytem typu Mosaic).
16. Należy stosować kable w powłokach trudnopalnych.
17. Przyrowadzeniu tras kablowych zachować bezpieczne odległości od innych instalacji.
18. Odległości między instalacjami należy zachować zgodnie z wymogami normy EN 50174-2.
19. Zdejmowanie płaszczki/izolacji kabla i rozplatanie par przewodów wykonać zgodnie z normą EN 50174 oraz wymogami producenta.
20. Oznakowanie komponentów wykonać zgodnie z normą EN 50174.
21. Kable ułożyć, uporządkować oraz wykonać połączenia uziemiające zgodnie z normą EN 50174 i z wymogami producenta.
22. Wszystkie kable powinny być oznaczone numerycznie, w sposób trwały, tak od strony gniazda, jak i od strony szafy teletechnicznej.
23. Te same oznaczenia należy umieścić w sposób trwały na gniazdach sygnałowych PEL w punktach przyłączeniowych użytkowników oraz na panelach krosowych.
24. Gniazda PEL w części elektrycznej muszą być zbudowane za pomocą gniazd 230V NFC61 (2P+T) z kluczem DATA.
25. Moduły Keystone mogą być montowane w gniazdach natynkowych lub w kanałach kablowych w ramach wielokrotnych tylko poprzez odpowiednie adaptory zgodne ze standardem Mosaic 45.

3.5. WYMAGANIA DLA POŚREDNICH PUNKTÓW DYSTRYBUCYJNYCH (PPD)

1. Punkty dystrybucyjne stanowią zamknięte szafy 19" wyposażone w sieciowy osprzęt pasywny (panele krosowe) i aktywny, elementy ułatwiające prowadzenie kabli krosowych (wieszaki, tablice, szczotki) oraz listwy zasilające przeznaczone do zasilania sieciowych urządzeń aktywnych. Punkty PPD zasilic z instalacji zasilania gwarantowanego (UPS).
2. W PPD przewidziano zastosowanie przełączników sieciowych.
3. Pomieszczenia PPD powinny być projektowane jako wydzielone pomieszczenia teletechniczne. Wyposażone one powinny być w system kontroli dostępu, system monitorowania warunków środowiskowych, system SSWiN oraz system wentylacji grawitacyjnej i system klimatyzacji.
4. Każde pomieszczenie PPD powinno zostać połączone traktem światłowodowym z pomieszczeniem GPD (Serwerownia), co najmniej dwoma trasami światłowodów w technologii SM oraz dwoma trasami światłowodów w technologii MM, o ilości włókien co najmniej 24 każdy. Z obu stron (PPD i GPD) trasy te powinny zostać zakończone poprzez kasety światłowodowe na panelach krosowych światłowodowych ze złączami LC/PC.
5. Każda szafa powinna być zasilona z wydzielonego obwodu elektrycznego. Na tylnej ścianie szafy należy zainstalować puszkę instalacyjną o stopniu ochrony np. IP55 w celu podłączenia głównego kabla zasilającego. Bezwzględnie należy połączyć lokalną szynę uziemiającą z szyną uziemiającą szafy żółtozielonym przewodem co najmniej LgY 16.

6. W każdym PPD, które obsługiwać będzie nową sieć elektryczno-logiczna zainstalować zostanie zasilacz UPS o mocy wyliczonej z bilansu mocy oraz zestaw rozdzielnic dystrybucyjnych zasilania gwarantowanego. Ostateczny dobór zasilaczy na etapie musi nastąpić na etapie Projektu Wykonawczego.
7. Zasilanie gwarantowane AC 230V dla sieci komputerowej oraz szaf teletechnicznych w PPD zaleca się wykonywać w konfiguracji kondygnacyjnych Rozdzielni Dystrybucyjnej (RD) zlokalizowanych w pobliżu pośrednich punktów dystrybucyjnych (PPD). Szafy rozdzielcze zasilania (RD) powinny być zamykane na zamek patentowy. Zasilanie w/w rozdzielnic powinno zostać zrealizowane z Rozdzielnicy Głównej Komputerowej (RGK).
8. Nie dopuszcza się łączenia okablowania instalacji elektrycznej w korytach.
9. W szafach 19" Wykonawca zainstaluje pola krosowe umożliwiające zmianę przeznaczenia gniazda znajdującego się w punkcie końcowym.
10. W każdym budynku (piętrze) objętym opracowaniem należy doprowadzić wszystkie kable do właściwych PPD.
11. Kable sieciowe zostaną wprowadzone do szafy z wykorzystaniem przepustów kablowych.
12. Preferowane jest wprowadzenie wiązki kabli przez wpust dolny, jeżeli zaistnieje taka potrzeba dopuszczalne jest wprowadzenie kabli przez przepust górny.
13. W szafie należy pozostawić zapas technologiczny kabla ok. 2m, pozwalający na swobodne wykonanie prac instalacyjnych oraz ew. przesunięcie szafy.
14. Wszelkie elementy okablowania pasywnego oraz urządzenia aktywne instalowane w szafie powinny zostać połączone z szyną uziemiającą szafy 19" za pomocą linek uziemiających.
15. Szafa 19" wraz z jej elementami Wykonawca połączy z uziomem otokowym budynku.
16. Parametry szaf:
 - 1) Stojące o głębokości min. 600mm lub wiszące dwusekcyjne o głębokości min. 600mm (dobór szaf do urządzeń i lokalizacji),
 - 2) Szafy muszą być dostarczone w stanie złożonym, gotowym do montażu paneli oraz osprzętu.
 - 3) Drzwi przednie szklane, zamykane na zamek. W przypadku zlokalizowania szafy w miejscach ogólnodostępnych: drzwi metalowe, zamykane na zamek.
 - 4) Możliwość otwierania na lewą/prawą stronę (możliwość przełożenia drzwi).
 - 5) Drzwi tylne pełne (w zależności od potrzeby osłony tylne perforowane).
 - 6) Regulowane stopki (w przypadku szaf stojących).
 - 7) Pełne uziemienie wszystkich sekcji szafy.
 - 8) Panel wentylacyjny sufitowy z termostatem (minimum 4 wentylatory).
 - 9) Przepusty kablowe od góry i od dołu ze szczotkowym przepustem kablowym,
 - 10) Rama rack z przodu i z tyłu.
 - 11) Organizery pionowe i poziome pomiędzy panelami krosowymi dla LAN dostępowego (co dwa panele krosowe).
 - 12) Listwy zasilająca jednofazowe, co najmniej 9 gniazd 230V (standard PL) bez bezpiecznika, podłączone do zamontowanego w szafie UPS.
 - 13) Osłony boczne demontowalne, zamykane na zamek.

3.5.1. DRZWI DLA POMIESZCZEŃ PPD

1. Drzwi metalowe o odporności ogniowej wg wymagań zasadniczych a jeśli tam nie jest to określone to o odporności min EI30, antywłamaniowe
2. Wymiarach w świetle min. 100x215, dostosowane do gabarytów instalowanych urządzeń
3. Przystosowane i wyposażone w lokalnie zarządzany system KD
4. Przystosowane i wyposażone w montaż kontaktronu dla systemu SSWiN
5. Wyposażone w dwa zamki klasy C
6. Wyposażone w samozamykacz

3.5.2. KLIMATYZATOR TYPU SPLIT DLA POMIESZCZEŃ PPD

1. Sprężarka podwójna rotacyjna DC
2. Klasa efektywności energetycznej w trybie chłodzenia: co najmniej A
3. Wymagane jest przedstawienie potwierdzenia wystawionego przez producenta lub generalnego dystrybutora, że producent dopuszcza pracę urządzeń w temperaturach zewnętrznych do -25°C

4. Sterownik przewodowy z menu w języku polskim
5. Możliwość wyprowadzenia sygnałów praca/awaria z jednostek wewnętrznych bez dodawania dodatkowego modułu elektronicznego
6. Możliwość podłączenia pod sterowanie centralne
7. Maksymalna długość instalacji chłodniczej (min.): 15 m
8. Maksymalna różnica wysokości instalacji chłodniczej (min.) : 10 m
9. Czynnik chłodniczy R410A,
10. Temperatura pracy (otoczenia) dla trybu chłodzenia : - 15°C ÷ +46°C
11. Temperatura pracy (otoczenia) dla trybu grzania : - 15°C ÷ +15°C
12. Zasilanie: 230V/1-fazowe/50Hz.
13. Zastosowany element rozprężny: elektroniczny zawór rozprężny w jednostce zewnętrznej
14. Tryb pracy: auto, chłodzenie, grzanie, wentylacja, odwilżanie
15. Sterowanie kierunkiem wypływu powietrza z pilota
16. Regulacja siły nawiewu z pilota
17. Tygodniowy programator czasowy: włącz i wyłącz
18. Klimatyzator wyposażony musi być w moduł pracy całorocznej i moduł restartu

3.5.3. SIEĆ ZASILANIA GWARANTOWANEGO I ZASILACZE NAPIĘCIA GWARANTOWANEGO UPS

1. W każdym budynku w którym planowana jest nowa sieć elektryczno-logiczna zainstalowany zostanie zasilacz UPS o mocy wyliczonej z bilansu mocy, oraz zestaw rozdzielnic dystrybucyjnych zasilania gwarantowanego.
2. W zakresie urządzeń zasilania awaryjnego UPS Zamawiający bazuje na rozwiązaniach firm Ablerelex Electronics Italy SRL oraz CAMCO Systemy Zasilania Awaryjnego. Dla zachowania identycznego stanu infrastruktury wymagane jest zastosowanie urządzeń podanych producentów tego typu rozwiązań lub uzgodnionych z Działem Informatyki zasilaczy zamiennych o podanych poniżej parametrach minimalnych.
3. Zasilacze awaryjne UPS należy dobrać w stosunku do ilości i mocy urządzeń (przy czym standardowe obciążenie UPS nie może przekraczać 75%). Do UPS dobrać moduł ByPass pozwalający na jego serwisowanie bez konieczności wyłączenia urządzeń sieciowych.
4. Jeżeli moc UPS w wymaganiach podstawowych nie przekracza 10kVA dopuszcza się instalację UPS typu rack.
5. Instalowane urządzenia UPS w zakresie zarządzania i sygnalizacji stanów pracy (monitoring) podłączyć do zaprojektowanej lub obecnie użytkowanej struktury sieci LAN.
6. Przełączenie zasilania należy wykonać w uzgodnieniu z Zamawiającym i po uzyskaniu zgody na tymczasowe wyłączenie zasilania w serwerowni lub/i sieci LAN.

3.5.3.1. UPS TYPU RACK

1. Jeżeli moc UPS-a w wymaganiach podstawowych nie przekracza 10kVA dopuszcza się instalację UPS-a typu rack
2. Montaż 4 punktowy na dwóch ramach rack
3. Typ pracy: line interactive
4. Czas utrzymania z baterii: min. 8 minut
5. Napięcie wyjściowe: 230V
6. Znamionowe napięcie wyjściowe: 230V lub 240V
7. Częstotliwość na wyjściu (synchronicznie z siecią): 47÷53 Hz przy częstotliwości nominalnej 50 Hz
8. Gniazda wyjściowe:
 - a) (8) IEC 320 C13
 - b) IEC 320 C19
 - c) IEC Jumpers
9. Zakres napięcia wejściowego w trybie podstawowym: 160 - 286V
10. Zmienny zakres napięcia wejściowego w trybie podstawowym: 151 - 302V
11. Czas pełnego ładowania akumulatora: 3 godziny
12. Komunikacja i zarządzanie:
 - a) Port komunikacyjny USB lub RS-232
 - b) Port komunikacyjny LAN (RJ45)
13. Parametry środowiskowe
 - a) Środowisko operacyjne: 0÷40°C

3.5.3.2. UPS TYPU WOLNOSTOJĄCY

Kategoria	Wymagania
1. Architektura	<ol style="list-style-type: none"> 1) Budowa modułowa umożliwiająca szybką i sprawną naprawę przez wymianę modułu 2) Topologia pracy – podwójna konwersja, VFI 3) Konfiguracja faz napięć wej/wyj - 3/3 4) Tolerancja napięcia wejściowego (praca normalna) - +/- 15% 5) Wejściowy współczynnik mocy dla 50% obciążenia - >=0,95 6) Wejściowy współczynnik mocy dla 100% obciążenia - >=0,98 7) Sprawność AC-AC dla obciążenia w zakresie 50-100% - (>=95%) 8) Zniekształcenia prądu wejściowego - <5% 9) Kształt prądu wejściowego - sinusoidalny 10) Możliwość współpracy z generatorem prądotwórczym – In <Ir 11) Znamionowa moc wyjściowa (VA / W) – wg wymagań podstawowych 12) Znamionowe napięcie wyjściowe - 3*400VAC 13) Znamionowa częstotliwość wyjściowa - 50Hz 14) Kształt napięcia wyjściowego - sinusoidalny 15) Odkształcenie napięcia wyjściowego dla obciążenia liniowego, symetrycznego - <=2% 16) Możliwość przeciążenia w czasie 60 sekund - >=150% 17) Dopuszczalny współczynnik szczytu obciążenia - >=3:1 18) Wbudowany automatyczny układ obejściowy
2. Baterie	<ol style="list-style-type: none"> 1) Czas podtrzymania: min. 12 min. 2) Akumulatory umieszczone na stelażu lub w szafie 3) Projektowana żywotność akumulatorów wg Eurobat >=10 lat 4) Musi być zapewniona: <ol style="list-style-type: none"> a) funkcja nieciągłego ładowania akumulatorów b) temperaturowa kompensacja napięcia ładowania akumulatorów c) automatyczny test baterii
3. Obsługiwane protokoły	<ol style="list-style-type: none"> 1) HTTP, HTTPS, IPv4, NTP, SMTP, SNMP v1, SNMP v2c, SNMP v3
4. Zarządzanie	<ol style="list-style-type: none"> 1) Oprogramowanie zarządzające z możliwością zamykania systemów operacyjnych poprzez sieć logiczną: Windows Server 2012, Microsoft Hyper-V 2012, Windows Server 2008, Microsoft Hyper-V 2012, Windows Server 2003, Windows 8, VMware, ESXi, VMware ESX, Red Hat Enterprise Linux, Ubuntu Linux, SuSE Linux Enterprise Server. 2) Moduł zarządzający WEB/SNMP - Możliwość diagnostyki UPSa 3) Powiadomianie o zdarzeniach przez e-mail 4) Zintegrowany z zasilaczem układ do pomiaru warunków środowiskowych w serwerowni – temperatury, z możliwością zdalnego odczytu i sygnalizacji. 5) Jeden port 10/100 TBase do nadzoru 6) Możliwość podłączenia wyłącznika awaryjnego 7) Oprogramowanie musi umożliwiać zdalny podgląd obciążenia zasilacza, czasu pracy na bateriach przy bieżącym obciążeniu, napięcia wejściowego i wyjściowego na poszczególnych fazach, częstotliwości wejściowej i wyjściowej, natężenia prądu wejściowego i wyjściowego na poszczególnych fazach, napięcia obwodu akumulatorów, temperatury wewnątrz UPS-a, bieżącego poboru mocy, stanu pracy UPS-a, komunikatów błędów i istotnych informacji o pracy UPS-a
5. Obudowa i instalacja	<ol style="list-style-type: none"> 1) Stopień ochrony IP20 2) Wyświetlacz LCD z komunikatami w języku polskim
6. Jakość wytwarzania	<ol style="list-style-type: none"> 1) Musi posiadać zgodność z normami CE - należ dostarczyć certyfikat
7. Wymagania dodatkowe	<ol style="list-style-type: none"> 1) Zaoferowany UPS musi być fabrycznie nowy i musi pochodzić z oficjalnego kanału sprzedaży na rynek polski. 2) Ponadto należy wykonać:

Kategoria	Wymagania
	a) końcowe obwody zasilające szafy teletechniczne b) wykonanie zewnętrznego bypassu serwisowego, który umożliwi bezprzerwowe przełączenie zasilania z pominięciem dostarczonego zasilacza na czas wykonywania czynności serwisowych. c) dostarczenie i zainstalowanie wyłącznika p.poż. dla oferowanego zasilacza awaryjnego

3.5.4. SYSTEM KONTROLI DOSTĘPU (KD)

1. System Kontroli Dostępu musi być oparty o czytniki kart zbliżeniowych.
2. System kontroli dostępu swoim zakresem obejmuje przejście kontrolowane jednostronnie do pomieszczeń teletechnicznych PPD.
3. Przejścia jednostronne należy wyposażyć w kontroler z czytnikiem kart magnetycznych oraz elektrozaczep z wbudowanym czujnikiem otwarcia.
4. System o pojemności min 32 przejść
5. Liczba dostarczonych kart kodowych – minimum 30 sztuk
6. System kontroli dostępu należy zaprojektować w oparciu o kontroler przystosowany do współpracy z czytnikami kart magnetycznych i zbliżeniowych pracującymi w standardach Wiegand
7. Zasięg czytnika minimum 5 cm
8. Pamięć zapisująca minimum 100.000 zdarzeń z każdego modułu kontroli dostępu
9. Liczba użytkowników minimum 500
10. Możliwość zarządzania przez sieć LAN
11. Kontrolery muszą być wyposażone w moduł umożliwiający komunikację poprzez sieć Ethernet.
12. Całość systemu będzie zarządzana i nadzorowana za pomocą specjalnego oprogramowania zainstalowanego na komputerze.
13. Zarządzanie systemem kontroli dostępu realizowane będzie za pośrednictwem centrali, która w oparciu o wbudowany interfejs Ethernet umożliwia zarządzanie systemem bezpośrednio przez sieć LAN/WAN
14. Nadzór nad pracą systemu kontroli dostępu umożliwi będzie na wskazanym przez Zamawiającego stanowisku komputerowym, gdzie Wykonawca dokona instalacji i konfiguracji systemu oraz przeszkoli personel Zamawiającego w jego użytkowaniu
15. System powinien umożliwiać zarządzanie nim z jednej konsoli i powinien być zintegrowany z użytkowanym w szpitalu systemem tego samego rodzaju.
16. System kontroli dostępu swoim zakresem obejmuje przejście kontrolowane jednostronnie lub dwustronnie do kontrolowanego pomieszczenia. Przejście jednostronne zostanie wyposażone w kontroler z czytnikiem kart magnetycznych oraz elektrozaczep z wbudowanym czujnikiem otwarcia.
17. System kontroli dostępu projektować w oparciu o kontroler przystosowany do współpracy z czytnikami kart magnetycznych lub zbliżeniowych pracującymi w standardach Wiegand. Kontrolery muszą być wyposażone w moduł umożliwiający komunikację poprzez sieć Ethernet. Całość systemu powinna być zarządzana i nadzorowana za pomocą specjalnego oprogramowania zainstalowanego na wskazanym komputerze. Rozmieszczenie punktów kontroli przejścia należy oznaczyć na rysunkach projektowych.
18. Projektując należy dokonać oceny typu przejść, tzn.: przejście jednostronnie kontrolowane (wejście: czytnik z klawiaturą; wyjście: klamka) lub przejście dwustronnie kontrolowane (wejście/wyjście: czytnik z klawiaturą)
19. W skład systemu muszą wchodzić co najmniej:
 - a) Kontroler dostępu oraz automatyki budynkowej. Zamawiający dysponuje już w swoich placówkach systemami KD i żąda możliwości integracji nowobudowanych systemów z obecnie użytkowanym. Projektując system KD należy dążyć do jego zgodności z systemem RACS 5 (firmy ROGER). W zależności od wersji, należy doprojektować kontroler umożliwiający obsługę określonej ilości przejść kontrolowanych jednostronnie/dwustronnie oraz co odpowiedniej ilości węzłów automatyki. Kontroler musi zapewnić rejestrację zdarzeń dla celów RCP oraz integrację z systemem alarmowym. Integracji z systemem alarmowym umożliwiać ma prezentację stanu strefy alarmowej oraz sterowanie jej stanem bezpośrednio z poziomu terminali dostępu. Kontroler udostępniać musi zaawansowany i wydajny sposób zarządzania użytkownikami systemu oraz kształtowania ich uprawnień. Proces konfiguracji kontrolerów systemu musi być realizowany współbieżnie, a ilość kontrolerów w systemie nie może wpływać na czas jego konfiguracji. Kontroler zarządzany musi być z poziomu aplikacji (w przypadku urządzenia firmy ROGER – oprogramowania VISO), która umożliwia współpracę z serwerową relacyjną

bazą danych np. typu Microsoft SQL Server lub darmową bazą plikową np. Microsoft SQL Server Compact. Zarządzanie systemem musi być realizowane z poziomu wielu stacji roboczych posiadających dostęp do oprogramowania zarządzającego i przez operatorów o różnym poziomie uprawnień. System udostępniać musi serwer integracji programowej umożliwiający swobodny dostęp do logu zdarzeń systemu jak i zarządzanie jego użytkownikami. Komunikacja z komputerem zarządzającym musi być realizowana za pośrednictwem sieci LAN/WAN z protokołem szyfrowanym metodą AES128 CBC.

- b) Czytniki zbliżeniowe są wewnętrznymi terminalami dostępu przeznaczonymi do pracy w systemie kontroli dostępu (preferowany system to system zgodny z posiadanym przez zamawiającego systemem ROGER RACS 5). Czytniki pełnią funkcję urządzenia podrzędnego względem kontrolera dostępu i nie mogą samodzielnie dozorować przejścia. Terminale umożliwiają zarówno odczyt numeru seryjnego karty zbliżeniowej (CSN) jaki i numeru programowalnego (PCN) zapisanego w szyfrowanych sektorach pamięci na karcie. Wykorzystanie programowalnego numeru karty zabezpiecza ją przed duplikowaniem (co zdecydowanie podnosi poziom bezpieczeństwa całego systemu kontroli dostępu). Czytniki z opcją IO wyposażone muszą być w zestaw linii wejściowych i wyjściowych, który mają umożliwiać kompletną obsługę przejścia bez konieczności wykorzystywania wejść i wyjść zlokalizowanych na kontrolerze dostępu lub module rozszerzeń. Czytniki muszą udostępniać co najmniej trzy parametryczne linie wejściowe, które mogą być indywidualnie sparametryzowane w zakresie czasu reakcji oraz topologii dołączonych styków i rezystorów. Opcjonalnie, wejścia mogą być skonfigurowane do trybu double wiring, który umożliwia dołączenie dwóch niezależnych styków NO lub NC do każdego z wejść i podwojenie w ten sposób liczby monitorowanych przez czytnik sygnałów wejściowych. Czytniki posiadać muszą dwa wyjścia tranzystorowe oraz jedno wyjście przekaźnikowe. Każde z wyjść może być w stanie spoczynkowym wyłączone (tzw. Polaryzacja normalna) lub załączone (tzw. Polaryzacja odwrotna). Komunikacja z kontrolerem odbywa się musi za pośrednictwem zmodyfikowanego standardu RS485, który dopuszcza tworzenie struktur okablowania typu gwiazda oraz drzewo. Magistrala komunikacyjna, do której dołączany jest czytnik może mieć długość do 1200 m i być wykonana przy pomocy dowolnego rodzaju kabla sygnałowego. Konfigurowanie urządzenia oraz aktualizację oprogramowania wbudowanego (firmware) przeprowadza się za pośrednictwem interfejsu RS485 i odpowiedniego oprogramowania (preferowane oprogramowanie to RogerVDM for Windows). Płyta czołowa czytnika wykonana musi być ze specjalnego tworzywa sztucznego o zbliżonej do szkła odporności na zarysowania i musi być odporne na stłuczenie. Obudowa czytnika posiadać musi neutralny wzorniczo wygląd, zbliżony do rozpowszechnionej stylistyki osprzętu elektrycznego. Czytniki powinny spełniać następujące minimalne wymagania techniczne:
- identyfikacja karta i/lub PIN;
 - obsługa kart 13,56 MHz MIFARE Ultralight, Classic;
 - odczyt CSN, MSN, SSN;
 - rozpoznanie długiego przyłożenia karty;
 - obsługa dodatkowego czytnika serii PRT;
 - interfejs komunikacyjny RS485;
 - obsługa wejść parametrycznych;
 - możliwość pracy wejść w trybie Double Wiring;
 - wyjścia tranzystorowe;
 - wyjścia przekaźnikowe;
 - klawisze funkcyjne;
 - ochrona antysabotażowa (tamper);
 - praca w warunkach zewnętrznych;
 - zasilanie 12 VDC;
 - zgodność z normą CE.
20. System kontroli dostępu swoim zakresem obejmuje przejście kontrolowane jednostronnie lub dwustronnie do wyznaczonych pomieszczeń (w tym pomieszczeń PPD). Przejście powinno zostać wyposażone w zintegrowany kontroler z czytnikiem kart magnetycznych (preferowany model to Mifire PRT66MF), który ma zapewnić autonomiczną i niezawodną pracę systemu. Każde drzwi trzeba wyposażyć z elektrozaczep (np. YS18NO12D) oraz zasilic zasilaczem impulsowym 12V (np. PSA 12015).
21. Czytniki zbliżeniowe (np. Mifare PRT66MF) mogą być wykorzystywane jako terminale podłączone do nadrzędnego kontrolera lub być skonfigurowane do pracy autonomicznej jako proste kontrolery dostępu. W pierwszym przypadku funkcjonalność czytnika ogranicza się jedynie do odczytu identyfikatora (karta/PIN) i przesłanie do kontrolera, który podejmuje dalsze działania. W przypadku pracy autonomicznej czytniki mogą samodzielnie dozorować pojedyncze przejście w oparciu o dane wpisane w

procesie ich konfiguracji. System będzie współdziałał z istniejącym systemem kontroli dostępu na zasadzie ujednolicenia standardu kart dostępu Mifare 1-k zgodnie z informacją przekazaną od Zamawiającego.

22. Preferowany model i parametry czytników:
 - czytnik/programator kart standardu ISO/IEC 14443A/Mifare - model PRT66MF;
 - praca w trybie terminalowym lub autonomicznym;
 - napięcie zasilania: 12V DC;
 - pobór prądu (średni): 65mA;
 - zasięg odczytu: do 6cm;
 - co najmniej 120 zaindeksowanych użytkowników;
 - identyfikacja: karta i/lub PIN;
 - historia 1024 zdarzeń;
 - dwa wejścia NO/NC;
 - dwa wyjścia tranzystorowe;
 - możliwość dołączenia ekspandera we/wy typu XM-2;
 - możliwość dołączenia dodatkowego czytnika serii PRT (obustronna kontrola przejścia);
 - programowanie manualne lub z komputera;
 - kontakt antysabotażowy: kontakt NC, 50mA/24V, IP67;
23. Preferowany model i parametry elektrozaczepek:
 - model YS18NO12D YOTOGLI;
 - symetryczny;
 - radialny: specjalna konstrukcja radialna, promieniowa mechanizmu języka elektrozaczepek powoduje otwarcie przy minimalnym wychyleniu. Umożliwia to montaż elektrozaczepek przy mniejszym podcięciu ościeżnicy;
 - szerokość 16,4mm, przeznaczony do stosowania w wąskich profilach;
 - wysokość 67mm;
 - NO - bez zasilania odblokowany (rewersyjny);
 - standardowy rozstaw śrub do montażu blach 52mm;
 - współpracuje ze standardowymi typami blach;
 - regulacja języka: +/- 1mm;
 - do drzwi prawych i lewych.

3.6. WYMAGANIA DLA KANALIZACJI TELETECHNICZNEJ

W zakresie rozbudowy sieci szkieletowej oraz dystrybucyjnej należy:

1. Ułożyć kanalizację teletechniczną pomiędzy budowanym obiektem i budynkiem, gdzie zlokalizowany jest Główny Punkt Dystrybucyjny (GPD) [serwerownia] lub wskazanym przez Dział Informatyki innym punktem dystrybucji sygnałów. Przy wykonywaniu kanalizacji teletechnicznej rozbudowę wykonać jako dwuotworową ze studniami typu SKR i SKO-2. Podejścia do budynków uszczelnić gazowo. Rury DVK łączyć ze sobą złączkami typ M lub MT.
2. Wykonać połączenia sieci szkieletowej pomiędzy budowanym obiektem i budynkiem, gdzie zlokalizowany jest Główny Punkt Dystrybucyjny (GPD) [serwerownia] lub wskazanym przez Dział Informatyki innym punktem dystrybucji sygnałów, a także wykonać relacje światłowodowe wewnątrz budynku pomiędzy poszczególnymi PPD. Każde połączenie między budynkowe wykonać dwoma trasami światłowodowymi SM, min. 24 włókien każdy.
3. Głębokość ułożenia kanalizacji powinna być taka, aby najmniejsze przykrycie liczone od poziomu nawierzchni do górnej powierzchni rury pierwotnej wynosiło min. 0,7m.
4. Przejście pod drogami z rur przewiertowych RHDPE 110/6,3.
5. W miejscach skrzyżowania kanalizacji teletechnicznej z innymi sieciami zabezpieczone poprzez założenie w miejscu skrzyżowania rury dwudzielnej (np. typu Arot A PS 110 lub A PS 160) .
6. Studzienki należy posadzić na zagęszczonej podsypce piaskowej.
7. Studnie izolowane abizolem.
8. Studnie obsypać gruntem rodzimym, zwracając uwagę na poziom pokrywy studni w stosunku do terenu.
9. Wejścia rur do studni należy uszczelnić.

10. Przy robotach ziemnych należy uwzględnić istniejące uzbrojenie terenu i zachować normatywne odległości.
11. Prace ziemne prowadzić ręcznie.
12. Dopuszcza się wykorzystanie w tym celu istniejącej kanalizacji teletechnicznej pod warunkiem, że jej stan techniczny będzie na to pozwalał i spełniał wymagania dla nowo projektowanych tras kanalizacji.
13. Wejścia kanalizacji do budynków uszczelnić gazowo.

3.7. WYMAGANIA DOTYCZĄCE KOMPLETNOŚCI WYKONANIA

1. Wykonawca musi posiadać odpowiedni status np. Licencjonowanego Przedsiębiorstwa do Projektowania i Instalacji, nadany bezpośrednio przez Producenta okablowania, potwierdzony umową, regulującą warunki udzielania gwarancji systemowej przez producenta.
2. Wykonawca ma dysponować osobami posiadającymi imienne dyplomy potwierdzające ukończenie kursów kwalifikacyjnych w zakresie: instalacji, pomiarów, nadzoru, wykrywania oraz eliminacji uszkodzeń, projektowania okablowania strukturalnego, zgodnie z normami międzynarodowymi oraz procedurami instalacyjnymi producenta okablowania.
3. Oferowany system okablowania strukturalnego musi być objęty programem min. 25 letniej gwarancji systemowej.
4. Wszystkie elementy systemu okablowania miedzianego i światłowodowego powinny być opracowane (tj. zaprojektowane, wykonane i wdrożone do oferty rynkowej), jako kompletne rozwiązania, celem uzyskania maksymalnych zapasów transmisyjnych oraz zapewnić uzyskanie certyfikatu producenta okablowania.
5. Wymaga się, aby wszystkie elementy okablowania (w szczególności: panele krosowe, gniazda, kabel, kable krosowe, płyty czołowe gniazd, prowadnice kablowe) spełniały warunek zapewnienia uzyskania certyfikatu producenta okablowania.
6. System okablowania strukturalnego musi obejmować kompletne rozwiązanie dla techniki miedzianej i światłowodowej, telekomunikacyjnej oraz szaf teleinformatycznych wraz z osprzętem. Elementy systemu okablowania powinny szczególnie być nastawione na uniwersalność, skalowalność, łatwość w montażu oraz prostotę i przejrzystość całości rozwiązań.
7. Wszystkie komponenty systemu okablowania muszą być zgodne z wymaganiami obowiązujących norm: ISO/IEC 11801 2 Ed. oraz EN 50173 2.Ed co musi być potwierdzone odpowiednimi certyfikatami. Należy zapewnić również certyfikat z niezależnego laboratorium posiadającego odpowiednią akredytację potwierdzający zgodność łącza klasy EA z normą ANSI/TIA-568-C.2 (2009-08) w zakresie testu łącza 2 konektorowego Permanent Link.

3.8. WARUNKI WYKONANIA I ODBIORU ROBÓT

Ogólne warunki wykonania i odbioru robót – prace projektowe

1. Wymaga się od Wykonawcy konsultacji roboczych z Zamawiającym oraz zorganizowania spotkań w celu uściślenia przyjętych rozwiązań projektowych, standardu wykończenia i wyposażenia.
2. Udzielania wyjaśnień, uzupełnień do Dokumentacji Projektowej w terminie maks. do 3 dni od zgłoszenia przez Zamawiającego.
3. Stawiania się na obiekt na wezwanie Zamawiającego, przy czym wezwanie lub zawiadomienie powinno być przesłane (fax./e-mail) min. na 2 dni robocze przed terminem spotkania. W przypadku nie wywiązywania się z powyższego obowiązku Zamawiający, wynikłe z tego tytułu straty pokryje z zatrzymanego zabezpieczenia należytego wykonania umowy. Zamawiający nie będzie ponosił kosztów pobytu na budowie bez wezwania bądź na wezwanie Wykonawcy robót.
4. Opracowania i pobytu na miejscu realizacji zadania wynikające z poprawienia błędów i uzupełnienia dokumentacji stanowiącej podstawę do realizacji robót Wykonawca wykonuje nieodpłatnie.

3.9. OGÓLNE WARUNKI WYKONANIA I ODBIORU ROBÓT - PRACE BUDOWLANE

1. Zamawiający będzie wymagał, aby organizacja robót, jakość użytych materiałów i jakość wykonania były zgodne z przedstawionymi we wszystkich zawartymi w tej dokumentacji wymaganiami. Zamawiający będzie kontrolował w tym zakresie działania Wykonawcy.

2. Wykonawca robót jest odpowiedzialny za jakość ich wykonania oraz za zgodność niniejszymi wytycznymi, Dokumentacją Projektową, poleceniami Zamawiającego, wskazanego Inspektora Nadzoru oraz sztuką budowlaną.
3. Wszystkie wykonane roboty i dostarczone materiały i urządzenia, w ramach niniejszego zamówienia, będą zgodne z zatwierdzoną przez Zamawiającego Dokumentacją Projektową i specyfikacjami technicznymi, a także obowiązującymi przepisami i normami.
4. Wykonawca jest odpowiedzialny za prowadzenie robót zgodnie z umową i ściśle przestrzeganie harmonogramu robót, oraz za jakość zastosowanych materiałów i wykonywanych robót, za ich zgodność z Dokumentacją Projektową, wymaganiami specyfikacji technicznych, projektu organizacji robót oraz poleceniami zarządzającego realizacją umowy.
5. Zamawiający przewiduje bieżącą kontrolę wykonywanych robót. Zamawiający będzie oceniać zgodność materiałów i robót z wymaganiami ogólnymi zawartymi w niniejszym opracowaniu, Dokumentacją Projektową oraz zawartą umową.
6. Na wykonawcy spoczywać będzie zapewnienie odpowiedniego dla charakteru wykonywanych projektów oraz prowadzonych robót, personelu technicznego (projektantów z uprawnieniami, kierownika budowy i robót w poszczególnych branżach) o czynnych uprawnieniach do pełnienia samodzielnych funkcji w budownictwie w specjalnościach wymaganych przy realizacji całego zamówienia.
7. Na wykonawcy spoczywać będzie całkowita odpowiedzialność za:
 - 1) organizację robót,
 - 2) zabezpieczenie osób trzecich,
 - 3) ochronę środowiska,
 - 4) warunki bhp,
 - 5) zabezpieczenie terenu robót,
 - 6) zabezpieczenie ciągów komunikacyjnych przyległych do terenu robót od następstw prowadzonych robót do dnia bezusterkowego odbioru końcowego przedmiotu zamówienia.
8. Wykonawca jest zobowiązany do zabezpieczenia placu robót w okresie trwania realizacji, aż do zakończenia prac i odbioru ostatecznego. Koszt zabezpieczania nie podlega dodatkowej zapłacie.
9. Wykonawca zobowiązany jest zabezpieczyć przed zanieczyszczeniami i pyłami wszelkie urządzenia i sprzęty kolidujące z wykonywanymi pracami (w tym w razie konieczności demontaż, wyniesienie, a następnie wniesienie i montaż sprzętu, urządzeń oraz mebli). Koszt tych prac ponosi Wykonawca.
10. O fakcie przypadkowego uszkodzenia instalacji Wykonawca bezzwłocznie.
11. Materiały nieodpowiadające wymaganiom jakościowym zostaną przez Wykonawcę wywiezione z terenu budowy.
12. Każdy rodzaj robót, w którym znajdują się nie zbadane i nie zaakceptowane materiały, Wykonawca wykonuje na własne ryzyko, licząc się z jego nieprzyjęciem i niezapłaceniem.
13. Wykonawca zapewni, aby tymczasowo składowane materiały, do czasu gdy będą one wykorzystane do robót, były zabezpieczone przed zanieczyszczeniami, zachowały swoją jakość i właściwość do robót i były dostępne do kontroli.
14. Zamawiający ustala następujące rodzaje odbiorów:
 - 1) Odbiór robót zanikowych i ulegających zakryciu,
 - 2) Odbiory częściowe po wykonaniu wcześniej uzgodnionego etapu prac,
 - 3) Odbiór końcowy.
15. Wywóz gruzu i ewentualnych odpadów powstałych w trakcie robót oraz utylizacji odpadów niebezpiecznych Wykonawca dokona we własnym zakresie. Wymagane jest usuwanie z ciągów komunikacyjnych zanieczyszczeń celem zachowania bezpieczeństwa. Odpady niebezpieczne należy zutylizować na własny koszt i we własnym zakresie.

3.10. MOŻLIWE DO WYSTĄPIENIA UTRUDNIENIA W WYKONYWANIU PRAC:

1. Obiekt jest czynny.
2. W obiekcie całą dobę wykonuje swoje prace personel medyczny.
3. W obiekcie stale przebywają pacjenci.
4. Czasowe ograniczenia w dostępie do pomieszczeń.
5. Ograniczenia i obostrzenia dotyczące zgody na prace hałaśliwe, uciążliwe i brudne.
6. Prace na wysokości.

3.11. WYMAGANIA DOTYCZĄCE MATERIAŁÓW

1. Gdziekolwiek w dokumentach przywołane zostaną konkretne normy i przepisy, które spełniać mają materiały, sprzęt i inne towary oraz wykonane i zbadane roboty, będą obowiązywać postanowienia najnowszego wydania lub poprawionego wydania przywołanych norm i przepisów o ile w warunkach umowy nie postanowi się inaczej. W przypadku, gdy przywołane normy i przepisy odnoszą się do konkretnego kraju lub regionu, mogą być również stosowane inne odpowiednie normy zapewniające równy lub wyższy poziom wykonania niż przywołane normy lub przepisy, pod warunkiem ich sprawdzenia i pisemnego zatwierdzenia przez Zamawiającego. Różnice pomiędzy przywołanymi normami, a ich proponowanymi zamiennikami muszą być dokładnie opisane przez Wykonawcę i przedłożone Zamawiającemu do zatwierdzenia.
2. Wyroby budowlane, stosowane w trakcie wykonywania robót budowlanych, mają spełniać wymagania polskich przepisów, a Wykonawca będzie posiadał dokumenty potwierdzające, że zostały one wprowadzone do obrotu, zgodnie z regulacjami ustawy o wyrobach budowlanych i posiadają wymagane parametry.
3. Specyficzne wyroby budowlane wytwarzane według zasad określonych w Dokumentacji Projektowej lub w specyfikacjach technicznych będą wymagały przeprowadzenia badań potwierdzających, że spełniają one oczekiwane parametry. Koszty przeprowadzenia tych badań obciążają Wykonawcę, a potrzeba tych badań i ich częstotliwość określą specyfikacje techniczne.

3.12. DODATKOWE WYTYCZNE INWESTORSKIE I UWARUNKOWANIA ZWIĄZANE Z BUDOWĄ I JEJ PRZEPROWADZENIEM

1. Roboty budowlane będą prowadzone w czynnym obiekcie użyteczności publicznej. Wykonawca ma obowiązek zabezpieczenia terenu budowy – frontu robót i znajdującego się na nim mienia, swoim kosztem i staraniem do czasu ostatecznego zakończenia robót i ich protokolarnego odbioru przez Zamawiającego. Roboty będą zorganizowane w sposób umożliwiający wykonywanie funkcji Zamawiającego, zapewniający bezpieczeństwo osób zatrudnionych oraz przebywających w obiekcie szpitala. Godziny robót oraz sposób korzystania z mediów (gaz, co, c.w.u., energia elektryczna, etc.) Wykonawca będzie uzgadniał z Zamawiającym przed rozpoczęciem robót.
2. Trasy prowadzenia przewodów transmisyjnych okablowania poziomego zostały skoordynowane z istniejącymi i wykonywanymi instalacjami w budynku m.in. dedykowaną oraz ogólną instalacją elektryczną, instalacją centralnego ogrzewania, wody, gazu, itp. Jeżeli w trakcie realizacji nastąpią zmiany tras prowadzenia instalacji okablowania (lub innych wymienionych wyżej) – należy ustalić właściwe rozproszczenie z Projektantem działającym w porozumieniu z Użytkownikiem końcowym.
3. Wszystkie korytka metalowe, drabinki kablowe, szafę kablową 19" wraz z osprzętem, łączówki telefoniczne wyposażone w grzebienie uziemiające oraz urządzenia aktywne sieci teleinformatycznej muszą być uziemione by zapobiec powstawaniu zakłóceń. Dedykowaną dla okablowania instalację elektryczną należy wykonać zgodnie z obowiązującymi normami i przepisami.
4. Wszystkie materiały wprowadzone do robót winny być nowe, nieużywane, najnowszych aktualnych wzorów, winny również uwzględniać wszystkie nowoczesne rozwiązania techniczne.
5. Różnice pomiędzy wymienionymi normami w projekcie a proponowanymi normami zamiennymi muszą być w pełni opisane przez Wykonawcę i przedłożone do zatwierdzenia przez Zamawiającego. W przypadku, kiedy ustalili się, że proponowane odchylenia nie zapewniają zasadniczo równorzędnego działania, Wykonawca zastosuje się do wymienionych w dokumentacji projektowej.

4. SYSTEM OZNACZEŃ (PASZPORTYZACJA)

W okablowaniu musi zostać zastosowany jednolity system opisu gniazd logicznych, paneli krosowych oraz kabli tworzących połączenie logiczne.

4.1. OZNACZENIE GNIAZD

NUMER-PPD / U_NUMER-PATCH-PANELA / NUMER-PORTU

np.

7/U2/1

gdzie:

NUMER-PPD - to numer szafy teletechnicznej, zapisany cyfrą (np. 7),

U_NUMER-PATCH-PANELA - to oznaczenie panelu krosowego w szafie (np. U2),

NUMER-PORTU – numer gniazda oznaczający konkretnego portu na panelu krosowym.

W przypadku punktów PEL dla montażu AP należy opisać je dodatkowo numerem **AP_NUMER**.

4.2. OZNACZENIE PANELU KROSOWEGO

U_NUMER-PATCH-PANELA / NUMER-PPD / NUMER-SZAFY-PPD

np.

U1/1/1

gdzie:

U_NUMER-PATCH-PANELA – to oznaczenie panelu krosowego w szafie (np. U1),

NUMER-PPD – numer punktu PPD (np.1),

NUMER-SZAFY-PPD – numer szafy teletechnicznej w danym PPD (np. 1),

Numerowanie od góry układu w szafie teletechnicznej danego PPD.

4.3. OZNACZENIE RELACJI ŚWIATŁOWODOWYCH

4.3.1. W GPD

NUMER-PPD / BUDYNEK

np. 1/6

gdzie:

NUMER-PPD – numer punktu PPD (np. 1),

BUDYNEK – numer budynku wg podziału administracyjnego szpitala (np. 6).

4.3.2. W PPD

4.3.2.1. RELACJA DO GPD

NUMER-PPD/GPD

np.

1/GPD

gdzie:

NUMER-PPD – numer punktu PPD (np. 1),

GPD – nazwa stała, określenie relacji do GPD.

4.3.2.2. W PPD RELACJA DO INNEGO PPD

NUMER-PPD-OBECNEGO / NUMER-PPD-NADRZĘDNEGO

np. 2/4

gdzie:

NUMER-PPD-OBECNEGO – numer PPD podrzędne (obecne) (np. 2),

NUMER-PPD-NADRZĘDNEGO – numer PPD nadrzędnego (np. 4).

4.4. OZNACZENIE PEL POD AP (WLAN)

W przypadku sufitów podwieszanych, tam gdzie AP będzie niewidoczny zastosować naklejkę z oznaczeniem **AP_NUMER** na stelażu sufitu, nad którym znajduje się punkt PEL dla podłączenia AP.

4.5. OZNACZENIE SZAF

Szafy teletechniczne oznaczać w widocznym miejscu, np. w prawym górnym rogu szafy na drzwiach/drzwiczkach oraz drugie oznaczenie w tym samym miejscu wewnątrz na froncie.

Oznaczać wg schematu:

PPD(GPD)-NUMER-PPD / NUMER_SZAFY-PPD

np. GPD/1

gdzie:

PPD(GPD)-NUMER-PPD – GPD (w przypadku GPD) lub PPD z podaniem numeru (np. GPD),

NUMER_SZAFY-PPD – numer szafy teletechnicznej w danym PPD (GPD).

5. SPRZĘT AKTYWNY SIECIOWY

1. W infrastrukturze Zamawiającego sieć lokalna LAN (w tym bezprzewodowa WLAN) oparta jest o urządzenia firmy Hewlett Packard Enterprise z linii produktowej Aruba.
2. Przy projektowaniu rozwiązania i w celu zachowania jednakowej struktury obsługowej oraz serwisowej należy sieć bezprzewodową WLAN oprzeć o co najmniej 1 (jeden) kontroler sieci - minimalnie w wersji modelu Aruba 7030 oraz punkty dostępowe AP tego samego producenta. W ramach wykonywanych prac należy uzgodnić z Działem Informatyki - liczbę koniecznych w dostawie sztuk, ilości i rodzaju wszystkich licencji produkcyjnych oraz ich fizyczne rozmieszczenie. Wraz z dostawą i uruchomieniem urządzenia oraz składowych całej podsieci WLAN należy przeprowadzić certyfikowane szkolenie z obsługi tego systemu dla co najmniej dwóch osób personelu informatycznego Zamawiającego na poziomie co najmniej HP Aruba Certified Mobility Associate (ACMA). W przypadku uzgodnienia z Działem Informatyki zastosowania sprzętu aktywnego innego producenta, wykonawca zobowiązany jest do dostawy i uruchomieniem urządzeń, licencji oraz składowych całej podsieci LAN/WLAN i dodatkowo przeprowadzić certyfikowane szkolenie z obsługi tego systemu dla co najmniej dwóch osób personelu informatycznego Zamawiającego na poziomie co najmniej Associate/Network Administrator.
3. Przy projektowaniu rozwiązania i w celu zachowania jednakowej struktury obsługowej oraz serwisowej należy sieć LAN oprzeć o przełączniki serii Aruba w wersji co najmniej 2930F i wyższą, w ilości zależnej od ilość portów w danym punkcie dystrybucyjnym doliczając do tego zapas w ilości co najmniej 15% wolnych portów przełącznika (np. gdy w jednym z punktów dystrybucyjnych posiadamy doprowadzonych 80 portów LAN [rozsztych na panelach krosowych], należy przeliczyć to jako $80 \cdot 15\%$ - co daje 92 porty, które należy uwzględnić w ilości dostarczonych przełączników).
4. W celu określenie ilość urządzeń AP (punktów dostępowych), Wykonawca musi wykonać symulowaną mapę pokrycia zasięgu i na tej podstawie wyliczyć ilości oraz dobrać odpowiedni rodzaj i ilość licencji dla kontrolera oraz urządzeń aktywnych sieci.
5. Przełączniki sieciowe wyposażone w porty dostępowe 1G (gigabitowe) w ilości zależnej od zapotrzebowania oraz porty 10G SFP+ do podłączenia do szkieletu sieci.
6. Przełączniki sieciowe muszą być wyposażone w moduły (wkładki) SFP/SFP+ do zestawienia połączenia między urządzeniami. Moduły przeznaczone do połączeń poprzez włókna jednomodowe odpowiednie do długości trasy. Moduły zakończone złączami duplex LC.
7. Należy uzgodnić z Działem Informatyki liczbę oraz rodzaj/model przełączników sieciowych odpowiednich do danego projektu.
8. Przełączniki muszą być zarządzalne i obsługiwać następujące technologie:
 - IPv6
 - ACL
 - IEEE 802.1D
 - IEEE 802.1Q (min 4096 vlan ID)
 - IEEE 802.1p
 - IEEE 802.1s
 - IEEE 802.1X
 - IEEE 802.3ad
 - IEEE 802.3az
 - Obsługa ramek JUMBO
 - QoS
 - OpenFlow min 1.3
9. Przełączniki sieciowe muszą spełniać poniższe wymagania:
 - 24 portowe: Throughput: min 95.2 Mpps, Switching capacity: min 128 Gbps
 - 48 portowe: Throughput: min 112.0 Mpps, Switching capacity: min 176 Gbps
10. Dla sieci CCTV wymagane są oddzielne przełączniki sieciowe, również wyposażone w porty typu uplink standardu 10G SFP+.
11. Do sieci CCTV należy stosować przełączniki z obsługą PoE.
12. Jeżeli przewidywana jest sieć bezprzewodowa lub telefonia VoIP należy zastosować przełącznik z obsługą PoE.

13. Należy stosować przełączniki do zamontowania w szafie rack, przełączniki muszą być wyposażone w akcesoria do montażu.
14. Należy unikać rozgałęzień sieci poprzez małe/biurkowe przełączniki. W przypadku konieczności rozdzielania sieci przełącznikiem biurkowym, przełącznik ten musi być zarządzalny i posiadać porty standardu 1G.
15. Przełącznik sieciowy powinien być kompatybilny z oprogramowaniem do zarządzania urządzeniami sieciowymi istniejącym u Zamawiającego, tj. HP IMC lub Aruba AirWave. W zakresie tym, należy uzgodnić szczegóły z Działem Informatyki. Wykonawca musi wraz z przełącznikami dostarczyć wszelkie wymagane licencje konieczne dla włączenia ich w oprogramowanie do monitorowania i zarządzania.
16. W celu zachowania najwyższych standardów cyberbezpieczeństwa i poufności danych medycznych, urządzenia i podsystemy (zwłaszcza medyczne) muszą być podłączane przewodowo (do wewnętrznej przewodowej sieci LAN) lub bezprzewodowo WLAN, z wykorzystaniem protokołów bezpieczeństwa w standardzie co najmniej WPA2-Enterprise (zabronione jest używanie protokołów zabezpieczeń starszych, w tym np. standardu WPA2, WPA2-Personal). W zastosowaniach, gdzie istnieje możliwość techniczna, preferowane jest wykorzystywanie standardu WPA3.

6. POMIARY

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

a. Kable miedziane - pomiary muszą być przeprowadzone miernikiem o dokładności pomiarów co najmniej Level IV (wg IEC 61935-1/Ed. 3) z odpowiednimi adapterami umożliwiającymi pomiar łącza stałego Permanent Link. Wykonawstwo pomiarów powinno być zgodne z normą PN-EN 50346:2004/A1+A2:2009. Wymagane parametry: Mapa połączeń (Wire Map), Długość (Length), Tłumienie (Attenuation), Opóźnienie propagacji (Propagation delay), Delay Skew, NEXT, PSNEXT, FEXT, PSFEXT, ACR, PSACR, ELFEXT, PSELFEXT, Insertion Loss, Return Loss.

b. Kable światłowodowe – pomiary powinny być wykonane zgodnie z normą PN-EN 14763-3:2009/A1:2010 oraz obejmować co najmniej pomiary metodą:

- reflektometryczną takich parametrów jak: pomiar tłumienia jednostkowego światłowodu [dB/km], pomiar tłumienia całkowitego łącza światłowodowego [dB], pomiar długości optycznej światłowodu [km], pomiar strat na połączeniach spawanych, złączach rozłącznych [dB], pomiar reflektancji złączy [dB],

- transmisyjną - pomiar mocy optycznej [dB].

Pomiary powinny być przeprowadzone wyłącznie przyrządami posiadającymi aktualne świadectwo kalibracji, które należy dołączyć do dokumentacji powykonawczej.

Wykonawca zobowiązany jest dostarczyć w wersji elektronicznej (na nośniku CD, DVD lub flash-usb) wyniki pomiarów reflektometrycznych składające się z:

1. tabel zawierających wszystkie niezbędne parametry określające jakość światłowodu, spawów i złączy rozłącznych,
2. reflektogramów (format *.pdf),
3. reflektogramów wygenerowanych przez urządzenie pomiarowe.

7. DOKUMENTACJA POWYKONAWCZA

Dokumentacja powykonawcza musi zawierać w szczególności:

1. raporty z pomiarów dynamicznych okablowania;
2. rzeczywiste trasy prowadzenia kabli transmisyjnych na rzutach budynków w skali nie mniejszej niż 1:100;
3. oznaczenia poszczególnych szaf, gniazd, kabli i portów w panelach krosowych;
4. lokalizację przebiegów przez ściany i podłogi;
5. karty katalogowe, instrukcje montażu i eksploatacji oraz certyfikaty wystawione przez akredytowane niezależne laboratoria testowe i inne dokumenty pozwalające ocenić zgodność proponowanego rozwiązania z wymaganiami niniejszego dokumentu;
6. certyfikat gwarancyjny producenta okablowania.

Raporty pomiarowe wszystkich torów transmisyjnych należy zawrzeć w dokumentacji powykonawczej i przekazać przy odbiorze.

8. WYMAGANIA NA ETAPIE PLANOWANIA, PROJEKTOWANIA I REALIZACJI INNYCH PRAC BUDOWLANYCH ORAZ REMONTOWYCH W ZAKRESIE UTRZYMANIA TRWAŁOŚCI PROJEKTOWEJ DLA SIECI TELETECHNICZNEJ ORAZ WYDZIELONEJ SIECI ZASILANIA GWARANTOWANEGO ZREALIZOWANEJ W RAMACH WSPARCIA FINANSOWEGO REGIONALNEGO PROGRAMU OPERACYJNEGO WOJEWÓDZTWA POMORSKIEGO DLA PROJEKTU "POMORSKIE E-ZDROWIE"

W zakresie prowadzonych prac przez Wykonawcę, pojawiać się może konieczność realizacji zadań związanych z wymogiem demontażu oraz ponownego odtworzenia (montażu) lub przebudowy infrastruktury teletechnicznej sieci lokalnej LAN, w skład której wchodzi m.in. elementy sieci pasywnej oraz gwarantowanego zasilania sieciowego.

Zważywszy, że Przedmiot Zamówienia obejmuje wykonanie prac mających lub mogących mieć wpływ na prace zrealizowane na rzecz Zamawiającego na podstawie umowy nr 97/18 z dnia 6 kwietnia 2018 roku (zwane dalej: „Pracami” lub „Siecią e-Zdrowie”), zawartej pomiędzy Zamawiającym i firmą ATEM-Polska Spółka z ograniczoną odpowiedzialnością z siedzibą w Gdyni [KRS 0000019400] [ATEM-Polska Sp. z o.o., ul. Łużycka 2, 81-537 Gdynia, tel. (+48 58) 662 29 12] (zwaną dalej: „Wykonawcą e-Zdrowie”), na skutek przeprowadzonego postępowania nr DAZ-ZP.272.33.2017 w ramach Projektu “Pomorskie e-Zdrowie”, o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego na podstawie ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (t.j. Dz.U. z 2015r. poz.2164 z późn. zm.) o wartości szacunkowej przekraczającej wyrażoną w złotych równowartość kwoty 5.186.000 euro na **“Budowę i dostosowanie infrastruktury pasywnej (w tym serwerownię), dostosowanie i rozbudowa sieci teleinformatycznych i sieci zasilania gwarantowanego wraz z dostawą budynkowych (centralnych) zasilaczy UPS”**, (dalej: „Projekt”), Wykonawca jest zobowiązany do dokonania wyboru jednego z trzech poniższych wariantów dotyczących odtworzenia Projektu (w przypadku jego uszkodzenia lub demontażu wskutek realizacji Zamówienia przez Wykonawcę), a także, przejęcia lub utrzymania gwarancji jakości udzielonej przez Wykonawcę e-Zdrowie na Prace zrealizowane w ramach Projektu oraz przejęcia lub utrzymania zobowiązań Wykonawcy e-Zdrowie wynikających z rękojmi za wady i odpowiedzialności za szkodę w zakresie Prac wykonanych w ramach Projektu.

O wyborze wariantu Wykonawca jest zobowiązany pisemnie zawiadomić Zamawiającego oraz Wykonawcę e-Zdrowie w terminie **7 dni od zawarcia Umowy z Zamawiającym** na wykonanie Przedmiotu Zamówienia. W przypadku niedokonania wyboru przez Wykonawcę, lub braku dojścia do porozumienia Wykonawcy i Wykonawcę e-Zdrowie w zakresie **Wariantu II** lub **III**, przyjmuje się, że Wykonawca dokonał wyboru **Wariantu I**.

Wybór jednego z poniższych Wariantów jest uprawnieniem Wykonawcy, jednakże, realizacja jednego z nich jest obowiązkiem Wykonawcy, który stanowi część niniejszego Zamówienia i winien zostać uwzględniony w cenie ofertowej Wykonawcy.

Zamawiający zrealizował budowę tej infrastruktury w ramach projektu dofinansowanego ze środków funduszy Unii Europejskiej (Regionalnego Programu Operacyjnego Województwa Pomorskiego) i zgodnie z założeniami oraz wytycznymi dla tego typu projektów jest zobowiązany do utrzymania trwałości wyników tego zadania przez określony w programie okres czasu (co najmniej 5 lat).

Ponadto wykonana w ramach tego projektu infrastruktura teletechniczna znajduje się w okresie gwarancji i serwisu wykonawcy tej infrastruktury.

Wspomniana infrastruktura sieciowa jest odebrana, opomiarowana i objęta 25-letnią gwarancją certyfikowaną przez producenta okablowania.

Wobec powyższego Wykonawca w ramach przeprowadzanych przez siebie prac, zobowiązany będzie do starannego demontażu, montażu (odtworzenia) oraz uzyskania co najmniej 25-letniej gwarancji producenta okablowania (certyfikatu) poddawanej pracom infrastruktury.

Wymaganymi parametrami podstawowymi są zachowanie co najmniej:

- niezmienionej ilości punktów elektryczno-logicznych (PEL) w stosunku do pierwotnej ich liczby (tzn. zachowania co najmniej ilości PEL sprzed realizacją inwestycji przez Wykonawcę, gdyż ich ilość objęta jest tzw. wskaźnikiem wykonania dla Projektu „Pomorskie e-Zdrowie”),
- zachowanie standardów materiałowych i producenckich zgodnych z demontowaną infrastrukturą,
- obligatoryjne objęcie odtworzonej infrastruktury co najmniej 25-letnią gwarancją producencką (certyfikacją),
- sporządzenie dokumentacji powykonawczej dla odtworzonej infrastruktury sieciowej,
- objęcie odtworzonej infrastruktury co najmniej 5-letnią gwarancją,
- objęcie odtworzonej infrastruktury co najmniej 3-letnim serwisem,
- objęcie odtworzonej infrastruktury rękojmią Wykonawcy.

W przypadku, gdy na etapie odtwarzania infrastruktury sieciowej, pojawi się konieczność jej rozbudowy o np. dodatkowe punkty PEL, zmiany jej przebiegów, konieczności przeprojektowania wymagań dla wydzielonej sieci zasilania, każdorazowo na wstępnym etapie projektowania Projektant/Wykonawca zobowiązany będzie do uzyskania uzgodnień z tym związanych z Zamawiającym.

Wymagania szczegółowe w zakresie specyfikacji prac, materiałów oraz urządzeń i sprzętu przedstawione są w opisanych w tym dokumencie zapisach.

W przypadku rozbudowy infrastruktury sieciowej wybudowanej w ramach „Projektu Pomorskie e-Zdrowie” o dodatkowe punkty PEL, należy zachować obecny reżim materiałowy, wykonawczy i odbiorowy, wskazany w powyższym opracowaniu.

Zabrania się dokonywania przedłużania okablowania sieci teletechnicznej w sposób niecertyfikowany, tzn. jeśli demontowane i przemieszczane punkty PEL wskazują zbyt krótkie zapasy kabla sieciowego LAN, Wykonawca musi ułożyć nowe okablowanie – bez dokonywania łączy różnych odcinków okablowania. Trasa kablowa pomiędzy panelem krosowy PPD a punktem PEL musi być wykonana ciągłym i nie łączonym kablem LAN.

Na etapie przygotowywania projektu, ale także podczas wykonywania instalacji teletechnicznej należy zwrócić szczególną uwagę na okablowanie wydzielonej sieci zasilania (230V). Należy dokonać bilansu obciążeń dla prawidłowo wyliczonych obwodów zasilania i stosownie je zabezpieczyć. Nie dopuszcza się przeciążenia obecnie użytkowanych obwodów rozdzielni RD poprzez podłączanie do nich nie obliczonych obciążeniowo obwodów sieci zasilania gwarantowanego. Wszelkie obwody elektryczne wydzielonej sieci zasilania gwarantowanego muszą być zabezpieczone urządzeniami typu UPS, o wyliczonych i odpowiednio dobranych parametrach technicznych. W przypadku uzyskania zgody na wykorzystanie w tym celu obecnie użytkowanych zasilaczy awaryjnych UPS, należy dostarczyć potwierdzone przez Projektanta/Wykonawcę wyliczenia odpowiedniego bilansu mocy i obciążeń.

Dozwolone jest – po uprzednim uzgodnieniu z Zamawiającym – wykorzystanie obecnie użytkowanych kanałów i tras kablowych, przy zachowaniu odpowiedniego zapasu technologicznego w tychże kanałach i trasach.

W zakresie wykorzystania wolnych przestrzeni w obecnie użytkowanych szafach teletechnicznych zlokalizowanych w pomieszczeniach PPD, bądź GPD, każdorazowo wymagana jest zgoda oraz uzgodnienie z Zamawiającym (Działem Informatyki). Projektant/Wykonawca może wykorzystać wskazane miejsca do montażu swoich urządzeń aktywnych oraz elementów pasywnych w tych pomieszczeniach i szafach, jeśli pozwolą na to warunki techniczne. Jeśli nie ma takiej możliwości, należy infrastrukturę taką oprzeć o wydzielone nowe PPD oraz odpowiednią szafę telekomunikacyjną.

8.1. WARIANT I - PRZEJĘCIE ODPOWIEDZIALNOŚCI PRZEZ WYKONAWCĘ

1. W przypadku jakiegokolwiek ingerencji Wykonawcy w Prace wykonane przez Wykonawcę e-Zdrowie w ramach Projektu, Wykonawca jest zobowiązany do przywrócenia na własny koszt prac do stanu poprzedniego, obejmującego w szczególności ponowny montaż i certyfikację infrastruktury i okablowania oraz wykonanie niezbędnych robót budowlanych i uzyskanie analogicznych lub wyższych parametrów wykonanej sieci. Wykonawca jest zobowiązany do wykonania prac odtworzeniowych Sieci e-Zdrowie przy użyciu urządzeń, sprzętu i infrastruktury o parametrach takich samych lub wyższych niż parametry urządzeń, sprzętu i infrastruktury wykorzystane do budowy Sieci e-Zdrowie, a także do stosowania analogicznych sposobów technologicznych budowy Sieci e-Zdrowie oraz ułożenia Sieci e-Zdrowie w analogiczny sposób do poprzedniego, a także uzyskania analogicznych certyfikatów w zakresie infrastruktury i okablowania. Kluczowym do zachowania elementem przy dokonywaniu modernizacji ww. sieci jest zachowanie wskaźnika wykonania dla Projektu Sieci e-Zdrowie, tzn. niezmnieszonej ilości punktów PEL w obszarze objętym inwestycją. Wykonawca jest zobowiązany do niezwłocznego, nie później niż **7 dni roboczych** przed planowanym rozpoczęciem prac, zawiadomienia Zamawiającego i Wykonawcę e-Zdrowie o terminie i zakresie planowanej ingerencji w Sieć e-Zdrowie, ze wskazaniem terminów i rodzajów prac planowanych do przeprowadzenia przez Wykonawcę oraz ich wpływie na Prace zrealizowane przez Wykonawcę e-Zdrowie w ramach Projektu. Wykonawca uzgodni też z Wykonawcą e-Zdrowia zakres współpracy (jeśli taka współpraca będzie zachodziła), uzyskując jego pisemną akceptację w zakresie wykonywanych prac oraz przejęcia odpowiedzialności przez Wykonawcę dla Sieci e-Zdrowie poddawanej modernizacji/przebudowie zgodnie z opisanymi poniżej (punkt 8.1) zasadami. Zawiadomienie, dokumenty uzgodnieniowe oraz pisemną akceptację Wykonawcy e-Zdrowia, Wykonawca dostarczy również Zamawiającemu.
2. W szczególności Wykonawca zobowiązany jest do odbudowy Sieci e-Zdrowie zgodnie z wytycznymi zawartymi w PFU Programie Funkcjonalno-Użytkowym mającym zastosowanie dla danej części prac i dla danej lokalizacji, stanowiącym załącznik do Specyfikacji Istotnych Warunków Zamówienia postępowania nr DAZ-ZP.272.33.2017 prowadzonego w ramach Projektu Pomorskie e-Zdrowie, o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego na podstawie ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (t.j. Dz.U. z 2015r. poz.2164 z późn. zm.) o wartości szacunkowej przekraczającej wyrażoną w złotych równowartość kwoty 5.186.000 euro na „**Budowę i dostosowanie infrastruktury pasywnej (w tym serwerownie), dostosowanie i rozbudowa sieci teleinformatycznych i sieci zasilania gwarantowanego wraz z dostawą budynkowych (centralnych) zasilaczy UPS**” oraz zgodnie z aktualnymi wymaganiami szczegółowymi w zakresie specyfikacji prac, materiałów oraz urządzeń i sprzętu przedstawionych w tym dokumencie.
3. Wykonawca przejmuje zobowiązania Wykonawcy e-Zdrowie wynikające z umowy nr 97/18 z dnia 6 kwietnia 2018 roku na „**Budowę i dostosowanie infrastruktury pasywnej (w tym serwerownie), dostosowanie i rozbudowę sieci teleinformatycznych i sieci zasilania gwarantowanego wraz z dostawą budynkowych (centralnych) zasilaczy UPS**”, w zakresie udzielonej gwarancji jakości, rękojmi za wady i odpowiedzialności za szkodę na zasadach ogólnych, w zakresie Prac wykonanych w ramach Projektu.
4. Wykonawca przejmuje zobowiązania określone w punkcie poprzednim w zakresie całości Prac wykonanych i istniejących na terenie obiektu, w którym Wykonawca wykonuje prace będące Przedmiotem Zamówienia w niniejszym postępowaniu.
5. Wykonawca po zakończeniu Przedmiotu Zamówienia oraz w celu uzyskaniu ostatecznego protokołu odbioru prac w zakresie branży teleinformatycznej, wystawi Zamawiającemu podpisany przez obie strony, dokument gwarancji, rękojmi oraz serwisu zawierający wszystkie wymienione poniżej warunki: zachowania gwarancji jakości, rękojmi, usuwania wad w infrastrukturze (awarii i usterek) i wad budowlanych, kar za opóźnienia w reakcji na zgłoszenie lub za opóźnienia w stosunku do terminu naprawy.
6. Wykonawca przejmuje i udziela Zamawiającemu gwarancji jakości (dalej zwanej "**gwarancją**"):
 - 1) na Infrastrukturę sprzętową pasywną na okres 5 lat. Ponadto Wykonawca będzie wykonywał Serwis Infrastruktury sprzętowej pasywnej przez okres 3 lat;
 - 2) na wykonane roboty budowlane z wyłączeniem robót budowlanych stanowiących Infrastrukturę sprzętową pasywną, na okres 5 lat;
 - 3) producenta na cały system okablowania strukturalnego LAN (okablowanie pionowe, okablowanie poziome, punkty dystrybucyjne, gniazda PEL (Punkt Elektryczno-Logiczny sieci LAN), połączenia systemowe, połączenia między budynkowe, itp.) na okres 25 lat;
 z tym zastrzeżeniem, iż bieg terminów określonych w niniejszym ustępie rozpoczął się w dniu 1 marca 2020 roku, a Wykonawca przejmuje odpowiedzialność z tytułu gwarancji na okres pozostały do upływu terminów wskazanych w niniejszym ustępie.

7. Wykonawca ponosi odpowiedzialność z tytułu rękojmi za Wady przez okres równy okresom gwarancji, o których mowa w ustępie poprzednim. Zamawiający może wykonywać uprawnienia z tytułu rękojmi za Wady niezależnie od uprawnień wynikających z gwarancji jakości.
8. Wykonawca ponosi odpowiedzialność za szkody na zasadach ogólnych przez okres pozostały do upływu terminów przedawnienia roszczeń.
9. Odpowiedzialność Wykonawcy o której mowa w niniejszym wariancie rozpoczyna się z dniem przejęcia frontu robót przez Wykonawcę.
10. W zakresie gwarancji Wykonawca jest zobowiązany do nieodpłatnego usuwania Wad ujawnionych w okresie wskazanym w ustępie 5.
11. Przyjęcie zgłoszenia Wady przez Wykonawcę, odbywać się będzie w okresie dostępności Wykonawcy wskazanym w **Tabeli nr 1** oraz **Tabeli nr 2** faksem lub drogą e-mailową na adres podany przez Wykonawcę. W ramach gwarancji Wykonawca zobowiązany jest do:
 - 1) usunięcia wszelkich Wad Infrastruktury sprzętowej pasywnej oraz Wad Infrastruktury sieciowej (Usterek oraz Awarii) w terminach wskazanych w **Tabeli nr 1**.

Tabela nr 1. Terminy usuwania Wad w infrastrukturze sprzętowej pasywnej oraz Wad w Infrastrukturze sieciowej

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	24/7/365	niezwłocznie, nie później niż 4 godziny od czasu przyjęcia zgłoszenia	Rozwiązanie zastępcze nie później niż 12 godzin od czasu przyjęcia zgłoszenia. Naprawa niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia.
USTERKA	W dni robocze pomiędzy 8.00 a 16.00. Zgłoszenie przesłane po 16.00, traktowane jest jak zgłoszenie przyjęte w następnym dniu roboczym o 8.00	niezwłocznie nie później niż 2 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia

- 2) usunięcia Wad budowlanych w terminach określonych w **Tabeli nr 2**.

Tabela nr 2. Terminy usuwania Wad budowlanych

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
WADA BUDOWLANA	W dni robocze pomiędzy 8.00 a 16.00. Zgłoszenie przesłane po 16.00, traktowane jest jak zgłoszenie przyjęte w następnym dniu roboczym o 8.00	niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 14 dni roboczych od dnia przyjęcia zgłoszenia

- 3) w przypadku Wady Wykonawca pokryje wszystkie koszty związane z ponowną instalacją Komponentów/Produktów wolnych od Wad.
- 4) dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego. Do czasu potwierdzenia zmiany kwalifikacji, uznaje się za obowiązującą kwalifikację pierwotną.
- 5) czas reakcji Wykonawcy i czas naprawy mogą być inne niż wskazane w **Tabeli nr 1** oraz **Tabeli nr 2**, jeżeli Zamawiający zaakceptuje zmianę kwalifikacji zgłoszenia, o której mowa w punkcie 4.
- 6) czas reakcji Wykonawcy i czas naprawy mogą być inne niż wskazane w **Tabeli nr 1** oraz **Tabeli nr 2** za zgodą Zamawiającego.
- 7) w przypadku braku możliwości usunięcia Wady lub przedstawienia rozwiązania zastępczego zdalnie, Wykonawca zobowiązany jest do usunięcia Wady bezpośrednio w lokalizacji Zamawiającego.
- 8) w przypadku niemożliwości usunięcia Wady w terminie wskazanym w **Tabeli nr 1** oraz **Tabeli nr 2**, dany Produkt zostanie wymieniony na nowy o równoważnych lub wyższych parametrach. W przypadku, gdy czas naprawy będzie dłuższy niż 6 tygodni lub jakikolwiek element Sieci e-Zdrowie będzie wymagał

naprawy po raz trzeci w czasie okresu gwarancyjnego Wykonawca będzie zobowiązany do jego wymiany na nowy, o co najmniej takich samych parametrach i standardach jak pierwotny.

- 9) Wykonawca w okresie trwania gwarancji, do 5 dnia każdego miesiąca, przedstawi Zamawiającemu, raport wykonanych napraw gwarancyjnych. Raport powinien zawierać co najmniej: numer zgłoszenia, kwalifikację zgłoszenia, godzinę i datę zgłoszenia, temat zgłoszenia, status zgłoszenia, godzinę i datę dostarczenia rozwiązania zastępczego (dla awarii), godzinę i datę usunięcia Wady, godzinę i datę wykonania reakcji Wykonawcy, czas naprawy, czas opóźnienia w postaci godzin lub dni (jeżeli jest) dla rozwiązania zastępczego lub usunięcia Wady. Raporty dotyczące elementów Sieci e-Zdrowie powinny być składane przez Wykonawcę przez okres pozostały do upływu 5 lat liczonych począwszy od dnia 1 marca 2020 roku.
12. Po upływie okresu realizowania przez Wykonawcę Serwisu Infrastruktury sprzętowej pasywnej jest on zobowiązany do informowania Zamawiającego o konieczności wykonania Serwisu w terminie 14 dni przed dniem, kiedy Serwis powinien zostać wykonany. Obowiązek, o którym mowa w zdaniu poprzednim trwa do końca okresu gwarancji.
13. Wykonawca ponosi odpowiedzialność z tytułu rękojmi za Wady przez okres równy okresom gwarancji, określonych powyżej.
14. Zamawiający może wykonywać uprawnienia z tytułu rękojmi za Wady niezależnie od uprawnień wynikających z gwarancji jakości.
15. Wykonawca zobowiązany będzie do uiszczania na rzecz Zamawiającego kar umownych w wysokości określonej poniżej, jako **procent od wynagrodzenia brutto należnego Wykonawcy**. Kary umowne naliczane będą:
 - 1). za opóźnienie w reakcji Wykonawcy na zgłoszenie:
 - a). AWARII w okresie gwarancyjnym - w wysokości 0,025%, za każdą rozpoczętą godzinę opóźnienia w stosunku do terminu określonego w **Tabeli nr 1**, liczoną od upływu terminu określonego w godzinach wyznaczonych jako czas reakcji,
 - b). USTERKI w okresie gwarancyjnym - w wysokości 0,35% za każdy rozpoczęty dzień opóźnienia w stosunku do terminu określonego w **Tabeli nr 1**, liczony od upływu terminu wyznaczonego jako czas reakcji,
 - c). WADY BUDOWLANEJ w okresie gwarancyjnym w wysokości 0,35%, za każdy rozpoczęty dzień opóźnienia w stosunku do terminu określonego w **Tabeli nr 2**, liczony od upływu terminu wyznaczonego jako czas reakcji,
 - 2). za opóźnienie w stosunku do terminu naprawy:
 - a). AWARII w okresie gwarancyjnym - w wysokości 0,04%, za każdą rozpoczętą godzinę opóźnienia w stosunku do terminu określonego w **Tabeli nr 1**, liczony od upływu terminu wyznaczonego jako czas naprawy,
 - b). USTERKI w okresie gwarancyjnym - w wysokości 0,5%, za każdy rozpoczęty dzień opóźnienia w stosunku do terminu określonego w **Tabeli nr 1**, liczony od upływu terminu wyznaczonego jako czas naprawy,
 - c). WADY BUDOWLANEJ w okresie gwarancyjnym - w wysokości 0,5%, za każdy rozpoczęty dzień opóźnienia w stosunku do terminu określonego w **Tabeli nr 2**, liczony od upływu terminu wyznaczonego jako czas naprawy.
16. Poprzez użyte w niniejszym wariantcie określenia rozumie się:
 - 1) **Awaria** - Kategoria Wady w Infrastrukturze sprzętowej pasywnej lub Infrastrukturze sieciowej oznaczająca brak działania lub niepoprawne działanie Sieci e-Zdrowie, u Zamawiającego, uniemożliwiający jego użytkowanie. Sytuacja, w której infrastruktura w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Komponentów/Produktów zamówienia.
 - 2) **Czas naprawy** - Należy przez to rozumieć czas, jaki może upłynąć pomiędzy pierwszym zgłoszeniem Wady, a Usunięciem Wady.
 - 3) **Czas Reakcji Wykonawcy** - Należy przez to rozumieć maksymalny czas jaki może upłynąć pomiędzy pierwszym zgłoszeniem Wady, a podjęciem działań przez Wykonawcę. Przez działania Wykonawcy rozumie się co najmniej dla wykonanych Robót budowlanych: podjęcie czynności technicznych w lokalizacji Zamawiającego zmierzających do usunięcia Wady.
 - 4) **Dni robocze** - Dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy, wskazanych w ustawie z dnia 18 stycznia 1951r. o dniach wolnych od pracy (Dz.U. z 2015r. poz. 90).
 - 5) **Infrastruktura Sieciowa** - Urządzenia i pasywne elementy sieci komputerowych LAN dostarczane przez Wykonawcę wchodzące w skład wdrażanego u Zamawiających rozwiązania będące częścią Robót budowlanych obejmujące w szczególności:
 - a. część pasywną sieci komputerowych LAN: kable, gniazda sygnałowe i elektryczne, panele, organizery, trasy kablowe, etc.,
 - b. wyposażenie pomieszczeń technicznych takich jak szafy i przetącznie,

- c. pozostałe instalacje elektryczne i systemy budynkowe.
- 6) **Infrastruktura Sprzętowa Pasywna** - Rozumiane jako urządzenia: UPS, Agregat, Klimatyzator, CCTV, SSWiN, KD, VESDA, SUG, System monitorowania infrastruktury i warunków klimatycznych w serwerowni – wskazane rodzajowo w PFU (Programie Funkcjonalno-Użytkowym) obowiązującym w ramach Projektu, odpowiednio dla każdej części zamówienia dla poszczególnych Podmiotów Lecznicych.
 - 7) **KD** - Kontrola Dostępu.
 - 8) **Komponent** - Komponent to integralna część dostawy i wdrożenia Sieci e-Zdrowie. Komponent powinien się składać przynajmniej z jednego Produktu lub wielu Produktów powiązanych ze sobą merytorycznie. Przyjęte Komponenty muszą być wspólne dla poszczególnych Zamawiających w przypadku Wykonawcy realizującego Sieć e-Zdrowie w więcej niż jednym Podmiocie Lecznicych. Komponent może być dedykowany dla wszystkich Podmiotów Lecznicych lub indywidualny.
Podstawowy podział Komponentów oczekiwany przez Zamawiających:
 - a. Sieci okablowania strukturalnego LAN
 - b. Infrastruktura zasilania gwarantowanego
 - c. Infrastruktura klimatyzacji i wentylacji
 - d. Systemy zabezpieczeń.
 - 9) **Okres dostępności Wykonawcy** - Należy przez to rozumieć przedział czasu w jakim Wykonawca jest gotowy do przyjęcia zgłoszenia Wad.
 - 10) **PD** - Punkt Dystrybucyjny.
 - 11) **PEL** - Punkt Elektryczno-Logiczny sieci LAN.
 - 12) **PPD** - Pośredni Punkt Dystrybucyjny. Lokalny punkt dystrybucyjny obsługujący najczęściej dany obszar roboczy lub piętro..
 - 13) **Produkt** - Elementarny efekt działań/prac/dostaw objętych całym zakresem Sieci e-Zdrowie, podczas realizacji Projektu w poszczególnych etapach.
 - 14) **Serwis** - Zespół czynności niezbędnych do zachowania gwarancji producenta (niezbędne przeglądy konserwacje i in.), wykonywany na zasadach wymaganych przez producenta (bez uwzględnienia materiałów eksploatacyjnych).
 - 15) **SSWiN** - System Sygnalizacji Włamania i Napadu.
 - 16) **SUG** - Stałe Urządzenie Gaśnicze.
 - 17) **Usterka** - Należy przez to rozumieć kategorię Wady w Infrastrukturze sprzętowej pasywnej lub Infrastrukturze sieciowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji (dostarczonej przez Wykonawcę e-Zdrowie oraz związanej i powstałej w wyniku wykonywania Prac w ramach Projektu) oraz SWZ obowiązującego w Projekcie, nie wpływając istotnie na pracę dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.
 - 18) **Usunięcie Wady** - Należy przez to rozumieć wykonanie prac w przedmiocie zamówienia realizowanym w ramach Projektu, przez Wykonawcę, w wyniku których nastąpi przywrócenie do stanu sprzed wystąpienia Wady wraz z usunięciem jej skutków.
 - 19) **VESDA** - System Wczesnej Detekcji Zadymienia i Pożaru
 - 20) **Wada** - Należy przez to rozumieć Wadę Infrastruktury sprzętowej pasywnej, Wadę Infrastruktury sieciowej, Wadę budowlaną.
 - 21) **Wada Budowlana** - Wszelkie wady wykonanych robót budowlanych (z wyłączeniem Infrastruktury pasywnej i Infrastruktury sieciowej) powodujące, że są one niezgodne z umową zawartą w ramach Projektu lub nie posiadają właściwości, które zgodnie z umową zawartą w ramach Projektu powinny posiadać.
 - 22) **Wada Infrastruktury Sprzętowej Pasywnej** - Należy przez to rozumieć Awarię lub Usterkę w Infrastrukturze sprzętowej pasywnej.
 - 23) **Wada Infrastruktury Sieciowej** - Należy przez to rozumieć Awarię lub Usterkę w Infrastrukturze sieciowej.
 - 24) **Zgłoszenie Wady** - Zdarzenie, w wyniku którego nastąpiło powiadomienie Wykonawcy o zaistniałej Wadzie.

8.2. WARIANT II – WYKONANIE PRAC PRZEZ WYKONAWCĘ E-ZDROWIE NA KOSZT WYKONAWCY I UTRZYMANIE ODPOWIEDZIALNOŚCI WYKONAWCY E-ZDROWIE

1. W przypadku planowanej ingerencji Wykonawcy w Prace wykonane przez Wykonawcę e-Zdrowie w ramach Projektu, Wykonawca jest zobowiązany do niezwłocznego, nie później niż **7 dni** roboczych przed planowanym rozpoczęciem prac, zawiadomienia Zamawiającego i Wykonawcę e-Zdrowie o terminie i zakresie planowanej ingerencji w Sieć e-Zdrowie, ze wskazaniem terminów i rodzajów prac planowanych do przeprowadzenia przez Wykonawcę oraz ich wpływie na Prace zrealizowane przez Wykonawcę e-Zdrowie w ramach Projektu. Wykonawca uzgodni też z Wykonawcą e-Zdrowia zakres współpracy, uzyskując jego pisemną akceptację w zakresie wykonywanych prac. Zawiadomienie, dokumenty uzgodnieniowe oraz pisemną akceptację Wykonawcy e-Zdrowia, Wykonawca dostarczy również Zamawiającemu.
2. Po uprzednim zawiadomieniu Wykonawcy, Wykonawca e-Zdrowie jest uprawniony do wstępu na teren budowy i kontroli wykonywania prac przez Wykonawcę w zakresie ich ingerencji w Prace wykonywane przez Wykonawcę e-Zdrowie w ramach Projektu. W przypadku zauważenia przez Wykonawcę e-Zdrowie jakichkolwiek nieprawidłowości, mogących skutkować brakiem możliwości odtworzenia Sieci e-Zdrowie lub braku możliwości utrzymania jej parametrów, Wykonawca e-Zdrowie jest uprawniony do złożenia Wykonawcy pisemnych zastrzeżeń ze wskazaniem terminu do ich usunięcia. W przypadku niezastosowania się przez Wykonawcę do złożonych przez Wykonawcę e-Zdrowie uwag w terminie wskazanym w treści zawiadomienia, Wykonawca e-Zdrowie będzie uprawniony do odmowy odtworzenia Prac wykonanych w ramach Projektu, a dla Wykonawcy wystąpią skutki jak gdyby dokonał wyboru **Wariantu I**.
3. Po wykonaniu przez Wykonawcę całości lub części prac objętych Przedmiotem Zamówienia w niniejszym postępowaniu, Wykonawca jest zobowiązany do niezwłocznego, jakkolwiek nie później niż w terminie **3 dni** roboczych od zakończenia wykonywania całości prac będących Przedmiotem Zamówienia w niniejszym postępowaniu, zawiadomić Zamawiającego i Wykonawcę e-Zdrowie o możliwości przeprowadzenia wizji lokalnej i przystąpienia do wykonania kalkulacji wyceny prac odtworzeniowych Sieci e-Zdrowie realizowanych przez Wykonawcę e-Zdrowie (dalej: „**Kalkulacja**”).
4. Po przeprowadzeniu wizji lokalnej i przedstawieniu Wykonawcy przez Wykonawcę e-Zdrowie Kalkulacji, o której mowa w ustępie poprzednim, Wykonawca może przystąpić do zlecenia Wykonawcy e-Zdrowie wykonanie prac odtworzeniowych Sieci e-Zdrowie za kwotę wskazaną w Kalkulacji. W tym celu Wykonawca e-Zdrowie i Wykonawca zawrą stosowne porozumienie, którego kopię otrzyma również Zamawiający. W przypadku zawarcia porozumienia zgodnie z niniejszym ustępem, Wykonawca umożliwi Wykonawcy e-Zdrowie wykonanie wszelkich niezbędnych prac koniecznych dla przywrócenia Sieci e-Zdrowie do stanu poprzedniego, w szczególności udostępni Wykonawcy e-Zdrowie front robót i przekaze wszelkie zdemontowane części infrastruktury Sieci zrealizowanej przez Wykonawcę e-Zdrowie, a także Wykonawca zobowiązuje się do udzielenia Wykonawcy e-Zdrowie wszelkich wskazówek, informacji i dokumentacji w zakresie niezbędnym do wykonania przez Wykonawcę e-Zdrowie prac objętych porozumieniem.
5. W przypadku zawarcia przez Wykonawcę i Wykonawcę e-Zdrowie porozumienia oraz wykonania przez Wykonawcę e-Zdrowie prac odtworzeniowych Sieci e-Zdrowie i zapłaty przez Wykonawcę całości wynagrodzenia na rzecz Wykonawcy e-Zdrowie zgodnie z przedstawioną Kalkulacją, Wykonawca e-Zdrowie utrzyma wszelkie zobowiązania wynikające z umowy nr 97/18 z dnia 6 kwietnia 2018 roku na „**Budowę i dostosowanie infrastruktury pasywnej (w tym serwerownie), dostosowanie i rozbudowę sieci teleinformatycznych i sieci zasilania gwarantowanego wraz z dostawą budynkowych (centralnych) zasilaczy UPS**”, w zakresie udzielonej gwarancji jakości, rękojmi za wady i odpowiedzialności za szkodę na zasadach ogólnych na Prace wykonane w ramach Projektu.
6. W przypadku jeżeli, po przeprowadzeniu wizji lokalnej, Wykonawca e-Zdrowie stwierdzi brak możliwości odtworzenia Sieci e-Zdrowie lub stwierdzi występowanie innych przeszkód w wykonaniu planowanych prac, może odstąpić od wykonania Kalkulacji, a dla Wykonawcy wystąpią skutki jak gdyby dokonał wyboru **Wariantu I**. Takie same skutki wystąpią w przypadku braku akceptacji Kalkulacji przez Wykonawcę oraz w przypadku braku zawarcia przez Wykonawcę i Wykonawcę e-Zdrowie porozumienia w zakresie wykonania prac odtworzeniowych Sieci e-Zdrowie, w terminie **14 dni** roboczych od przedstawienia Wykonawcy Kalkulacji sporządzonej przez Wykonawcę e-Zdrowie.

8.3. WARIANT III - WYKONANIE PRAC PRZEZ WYKONAWCĘ I UTRZYMANIE ODPOWIEDZIALNOŚCI WYKONAWCY E-ZDROWIE W PRZYPADKU AKCEPTACJI PRAC

1. W przypadku planowanej ingerencji Wykonawcy w Prace wykonane przez Wykonawcę e-Zdrowie w ramach Projektu, Wykonawca jest zobowiązany do niezwłocznego, nie później niż **7 dni** roboczych przed planowanym rozpoczęciem prac, do zawiadomienia Zamawiającego i Wykonawcę e-Zdrowie o terminie i zakresie planowanej ingerencji w Sieci e-Zdrowie, ze wskazaniem terminów i rodzajów prac planowanych do przeprowadzenia przez Wykonawcę oraz ich wpływie na Prace zrealizowane przez Wykonawcę e-Zdrowie w ramach Projektu. Wykonawca uzgodni też z Wykonawcą e-Zdrowia zakres współpracy, uzyskując jego pisemną akceptację w zakresie wykonywanych prac. Zawiadomienie, dokumenty uzgodnieniowe oraz pisemną akceptację Wykonawcy e-Zdrowia, Wykonawca dostarczy również Zamawiającemu.
2. Wykonawca jest zobowiązany do przywrócenia na własny koszt Sieci e-Zdrowie do stanu poprzedniego, obejmującego w szczególności ponowny montaż i certyfikację infrastruktury i okablowania oraz wykonanie niezbędnych robót budowlanych i uzyskanie analogicznych lub wyższych parametrów wykonanej Sieci e-Zdrowie. Wykonawca jest zobowiązany do wykonania prac odtworzeniowych Sieci e-Zdrowie przy użyciu urządzeń, sprzętu i infrastruktury o parametrach takich samych lub wyższych niż parametry urządzeń, sprzętu i infrastruktury wykorzystane do budowy Sieci e-Zdrowie, a także do stosowania analogicznych sposobów technologicznych budowy Sieci e-Zdrowie oraz ułożenia Sieci e-Zdrowie w analogiczny sposób do poprzedniego, a także uzyskania analogicznych certyfikatów w zakresie infrastruktury i okablowania (zgodnie z aktualnymi wymaganiami szczegółowymi w zakresie specyfikacji prac, materiałów oraz urządzeń i sprzętu przedstawionych w tym dokumencie).
3. W szczególności Wykonawca zobowiązany jest do odbudowy Sieci e-Zdrowie zgodnie z wytycznymi zawartymi w PFU Programie Funkcjonalno-Użytkowym mającym zastosowanie dla danej części prac i dla danej lokalizacji, stanowiącym załącznik do Specyfikacji Istotnych Warunków Zamówienia postępowania nr DAZ-ZP.272.33.2017 prowadzonego w ramach Projektu Pomorskie e-Zdrowie, o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego na podstawie ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (t.j. Dz.U. z 2015r. poz.2164 z późn. zm.) o wartości szacunkowej przekraczającej wyrażoną w złotych równowartość kwoty 5.186.000 euro na „**Budowę i dostosowanie infrastruktury pasywnej (w tym serwerownie), dostosowanie i rozbudowa sieci teleinformatycznych i sieci zasilania gwarantowanego wraz z dostawą budynkowych (centralnych) zasilaczy UPS**” oraz zgodnie z aktualnymi wymaganiami szczegółowymi w zakresie specyfikacji prac, materiałów oraz urządzeń i sprzętu przedstawionych w tym dokumencie.
4. Wykonawca e-Zdrowie jest uprawniony do wstępu na teren budowy i prowadzenia czynności nadzoru oraz kontroli wykonywania prac przez Wykonawcę w zakresie ingerencji w Sieć e-Zdrowie, a także jest uprawniony do sprawowania odpłatnego (płatnego przez Wykonawcę na zasadach zawartych w niniejszym wariantcie) nadzoru nad wykonywaniem przez Wykonawcę prac mających na celu przywrócenie Sieci e-Zdrowie do stanu poprzedniego zgodnie z postanowieniami niniejszego wariantu.
5. Za wykonywanie przez Wykonawcę e-Zdrowie czynności nadzoru, o których mowa w ustępie poprzednim, Wykonawca jest zobowiązany do zapłaty na rzecz Wykonawcy e-Zdrowie kwoty **180,00** złotych netto za każdą rozpoczętą godzinę sprawowania nadzoru. Zakres, forma i harmonogram sprawowania nadzoru uzgodniona musi zostać pomiędzy Wykonawcą i Wykonawcą e-Zdrowia w formie pisemnej na etapie procesu składania zawiadomienia, o którym mowa w punkcie 8.3 ust.1 (powyżej).
6. W przypadku zauważenia przez Wykonawcę e-Zdrowie jakichkolwiek nieprawidłowości, mogących skutkować brakiem możliwości odtworzenia Sieci e-Zdrowie lub braku możliwości utrzymania jej parametrów, Wykonawca e-Zdrowie jest uprawniony do złożenia Wykonawcy pisemnych zastrzeżeń ze wskazaniem terminu do ich usunięcia. W przypadku niezastosowania się przez Wykonawcę do złożonych przez Wykonawcę e-Zdrowie uwag w terminie wskazanym w treści zawiadomienia, Wykonawca e-Zdrowie będzie uprawniony do odmowy akceptacji prac odtworzeniowych Sieć e-Zdrowie wykonanych przez Wykonawcę, a dla Wykonawcy wystąpią skutki jak gdyby dokonał wyboru **Wariantu I**.
7. Po wykonaniu przez Wykonawcę całości prac odtworzeniowych Sieć e-Zdrowie, zgodnie z postanowieniami niniejszego wariantu, Wykonawca jest zobowiązany do niezwłocznego, jakkolwiek nie później niż w terminie **3 dni** roboczych od zakończenia wykonywania całości prac, zawiadomienia Zamawiającego oraz Wykonawcę e-Zdrowie o możliwości przeprowadzenia odpłatnej (płatnej przez Wykonawcę na zasadach określonych w niniejszym wariantcie) wizji lokalnej i przystąpienia do oceny wykonanych prac, w szczególności oceny prawidłowości wykonania Sieci e-Zdrowie zgodnie z warunkami niniejszego wariantu, a także oceny utrzymania parametrów i uzyskania wymaganej certyfikacji infrastruktury i okablowania (dalej: „**Opomiarowanie**”).

8. Za wykonywanie przez Wykonawcę e-Zdrowie czynności Opomiarowania, o których mowa w ustępie poprzednim, Wykonawca jest zobowiązany do zapłaty na rzecz Wykonawcy e-Zdrowie wynagrodzenia ustalonego na podstawie stawek przedstawionych w **Załączniku A**.
9. W przypadku, jeżeli po wykonaniu Opomiarowania, Wykonawca e-Zdrowie i Zamawiający pisemnie potwierdzą prawidłowość wykonania przez Wykonawcę prac odtworzeniowych Sieci e-Zdrowie, bez żadnych zastrzeżeń, Wykonawca e-Zdrowie utrzyma wszelkie zobowiązania wynikające z umowy nr 97/18 z dnia 6 kwietnia 2018 roku na „**Budowę i dostosowanie infrastruktury pasywnej (w tym serwerownie), dostosowanie i rozbudowę sieci teleinformatycznych i sieci zasilania gwarantowanego wraz z dostawą budynkowych (centralnych) zasilaczy UPS**”, w zakresie udzielonej gwarancji jakości, rękojmi za wady i odpowiedzialności za szkodę na zasadach ogólnych na Prace wykonane w ramach Projektu. W przeciwnym wypadku dla Wykonawcy wystąpią skutki jak gdyby dokonał wyboru **Wariantu I**, w szczególności Wykonawca obowiązany będzie do usunięcia Wad wykonanej Sieci e-Zdrowie i będzie ponosił wszelką odpowiedzialność za szkody wynikające z nieprawidłowości w zakresie działania Sieci e-Zdrowie.

Załącznik A: Zasady ustalenia wynagrodzenia Wykonawcy e-Zdrowie [ceny netto]

POMIARY

1szt PEL (2xRJ45 + 2x230Vdata)

KNR AT-15 0118-01	Wykonanie pomiarów torów transmisyjnych - pierwsza linia	miar	1		
	R	rg	0,84	20,00 zł	16,80 zł
	S				
at154	przyrząd pomiarowy okablowania strukturalnego kpl.	m-g	0,42	20,00 zł	8,40 zł
at155	środek łączności bezprzewodowej kpl.	m-g	0,42	20,00 zł	8,40 zł
	Koszty pośrednie (R+S)		70,5%		23,69 zł
	Zysk (R+S+Kp)		12,3%		7,05 zł
	Razem jedn.				64,33 zł
	Razem				64,33 zł

KNR AT-15 0118-02	Wykonanie pomiarów torów transmisyjnych - każda następna linia	miar	1		
	R	rg	0,3	20,00 zł	6,00 zł
	S				
at154	przyrząd pomiarowy okablowania strukturalnego kpl.	m-g	0,15	20,00 zł	3,00 zł
at155	środek łączności bezprzewodowej kpl.	m-g	0,15	20,00 zł	3,00 zł
	Koszty pośrednie (R+S)		70,5%		8,46 zł
	Zysk (R+S+Kp)		12,3%		2,52 zł
	Razem jedn.				22,98 zł
	Razem				22,98 zł

KNNR 5 1303-01	Pomiar rezystancji izolacji instalacji elektrycznej - obwód 1-fazowy (pomiar pierwszy)	miar	1		
	R	rg	0,63	20,00 zł	12,60 zł
	Koszty pośrednie (R+S)		70,5%		8,88 zł
	Zysk (R+S+Kp)		12,3%		2,64 zł
	Razem jedn.				24,13 zł
	Razem				24,13 zł

KNNR 5 1303-02	Pomiar rezystancji izolacji instalacji elektrycznej - obwód 1-fazowy (każdy następny pomiar)	miar	1		
	R	rg	0,42	20,00 zł	8,40 zł
	Koszty pośrednie (R+S)		70,5%		5,92 zł
	Zysk (R+S+Kp)		12,3%		1,76 zł
	Razem jedn.				16,08 zł

Razem						16,08 zł
-------	--	--	--	--	--	-----------------

KNR-W 5-08 0902-05	Sprawdzenie samoczynnego wyłączenia zasilania - próby działania wyłącznika różnicowoprądowego - pierwszy	pomiar	1			
	R	rg	0,33	20,00 zł		6,60 zł
	Koszty pośrednie (R+S)		70,5%			4,65 zł
	Zysk (R+S+Kp)		12,3%			1,38 zł
	Razem jedn.					12,64 zł
	Razem					12,64 zł

KNR-W 5-08 0902-06	Sprawdzenie samoczynnego wyłączenia zasilania - próby działania wyłącznika różnicowoprądowego - każdy następny	pomiar	1			
	R	rg	0,27	20,00 zł		5,40 zł
	Koszty pośrednie (R+S)		70,5%			3,81 zł
	Zysk (R+S+Kp)		12,3%			1,13 zł
	Razem jedn.					10,34 zł
	Razem					10,34 zł

KNNR 5 1301-01	Sprawdzenie i pomiar 1-fazowego obwodu elektrycznego niskiego napięcia	pomiar	1			
	R	rg	1,3	20,00 zł		26,00 zł
	Koszty pośrednie (R+S)		70,5%			18,33 zł
	Zysk (R+S+Kp)		12,3%			5,45 zł
	Razem jedn.					49,78 zł
	Razem					49,78 zł

Suma netto **200,28 zł**

Każdorazowo do każdego odtworzenia należy doliczyć koszt związany z wykonaniem dokumentacji przeprowadzeniem certyfikacji odtwarzanych gniazd PEL:

INNE					
Kalkulacja własna Uproszczona	Wykonanie dokumentacji powykonawczej	Kpl.	1		
	Razem				1 500,00 zł

9. WARUNKI I PARAMETRY DOSTĘPU ZDALNEGO DO WEWNĘTRZNYCH SIECI I STRUKTUR INFORMATYCZNYCH SPÓŁKI

Spółka udziela dostępu zdalnego (serwisowego, konserwacyjnego oraz operacyjnego) w ramach procedury I-108-011-27001: „Zasady serwisu zdalnego”. Zgodnie z tą procedurą, dostęp zdalny do informatycznych struktur wewnętrznych może być realizowany przez podmiot zewnętrzny wyłącznie na dwa sposoby:

1. Połączenie VPN w układzie site-to-site z wykorzystaniem protokołu IPSec.
2. Połączenie VPN w układzie Client-to-Site z wykorzystaniem dedykowanego klienta PaloAlto GlobalProtect i imiennych kont osobowych dla serwisantów dostawcy.

Zabronione jest wykorzystywanie połączeń VPN typu „calling home” oraz wszelkich technologii połączeń zdalnych za pomocą rozwiązań połączeń pośrednich (np. typu TeamViewer, MyRomm, etc.)

Dostawca systemów/usług zobowiązany jest na etapie podpisywania umowy lub najpóźniej podczas realizacji wdrożenia systemów/usług przekazać Działowi Informatyki Spółki:

1. Informacje pozwalające na zweryfikowanie celowości prośby, np. numer zawartej umowy umożliwiającej świadczenie usługi zdalnej oraz przekazanie informacji, kto (personalnie) po stronie Spółki odpowiada za realizację umowy.
2. Listę personelu uprawnionego do podłączenia zdalnego i dostępu do konkretnych zasobów sieciowych oraz aplikacyjnych.
3. Określić listę zasobów (urządzeń, struktur, systemów) do których zgodnie z umową (zamówieniem) potrzebował będzie dostępu zdalnego i w jakim zakresie (numery portów, nazwy usług itd.,)
4. Określić z jakich publicznych adresów IP będzie inicjował połączenia do sieci wewnętrznej Spółki.

Wszystkie powyższe informacje należy przekazać do Działu Informatyki pod adres poczty elektronicznej: it@szpitalpomorskie.eu.

Na podstawie przekazanych informacji Dział Informatyki dokona analizy zasadności, celowości i wykonalności technicznej połączenia oraz dokona w wyniku tej analizy odpowiedniej konfiguracji połączenia VPN oraz rejestracji kont pozwalających na dostęp do wnioskowanych zasobów Spółki.

Dział Informatyki Spółki zachowuje sobie prawo do stałego monitorowania stanu połączenia oraz treści komunikacji przekazywanej w obu stronach transmisji. W przypadku stwierdzenia zagrożenia dla wewnętrznych struktur informatycznych Spółki może w każdej chwili wyłączyć konta i usługi zagrażające bezpieczeństwu.

W zakresie realizowanej umowy głównej, wiążącej się z koniecznością realizacji dostępu zdalnego do systemów/usług, dostawa musi posiadać również podpisane w formie załącznika **ZASADY UDZIELENIA ZDALNEGO DOSTĘPU DO ZASOBÓW**. Jest to wewnętrzny formalny dokument pozwalający na rozpoczęcie procesu udzielenia zdalnego dostępu do zasobów (aktualny wzór wskazanego załącznika dostępny jest w Dziale Informatyki).

Wszelkie urządzenia medyczne i wspierające proces leczenia pacjentów **NIE** mają możliwości realizacji bezpośredniego i niczym nie ograniczonego dostępu do sieci zewnętrznej Internet.

9.1. PRZYJĘTY I OBOWIĄZUJĄCY STANDARD POŁĄCZENIA VPN W SZPITALACH POMORSKICH SP. Z O.O.

Połączenie IPSec o architekturze site-to-site:

Wersja: **IKEv2**

Konfiguracja:

Phase 1:

Szyfrowanie: AES-256-CBC
Autentykacja: SHA512
Diffie-Hellman Group: 20
Key Lifetime: 3600 sekund

Phase 2:

Szyfrowanie: AES-256-CBC
Autentykacja: SHA512

Diffie-Hellman Group: 20
Key Lifetime: 3600 sekund

10. SPRZĘT SERWEROWY I MACIERZOWY WYKORZYSTYWANY W SPÓŁCE

Poniżej przedstawiono minimalne parametry urządzeń typu serwery i macierze dopuszczone do pracy w infrastrukturze IT Spółki.

Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producenta, musi być nowy, wcześniej nieużywany. Urządzenia muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim. Wersja angielska dopuszczalna jest w przypadku braku dostępności wersji polskiej dokumentacji. Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp., materiały instalacyjne typu szyny, zabezpieczenia, organizery kabli itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Dział Informatyki Spółki.

Wszystkie serwery, macierze, komputery, drukarki itp. oraz urządzenia zasilane przez zasilacze pośrednie muszą posiadać oznakowanie standardu CE oraz nie mogą być w fazie End-Of-Life (EOL).

Wszystkie urządzenia zasilane przez zasilacze pośrednie muszą współpracować z siecią energetyczną o parametrach: 230V±10%, 50Hz.

Wszystkie ewentualne nazwy własne i marki handlowe urządzeń i elementów zawarte w opisie, zostały użyte w celu sprecyzowania oczekiwań jakościowych i technologicznych Zamawiającego i użyto ich jedynie w celu przykładowym.

Dopuszczone jest zastosowanie urządzeń, w których poszczególne podzespoły, bądź materiały wymienione w poniżej mogą być zastąpione urządzeniami, bądź materiałami/elementami równoważnymi. Poprzez pojęcie materiałów/elementów i urządzeń równoważnych należy rozumieć w tym wypadku materiały zapewniające uzyskanie parametrów technicznych nie gorszych od założonych w opisie poniżej. Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości i parametrów urządzenia w stosunku do przewidzianych w poniższym opisie.

Z uwagi na wdrożony oraz utrzymywany przez Zamawiającego centralny i zintegrowany system do automatyzacji zarządzania swoją infrastrukturą IT producenta HPE o nazwie OneView, wymagana jest kompatybilność oferowanego rozwiązania z tymże systemem grupowego nadzoru i zarządzania nad infrastrukturą.

W celu zagwarantowania równoważności dla tego systemu zarządzania infrastrukturą, przyjmuje się, że za równoważny system uznaje się system zarządzania, który zapewni:

- Możliwość budowania infrastruktury definiowanej programowo.
- Automatyzacja definiowana programowo dla szybszego wdrażania i zwiększanie produktywności infrastruktury IT.
- Tworzenie katalog szablonów infrastruktury zoptymalizowanych pod kątem obciążeń, dla szybszego i niezawodnego udostępniania zasobów obliczeniowych, pamięci masowej i sieci szkieletowej. Szablony te umożliwiają szybką aprowizację systemów fizycznych, wirtualnych i kontenerowych, w tym ustawień systemu BIOS, lokalnej konfiguracji macierzy RAID, linii bazowej oprogramowania układowego, udostępnionej pamięci masowej i innych. Inteligencja definiowana programowo umożliwi jednoczesne uruchamianie wielu aplikacji z powtarzalnymi szablonami, które zapewniają wysoką niezawodność, spójność i kontrolę.
- Skonsolidowany i jednolity interfejs zarządzania wspierany również dedykowanym API zapewniający ujednolicony widok kondycji serwerów, profili, obudów, pamięci masowej i sieci, monitorować kondycję całej infrastruktury i wysyłać zdefiniowane alerty.
- Jednolite źródło zarządzania aktualizacjami oprogramowania układowego i sterowników w predefiniowanych szablonach oraz zmianami konfiguracji.
- Wykorzystywanie szablonów oprogramowania opartych na kodzie, którym można w pełni opisać i skomponować wszystkie zasoby fizyczne wymagane dla aplikacji, hosta wirtualnego lub infrastruktury kontenera.

- Ujednolicony interfejs API REST w zakresie automatyzacji, zapewniając dostawcom szeroką gamę narzędzi do automatyzacji i integracji, w tym Ansible by Red Hat, PowerShell, Python, Terraform i VMware vRealize Orchestrator, Microsoft System Center Server.
- Możliwość łączenia infrastruktury definiowanej programowo z rdzenia do zasobów chmurowych poprzez udostępnianie gotowej infrastruktury chmury prywatnej ze zróżnicowanym ekosystemem partnerów.
- Obsługa resetowania i zarządzania zdalnego serwerów z wykorzystaniem technologii HPE iLO Advanced (w tym zdalny dostęp do konsoli zarządzania zasilaniem serwerów oraz dzienników zdarzeń).
- Konsola z wirtualną sesją KVM, jednocześnie rejestrująca i zapisująca wideo z ekranu do późniejszego przeglądu.
- Wsparcie dla nośników wirtualnych USB.
- Wizualizacja danych procesora, zasilania i temperatury dla serwerów z możliwością zarządzania nimi.
- Filtrowanie zdarzeń związanych z połączeniami domowymi.
- Obsługa stref równorzędnych sieci SAN dla przełączników Brocade SAN.
- Widok mapy, umożliwiający wizualizację relacji między urządzeniami, aż do najwyższych poziomów infrastruktury centrum danych.
- Inteligentne wyszukiwanie w zakresie dowolnie zdefiniowanych kryteriów (zasoby, alerty itd.).
- Wyświetlanie i filtrowanie wszystkich zadań systemowych i alertów.
- Dostęp mobilny poprzez wykorzystanie skalowalnego, nowoczesnego interfejsu użytkownika opartego na HTML5.
- Obsługa i wsparcie dla serwerów, macierzy, przełączników: HPE ProLiant, HPE Synergy, HPE BladeSystem, HPE Apollo, HPE SimpliVity, HPE Alletra, HPE 3PAR, HPE Primera, HPE Superdome i HPE Superdome Flex, HPE B-series, Brocade Fiber Channel SAN, HPE FlexFabric, Cisco Nexus/MDS.
- Implementacja logowania jednokrotnego (SSO) do HPE iLO i Onboard Administrator.
- Rejestrowanie wszystkich działań użytkownika w dzienniku inspekcji.
- Obsługiwanie opcje uwierzytelniania i autoryzacji usług katalogowych opartych na LDAP/AD.
- Zabezpieczenie systemu poprzez ograniczenie liczby otwartych portów, ograniczenie dostępu do wiersza polecenia i ograniczenie dostępu do graficznego interfejsu użytkownika
- Szyfrowanie wrażliwych danych, w tym danych pobieranych (np. zrzuty wsparcia, pliki kopii zapasowych).
- Zaimplementowany system raportowy o konfiguracji z możliwością eksportu np. do pliku Ms Excel.
- Przeglądanie i monitorowanie systemów pamięci masowej.
- Aproprowizowanie nowych lub istniejących woluminów pamięci masowej SAN dla serwerów.
- Konfigurowanie równoważenia obciążenia, nadmiarowych ścieżek danych z serwerów do woluminów pamięci masowej SAN.
- Tworzenie szablonów woluminów w celu aproprowizacji wielu woluminów o tej samej konfiguracji.
- Automatyzacja podziału na strefy sieci SAN w sieciach SAN Fiber Channel.
- Obsługa topologii sieci SAN z przełączaną siecią szkieletową i bezpośrednim dołączaniem (FlatSAN) w celu konfigurowania ścieżek danych między serwerami zarządzanymi HPE OneView, HPE 3PAR StoreServ, Alletra 9000 i StoreVirtual Storage Systems (protokoły FC lub FCoE).
- Zarządzanie sieciami brzegowymi serwerów oraz macierzy SAN.

W tym zakresie proponowane rozwiązanie sprzętowe musi współpracować w pełni (być kompatybilne w całości) z rozwiązaniem systemu zarządzania infrastrukturą HPE OneView lub równoważnym opisanym powyżej, z tym zastrzeżeniem, że Wykonawca proponując inne rozwiązanie sprzętowe, a tym samym system zarządzania infrastrukturą będzie zobowiązany do zakupu, wdrożenia i implementacji obecnej w Spółce infrastruktury serwerowo-macierzowej do nowego rozwiązania zarządzania infrastrukturą IT.

10.1. MACIERZE DYSKOWE

A. Obudowa

1. Urządzenie musi być dostarczone ze wszystkimi komponentami do instalacji w szafie RACK 19”.
2. Obudowa podstawowa o wysokości co najwyżej 4U musi zawierać co najmniej dwa kontrolery macierzowe.

B. Architektura

1. Urządzenie musi składać się z pojedynczej macierzy dyskowej zarządzanej z jednego interfejsu GUI, CLI. Za pojedynczą macierz uznaje się rozwiązanie, w którym wszystkie kontrolery są wbudowane wewnątrz w ramach jednej obudowy lub połączone poprzez przełączniki SAN, jednak rozwiązanie takie musi gwarantować zarządzanie z jednego interfejsu GUI, CLI.

2. Kontrolery macierzowe muszą wykorzystywać protokołów NVMe do komunikacji z dyskami/modułami zamontowanymi w obudowie. Zamawiający dopuszcza stosowanie wyłącznie protokołu NVMeOF do komunikacji z półkami dyskowymi podłączonymi do kontrolerów. Nie dopuszcza się zastosowania rozwiązania, które umożliwia stosowanie dysków SAS/NL-SAS/SAS-SSD.

C. Pojemność

1. Całkowita pojemność brutto (fizyczna) macierzy musi być ustalona zgodnie z oczekiwaniami danego zamówienia (w ramach którego dostarczana jest macierz) i musi być zbudowana wyłącznie w oparciu o dyski/moduły dyskowe NVMe.
2. Macierz zbudowana wyłącznie za pomocą modułów Flash NVMe musi zapewnić, aby każdy moduł Flash NVMe był odporny na awarię całego chip'a w ramach pojedynczego modułu. Awaria całego chip'a (pierwszego) nie może powodować wyłączenia modułu.
3. Wymagane jest dostarczenie określonej dla liczby dysków/modułów Flash w technologii NVMe na każdą zaoferowaną parę kontrolerów macierzowych (w zależności od realizowanego zamówienia).
4. Możliwość rozbudowy macierzy do min. 240 dysków.

D. Kontrolery macierzowe

1. Minimum 2 kontrolery pracujące w trybie active-active umożliwiającym równoczesną prezentację danego wolumenu logicznego równocześnie przez wszystkie kontrolery (również po rozbudowie do maksymalnej konfiguracji). Nie dopuszcza się macierzy pracujących w trybie asymetrycznego Active-Active (ALUA)
2. Macierz musi umożliwiać podniesienie wydajności i niezawodności poprzez rozbudowę do minimum czterech kontrolerów macierzowych pracujących w trybie active-active.
3. Każdy kontroler musi obsługiwać protokołów NVMe (Non-Volatile Memory Express).
4. Każda para kontrolerów musi obsługiwać min. 120 dysków / modułów Flash.

C. Pamięć cache

1. Macierz musi być wyposażona w co najmniej 512 GB pamięci podręcznej cache.
2. Każdy z kontrolerów macierzowych musi udostępniać co najmniej 256 GB pamięci podręcznej cache.
3. Zamawiający nie dopuszcza możliwości zastosowania dysków SSD lub kart pamięci Flash jako rozszerzenia pamięci cache.

D. Interfejsy

1. Macierz w chwili dostawy musi posiadać 8 aktywnych portów FC 32 Gb/s obsadzonych wkładkami FC 32 Gb/s.
2. Macierz w chwili dostawy musi posiadać 8 aktywnych portów iSCSI 10/25 Gb/s obsadzonych wkładkami iSCSI 10 Gb/s SR.
3. Możliwość rozbudowy do min. 48 portów FC/iSCSI.
4. Minimum 4 porty Ethernet (2 porty na kontroler) do zarządzania.
5. Minimum 4 porty 100 Gb/s (2 porty na kontroler) do komunikacji z półkami dyskowymi.
6. Porty FC muszą obsługiwać protokołów NVMe-o-F (NVMe over Fabrics).

E. Funkcje niezawodnościowe

1. Brak pojedynczego punktu awarii. Wszystkie krytyczne komponenty macierzy takie jak: kontrolery macierzowe, porty FC do serwerów, porty do dysków, pamięć podręczna cache, zasilacze i wentylatory muszą być redundantne tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu. Komponenty te muszą być wymienne w trakcie pracy macierzy (typu Hot-Swap).
2. Macierz musi cechować wsparcie dla zasilania z dwóch niezależnych źródeł prądu jednofazowego o napięciu 200-240V i częstotliwości 50-60Hz poprzez nadmiarowe zasilacze typu Hot-Swap. Macierz musi być odporna na zaniki napięcia, tzn. chwilowy zanik napięcia nie powinien przerywać pracy macierzy.

F. Sposób zabezpieczenia danych

1. Macierz musi obsługiwać RAID-6 w konfiguracji zabezpieczającej przed awarią 2 dysków / modułów Flash. Funkcjonalność musi być osiągnięta bez zastosowania dedykowanych dysków zapasowych (hot spare drives).
2. Macierz musi posiadać wbudowane sprzętowo na nośnikach dyskowych dysków/modułów Flash szyfrowanie oparte o certyfikat FIPS 140-2. Administrator musi mieć możliwość podjęcia decyzji o aktywowaniu szyfrowania.
3. Macierz musi posiadać funkcję szyfrowania danych, uniemożliwiając odczyt danych z usuniętych z macierzy dysków/modułów Flash.

G. Zarządzenie

1. Zarządzanie macierzą (tzn. zarządzanie co najmniej wszystkimi: portami We/Wy, woluminami, nośnikami NVMe, klonowaniem, replikacją) musi być realizowane z jednego interfejsu GUI, CLI niezależnie od liczby zainstalowanych kontrolerów macierzowych.
2. Macierz musi umożliwiać zarządzanie przez redundantne interfejsy Ethernet 1 Gbps i za pomocą przeglądarki internetowej protokołem HTTPS.
3. Zarządzanie musi umożliwić aktualizację daty i czasu z serwera NTP.
4. Zarządzanie musi umożliwić konfigurację wysyłania raportów serwisowych (callhome) w sposób automatyczny i regularny (np. raz na 2 dni).
5. Zarządzanie musi umożliwić konfigurację powiadomień o błędach i ostrzeżeniach do serwera SNMP.

H. Zarządzanie grupami dyskowymi oraz dyskami logicznymi

1. Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych oraz wielkości grup dyskowych (przez dodanie dysków) z poziomu kontrolera macierzowego bez przerywania pracy macierzy i bez przerywania dostępu do danych.
2. Macierz musi obsługiwać dynamiczne zwiększanie rozmiaru wolumenów (LUN) do 64 TB. Zamawiający zastrzega sobie prawo wykonania testu potwierdzającego możliwość założenia woluminu o wielkości 1 TB i zwiększanie jego rozmiaru do 64 TB, a następnie zapisania na nim danych do 100% pojemności.
3. Musi istnieć możliwość zdefiniowania, co najmniej 60 000 LUN w ramach oferowanej macierzy dyskowej.
4. Macierz musi umożliwiać rozłożenie pojedynczego dysku/woluminu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.

I. Thin Provisioning

1. Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie Thin Provisioning.
2. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Odzyskiwanie przestrzeni musi zachodzić automatycznie bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych – wymagana obsługa standardu T10 SCSI UNMAP.

J. Deduplikacja/kompresja danych

1. Macierz musi posiadać funkcjonalność deduplikacji i kompresji, którą można stosować na macierzy produkcyjnej dla wszystkich rodzajów danych.
2. Macierz musi posiadać funkcjonalność deduplikacji i kompresji danych w trybie inline bez wcześniejszego zapisywania danych na nośnikach dyskowych w formie nieskompresowanej i niezdeduplikowanej.
3. Macierz musi zapewniać kompresję i deduplikację danych na poziomie blokowym. Musi istnieć możliwość uruchomienia deduplikacji i kompresji na poziomie pojedynczych wolumenów logicznych.
4. Musi istnieć możliwość wykonania operacji odwrotnej – wyłączenia deduplikacji na określonych woluminach.
5. Możliwość zdefiniowania w macierzy woluminów korzystających równocześnie z różnych technik redukcji pojemności: thin-provisioning, deduplikacja i kompresja.

K. Wewnętrzne kopie migawkowe

1. Macierz musi umożliwiać dokonywanie na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez konieczności wcześniejszego alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 2 000 kopii migawkowych per wolumen logiczny i minimum 60 000 wszystkich kopii migawkowych.
2. Macierz musi zapewniać, że zmiana wielkości woluminu źródłowego nie wpłynie na zawartość i dostępność istniejących migawek.

L. Zdalna replikacja danych

1. Macierz musi posiadać funkcjonalność replikacji danych z inną macierzą tego samego producenta na poziomie kontrolerów (bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy). Musi istnieć możliwość jednoczesnej natywnej replikacji w trybach synchronicznym i asynchronicznym. Funkcjonalność replikacji danych musi być natywnym narzędziem macierzy.
2. Macierz musi wspierać następujące tryby replikacji zdalnej: jeden do jednego, jeden do wielu, wiele do jednego oraz replikację jednego wolumenu logicznego (tych samych danych) do dwóch innych niezależnych ośrodków za

pomocą replikacji synchronicznej i asynchronicznej. Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem oraz zamiany ról oryginału i kopii (dla określonej pary dysków logicznych LUN macierzy) z poziomu interfejsu administratora.

3. Administrator musi mieć możliwość zmiany trybu replikacji z synchronicznej na asynchroniczną i odwrotnie.

M. Migracja wolumenów logicznych

1. Macierz musi mieć możliwość wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy różnymi typami macierzy dyskowych tego samego producenta.

2. Macierz musi mieć możliwość wykonania migracji wolumenów logicznych pomiędzy różnymi typami macierzy dyskowych tego samego producenta bez zatrzymywania aplikacji korzystającej z tych wolumenów. Wymaga się, aby zasoby źródłowe podlegające migracji oraz zasoby, do których są migrowane mogły być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach.

N. Ciągła dostępność do danych

1. Macierz dyskowa musi umożliwiać pracę w trybie Metro Cluster z drugą macierzą dyskową tego samego typu w celu umożliwienia rozciągnięcia klastra VMware na dwie lokalizacje DC1 i DC2.

2. Macierz musi zapewniać możliwość zbudowania rozwiązania typu Metro Cluster w modelu Non-Uniform oraz w modelu Uniform.

3. Macierze połączone w Metro Cluster muszą pracować w trybie Active-Active z zastrzeżeniem, że każdy dystrybuowany wolumen logiczny musi być dostępny do zapisu dla dowolnego hosta znajdującego się w DC1 lub w DC2 i podłączonego lokalnie do macierzy znajdującej się w danym DC. Wszystkie zapisy do dowolnego zasobu dystrybuowanego i w dowolnej lokalizacji muszą być realizowane lokalnie, czyli bez wykorzystania połączeń DC1-DC2 między hostem a macierzą.

O. Zarządzanie wydajnością

Macierz musi umożliwiać konfigurację gwarancji wydajności typ QoS (możliwość definiowania progów minimalnych i maksymalnych) dla wybranych wolumenów logicznych w zakresie takich parametrów jak: wydajność w IOPS, wydajność w MB/s.

P. Wsparcie zarządzania operacyjnego

Możliwość dostępu przez dedykowany portal internetowy producenta do bieżących informacji dotyczących konfiguracji macierzy oraz zaleceń dla obsługiwanego przez nią środowiska pracy w tym:

- zaleceń dot. aktualizacji oprogramowania macierzy z podziałem na krytyczne oraz rekomendowane,
- analiz i obrazowania trendów dotyczących wydajności (średnich i maksymalnych wartości: MB/s, IO/s, czasu obsługi, długości kolejki) dla udostępnianych zasobów (LUNów),
- zajętości, obciążenia kontrolerów macierzy,
- analiz wydajności platformy wirtualizacji VMware na poziomie:
 - klastra (wykorzystanie CPU/RAM, serwery przeciążone),
 - serwera (Top10 serwerów wykorzystujących CPU/RAM),
 - datastore'ów (MB/s, IO/s czas realizacji operacji z rozbiem na odczyty i zapisy; historii i trendu zajętości),
 - maszyn wirtualnych (średnia: zajętość, wykorzystanie vCPU, vMEM, przepustowość MB/s oraz IO/s w rozbiem na zapisy i odczyty w ciągu ostatnich 24h, histogramu wykorzystanej pojemności, czasu obsługi ze wskazaniem składowych generowanych na serwerze i infrastruktury pamięci masowej),
 - dysku wirtualnego (przepustowość MB/s oraz IO/s w rozbiem na zapisy i odczyty w ciągu ostatnich 24h, histogramu czasu obsługi z rozbiem na zapisy i odczyty).
- analiz i monitorowania poprawności konfiguracji w kontekście predykcji potencjalnych problemów i automatycznej generacji działań naprawczych w kontekście dobrych praktyk Producenta dla oferowanego urządzenia w środowisku Zamawiającego,
- historii i bieżącego statusu zgłoszeń serwisowych.

Powyżej wymienione funkcjonalności muszą być dostępne w usłudze wsparcia. Jeżeli wyżej wymienione funkcjonalności nie są dostępne w usłudze wsparcia, należy dostarczyć platformę monitorującą oferującą takie usługi wraz z niezbędnymi licencjami oraz pulę 120 osobodni (do wykorzystania w ciągu 5-letniego okresu wsparcia) specjalisty autoryzowanego serwisu producenta na prace polegające na analizie, obserwacji i raportowaniu:

- trendów dotyczących wydajności i zajętości i obciążenia komponentów macierzy,
- poprawności konfiguracji w kontekście dobrej praktyki,

- błędów zgłaszanych przez macierz, urządzenia sieciowe, platformy wirtualizacji, systemy operacyjne, bazy danych i aplikacje biznesowe,
- podsumowania zgłoszeń serwisowych i zaleceń z ostatniego miesiąca.

R. Podłączanie zewnętrznych systemów operacyjnych

1. Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności - co najmniej dwoma ścieżkami. Macierz dyskowa musi wspierać obsługę minimum 256 hostów podłączonych poprzez sieć SAN.
2. Macierz musi wspierać podłączenie następujących systemów operacyjnych: Citrix XenServer V7.x, HP-UX 11iv3(11.31), IBM AIX 7.2, IBM Power VM VIOS 3.1.2.x, Windows 2016, 2019 i 2022, Oracle Linux 7.x i 8.x, Oracle Solaris 11.4, Red Hat Linux 7.x, 8.x i 9.x, SUSE Linux 12 i 15, VMware vSphere ESX 7.x i 8.x lub nowsze do wykorzystywania przez Zamawiającego. Informacja potwierdzająca spełnienie wymagania musi być opublikowana na ogólnodostępnej stronie internetowej.
3. Macierz musi posiadać wsparcie producenta dla następujących systemów klastrowych: Citrix HA, HP MC/Service Guard, IBM Power HA, MS Windows Failover Clustering, Oracle RAC, Oracle VM Cluster, Red Hat Cluster Server, Sun Solaris Cluster, VMware HA do wykorzystywania przez Zamawiającego. Informacja potwierdzająca spełnienie wymagania musi być opublikowana na ogólnodostępnej stronie internetowej.
4. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Preferowane jest rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. W przypadku stosowania rozwiązań firmowych/własnych – konieczna jest ich certyfikacja dla platform: Windows 2016+, RHEL 7.x+, SUSE 12+, VMware 6.5+.
5. Macierz musi obsługiwać funkcję separacji woluminów dyskowych prezentowanych przez ten sam port FC macierzy pomiędzy różnymi typami hostów.
6. Jeżeli do obsługi powyższych funkcji wymagane są dodatkowe licencje, należy je dostarczyć dla całej maksymalnej pojemności urządzenia.

S. Wsparcie VMware VVol/VASA

Macierz musi spierać specyfikację VASA 3.0 firmy VMware, bez konieczności instalacji dedykowanego plug-in lub maszyny wirtualnej, w zakresie:

- sprzętowej realizacji migawki pojedynczych maszyn wirtualnych,
- natychmiastowego i automatycznego odzyskiwania przestrzeni w przypadkach skasowania i/lub migracji maszyny wirtualnej,
- automatycznej, sprzętowej realizacji funkcji „VVols array-based thin provisioning” zastępujący programową realizację (VMware vSphere thin provisioning),
- sprzętowej realizacji funkcji „Thin deduplication” z granulacją na poziomie wybranych maszyn wirtualnych,
- sprzętowej realizacji funkcji QoS zarządzana przez „VM resource controls and Storage I/O Control” z granulacją na poziomie wybranych maszyn wirtualnych,
- rozdzielenia przestrzeni danych i snapshotów z granulacją na poziomie wybranych maszyn wirtualnych (VVol).

T. Wymagania wydajnościowe

Macierz musi zapewnić wydajność nie mniejszą niż 150 000 IOPs z włączoną deduplikacją i kompresją danych przy następującym obciążeniu:

- 70% odczytów,
- blok 8kB,
- 100% ruchu losowego,
- czas odpowiedzi < 1ms,
- trafienia w cache < 5%.

U. Fizyczne wymiary rozwiązania

W przypadku, jeśli oferowane rozwiązanie zajmuje więcej niż 4U oferent należy dostarczyć i zainstalować szafę rack 19” o wysokości 42U wraz z 2 zarządzalnymi listwami zasilania 20x13.

W. Licencje

Bezterminowe licencje na wszystkie wyżej wymienione funkcjonalności muszą być dostarczone dla maksymalnej pojemności macierzy.

X. Certyfikaty i standardy

1. Oferowana macierz musi być wyprodukowana zgodnie z normami ISO 9001:2015 i ISO 14001:2015.
2. Oferowana macierz musi posiadać deklarację zgodności CE.
3. Wszystkie wymagane certyfikaty należy załączyć do oferty.

Y. Gwarancja i serwis

1. Minimum 3-letnia gwarancja oraz usługi proaktywnego wsparcia producenta w miejscu instalacji.
2. Minimum 3-letnia gwarancja wymiany dysków SSD/modułów flash NVMe w przypadku ich uszkodzenia bez względu na przyczynę awarii
3. Serwis macierzy świadczony przez producenta macierzy w trybie 7 dni w tygodniu przez 24 godziny.
4. Kontakt z pracownikami serwisu będzie prowadzony w języku polskim przez 24 godziny na dobę.
5. Czas naprawy usterki macierzy 24 godziny od momentu zdiagnozowania problemu.
6. Zamontowane w macierzy nośniki danych pozostają w Dziale Informatyki Spółki. W szczególności dotyczy to przypadku uszkodzenia nośnika danych (dysku). Nie dopuszcza się wnoszenia poza Spółkę dysków używanych w zamawianym sprzęcie.
7. W okresie trwania gwarancji/usług wsparcia należy zapewnić prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy.

Z. Dodatkowe wymagania

Wymaga się dostarczenia urządzenia (macierzy dyskowej), gdzie części składowe zarówno sprzętowe (HW) jak i programowe (SW) powinny być opatrzone odpowiednim numerem części (PN) producenta oferowanej macierzy. Urządzenie (macierz) musi spełniać wyspecyfikowane powyżej funkcjonalności. Każda z funkcjonalności musi znaleźć swoje potwierdzenie w powszechnie dostępnej dokumentacji technicznej producenta.

10.2. SERWERY

W tym zakresie proponowane rozwiązanie sprzętowe musi współpracować w pełni (być kompatybilne w całości) z rozwiązaniem systemu zarządzania infrastrukturą HPE OneView lub równoważnym opisanym powyżej, z tym zastrzeżeniem, że Wykonawca proponując inne rozwiązanie sprzętowe, a tym samym system zarządzania infrastrukturą będzie zobowiązany do zakupu, wdrożenia i implementacji obecnej infrastruktury serwerowo-macierzowej Spółki do nowego rozwiązania zarządzania infrastrukturą IT.

A. Obudowa

Maksymalnie 4U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia).

B. Procesor

Ilość i parametry procesorów zależne są od wdrażanego zakresu systemów instalowanych w ramach infrastruktury IT Spółki. Zakłada się zastosowanie co najmniej jednego procesora szesnasto-rdzeniowego, klasy x86 - 64 bity, pracujący z częstotliwością bazową min. 3.0 GHz i osiągający w testach SPECrate2017_int_base wynik nie gorszy niż 170 punktów, dla testu oferowanego modelu serwera z 1 procesorem (Wynik testu musi być opublikowany na stronie www.spec.org). Przedstawione założenie jest parametrem minimalnym.

C. Płyta główna

Wspierająca zastosowanie procesora do 128 rdzeni, mocy do min. 360W i taktowaniu CPU do min. 4 GHz.
Płyta główna z minimum 12 slotami na pamięć i umożliwiającą instalację do minimum 3 TB pamięci RAM RDIMM.
Sloty rozszerzeń
Min. 2 aktywne gniazda PCI-Express generacji 5, x16 (szybkość slotu - bus width).
Po zainstalowaniu powyższych kart, w serwerze musi pozostać minimum 1 wolny slot PCIe 5.0 x16 pełnej wysokości, gotowy do obsadzenia dodatkową kartą.

D. Pamięć operacyjna

Min. 128GB RDIMM DDR5 4800 MT/s w modułach pamięci o pojemności min. 32GB każdy

E. Dysk twardy

Zatoki dyskowe gotowe do zainstalowania min. 16 dysków SFF typu Hot Swap, SAS/SATA/NVMe SSD 2,5".

Opcja rozbudowy/rekonfiguracji serwera o dodatkowe 8 dysków typu Hot Swap, SAS/SATA/NVMe SSD, 2,5" montowane z przodu obudowy.

Zainstalowana ilość dysków, ich rodzaj i sposób montażu zależny od konfiguracji oferowanego rozwiązania systemowego realizowanego przez wskazane urządzenie serwerowe.

Przykładowo: Zainstalowane min. 2 szt. dysków SSD 480 GB Read Intensive, typu Hot Plug oraz min. 10 szt. dysków SSD 1,92 TB Mixed Use, typu Hot Plug

F. Kontroler

Zainstalowany kontroler dyskowy wyposażony w min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60, zapewniającego obsługę min. 16 napędów dyskowych SATA/SAS/NVMe SSD.

G. Interfejsy sieciowe

Zainstalowana karta sieciowa dwuportowa 10/25Gb SFP28, wyposażona w moduły 10G SFP+ SR w każdym z portów oraz zainstalowana karta sieciowa czteroportowa 1Gb Base-T.

H. Karta graficzna

Zintegrowana karta graficzna

I. Porty

5 x USB 3.2 (w tym min. 1 port wewnętrzny)

1x VGA

Możliwość rozbudowy/rekonfiguracji o port szeregowy typu DB9/DE-9 (9-pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express

J. Zasilacz

Co najmniej 2 sztuki, typu Hot-plug, redundantne, każdy o mocy minimum 1000 W z certyfikacją Titanium lub wyższą.

K. Chłodzenie

Zestaw wentylatorów redundantnych typu hot-plug

L. Bezpieczeństwo

Serwer wyposażony w moduł TPM 2.0 oraz czujnik otwarcia obudowy.

M. Karta/moduł zarządzający

Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slotcie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:

- monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe
- praca w trybie bezagentowym - bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP
- dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub przez współdzielony port zintegrowanej karty sieciowej serwera
- dostęp do karty zarządzającej z poziomu przeglądarki webowej (GUI), z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP), z poziomu skryptu (XML/Perl), poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)
- wbudowane narzędzia diagnostyczne
- zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego
- obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie
- wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
- przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)
- obsługa zdalnego serwera logowania (remote syslog)

- wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury, z możliwością podłączenia wirtualnych napędów CD/DVD i obrazów iso.
- mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie
- funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności
- monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji
- konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)
- zdalna aktualizacja oprogramowania (firmware)
- zarządzanie grupami serwerów, w tym:
 - tworzenie i konfiguracja grup serwerów
 - sterowanie zasilaniem (wł/wył)
 - ograniczenie poboru mocy dla grupy (power capping)
 - aktualizacja oprogramowania (firmware)
 - wspólne wirtualne media dla grupy
- możliwość równoczesnej obsługi przez 6 administratorów
- autentykacja dwuskładnikowa (Kerberos)
- wsparcie dla Microsoft Active Directory
- obsługa SSL i SSH
- enkrypcja AES/3DES dla zdalnej konsoli
- wsparcie dla IPv4 oraz IPv6, obsługa SNMP v3 oraz RESTful API
- możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)

N. Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych

Zapewnia wsparcie dla:

- Microsoft Windows Server 2019, 2022
- Red Hat Enterprise Linux (RHEL) 8.x, 9.x
- SUSE Linux Enterprise Server (SLES) 15
- VMware ESXi 7.x, 8.x

O. Wsparcie techniczne

Minimum 3-letnia gwarancja producenta na części, robociznę i naprawę w miejscu instalacji typu On-Site w trybie 24/7. Możliwość zgłaszania problemów w trybie 24/7.

Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń.

Zamontowane w serwerze nośniki danych pozostają w Dziale Informatyki Spółki. W szczególności dotyczy to przypadku uszkodzenia nośnika danych (dysku). Nie dopuszczalne jest wynoszenia poza Spółkę dysków używanych w zamawianym sprzęcie.

P. Oprogramowanie

Do każdego serwera należy dostarczyć licencję Microsoft Windows Server 2022 16-core Standard Reseller Option Kit en/cs/pl/ru/sv SW (wystawiona na dane Spółki).

Licencja oprogramowania na nośniku CD/DVD lub udostępnienie oprogramowania drogą elektroniczną poprzez dostęp do strony internetowej zawierającej dane oprogramowanie. Licencja - bez ograniczeń czasowych.

Warunki licencjonowania muszą zezwalać na korzystanie oprogramowania na maszynie wirtualnej oraz na przeniesienie licencji systemu operacyjnego na inny fizyczny lub wirtualny serwer.

Dopuszczone jest stosowanie produktu równoważnego, którego funkcjonalność pokrywa się z funkcjami powyższego oprogramowania systemowego (np. w przypadku konieczności implementacji serwera dla zadań opartych o inne systemy operacyjne, np. konieczność zastosowania systemu operacyjnego rodziny Linux). W przypadku rozwiązania równoważnego wymagane jest przeprowadzenia przez wykonawcę migracji i wdrożenia oprogramowania (instalacja na wszystkich stanowiskach wskazanych przez Dział Informatyki Spółki) oraz przeprowadzenie szkolenia dla pracowników Działu Informatyki w zakresie obsługi tego oprogramowania systemowego.

Warunki równoważności dla tego zakresu określono jako:

- instalacja i użytkowanie aplikacji 32- i 64- bitowych na dostarczonym serwerowym systemie operacyjnym,
- w ramach dostarczonej licencji zawarta możliwość instalacji oprogramowania na serwerze wieloprocesorowym
- obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych)

- wielkość obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego – przynajmniej 4TB
- obsługa dostępu wielościeżkowego do zasobów LAN poprzez karty Gigabit Ethernet i szybsze, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu
- praca w roli klienta domeny Microsoft Active Directory
- zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2022
- zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP).
- zawarta możliwość uruchomienia roli serwera DNS
- zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP)
- zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory
- zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory
- zawarta możliwość uruchomienia roli serwera stron WWW
- dostępny hypervisor umożliwiający uruchamianie wirtualnych systemów w ramach zasobów sprzętowych serwera
- w ramach licencji zawarte prawo do wirtualizacji dwóch systemów na zasobach sprzętowych serwera
- w ramach licencji zawarte prawo do pobierania poprawek systemu operacyjnego
- wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów)

Używanym oprogramowaniem przez Zamawiającego w przypadkach opisanych jak powyżej Microsoft Windows Server Standard 2022, dostarczone oprogramowanie musi współpracować z oprogramowaniem obecnie posiadanym przez Zamawiającego.

Rozwiązanie równoważne musi zapewnić:

- a. Współpraca z procesorami o architekturze x86-64.
 - b. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
 - c. W ramach dostarczonej licencji zawarta możliwość instalacji oprogramowania na serwerze wyposażonym w 8 rdzeni.
 - d. Obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych).
 - e. Pojemność obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego - co najmniej 4TB.
 - f. Obsługa dostępu wielościeżkowego do zasobów LAN poprzez kontrolery Gigabit Ethernet, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) - natywnie lub z wykorzystaniem sterowników producenta sprzętu.
 - g. Praca w roli klienta domeny Microsoft Active Directory.
 - h. Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2022.
 - i. Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP).
 - j. Zawarta możliwość uruchomienia roli serwera DNS.
 - k. Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP).
 - l. Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
 - m. Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
 - n. Zawarta możliwość uruchomienia roli serwera stron WWW.
 - o. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
 - p. W ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych.
 - r. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
 - s. Wszystkie wymienione w tabeli parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Spółkę dodatkowych kosztów).
- Dopuszcza się możliwość dostarczenia oprogramowania w wersji najnowszej dostępnej na rynku.

Warunki licencji oprogramowania systemowego równoważnego w każdym aspekcie licencjonowania muszą być nie gorsze niż licencje o programowania wskazanego powyżej w stosunku do którego jest ono równoważne.
Warunki i zakres subskrypcji licencji dla oprogramowania systemowego równoważnego muszą być nie gorsze niż dla oprogramowania wskazanego powyżej w stosunku do którego jest ono równoważne.