Szpitale Pomorskie 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 SZPITALE POMORSKIE Sp. z o.o.

| Opracowanie: | Data: | Podpisy: |
|---|---|---|
| Wojciech Wrześniewski – Kierownik Działu Informatyki | 20.11.20 | KIEROWNIK Dział Informatyki i Informatyzacji Wojciech Wrześniewski |

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

**Zmiany dokumentu:**

| Lp. | Data | Imię i nazwisko | Wersja | Opis i referencja do poprzedniej wersji |
|---|---|---|---|---|
| 1 | 2020.02.07 | Wojciech Wrześniewski | 4.2 | Opracowanie |
| 2 | 2020.10.01 | Wojciech Wrześniewski | 4.3 | Doprecyzowanie zapisów punktu 8.2 i 8.3 |
| 3 | 2022.12.13 | Wojciech Wrześniewski | 4.4 | Rozszerzenie zapisów punktu 1 |
| 4 | 2024.03.25 | Wojciech Wrześniewski | 4.5 | Aktualizacja i dodanie minimalnych wymagań dla sprzętu |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |

# SPIS TREŚCI

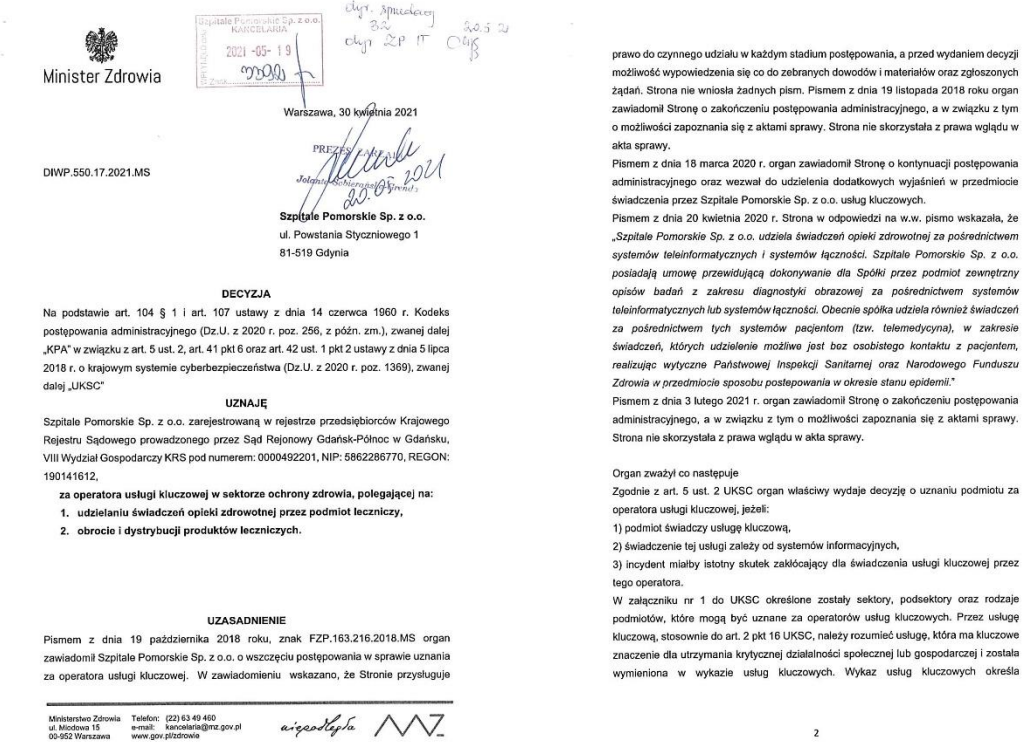
# 1. PRZEDMIOT OPRACOWANIA

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 Zamawiającym, 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.**



Minister Zdrowia

Szpitale Pomorskie Sp. z o.o. KANCELARIA 2021 -05- 19

Warszawa, 30 kwietnia 2021

DIWP.550.17.2021.MS

**Szpitale Pomorskie Sp. z o.o.**
ul. Powstania Styczniowego 1
81-519 Gdynia

**DECYZJA**

Na podstawie art. 104 § 1 i art. 107 ustawy z dnia 14 czerwca 1960 r. Kodeks 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 postepowania 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

Ministerstwo Zdrowia
ul. Miodowa 15
00-952 Warszawa

Telefon: (22) 63 49 460
e-mail: kancelaria@mz.gov.pl
www.gov.pl/zdrowia

2

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 określana 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 - Szpitale Pomorskie Sp. z o.o. świadczy usługi kluczowe, o których mowa w załączniku do rozporządzenia „Wykaz usług kluczowych oraz progi 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.



**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 skorzystania 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 Życiński
Zastępca Dyrektora
/dokument podpisany elektronicznie/



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 Zarzadzania 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:

**Szpitale Pomorskie Sp. z o.o.**
**Szpital Morski im. PCK**

**ul. Powstania Styczniowego 1**
**81-519 Gdynia**

Biuro Certyfikacji Systemów Zarządzania Polskiego Rejestru Statków S.A., al. gen. Józefa Hallera 126, 80-416 Gdańsk, zaświadcza, że 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 ZDROWOTNYCHYCH SŁUŻĄCYCH UTRZYMANIU, PRZYWRACANIU I POPRAWIE ZDROWIA, PROFILAKTYKA ZDROWIA W ZAKRESIE DZIAŁALNOŚCI LECZENICZEJ SZPITALI POMORSKICH SP. Z O.O.**

*SZCZEGÓŁOWY ZAKRES CERTYFIKACJI OKREŚLA ZAŁĄCZNIK DO NINIEJSZEGO CERTYFIKATU*

W OBSZARZE ISMS CERTYFIKAT OBOWIĄZUJE ŁĄCZNIE Z DEKLARACJĄ STOSOWANIA ED.2 Z DNIA 01.03.2019

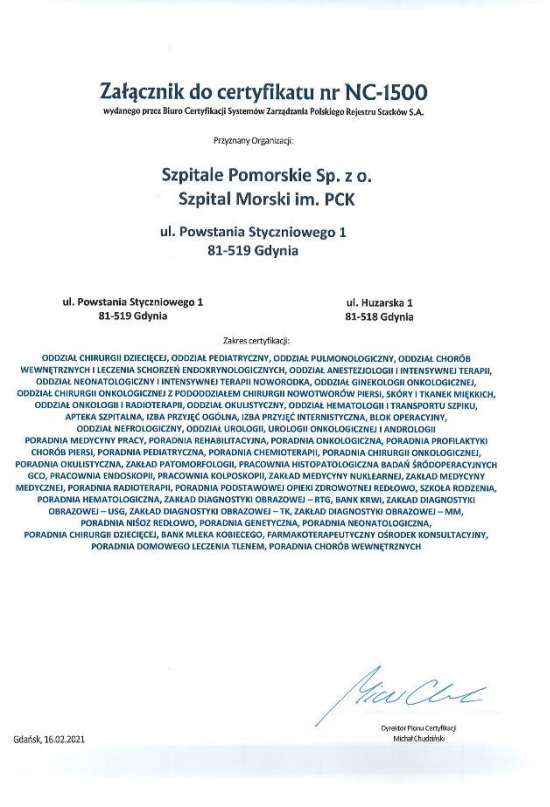
Certyfikat QMS, EMS, HSMS i ISMS jest ważny do: **15.02.2024**
Niniejszy Certyfikat unieważnia i zastępuje Certyfikat ISMS NC-1500/1 z dnia: **12.12.2020**
Certyfikat BHP jest ważny do: **30.09.2021**

Gdańsk, 16.02.2021

Dyrektor Pionu Certyfikacji
Michał Chudziński

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

www.prs.pl



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

Przyznany Organizacji:

**Szpitale Pomorskie Sp. z 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 DZIECIĘCEJ, ODDZIAŁ PEDIATRYCZNY, ODDZIAŁ PULMONOLOGICZNY, ODDZIAŁ CHORÓB WEWNĘTRZNYCH I LECZENIA SCHORZEŃ ENDOKRYNOLOGICZNYCH, ODDZIAŁ ANESTEZJOLOGII I INTENSYWNEJ TERAPII, ODDZIAŁ NEONATOLOGICZNY I INTENSYWNEJ TERAPII NOWORODKA, ODDZIAŁ GINEKOLOGII ONKOLOGICZNEJ, ODDZIAŁ CHIRURGII ONKOLOGICZNEJ Z PODODDZIAŁEM CHIRURGII NOWOTWORÓW PIERSI, SKÓRY I TKANEK MIĘKKICH, 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 MEDYCYNY PRACY, PORADNIA REHABILITACYJNA, PORADNIA ONKOLOGICZNA, PORADNIA PROFILAKTYKI CHORÓB PIERSI, PORADNIA PEDIATRYCZNA, PORADNIA CHEMIOTERAPII, PORADNIA CHIRURGII ONKOLOGICZNEJ, PORADNIA OKULISTYCZNA, ZAKŁAD PATOMORFOLOGII, PRACOWNIA HISTOPATOLOGICZNA BADAŃ ŚRÓDOPERACYJNYCH GCO, PRACOWNIA ENDOSKOPII, PRACOWNIA KOLPOSKOPII, ZAKŁAD MEDYCYNY NUKLEARNEJ, ZAKŁAD MEDYCYNY MEDYCZNEJ, PORADNIA RADIOTERAPII, PORADNIA PODSTAWOWEJ OPIEKI ZDROWOTNEJ REDŁOWO, SZKOŁA RODZENIA, PORADNIA HEMATOLOGICZNA, ZAKŁAD DIAGNOSTYKI OBRAZOWEJ – RTG, BANK KRWI, ZAKŁAD DIAGNOSTYKI OBRAZOWEJ – USG, ZAKŁAD DIAGNOSTYKI OBRAZOWEJ – TK, ZAKŁAD DIAGNOSTYKI OBRAZOWEJ – MM, PORADNIA NIŻOZ REDŁOWO, PORADNIA GENETYCZNA, PORADNIA NEONATOLOGICZNA, PORADNIA CHIRURGII DZIECIĘCEJ, BANK MLEKA KOBIECEGO, FARMAKOTERAPEUTYCZNY OŚRODEK KONSULTACYJNY, PORADNIA DOMOWEGO LECZENIA TLENEM, PORADNIA CHORÓB WEWNĘTRZNYCH**

Gdańsk, 16.02.2021

Dyrektor Pionu Certyfikacji
Michał Chudziński

Wobec powyższego niezbędne jest by wewnętrzna struktura Spółki posiadały i utrzymywały 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 proces 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 incydentem”
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 postepowania 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-: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 czołowe 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 akredytacje potwierdzający 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 prze 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 wykonywania 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. Telefonia. 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 złączowe. 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 Commericial 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 WIĄŻĄCEGO 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 Surwey"), 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 najbliższych 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 zasilić 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 oprzeć 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: zalania, 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 światłowodem 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 światłowodowy jednomodowym SM 24J-E (kategorii OS2). Dodatkowo, w celu uniewrażliwienia 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. Wszystkie 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 (kabli 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 umowa podpisana 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/kanału (Producent zagwarantuje, że łącze stałe bądź kanał transmisyjny zbudowany z jego komponentów przez okres 25 lat będzie charakteryzował się parametrami transmisyjnymi spełniającymi wymogi stawiane przez normę PN-EN 50173-1:2011 dla klasy 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 uzgodnieniem 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$^{o}$ 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 uchwytu 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 500HMz, 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 modularnym 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 kablowe zamontowane na płycie frontowej panela.
6. Uchwyty kablowe 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 kablowych (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 kablowa 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 modularnym - 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)<br>IEC 60754 część 1 i 2 (emisja gazów kwaśnych)<br>IEC 61034 część 1 i 2 (emisja dymu) |
| 2. | Konstrukcja: | 4,8,12 lub 24 włókien 9/125µm w buforze 250µm w luźnej tubie |

| OPIS: | ŚWIATŁOWÓD JEDNOMODOWY Z WŁÓKNAMI 9/125µM - KATEGORIA OS2 | | | | | |
|---|---|---|---|---|---|---|
| 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 1310nm (dB/km) | | Tłumienie 1550nm (dB/km) | | Długość fali odcięcia (nm) | |
| | < 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)<br>IEC 60754 - część 1 i 2 (emisja gazów kwaśnych)<br>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)<br>IEC 60754 - część 1 i 2 (emisja gazów kwaśnych)<br>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 blokowaną szufladę, w celu umożliwienia łatwego dostępu przy montażu modułów zatrzaskowych i ewentualnej rekonfiguracji połączeń w komfortowej odległości od szafy kablowej.
2. Mechanizm zamykania szuflady ma być zatrzaskowy, 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 ilość włókien, typie kabla, sposobie instalacji, sposobie zakończenia.
5. Wszystkie włókna światłowodowe muszą mieć strukturę ciągła 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 przeznaczonej 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 wykonującą, 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 zawiesiami, 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 Technik 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. Przyprowadzeniu tras kablowych zachować bezpieczne odległości od innych instalacji.
18. Odległości między instalacjami należy zachować zgodnie z wymogami normy EN 50174-2.
19. Zdejmowanie płaszcza/izolacji kabla i rozplatanie par przewodów wykonać zgodnie z normą EN 50174 oraz wymogami producenta.
20. Oznakowanie komponentów wykonać zgodne 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 ramkach wielokrotnych tylko poprzez odpowiednie adaptery 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 zasilić 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 ściance 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:
    a) Stojące o głębokości min. 600mm lub wiszące dwusekcyjne o głębokości min. 600mm (dobór szaf do urządzeń i lokalizacji),
    b) Szafy muszą być dostarczone w stanie złożonym, gotowym do montażu paneli oraz osprzętu.
    c) Drzwi przednie szklane, zamykane na zamek. W przypadku zlokalizowania szafy w miejscach ogólnodostępnych: drzwi metalowe, zamykane na zamek.
    d) Możliwość otwierania na lewą/prawą stronę (możliwość przełożenia drzwi).
    e) Drzwi tylne pełne (w zależności od potrzeby osłony tylne perforowane).
    f) Regulowane stopki (w przypadku szaf stojących).
    g) Pełne uziemienie wszystkich sekcji szafy.
    h) Panel wentylacyjny sufitowy z termostatem (minimum 4 wentylatory).
    i) Przepusty kablowe od góry i od dołu ze szczotkowym przepustem kablowym,
    j) Rama rack z przodu i z tyłu.
    k) Organizery pionowe i poziome pomiędzy panelami krosowymi dla LAN dostępowego (co dwa panele krosowe).
    l) Listwy zasilająca jednofazowe, co najmniej 9 gniazd 230V (standard PL) bez bezpiecznika, podłączone do zamontowanego w szafie UPS.
    m) 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 Ablerex 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 wyłączania 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 potrzymania 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 – Parametry minimalne

| Kategoria | Wymagania |
|---|---|
| 1. Architektura | 1) Budowa modułowa umożliwiająca szybką i sprawną naprawę przez wymianę modułu<br>2) Topologia pracy – podwójna konwersja, VFI<br>3) Konfiguracja faz napięć we/wy - 3/3<br>4) Tolerancja napięcia wejściowego (praca normalna) - +/- 15%<br>5) Wejściowy współczynnik mocy dla 50% obciążenia - >=0,95<br>6) Wejściowy współczynnik mocy dla 100% obciążenia - >=0,98<br>7) Sprawność AC-AC dla obciążenia w zakresie 50-100% - (>=95%)<br>8) Zniekształcenia prądu wejściowego - <5%<br>9) Kształt prądu wejściowego - sinusoidalny<br>10) Możliwość współpracy z generatorem prądotwórczym – In <Ir<br>11) Znamionowa moc wyjściowa (VA / W) – wg wymagań podstawowych<br>12) Znamionowe napięcie wyjściowe - 3*400VAC<br>13) Znamionowa częstotliwość wyjściowa - 50Hz<br>14) Kształt napięcia wyjściowego - sinusoidalny<br>15) Odkształcenie napięcia wyjściowego dla obciążenia liniowego, symetrycznego - <=2%<br>16) Możliwość przeciążenia w czasie 60 sekund - >=150%<br>17) Dopuszczalny współczynnik szczytu obciążenia - >=3:1<br>18) Wbudowany automatyczny układ obejściowy |
| 2. Baterie | 1) Czas podtrzymania: min. 12 min.<br>2) Akumulatory umieszczone na stelażu lub w szafie<br>3) Projektowana żywotność akumulatorów wg Eurobat >=10 lat<br>4) Musi być zapewniona:<br>a) funkcja nieciągłego ładowania akumulatorów<br>b) temperaturowa kompensacja napięcia ładowania akumulatorów<br>c) automatyczny test baterii |
| 3. Obsługiwane protokoły | 1) HTTP, HTTPS, IPv4, NTP, SMTP, SNMP v1, SNMP v2c, SNMP v3 |
| 4. Zarządzanie | 1) Oprogramowanie zarządzające z możliwością zamykania systemów operacyjnych poprzez sieć logiczną: rodzina systemów Windows Server (w najnowszej utrzymywanej w Spółce wersji), Microsft Hyper-V (w najnowszej utrzymywanej w Spółce wersji), WMware ESXi, VMware ESX (w najnowszej utrzymywanej w Spółce wersji), rodzina systemów Linux: Debian, Red Hat Enterprise Linux, Ubuntu Linux, SuSE Linux Enterprise Server (w najnowszej utrzymywanej w Spółce wersji).<br>2) Moduł zarządzający WEB/SNMP - Możliwość diagnostyki UPSa<br>3) Powiadamianie o zdarzeniach przez e-mail<br>4) Zintegrowany z zasilaczem układ do pomiaru warunków środowiskowych w serwerowi – temperatury, z możliwością zdalnego odczytu i sygnalizacji.<br>5) Jeden port 10/100 TBase do nadzoru<br>6) Możliwość podłączenia wyłącznika awaryjnego<br>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 |

| Kategoria | Wymagania |
|---|---|
| | 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 | 1) Stopień ochrony IP20<br>2) Wyświetlacz LCD z komunikatami w języku polskim |
| 6. Jakość wytwarzania | 1) Musi posiadać zgodność z normami CE - należ dostarczyć certyfikat |
| 7. Wymagania dodatkowe | 1) Zaoferowany UPS musi być fabrycznie nowy i musi pochodzić z oficjalnego kanału sprzedaży na rynek polski.<br>2) Ponadto należy wykonać:<br>a) końcowe obwody zasilające szafy teletechniczne<br>b) wykonanie zewnętrznego bypassu serwisowego, który umożliwi bezprzerwowe przełączenie zasilania z pominięciem dostarczonego zasilacza na czas wykonywania czynności serwisowych.<br>c) dostarczenie i zainstalowanie wyłącznika p.poż. dla oferowanego zasilacza awaryjnego |

## 3.5.4. SYSTEM KONTROLI DOSTĘPU (SKD), SYSTEM SYGNALIZACJI WŁAMANIA i NAPADU (SSWiN), SYSTEM PPOŻ (SSP), AUTOMATYCZNEGO GASZENIA POŻARU (SUG), SYSTEM TELEWIZJI DOZOROWEJ (CCTV)

### 3.5.4.1. SYSTEM KONTROLI DOSTĘPU (SKD)

1. System SKD musi obsługiwać karty zbliżeniowe w standardzie MIFARE oraz Mifare DesFire.
2. System SKD musi obsługiwać karty zbliżeniowe Dualne/Hybrydowe, zawierające warstwę zbliżeniową w standardzie MIFARE Classic, MIFARE DesFire, oraz warstwę stykową (SmartCard) obsługującą standard dla certyfikatów systemu Microsoft PKI (x509).
3. Dostarczone karty muszą być białe, przygotowane do personalizacji metodą nadruku warstwy personalizującej, dedykowaną drukarką użytkownika końcowego.
4. System SKD musi umożliwiać integrację z systemem SSWiN w zakresie sygnalizacji naruszeń jak siłowe wejście, użycie przycisku wyjścia ewakuacyjnego, naruszenie instalacji (otwarcie obudowy kontrolera lub modułu rozszerzeń, naruszenie linii sabotażowych, etc.).
5. System SKD musi umożliwiać dwukierunkową integrację z systemem SSWiN w zakresie uzbrajania i rozbrajania stref i partycji w systemie alarmowym, skojarzonych ze wskazanymi czytnikami.
6. System SKD musi realizować komunikację pomiędzy kontrolerami a stacją administracyjną, poprzez sieć IP.
7. System SKD musi współpracować z posiadanymi i wykorzystywanymi przez Spółkę systemami SSWiN i SKD, w tym wykorzystywać posiadane rozwiązania w zakresie monitoringu i zarządzania elementami systemu. Dokładne informacje o wykorzystywanych obecnie systemach, dostępne są do wglądu w siedzibie Spółki (po kontakcie z Działem Informatyki). Obejmuje on swoim zasięgiem PPD, serwerownie oraz wskazane pomieszczenia Działu Informatyki Spółki. System powinien być objęty integracją z innymi systemami kontroli i nadzoru technicznego (systemem KD, SSWiN, PPOŻ, CCTV, system SUG, systemami klimatyzacji).
8. System SKD powinien być zdolny do obsługi minimum 1000 kart zbliżeniowych oraz minimum 300 przejść dwustronnych. Przejścia jednostronne należy wyposażyć w kontroler z czytnikiem kart magnetycznych oraz elektrozaczep z wbudowanym czujnikiem otwarcia.
9. System SKD musi posiadać własne zasilanie buforowe, gwarantujące pracę systemu wraz z obsługą pełnej funkcjonalności wszystkich przejść, przez okres minimum 48 godzin, od zaniku zasilania podstawowego.
10. System SKD musi wspierać zamki elektromechaniczne. 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).
11. System SKD musi zostać dostarczony z kompletem licencji, pozwalających na obsługę wszystkich przejść, zgodnie z aranżacją zawartą w dokumentacji dostępnej do wglądu w siedzibie Spółki, w tym licencji do zarządzania lokalnie i zdalnie każdym z przejść ze stanowiska centralnego administratora, jeżeli takie licencje będą niezbędne.
12. System SKD musi wspierać moduł rejestracji czasu pracy dla minimum 1000 użytkowników/kart w systemie.

13. System SKD musi zostać dostarczony z czytnikami z klawiszami funkcyjnymi, umożliwiającymi obsługę funkcji RCP (minimum: wejście, wyjście, wyjście służbowe).
14. System SKD musi wpierać mechanizm blokady wielokrotnego wejścia z czasowym resetem (Timed Anti-passback).
15. System SKD musi wpierać mechanizm parowania drzwi w tzw. śluzę (blokada sparowanych drzwi).
16. System SKD musi posiadać minimum 8 sterowalnych wyjść per kontroler, w tym 2 wyjścia przekaźnikowe dla urządzeń typu zamek, rygiel, sygnalizator akustyczno/optyczny, z możliwością dalszej rozbudowy liczby wejść i wyjść przez dodatkowe moduły.
17. System SKD musi wspierać minimum następujące nośniki dla jednego identyfikatora: odcisk palca, karta MIFARE w tym karta MIFARE DesFire z kluczami do 4k, pin.
18. System SKD musi posiadać bufor zdarzeń w każdym kontrolerze, zdarzenia powinny być zapisywane na wymiennym nośniku – np. wymiennej karcie pamięci, tak aby możliwe było ich odczytanie w razie awarii kontrolera.
19. Systemu powinien posiadać interfejs Ethernet, do komunikacji w sieci IPv4.
20. Każdy kontroler powinien posiadać wbudowany zasilacz impulsowy, z modułem zasilania buforowego.
21. Komunikacja w obrębie kontrolerów oraz pomiędzy kontrolerem a stacją zarządzającą, powinna być szyfrowana.
22.Kontrolery powinny umożliwiać upgrade firmware, zmianę licencji, zmianę liczby obsługiwanych drzwi, w zależności od potrzeb i zmian zachodzących w Spółce.
23. Kontrolery systemu SKD powinny umożliwiać aktualizację ich ustawień w tym import danych o kartach i uprawnieniach, bez przerywania pracy bieżącej (brak wstrzymywania obsługi przejść na czas wysyłania nowych danych do kontrolerów).
24. System SKD powinien umożliwiać odczyt numeru seryjnego karty zbliżeniowej (CSN), oraz odczyt numeru programowalnego (PCN) zapisanego w szyfrowanym sektorze pamięci karty.
25. System SKD powinien umożliwiać rozpoznanie tzw. „długiego przyłożenia karty".
26. Czytniki systemu SKD powinny być wyposażone w obwód sabotażowy, w tym w TAMPER, sygnalizujący zdemontowanie lub manipulowanie czytnikiem.
27. Obudowy wszystkich modułów i zasilaczy, powinny być wyposażone w linie i czujniki sabotażowe.
28. Jeżeli do licencji lub oprogramowania dostarczonego z systemem, niezbędny jest klucz sprzętowy, należy go dostarczyć w ramach niniejszego Zamówienia.
29. Wraz z dostawą urządzeń systemu SKD i niezbędnym oprogramowaniem, należy dostarczyć dwa nabiurkowe czytniki dla administratorów systemu, obsługujące karty dostarczone w ramach niniejszego Zamówienia,
30. Wraz z dostawą kontrolerów, należy dostarczyć wymienne nośniki pamięci dla tych kontrolerów, zgodnie z niniejsza specyfikacją.
31. Wraz z dostawą systemu SKD należy dostarczyć drukarkę oraz oprogramowanie do personalizacji kart plastikowych z warstwą elektroniczną oraz materiały eksploatacyjne, do drukarki, zgodnie z poniższą specyfikacją:
a) Rodzaj druku: monochromatyczny (termotransferowy), kolorowy (sublimacyjny)
b) Typ wydruku: jednostronny
c) Rozdzielczość drukowania: minimum 300dpi
d) Automatyczny podajnik kart o pojemności minimum 100 kart
e) Prędkość wydruku: druk monochromatyczny minimum 400 kart / godzinę, druk kolorowy minimum 150 kart na godzinę
f) Zdolność drukowania kodów i symboli: minimum 1D i 2D
g) Obsługa kart zgodnych z ISO 7811, JIS Type II
h) Zadruk karty w trybie od krawędzi- do krawędzi
i) Wbudowana pamięć minimum 128MB
j) Interfejs: minimum USB
k) Wbudowana lub rozbudowana poprzez dodatkowe moduły funkcjonalność kodowania kart chipowych oraz kart zbliżeniowych
l) Wraz z drukarką należy dołączyć oprogramowanie do projektowania strony graficznej karty, sterowniki oraz oprogramowanie wykonawcze do drukarki dla systemu Windows 10/11, obsługujące wydruk, personalizację o raz wgrywanie danych na karty zbliżeniowe i chipowe.
m) W zestawie powinny znaleźć się: drukarka, niezbędne rozszerzenia dodatkowych funkcji, zestaw materiałów eksploatacyjnych, niezbędnych do zadruku 1000 kart w kolorze i 500 kart w druku monochromatycznym, zasilacz, niezbędne okablowanie, akcesoria czyszczące, nośniki z oprogramowaniem.
n) Gwarancja na minimum 24 miesiące.

32. W przypadku montażu zamków elektromechanicznych dla szaf RACK, należy wycenić i wykonać instalację kablową, oraz wycenić i wykonać dostawę dodatkowego kontrolera i zasilacza. Całość prac dotyczących szaf RACK będzie wykonana w obrębie jednego wskazanego pomieszczenia.
33. Kontroler dostępu oraz automatyki budynkowej – Spółka 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.
34. Czytniki zbliżeniowe są wewnętrznymi terminalami dostępu przeznaczonymi do pracy w systemie kontroli dostępu (preferowany system to system zgodny z posiadanym przez Spółkę 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 odpornego 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.

35. System kontroli dostępu swoim zakres 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 zasilić zasilaczem impulsowym 12V (np. PSA 12015).
36. Czytniki zbliżeniowe (np. Mifare PRT66MF) mogą być wykorzystywany jako terminale podłączone do nadrzędnego kontrolera lub być skonfigurowany 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 informacja przekazaną przez Spółkę.

A. 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 dołączenie ekspandera we/wy typu XM-2;
   - możliwość dołączenie dodatkowego czytnika serii PRT (obustronna kontrola przejścia);
   - programowanie manualne lub z komputera;
   - kontakt antysabotażowy: kontakt NC, 50mA/24V, IP67;

B. Preferowany model i parametry elektrozaczepu:
   - model YS18NO12D YOTOGI;
   - symetryczny;
   - radialny: specjalna konstrukcja radialna, promieniowa mechanizmu języka elektrozaczepu powoduje otwarcie przy minimalnym wychyleniu. Umożliwia to montaż elektrozaczepu 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.

### 3.5.4.2. SYSTEM GASZENIA MUSI BYĆ OPARTY O GASZENIE GAZEM (SUG)

Należy zastosować Stałe Urządzenie Gaśnicze oparte o niskie ciśnienie tzn max 50 bar. Na etapie Projektu Wykonawczego należy przeanalizować konieczność instalacji klapy odciążającej oraz instalacji przewietrzania. Przed oddaniem SUG do użytkowania przeprowadzić test szczelności pomieszczenia. Butle należy montować w bezpośredniej bliskości serwerowni lub jeżeli będzie miejsce w serwerowni.

Wymagania:

1. Gaz przeznaczony do gaszenia pracujących urządzeń elektronicznych.
2. Sterowanie przy pomocy wydzielonej zainstalowanej w pomieszczeniu centrali.
3. Centrala musi zostać skomunikowana z centralą ogólnobudynkową (jeśli istnieje).
4. Przycisk STOP min 1 szt.
5. Przycisk START min 1 szt.
6. Pomieszczenie uszczelnić ppoż.
7. Zamontować samozamykacz na drzwiach.
8. Wzmocnić okna jeżeli będzie taka potrzeba.

9. Gaz o potencjale niszczenia warstwy ozonowej (ODP=1).
10. Gaz o potencjale efektu cieplarnianego (GWP=1).
11. System musi posiadać certyfikat CNBOP i znak CE.
12. System umożliwiający monitoring z jednej konsoli dla wszystkich placówek szpitalnych Spółki.
13. System powinien być objęty integracją z innymi systemami kontroli i nadzoru technicznego (systemem KD, SSWiN, PPOŻ, CCTV, system SUG, systemami klimatyzacji).
14. System powinien być zintegrowany z budynkowym i obiektowym systemem powiadamiania pożarowego Spółki.

### 3.5.4.3. SYSTEM SYGNALIZACJI WŁAMANIA i NAPADU (SSWIN)

1. System SSWiN powinien spełniać wymagania norm serii EN50131 dla urządzeń spełniających wymagania Grade 3.
2. Centrala alarmowa powinna być wyposażona we własny zasilacz buforowy, z diagnostyką awarii i problemów z zasilaniem.
3. Centrala powinna obsługiwać minimum 256 wejść z parametryzacją rezystorową, w tym z parametryzacją 3EOL.
4. System powinien umożliwiać rozbudowę wyjść do łącznej ich liczby 256 wyjść.
5. Centrala powinna umożliwiać podział systemu SSWiN minimum na 24 strefy i 8 partycji.
6. Centrala powinna być wyposażona w pamięć zdarzeń, z możliwością zarejestrowania minimum 18 tyś zdarzeń.
7. Centrala powinna umożliwiać obsługę minimum 120 standardowych użytkowników.
8. Centrala powinna umożliwiać upgrade firmware.
9. Centrala powinna umożliwiać podłączenie minimum 12 manipulatorów w tym obsługę manipulatorów wirtualnych.
10. System SSWiN należy wyposażyć w czujki pasywne PIR oraz czujki dualne PIR, zgodnie z dokumentacją i aranżacją, jaka dostępna jest do wglądu w siedzibie Spółki (po uprzednim kontakcie z Działem Informatyki).
11. Czujki powinny spełniać wymagania klasy Grade 3, oraz wspierać parametryzację linii.
12. System SSWiN należy wyposażyć w manipulatory z wyświetlaczem LCD, podświetlaną klawiaturą. Poprzez manipulator możliwe musi być sterowanie systemem, sprawdzenie i sygnalizacja stanu systemu lub poszczególnych stref, wezwanie pomocy lub włączenie alarmu napadowego.
13. System SSWiN należy wyposażyć w jeden manipulator z dużym wyświetlaczem dotykowym, umożliwiającym przegląd stanu sytemu, sterowanie systemem, konfigurowaniem i/lub uruchamianiem złożonych akcji (makr) w systemie przy pomocy panelu graficznego.
14. System SSWiN powinien zostać wyposażony w minimum jeden moduł komunikacji IP, pozwalający na zdalne monitorowanie i zarządzanie systemem z centralnej stacji administracyjnej.
15. System SSWiN powinien poprzez odpowiedni moduł i/lub oprogramowanie, umożliwiać centralne zarządzanie wieloma systemami rozporoszonymi geograficznie. Szczegóły tych systemów są do wglądu w siedzibie Spółki.
16. System SSWiN poprzez moduł komunikacji IP, powinien umożliwiać wysyłanie wiadomości email, oraz sterowanie systemem alarmowym poprzez dedykowane aplikacje na urządzenia mobilne, przy zachowaniu szyfrowanego kanału komunikacji.
17. Wraz z systemem SSWiN należy dostarczyć niezbędne licencje i oprogramowanie do zdalnego zarządzania obecnie wykorzystywanymi oraz systemem dostarczonym w ramach niniejszego postępowania, z wykorzystaniem sieci IPv4.
18. System SSWiN musi zostać dostarczony wraz z modułem komunikacji SMS/GPRS obsługującego dwie karty SIM dla dwóch różnych operatorów. Moduł ten powinien umożliwiać wysyłanie programowalnych komunikatów alarmowych/informujących o stanie lub istotnych zmianach w systemie poprzez krótkie wiadomości tekstowe lub transmisję GPRS. System powinien umożliwiać obsługę minimum 4 komunikatów zgłaszanych przez centralę alarmową (brak zasilania, sabotaż, alarm, powrót zasilania), Karty SIM do systemu dostarczy Spółka.
19. System SSWiN powinien zostać dostarczony wraz z wyniesionym modułem komunikacji szyfrowanej, oraz niezbędnym modułem rozszerzeń wej/wyj, w celu podłączenia do systemu oddalonego pomieszczenia., znajdującego się w siedzibie Spółki. W pomieszczeniu tym należy zamontować 2 czujki dualne, zestaw kontaktronów dla drzwi, sygnalizator akustyczno-optyczny, oraz manipulator do obsługi strefy. Szczegółowe informacje dostępne są do wglądu w siedzibie Spółki.
20. System SSWiN powinien zostać dostarczony wraz z drukarką zdarzeń, spełniającą poniższe wymagania:
    a) drukarka przystosowana do pracy w pionie (wisząca na ścianie)
    b) drukarka z dwukierunkowym drukiem termicznym
    c) ruchoma ośmio-punktowa głowica (matryca znaku 8x8 punktów)

d) szybkość wydruku minimum 0,5 wiersza/s
e) liczba znaków w wierszu: 40, 80
f) interfejs odpowiedni dla komunikacji z centralą alarmową (RS232, RS485, RS422, etc)
g) sprzętowy protokół transmisji z DTR
h) warunki pracy 5-35% stopni Celsjusza przy wilgotności względnej 10-80% bez kondensacji
i) drukarka w komplecie z zasilaczem i kablem interfejsowym
j) rozmiar papieru termicznego – rolki dedykowane drukarce, o długości papieru minimum 20m

21. Wraz z drukarką należy dostarczyć 20 rolek papieru termicznego do drukarki
22. Wraz z systemem SSWiN i SKD należy dostarczyć układ zdalnego sterowania, do otwierania drzwi na poziomie recepcji/sekretariatu (dwa moduły, każdy z dwoma jednokanałowymi pilotami radiowymi ze zmiennym kodem) – jeśli tego zakresu inwestycji dotyczy realizacja przedsięwzięcia (ustalane na etapie inwestycji z Działem Informatyki Spółki). Otwieranie przejścia z użyciem pilota, powinno się odbywać poprzez system alarmowy, tak aby możliwe było wyłączenie jego obsługi po godzinach funkcjonowania recepcji/sekretariatu.
23. System SSWiN powinien zostać dostarczony z niezbędnymi modułami, zasilaczami i akumulatorami, gwarantującymi bezprzerwową pracę systemu, przy zachowaniu pełnej funkcjonalności przez okres minimum 72h od momentu zaniku zasilania podstawowego.
24. System SSWiN musi posiadać 24h linie sabotażowe i linie alarmowe dla ochrony elementów systemu SKD, systemu SSWiN oraz systemu CCTV. Szczegóły rozwiązania dostępne są do wglądu w siedzibie Spółki.
25. Urządzenia i szafki/skrzynki osprzętu SSWiN powinny zostać wyposażone w tampery sygnalizujące próbę demontażu i otwarcia szafek.
26. Należy zastosować minimum jedną (jedna na każdej kondygnacji w przypadku wielu pięter najmowanej powierzchni) zewnętrzną syrenę z sygnalizacją optyczno-dźwiękową, z podtrzymaniem, w klasie Grade 3.
27. Należy zastosować jedną zewnętrzną syrenę z sygnalizacją optyczno-dźwiękową, z podtrzymaniem, w klasie Grade 3.
28. Należy zaplanować sygnalizację dźwiękiem zwłoki potrzebnej do uzbrojenia i rozbrojenia systemu plus sygnalizacja na wskazanym czytniku SKD stanu strefy wewnątrz powierzchni Spółki (nie należy sygnalizować żadnych funkcji systemu SSWiN na czytnikach zewnętrznych).
29. W systemie SSWiN w module powiadomień mailowych oraz SMS należy zaprogramować minimum następujące powiadomienia (zakres należy każdorazowo ustalić z Działem Informatyki Spółki):

- brak zasilania
- powrót zasilania
- cichy alarm + linia dozorowa/sabotażowa
- głośny alarm + linia dozorowa/sabotażowa
- użycie przycisku ewakuacyjnego + nr/opis drzwi
- wejście siłowe + nr/opis drzwi
- awaria akumulatora/systemu
- należy uruchomić powiadomienia dla alarmu z systemu CCTV (np. zanik kamery, brak zasilania, nieprawidłowe hasło, awaria rejestratora)
- informację o otwarciu drzwi systemu SKD przez sygnał z systemu ppoż budynku.

30. System Sygnalizacji Włamania i Napadu instalowany będzie w pomieszczeniu chronionym.
31. System umożliwiający zarządzanie z jednej konsoli dla wszystkich placówek szpitalnych Spółki.
32. System powinien być objęty integracją z innymi systemami kontroli i nadzoru technicznego (systemem KD, SSWiN, PPOŻ, CCTV, system SUG, systemami klimatyzacji).

### 3.5.4.4. SYSTEM TELEWIZJI DOZOROWEJ (CCTV)

1. Dostawa ma obejmować kompletny i działający system telewizji dozorowej, na podstawie zatwierdzonego przez Spółkę projektu wykonawczego zrealizowanego wg poniższych wytycznych. Oczekiwane jest oznaczenie stref monitorowanych przez CCTV w sposób estetyczny, widoczny i czytelny (uzgodniony z Działem Informatyki Spółki), za pomocą odpowiednich znaków graficznych, przed wejściami do każdej z tych stref.
2. W ramach realizacji należy dostarczyć odpowiednie kamery w liczbie określonej na etapie projektowania.
3. Spółka oczekuje dostawy kamer zgodnych z poniższą specyfikacją (w zależności od ustaleń projektowych):

<u>- Kamera typu A – kamera identyfikacyjna</u>

a) Przetwornik 1/2.5” lub 1/2.9” lub 1/3” STARVIS CMOS, minimum 8MPx
b) Obsługa kompresji wideo w standardzie H.264, H265, MJPEG
c) Obsługa rozdzielczości: 8MPx, 6MPx, 4MPx, 2MPx
d) Obsługa minimum 2 strumieni video, przy jednoczesnym spełnieniu wymagań:
- strumień podstawowy (pierwszy) minimum 1-15kl/s (fps) przy rozdzielczości 8MPx

- strumień dodatkowy (drugi i kolejny) minimum 1-20kl/s (fps) przy rozdzielczości D1/CIF

e) Automatyczny balans bieli (AWB) z możliwością wyboru trybu ręcznego lub automatycznego

f) Automatyczna kontrola wzmocnienia sygnału (AGC) z możliwością wyboru trybu ręcznego lub automatycznego

g) Cyfrowa redukcja szumów (DNR / 2DNR / 3DNR)

h) Stosunek szumu do sygnału na poziomie nie gorszym niż 50dB (S/N >50dB)

i) Kompensacja światła tła (BLC)

j) Mechaniczny filtr podczerwieni (ICR)

k) Sprzętowa regulacja dynamiki w szerokim zakresie 120dB (WDR)

l) Automatyczna kompensacja balansu bieli (ATW)

m) Elektroniczna stabilizacja obrazu dla sieci 50Hz (EIS)

n) Kompensacja światła punktowego, np. reflektora, latarki, etc. (HLC)

o) Migawka o parametrach nie gorszych niż 1/3-1/100000s, z możliwością wyboru trybu ręcznego lub automatycznego, z zabezpieczeniem przed migotaniem dla sieci 50Hz

p) Obiektyw regulowany z motozoom 2,8-12mm

q) Czułość dla trybu nocnego (włączony IR) na poziomie 0 Lux

r) Promiennik podczerwieni o zasięgu skutecznym min. 30m, na diodach mocy (tzw. 3-ciej generacji)

s) Funkcje inteligentnej analizy obrazu i otoczenia, minimum w zakresie:

- przekroczenie zdefiniowanej przez użytkownika linii
- detekcja intruza w obserwowanej przestrzeni
- pozostawienie lub zaginięcie obiektu w obserwowanej przestrzeni
- obrót lub lustrzane odbicie obrazu
- wykrycie twarzy
- detekcja audio
- obsługa stref prywatności

t) Zgodność z sieciowym standardem ONVIF

u) Liczba klatek na sekundę: minimum 15kl/s (fps) dla rozdzielczości 8MPx, minimum 20kl/s (fps) dla rozdzielczości 6MPx, minimum 25kl/s (fps) dla rozdzielczości 4MPx.

v) Kamera z obsługa kart SD – każda kamera powinna być wyposażona w złącze micro-SD lub SD obsługujące karty do 128GB, każda kamera typu A powinna być wyposażona w kartę SD o pojemności minimum 128GB.

w) Kamera z obsługą funkcji nagrywania na karcie SD w przypadku zaniku rejestratora, lub problemów z komunikacją sieciową (możliwość lokalnej rejestracji obrazu na wymienialnej pamięci).

x) Wbudowany serwer WWW do obsługi i konfiguracji kamery.

y) Obsługa wielu użytkowników, wraz z mechanizmami gradacji uprawnień dla tych użytkowników, w tym możliwość zdefiniowania minimum 6 użytkowników z różnymi uprawnieniami

z) Wejście audio – 1 kanał

aa) Wyjście audio – 1 kanał

bb) Zasilanie PoE zgodne z 802.3af

cc) Interfejs sieciowy RJ45 – Ethernet o przepustowości minimum 10/100Mbits

dd) Obsługa: IPv4, HTTP, HTTPS, SSL, TCP/IP, UDP, ICMP, IGMP, SNMP, NTP, DHCP, DNS, FTP, 802.1x,

ee) Uchwyt 3D modułu kamery wewnątrz obudowy, pozwalający na precyzyjna regulację kąta widzenia oraz obserwowanego obszaru

ff) Klasa odporności na wandalizm – IK10

gg) klasa szczelności – minimum IP65

hh) Ze względu na montaż na suficie podwieszanym:

- waga poniżej 1kg
- do każdej kamery należy dostarczyć odpowiedni zestaw montażowy (kamera montowana nawierzchniowo)

<u>- Kamera typu B – kamera korytarzowa</u>

a) Przetwornik 1/2.5” lub 1/2.9” lub 1/3” progressive scan CMOS, minimum 4MPx

b) Obsługa kompresji wideo w standardzie H.264, MJPEG

c) Obsługa rozdzielczości: 4MPx, 2MPx

d) Obsługa minimum 2 strumieni video, przy jednoczesnym spełnieniu wymagań:

- strumień podstawowy (pierwszy) minimum 1-20kl/s (fps) przy rozdzielczości 8MPx
- strumień dodatkowy (drugi i kolejny) minimum 1-20kl/s (fps) przy rozdzielczości D1/CIF

e) Automatyczny balans bieli (AWB) z możliwością wyboru trybu ręcznego lub automatycznego

f) Automatyczna kontrola wzmocnienia sygnału (AGC) z możliwością wyboru trybu ręcznego lub automatycznego
g) Cyfrowa redukcja szumów (DNR / 2DNR / 3DNR)
h) Stosunek szumu do sygnału na poziomie nie gorszym niż 50dB (S/N >50dB)
i) Kompensacja światła tła (BLC)
j) Mechaniczny filtr podczerwieni (ICR)
k) Sprzętowa regulacja dynamiki w szerokim zakresie 120dB (WDR)
l) Automatyczna kompensacja balansu bieli (ATW)
m) Elektroniczna stabilizacja obrazu dla sieci 50Hz (EIS)
n) Obsługa stref prywatności (możliwość zdefiniowania minimum 4 stref)
o) Obiektyw regulowany z motozoom 2,8-12mm
p) Czułość dla trybu nocnego (włączony IR) na poziomie 0 Lux
q) Promiennik podczerwieni o zasięgu skutecznym min. 30m, na diodach mocy (tzw. 3-ciej generacji)
r) Funkcje inteligentnej analizy obrazu i otoczenia, minimum w zakresie:
- przekroczenie zdefiniowanej przez użytkownika linii
- detekcja intruza w obserwowanej przestrzeni
- pozostawienie lub zaginięcie obiektu w obserwowanej przestrzeni
- obrót lub lustrzane odbicie obrazu
- wykrycie twarzy
s) Zgodność z sieciowym standardem ONVIF
t) Funkcja korytarzowa – funkcja zmiany kadrowania, umożliwiająca lepszą obserwację/monitoring długich i wąskich przejść
u) Liczba klatek na sekundę: minimum 20kl/s (fps) dla rozdzielczości 4MPx, minimum 25kl/s (fps) dla rozdzielczości 4MPx
v) Kamera z obsługą kart SD – każda kamera powinna być wyposażona w złącze micro-SD lub SD obsługujące karty do 128GB, każda kamera typu A powinna być wyposażona w kartę SD o pojemności minimum 64GB
w) Kamera z obsługą funkcji nagrywania na karcie SD w przypadku zaniku rejestratora, lub problemów z komunikacją sieciową (możliwość lokalnej rejestracji obrazu na wymienialnej pamięci)
x) Wbudowany serwer WWW do obsługi i konfiguracji kamery
y) Obsługa wielu użytkowników, wraz z mechanizmami gradacji uprawnień dla tych użytkowników, w tym możliwość zdefiniowania minimum 6 użytkowników z różnymi uprawnieniami
z) Wejście audio – 1 kanał, Wyjście audio – 1 kanał
aa) Wjście alarmowe – 1 kanał, Wyjście alarmowe – 1 kanał
bb) Zasilanie PoE zgodne z 802.3af
cc) Interfejs sieciowy RJ45 – Ethernet o przepustowości minimum 10/100Mbits
dd) Obsługa: IPv4, HTTP, HTTPS, SSL, TCP/IP, UDP, ICMP, IGMP, SNMP, NTP, DHCP, DNS, FTP, 802.1x,
ee) Uchwyt 3D modułu kamery wewnątrz obudowy, pozwalający na precyzyjna regulację kąta widzenia oraz obserwowanego obszaru
ff) Klasa odporności na wandalizm – IK10
gg) klasa szczelności – minimum IP65
hh) Ze względu na montaż na suficie podwieszanym:
- waga poniżej 1kg
- do każdej kamery należy dostarczyć odpowiedni zestaw montażowy (kamera montowana nawierzchniowo)

<u>- Kamera typu C – kamera obrotowa typu PTZ</u>

a) Przetwornik 1/2.8” lub 1/2.9” lub 1/3” progressive scan CMOS, minimum 2MPx
b) Obsługa kompresji wideo w standardzie H.264, MJPEG
c) Obsługa rozdzielczości: 2MPx, 1080p
d) Obsługa minimum 2 strumieni video, przy jednoczesnym spełnieniu wymagań:
- strumień podstawowy (pierwszy) minimum 1-25kl/s (fps) przy rozdzielczości 2MPx
- strumień dodatkowy (drugi i kolejny) minimum 1-25kl/s (fps) przy rozdzielczości D1/CIF
e) Automatyczny balans bieli (AWB) z możliwością wyboru trybu ręcznego lub automatycznego
f) Automatyczna kontrola wzmocnienia sygnału (AGC) z możliwością wyboru trybu ręcznego lub automatycznego
g) Cyfrowa redukcja szumów (DNR / 2DNR / 3DNR)
h) Stosunek szumu do sygnału na poziomie nie gorszym niż 50dB (S/N >50dB)

i) Kompensacja światła tła (BLC)
j) Mechaniczny filtr podczerwieni (ICR)
k) Sprzętowa regulacja dynamiki (DWDR)
l) Automatyczna kompensacja balansu bieli (ATW)
m) Auto Iris – automatyczna regulacja otwarcia przesłony, tak aby zapewnić niezbędną ilość światła
n) Auto Focus – automatyczne regulacja ostrości obrazu
o) Obiektyw regulowany z motozoom minimum w zakresie 2,7-11mm
p) Minimum 4 krotny zoom optyczny
q) Minimum 14 krotny zoom cyfrowy
r) Obsługa stref prywatności – minimum 24 strefy prywatności pozwalające na wskazanie z poziomu kamery, obszaru maskowanego w monitorowanej przestrzeni
s) Zakres obrotu kamery PTZ:
- poziom: 360 stopni
- pion: 90 stopni
t) Prędkość obrotu kamery PTZ:
- poziom: minimum 80 stopni na sekundę
- pion: minimum 60 stopni na sekundę
u) Obsługa protokołów (po sieci, oraz poprzez interfejs szeregowy) dla sterowania ruchem kamery PTZ, minimum: Pelco-P, Pelco-D, standard producenta kamery, standard producenta rejestratora dostarczanego w niniejszym zamówieniu (wymagana współpraca w zakresie obsługi PTZ pomiędzy kamerą, rejestratorem i klawiaturą sterującą.
v) Czułość dla trybu nocnego (włączony IR) na poziomie 0 Lux
w) Promiennik podczerwieni o zasięgu skutecznym min. 20m, na diodach mocy (tzw. 3-ciej generacji)
x) Funkcje inteligentnego sterowania i pozycjonowania kamery w zakresie minimum:
- presety dla pozycjonowania kamery (minimum 200 presetów)
- trasy patrolowe (minimum 4 trasy)
- tury (minimum 8 tur)
- auto-skan (minimum 4 auto skany)
y) Rejestrator powinien mieć możliwość ustawienia parametru na wybranych nagraniach, blokującego to nagranie przed automatycznym skasowaniem (np. poprzez ww. mechanizm), celem wykorzystania do prowadzonych postępowań dowodowych itp.
z) Rejestrator powinien być przystosowany do zasilania z sieci 230V, 50Hz.

4. Spółka oczekuje dostawy rejestratora sieciowego z zawansowanymi funkcjami analizy obrazu, zgodnego z poniższą specyfikacją:
a) Rejestrator wraz z kamerami musi pochodzić od tego samego producenta.
b) Rejestrator musi wspierać standard ONVIF.
c) Rejestrator przystosowany do montażu w szafie RACK.
d) Rejestrator musi obsłużyć minimum 32 kamer IP o rozdzielczości minimum 12Mpix każda.
f) Rejestrator musi posiadać pasmo dla strumieni wideo o wielkości minimum 320 Mb/s.
g) Rejestrator musi umożliwiać montaż minimum 8 dysków, każdy o pojemności minimum 4TB.
h) Rejestrator powinien zostać wyposażony w maksymalną liczbę dysków. Ponadto Spółka oczekuje dostawy 4 dysków jako części zapasowe.
i) Rejestrator powinien posiadać minimum 2 porty HDMI oraz jedno wyjście VGA lub DVI.
k) Rejestrator powinien posiadać minimum dwa porty sieciowe Ethernet 10/1000/1000Mb/s.
l) Rejestrator powinien obsługiwać następujące tryby RAID: RAID 1, RAID 5.
m) Rejestrator powinien obsługiwać dyski twarde, SATA III o pojemności minimum 4TB.
n) Rejestrator powinien umożliwiać rozbudowę pojemności dyskowej poprzez podłączenie zewnętrznej pamięci masowej / macierzy lub zewnętrznego dysku przez sieć lub złącze eSATA.
m) Rejestrator powinien być wyposażony w 2 porty USB, z czego minimum jeden powinien być w standardzie USB 3.0.
n) Rejestrator powinien posiadać minimum 16 wejść i minimum 4 wyjścia alarmowe.
o) Rejestrator powinien umożliwiać:
- rejestrowanie obrazu z kamer
- odtwarzanie nagrań z dysków twardych
- wyświetlanie obrazu na żywo
- realizacja zdalnego podglądu przez sieć Internet
- tworzenie kopii zapasowej przez port USB lub sieć

- współpracę z kamerami IP 12Mpx (wraz z obsługą kamer o niższej rozdzielczości: 5Mpx, 3Mpx, 1080p, 720p)
- obsługa minimum dwóch strumieni IP z kamer
- monitorowanie stanu dysków, utylizacji dysków i wolnej przestrzeni.
- wielopoziomowe zarządzanie uprawnieniami użytkowników
- zarządzanie poprzez graficzny interfejs oparty o WEB lub dedykowaną aplikację
- współpracę z kamerami w standardach ONVIF,
- wsparcie kompresji minimum H.264 i H.265
- różne tryby zapisu wideo (minimum: ciągły, alarmowy, detekcja ruchu, analityki z kamer)
- zarządzanie harmonogramem rejestracji i trybem rejestracji dla każdej kamery
- obsługę dysków zewnętrznych poprzez złącze eSATA
- wyszukiwania, archiwizowanie i nagrywanie materiałów na nośnikach wymiennych

r) Rejestrator powinien być wyposażony w mechanizmy inteligentnej analizy obrazu, w tym wykorzystanie tego mechanizmu do wyzwalania nagrywania lub wyjść alarmowych w następujących sytuacjach:

- przekroczenie wirtualnej linii
- wtargnięcie w zastrzeżony obszar
- zmiana monitorowanego obszaru
- detekcja twarzy
- detekcja audio
- zliczanie osób

s) Rejestrator powinien być wyposażony w funkcję umożliwiającą zasłonięcie części obrazu otrzymanego z kamer, tzw. strefa prywatności,

t) Rejestrator powinien mieć oprogramowanie, umożliwiające samodzielną instalację aktualizacji i wgrywanie poprawek dostarczonych przez producenta,

u) Rejestrator powinien mieć możliwość ustawienia parametru nagrywania określającego ilość dni po których nastąpi automatyczne skasowanie nagrań starszych niż ustawiony parametr,

w) Rejestrator powinien mieć możliwość ustawienia parametru na wybranych nagraniach, blokującego to nagranie przed automatycznym skasowaniem (np. poprzez ww. mechanizm), celem wykorzystania do prowadzonych postępowań dowodowych itp.

z) Rejestrator powinien być przystosowany do zasilania z sieci 230V, 50Hz.

5. Spółka oczekuje dostawy dedykowanych dysków twardych do dostarczonych rejestratorów. Dyski muszą być dedykowane przez producenta dysku do pracy ciągłej. Dostarczone dyski powinny spełniać poniższe wymagania:

- Dyski do rejestratora 128 kanałowego:
  a) Dysk wewnętrzny HDD
  b) Interfejs SATA III
  c) przepustowość 6Gbps
  d) prędkość obrotowa 7200RPM
  e) format dysku 3,5”
  f) pojemność 8TB
  g) pamięć podręczna 64MB
  h) przeznaczenie – praca ciągła w rejestratorach CCTV
  i) pobór mocy – poniżej 6W
- Dyski do rejestratora 16 kanałowego:
  a) Dysk wewnętrzny HDD
  b) Interfejs SATA III
  c) przepustowość 6Gbps
  d) prędkość obrotowa 7200RPM
  e) format dysku 3,5”
  f) pojemność 4TB
  g) pamięć podręczna 64MB
  h) przeznaczenie – praca ciągła w rejestratorach CCTV
  i) pobór mocy – poniżej 6W

6. Spółka oczekuje dostawy monitorów przemysłowych do pracy ciągłej, przeznaczonych do obsługi systemu CCTV, wg poniższej specyfikacji:

a) przekątna minimum 27”:
b) rozdzielczość minimum 3840x2160

c) format ekranu 16:9
d) wejścia:
- minimum 2x HDMI
- minimum 1x DVI
- minimum 1x DisplayPort

e) wyjścia:
- minimum 1 wyjście audio

f) cyfrowy filtr obrazu 3D
g) redukcja szumów NR
h) automatyczna detekcja sygnału PAL/NTSC
i) kontrast minimum 10000:1
j) czas reakcji: 5ms
k) jasność minimum 3000cd/m2
l) funkcja regulacji jasności monitora w zależności od oświetlenia otoczenia z możliwością przełączenia między trybem ręcznym i automatycznym
l) możliwość mocowania przy użyciu uchwytów w standardzie VESA 100x100
m) monitor dedykowany do pracy ciągłej 24/7
n) wraz z monitorami należy dostarczyć:
n1) uchwyty biurkowe z montażem VESA 100x100, o następującej specyfikacji:
- pionowe mocowanie 2 monitorów do 28” w układzie jeden nad drugim
- regulacja pochylenia i wzajemnego ułożenia powierzchni monitorów względem siebie
- uchwyt bez wysięgników pantografowych oraz przegubowych, zajmujący jak najmniej miejsca (tj, nie wychodzący poza obrys biurka oraz nie wchodzący na powierzchnie biurka więcej niż 12 cm) bez monitorów
- uchwyt oparty o jedną pionową szynę/prowadnicę dla ruchomych/przesuwnych (w zakresie szyny) uchwytów typu VESA
- mocowania dla monitorów w standardzie VESA powinny być wyposażone w mechanizm swobodnej regulacji pochylenia monitorów w zakresie: +/- 5 stopni w pionie i +/- 10 stopni w poziomie
- jeden punkt mocowania do biurka gwarantujący stabilność i trwałość mocowania

n2) uchwyty nabiurkowe z montażem VESA 75x75 oraz 100x100, o następującej specyfikacji:
- poziome mocowanie 3 monitorów do 27”, w układzie wertykalnym, tj. jeden obok drugiego
- regulacja pochylenia i wzajemnego ułożenia powierzchni monitorów względem siebie
- uchwyt bez wysięgników pantografowych, oraz „tzw. rozkładanych”, zajmujący jak najmniej miejsca (tj, nie wychodzący poza obrys biurka oraz nie wchodzący na powierzchnie biurka więcej niż 15 cm) bez monitorów
- uchwyt posiadający jedną poziomą szynę/prowadnicę dla montażu ruchomych/przesuwnych (w zakresie szyny) mocowań monitorów typu VESA,
- konstrukcja uchwytu biurkowego, powinna umożliwiać ustawienie powierzchni monitorów w sposób ergonomiczny dla użytkownika, tj. po linii będącej fragmentem okręgu, tzw. układ „paraboliczny”, zapewniając taką samą widoczność monitorów z jednego punktu
- mocowania dla monitorów w standardzie VESA powinny być wyposażone w mechanizm swobodnej regulacji pochylenia monitorów w zakresie minimum: +/- 5 stopni w pionie i +/- 10 stopni w poziomie
- do dwóch punktów mocowania uchwytu do biurka gwarantujących stabilność i trwałość mocowania

n3) przewody zasilające dla monitorów
n4) przewody HDMI 4K o długości 4mb każdy, przekrój kabla owalny, przewody 32AWG TC, 19 pin
n5) przewody typu display-port o długości 3mb każdy, przekrój kabla owalny
n6) zestaw filtrów prywatyzujących dla dostarczonych monitorów 27”-28”, z mocowaniem filtra do monitora umożliwiającym wielokrotny demontaż i ponowny montaż filtra
n7) zestaw filtrów prywatyzujących dla monitorów 24” z mocowaniem filtra do monitora umożliwiającym wielokrotny demontaż i ponowny montaż filtra
n8) zestawy do czyszczenia monitorów, o następującej zawartości:
- dwie ściereczki z mikrofibry o wymiarach minimum 20x20cm
- środek antystatyczny do czyszczenia matrycy monitora o pojemności minimum 400ml
- środek antystatyczny do czyszczenia obudowy monitora o pojemności minimum 400ml

- powietrze sprężone o pojemności minimum 600ml

7. Spółka oczekuje dostawy przenośnego monitora serwisowego z funkcjami testowania do CCTV, zgodnie z poniższą specyfikacją:

a) Urządzenie przenośne zasilane akumulatorem o pojemności minimum 5000mAh

b) minimum 7” wyświetlacz o rozdzielczości minimum 1920x1200 px

c) Wyświetlacz wyposażony w pojemnościowy ekran dotykowy

d) Obsługa następujących standardów wizyjnych:

- AHD – do minimum 4MPx
- HD-CVI – do minimum 4MPx
- HD-TVI – do minimum 4MPx
- TCP/IP – włącznie z 4k
- HD-SDI / EX-SDI
- CVBSS – PAL/NTSC

e) Wejścia wideo:

- 1 szt AHD/HD-CVI/HD-TVI/CVBS w postaci gniazda BNC
- 1 szt HD-SDI / EX-SDI w postaci gniazda BNC
- 1 szt HDMI

f) Wyjścia wideo:

- 1 szt CVBS w postaci gniazda BNC
- 1 szt HDMI

g) Porty LAN:

- 2 sztuki do współpracy z kamerami i switchami PoE
- porty ze źródłem zasilania dla urządzeń zasilanych w standardzie PoE

h) Wejście audio – 1 szt. typu jack 3,5mm

i) Wyjście audio – 1 szt. typu jack 3,5mm

j) Porty szeregowe: RS-232 oraz RS-485 (możliwość ustawienia prędkości transmisji w zakresie 150-115200 baudów/s)

k) Obsługa minimum następujących protokołów:

- Pelco-D
- Pelco-P,
- SAMSUNG,
- Panasonic,
- SONY-EVI,
- LG-MULTIX,
- HIKVISION/BCS/DAHUA,
- DH-YTC,
- SAMSUNG-SPD,
- Siemens,
- BOSCH OSRD

l) Miernik poziomu sygnału wideo dla sygnałów CVBS – mV (PAL), IRE (NTSC)

m) Generowanie sygnału kontrolnego wideo w zakresie:

- generator sygnału kontrolnego
- generowanie kolorowych pasów w standardzie PAL/NTSC
- generowanie czarnego lub niebieskiego ekranu/planszy

n) zdolność testowania połączenia kabli UTP lub kabli telefonicznych ze złączem RJ45

o) zdolność do wykrywania przewodu w wiązce

p) zdolność testowania i prezentacji poleceń z urządzeń sterujących dla komunikacji poprzez standard RS-232 lub RS-485

q) zdolność do testowania mocy optycznej w kablach światłowodowych w zakresie minimum -60/+10dBm

r) zdolność do wizualnej lokalizacji uszkodzeń włókien światłowodowych (VLS/VFL)

s) funkcja reflektometru dla kabli UTP i koncentrycznych (TDR - zdolność do wykrywania i lokalizacji miejsca przerwania okablowania)

t) Urządzenie powinno być wyposażone w moduł WIFI

u) Obsługa poprzez graficzne menu dotykowe, wyświetlane na wbudowanym wyświetlaczu

v) Urządzenie powinno obsługiwać minimum następujący zakres funkcji:

- Test kamer AHD, HD-CVI, HD-TVI, HD-SDI, PAL/NTSC

- Test kamer IP
- Obsługa kompresji H.264, H.265, MJPEG
- Obsługa protokołu ONVIF, w tym wyszukiwanie i podgląd obrazu z kamer ze standardem ONVIF
- Sterowanie obrotowymi kamerami typu PTZ
- Podgląd obrazu z kamer IP (przy użyciu wbudowanych aplikacji)
- Wbudowana przeglądarka internetowa
- Generator sygnału kontrolnego
- Monitorowanie połączeń LAN
- Skaner adresów IP w sieci IPv4
- Testowanie łącza i komunikacji za pomocą pakietów ICMP
- Wykrywanie aktywnego portu w switchu
- Test skrętki komputerowej
- Miernik zasilania PoE
- Identyfikacja przewodu w wiązce
- Zapis wideo z podłączanej kamery na kartę SD
- Odtwarzanie nagrań z karty SD

w) zdolność działania jako źródło zasilania dla odbiorników PoE

x) zasilacz /ładowarka w zestawie

y) zestaw kabli połączeniowych i testowych dla złącz w tym dla miernika mocy optycznej

8. Spółka oczekuje dostawy wideodomofonu z następującymi wymaganiami minimalnymi:

a) Rozdzielczość kamery musi umożliwiać rozpoznanie twarzy jednak nie może być mniejsza niż 640x480pix, funkcjonalność ta musi być realizowana przy oświetleniu jakie znajduje się przed wejściem gdzie będzie zamontowany wideodomofon w razie konieczności powinien być wyposażony w oświetlacz IR,

b) Powinien zapewnić integrację z systemem SKD w zakresie otwarcia strefy chronionej oraz umożliwić przekazanie sygnału wideo do rejestratora CCTV,

c) System domofonu musi mieć niezależne zasilanie lub stosowne zabezpieczenia linii zasilającej i linii komunikacyjnej, tak aby niemożliwe było uszkodzenie systemu SKD, SSWiN czy CCTV poprzez zwarcie w panelu zewnętrznym, lub poprzez podanie wysokiego napięcia (np. z tasera) na elementy elektroniczne panelu zewnętrznego.

d) System powinien być zamontowany we wskazanym przez Dział Informatyki miejscu i obsługiwać wskazane przez Spółkę przejścia.

9. Spółka wraz z dostawą w/w urządzeń, w zależności od potrzeb i ustaleń oczekuje również dostawy niezbędnego sprzętu uzupełniającego (o parametrach wskazanych poniżej) takiego jak:

- bezprzerwowych, bezstykowych urządzeń przełączających źródło zasilania – tzw. ATS, zgodnie z następującą specyfikacją:

a) Urządzenia powinny obsługiwać zasilanie z dwóch niezależnych linii zasilających, jednofazowych, o napięciu znamionowym 230V, 50Hz AC

b) Maksymalny czas przełączenia pomiędzy źródłami zasilania nie powinien przekraczać 20ms

c) Minimalny prąd znamionowy dla urządzenia: 16A

d) Maksymalny prąd znamionowy dla urządzenia: 20A

e) Urządzenia powinny być wyposażone we wskaźniki stanu zasilania dla obydwu źródeł, oraz ogólny stan urządzenia

f) Złącza wejściowe (zasilające): gniazdo IEC 320 C20 – 2szt – po jednej sztuce dla każdego źródła zasilania

g) Złącza wyjściowe (odbiory): gniazdo IEC 320 C19 – 1szt, gniazdo IEC 320 C13 – minimum 4 szt.

h) Złącza komunikacyjne - porty RJ45

i) Obsługa SSH oraz SNMP

j) Możliwość zarządzania z poziomu CLI, poprzez komunikację SSH lub złącze szeregowe

k) Urządzenia dedykowane do montażu w szafie RACK 19”, o wymiarze 1U

l) Urządzenia powinny być dostarczone z kompletem kabli zasilających w standardzie IEC 320 C20-C19

m) Urządzenia powinny posiadać zdolność pracy przy temperaturze 15-50 stopni Celsjusza

n) Urządzenia powinny posiadać zdolność pracy przy wilgotności względnej 30-70% bez kondensacji

o) Urządzenia powinny być zabezpieczone w zabezpieczenie przeciwprzepięciowe dla prądu minimum 10kA

- urządzeń i akcesoriów połączeniowych służących realizacji inwestycji typu patchcord, patchpanel 19", kable i przewody HDMI, kable i przewody wizyjne, kable i przewody zasilające (w uzgodnionej z Zamawiającym ilościach i parametrach)
- urządzeń typu spliter HDMI Xx4 (gdzie X - w zależności od potrzeb projektu):
    - jedno wejście, minimum X wyjścia HDMI
    - jednoczesne wyświetlanie obrazu na X monitorach z jednego źródła
    - obsługa źródła Ultra HD oraz czterech wyświetlaczy Ultra HD
    - obsługa rozdzielczości Ultra HD 4k2k@50/60Hz (3840x2160p)
    - obsługa kabli HDMI o długości 20m na wejściu oraz 25 m na wyjściu
    - wsparcie HDCP w wersji minimum 2.0
    - wsparcie HDMI w wersji minimum 2.0a
    - wsparcie rozdzielczości wideo VESA QSXGA@60Hz
    - w zestawie zasilacz
- automatyczny przełącznik priorytetowy HDMI Xx1 (gdzie X - w zależności od potrzeb projektu):
    - X porty wejściowe, jeden port wyjściowy
    - obsługa źródeł Ultra HD oraz wyświetlacza Ultra HD
    - obsługa rozdzielczości Ultra HD 4k2k@50/60Hz (3840x2160p)
    - wsparcie dla HDCP i HDMI-CEC
    - wzmacnianie sygnału na porcie wyjściowym
    - automatyczne przełączanie wg priorytetów (przełączenie na nowy sygnał, a po jego zaniku powrót na kolejny aktywne źródło, przy założeniu priorytetu ostatnio używanego źródła)
    - w zestawie zasilacz
- matryca HDMI Xx, gdzie (X - w zależności od potrzeb projektu):
    - X porty wejściowe, X porty wyjściowe
    - wsparcie rozdzielczości 4k@60Hz
    - złącze RS232 do sterowania matrycą
    - złącze RJ45 Ethernet/IP do sterowania matrycą
    - dostępna aplikacja na system operacyjny Microsoft Windows do sterowania matrycą via Ethernet/IP oraz RS232
    - wsparcie zarządzania przez WEB GUI
    - przepustowość 18Gbps
    - wsparcie HDCP minimum 2.2 dla wejścia i wyjścia
    - wsparcie HDMI minimum 1.4 dla wejścia i wyjścia
    - wsparcie HDR10
    - dowolne rutowanie X wejściowych sygnałów HDMI na dowolne X wyjścia HDMI
    - w zestawie zasilacz oraz niezbędne okablowanie dla portu RS232
- extender HDMI umożliwiający podłączenie monitora i przesłanie sygnału po skrętce komputerowej (pasywnie) na odległość do 100 m (2 sztuki) o rozdzielczości obrazu minimum 2Mpix.

### 3.5.4.5. SYSTEM SYGNALIZACJI POŻAROWEJ (PPOŻ SSP)

1. Centrala sygnalizacji pożaru

Centrala sygnalizacji pożarowej, przeznaczona do:
- wykrywania i sygnalizowania zagrożenia pożarowego po odebraniu informacji od współpracujących z nią czujek i ręcznych ostrzegaczy pożarowych,
- koordynowania pracy wszystkich urządzeń w systemie oraz podejmowania decyzji o zainicjowaniu alarmu pożarowego,
- wysterowaniu urządzeń sygnalizacyjnych i przeciwpożarowych oraz o przekazaniu informacji do centrum monitorowania lub systemu nadzoru,
- ochrony przeciwpożarowej różnego rodzaju obiektów, zwłaszcza dużych lub rozległych np. hoteli, biurowców, magazynów, obiektów zabytkowych, „inteligentnych" budynków z dużą liczbą współpracujących urządzeń automatyki pożarowej.

Centrala sygnalizacji pożarowej o architekturze rozproszonej. Składa się z wielu zunifikowanych modułów różnych typów, umieszczonych w standardowych obudowach, które pojedynczo lub połączone w zestawy (tzw. węzły), mogą być rozmieszczone w różnych punktach chronionego obiektu, nawet znacznie od siebie oddalonych. Odległości pomiędzy węzłami centrali mogą wynosić do 1200m w przypadku kabla miedzianego lub nawet do 15 kilometrów w przypadku stosowania światłowodu jednomodowego. Wszystkie moduły, w obrębie pojedynczego

węzła oraz węzły pomiędzy sobą, połączone są wspólną, podwójną (redundantną) cyfrową magistralą komunikacyjną.
Centrala składa się z:
· paneli sterujących z wyświetlaczem dotykowym 10”,
· modułów funkcjonalnych:
- linii dozorowych
- kontrolno-sterujących
- wyjść przekaźnikowych
- wyjść potencjałowych
- wyjść przekaźnikowych wysokonapięciowych
- wejść kontrolnych
- zasilania
- drukarki
- transmisji
Panele sterujące oraz moduły, zamontowane są w obudowach o standardowych wymiarach, które można ze sobą łączyć mechanicznie. Połączone mechanicznie obudowy tworzą węzeł centrali. Każdy węzeł musi być wyposażony w przynajmniej jeden moduł zasilacza. Centrala musi posiadać przynajmniej jeden węzeł, w którym zamontowany jest główny panel o numerze 1. Jest to tzw. węzeł główny centrali i może być tylko jeden w instalacji. Pozostałe wyposażenie centrali tworzy tzw. węzły wyniesione, które muszą być podłączone do węzła głównego centrali. Komunikacja pomiędzy węzłami odbywa się za pomocą zdublowanego połączenia kablowego (RS-485) lub zdublowanej pary światłowodów. W każdym węźle centrali (oprócz zasilacza) mogą znajdować się moduły funkcjonalne realizujące podłączenie linii dozorowych, lub do bezpośredniego sterowania lub kontroli urządzeń automatyki pożarowej. W każdym węźle wyniesionym może znajdować się panel sterujący pełniący funkcję dodatkowego terminala obsługowego oraz redundantnego kontrolera w przypadku awarii węzła Master.

2. Wielosensorowa czujka dymu i ciepła
Przeznaczona do wykrywania początkowego stadium rozwoju pożaru, podczas którego pojawia się dym i/lub następuje wzrost temperatury. Charakteryzuje się znaczną odpornością na ruch powietrza i na zmiany ciśnienia. Może pracować w adresowalnych pętlowych liniach dozorowych central sygnalizacji pożarowej systemu. Czujka wyposażona jest w wewnętrzny izolator zwarć. Instalowana jest w gnieździe pożarowym. Wykrywa pożary testowe od TF1 do TF6 oraz TF8.
Dane techniczne:
· prąd dozorowania: 150µA
· zasilanie: z centrali sygnalizacji pożarowej
· wykrywane pożary testowe: TF1 do TF6 oraz TF8
· temperatura pracy: -25ºC ÷ +65ºC

3. Optyczna czujka dymu
Przeznaczona do wykrywania widzialnego dymu, towarzyszącego powstawaniu większości pożarów. Umożliwia wykrycie pożaru w jego początkowym stadium, gdy materiał jeszcze się tli, co następuje na ogół długo przed wybuchem otwartego płomienia i zauważalnym wzrostem temperatury, charakteryzuje się znaczną odpornością na wiatr, na zmiany ciśnienia i kondensację pary wodnej, ma dużą czułość na dym. Może współpracować w adresowalnych pętlowych liniach dozorowych central sygnalizacji pożarowej systemu. Czujka wyposażona jest w wewnętrzny izolator zwarć. Instalowana jest w gnieździe pożarowym. Wykrywa pożary testowe od TF1 do TF5 oraz TF8.
Dane techniczne:
· prąd dozorowania: 150µA
· zasilanie: z centrali sygnalizacji pożarowej
· wykrywane pożary testowe: TF1 do TF6 oraz TF8
· temperatura pracy: -25ºC ÷ +55ºC

4. Osłona przeciwwietrzna
Jest przewidziana do współpracy z czujkami dymu nadzorujących powietrze w kanałach wentylacyjnych i innych, gdzie ze względu na przekrój kanału, szybki ruch powietrza i inne czynniki, bezpośrednie zainstalowanie samej czujki w kanale nie jest możliwe.

5. Gniazdo czujki

Jest przeznaczone do mocowania czujek na suficie i dołączenia do nich przewodów linii dozorowej.

6. Liniowa czujka dymu
Przeznaczona do wykrywania dymu powstającego we wczesnym stadium rozwoju pożaru, nadaje się zwłaszcza do ochrony pomieszczeń, gdzie w pierwszej fazie pożaru spodziewane jest pojawienie się dymu i tam, gdzie ze względu na dużą powierzchnię pomieszczenia należałoby dla jego ochrony, zastosować dużą liczbę punktowych czujek dymu. Czujki są przy tym (w porównaniu do czujek punktowych dymu) czułe na średnią wartość gęstości dymu, na długiej drodze wiązki promieniowania podczerwonego, a zatem są szczególnie przydatne do stosowania pod wysokimi sufitami/stropami lub tam, gdzie dym może ulec przed detekcją rozproszeniu na dużym obszarze. Cechą charakterystyczną czujki jest umieszczenie nadajnika i odbiornika w jednej obudowie oraz współpraca z reflektorem lub zespołem reflektorów umieszczonym naprzeciwko, w obudowie czujki znajduje się celownik laserowy, który ułatwia wyosiowanie drogi optycznej pomiędzy czujką a reflektorem/zespołem reflektorów. Może pracować w adresowalnych pętlowych liniach dozorowych central sygnalizacji pożarowej. Czujka wyposażona jest w wewnętrzny izolator zwarć. Wykrywa pożary testowe od TF1 do TF5 oraz TF7 i TF8. Może pracować w pomieszczeniach zamkniętych, w zakresie temperatur -25°C do +55°C i wilgotności względnej do 95 % przy 40°C. Zasięg pracy czujki to od 5 do 100m w zależności od zastosowanego reflektoru lub zespołu reflektorów.
Dane techniczne:
· Pobór prądu w trybie dozorowania: max. pobór pradu czujki z linii konwencjonalnej 2,2 mA lub 5 mA
· Pobór prądu w trybie alarmowania: 20 mA
· wykrywane pożary testowe: TF1 do TF6 oraz TF8
· temperatura pracy: -25ºC ÷ +55ºC

7. Wskaźnik zadziałania czujki
Jest przeznaczony do optycznego informowania o stanie alarmowania czujki lub grupy czujek pożarowych w instalacji sygnalizacji pożarowej. Przewidziany jest do pracy w instalacjach konwencjonalnych i adresowalnych.
Dane techniczne:
· Dopuszczalny prąd płynący przez wskaźnik: 20 mA
· Max przekrój dołączanych przewodów: 1,5 mm2

8. Ręczny ostrzegacz pożaru wewnętrzny
Przeznaczony do ręcznego uruchomienia systemu sygnalizacji pożarowej przez osobę, która zauważyła pożar. Uruchomienie ostrzegacza przebiega dwuetapowo i polega na uderzeniu w szybkę zabezpieczającą i wciśnięciu przycisku. Ręczne ostrzegacze pożarowe produkowane są w wersji do instalowania wewnątrz tynku. Instalowanie ostrzegaczy na tynku wymaga użycia ramki maskującej.
Dane techniczne:
· prąd dozorowania: 135µA
· zasilanie: z centrali sygnalizacji pożarowej
· szczelność obudowy: IP 30
· temperatura pracy: -25ºC ÷ +70ºC

9. Ręczny ostrzegacz pożaru zewnętrzny
Przeznaczony do ręcznego uruchomienia systemu sygnalizacji pożarowej przez osobę, która zauważyła pożar. Uruchomienie ostrzegacza przebiega dwuetapowo i polega na uderzeniu w szybkę zabezpieczającą i wciśnięciu przycisku. Ręczne ostrzegacze pożarowe produkowane są w wersji do instalowania wewnątrz tynku. Instalowanie ostrzegaczy na tynku wymaga użycia ramki maskującej. Ostrzegacze wyposażone są w wewnętrzne izolatory zwarć, ostrzegacz o podwyższonej szczelności.
Dane techniczne:
· prąd dozorowania: 135µA
· zasilanie: z centrali sygnalizacji pożarowej
· szczelność obudowy: IP 55
· temperatura pracy: -25ºC ÷ +70ºC

10. Uniwersalne elementy kontrolno-sterujące przeznaczone do :
· sterowania automatycznych urządzeń zabezpieczających, przeciwpożarowych,
· kontroli zadziałania ww. urządzeń,
· sterowania sygnalizatorami,

· kontroli stanu dowolnych urządzeń.

Wejścia niskonapięciowe (NN) elementu umożliwiają podłączenie niezależnych, bezpotencjałowych zestyków normalnie zwartych lub normalnie rozwartych. Wejścia wysokonapięciowe (WN) elementu umożliwiają podłączenie niezależnych zestyków przy napięciu do 230 VAC lub 220 VDC. Przystosowany jest do pracy wewnątrz i na zewnątrz obiektów (szczelność obudowy IP66) w zakresie temperatur od -40°C do +85°C i wilgotności względnej do 95% przy 40°C. Przewidziany jest do pracy wyłącznie w adresowalnych liniach dozorowych central sygnalizacji pożarowej systemu.

Typy zastosowane w projekcie:
· 4we – wyposażony w 4 wejścia niskonapięciowe,
· 4wy – wyposażony w 4 wyjścia,
· 2we/2wy – wyposażony w 2 wejścia niskonapięciowe, 2 wyjścia,
· 4we/4wy – wyposażony w 4 wejścia niskonapięciowe, 4 wyjścia,
· 2we/2wy – wyposażony w 2 wejścia wysokonapięciowe, 2 wyjścia,

Element kontrolno-sterujący wyposażony jest w wewnętrzny izolator zwarć, który odcina sprawną część linii dozorowej od sąsiadującej części zwartej. Max. prąd przełączny dla styków przekaźnika to 2A, max napięcie 250VAC/220VDC, max. moc 62,5VA/60W. Działanie elementów może być programowane i polega na wyborze:
· rodzaju pracy wyjścia sterującego,
· możliwości kontroli ciągłości przewodu podłączonego do wyjścia sterującego,
· stany bezpiecznego wyjścia sterującego – funkcja „fail safe”,
· funkcji jaką spełnia wejście,
· sposobu działania wejścia niskonapięciowego (NO, NC) lub wejścia wysokonapięciowego,
· czasów opóźnienia wysterowania, wysterowania, opóźnienia kasowania i kasowania.

11. Sygnalizator wewnętrzny
Pożarowy sygnalizator akustyczno-optyczny przeznaczony jest do sygnalizowania pożaru wewnątrz budynków.
Dane techniczne:
· napięcie zasilania: 16 – 32,5VDC
· pobór prądu w stanie działania: < 75mA
· natężenie dźwięku w odległości 1m: > 100dB
· rodzaj środowiska pracy: Typ B
· stopień ochrony: IP 33
· zakres temperatury pracy: -25ºC ÷ +55ºC

12. Sygnalizator zewnętrzny
Pożarowy sygnalizator akustyczno-optyczny przeznaczony jest do sygnalizowania pożaru na zewnątrz budynków.
Dane techniczne:
· napięcie zasilania: 16 – 32,5VDC
· pobór prądu w stanie działania: < 0,45A
· pobór mocy w stanie alarmowania: < 1,8W
· natężenie dźwięku w odległości 1m: > 110dB
· rodzaj środowiska pracy: Typ B
· stopień ochrony: IP 33C
· zakres temperatury pracy: -25ºC ÷ +70ºC

13. Puszka połączeniowa PH90
Puszka instalacyjna do systemów pożarowych wykonana jest z blachy ocynkowanej pokrytej czerwoną farbą proszkową. Zawiera ona kostki ceramiczne wraz z bezpiecznikiem przeciążeniowym jednorazowego zadziałania. Puszka posiada osobne zaciski do podłączenia wejścia linii sygnałowej, osobne do podłączenia wyjścia linii sygnałowej oraz osobne do podłączenia sygnalizatora lub innego urządzenia poprzez bezpiecznik. Puszka posiada dwa otwory do mocowania jej przy pomocy metalowych kołków do sufitu lub ściany.
· napięcie zasilania: max 125VAC
· zakres prądowy: zależnie od prądu zadziałania bezpiecznika
· średnica kabla instalacyjnego: max Ø 10mm
· przekrój przewodu: max 2,5 mm²

· szczelność obudowy: IP20

14. Zasilacz buforowy 24V
Zasilacze te służą do zasilania gwarantowanym napięciem 24V urządzeń:
- sygnalizacji pożarowej wg PN-EN 54-4/A2:2007
- kontroli rozprzestrzeniania dymu i ciepła wg PN-EN 12101-10:2007
- przeciwpożarowych wg Rozp. MSWiA z dn. 20.6.2007 (Dz.U. nr 143, poz. 1002, zm. dn. 27.4.2010)
CECHY CHARAKTERYSTYCZNE
- jednoczesna zgodność z wieloma dokumentami normatywnymi – możliwość zastosowania jednego typu zasilacza do różnych urządzeń ochrony przeciwpożarowej
- odporność na trudne warunki pracy (-25…+75°C, IP44)
- mały prąd na potrzeby własne
- sygnalizacja wysokiej rezystancji obwodu bateryjnego oraz możliwość odczytu aktualnej wartości rezystancji
- komunikacja RS232/485
- niska awaryjność (0,5% w ciągu trzech lat)
- dwa wyjścia
WYPOSAŻENIE
- metalowa szafka wisząca z zamkiem, mieści baterię akumulatorów
- zespół sygnalizacji świetlnej LED stanu pracy zasilacza
- sygnalizacja zdalna: uszkodzenie sieci i uszkodzenie baterii (dla każdego rodzaju dostępne trzy styki przekaźnika)
- zabezpieczenia przeciążeniowe obwodów wyjściowych i baterii
- wewnętrzny rozłącznik głębokiego rozładowania
- wejście alarmu zewnętrznego
- wewnętrzna sonda temperaturowa
ZGODNOŚĆ Z WYMAGANIAMI BEZPIECZEŃSTWA
Zasilacze spełniają wymagania dyrektyw:
- 2006/95/WE Niskonapięciowe wyroby elektryczne (PN-EN 60950-1:2007 Bezpieczeństwo urządzeń),
- 2004/108/WE Kompatybilność elektromagnetyczna,
- 89/106/EWG Wyroby budowlane.
PODSTAWOWE PARAMETRY
- Znamionowe napięcie zasilania 230V +10% -15%
- Znamionowe napięcie wyjściowe (w temperaturze 25°C) 27,1V
- Pobór prądu z akumulatora na potrzeby własne zasilacza max 35mA
- Maksymalna rezystancja obwodu akumulatora 250mΩ
- Liczba współpracujących akumulatorów 2
- Liczba wyjść zabezpieczonych osobnymi bezpiecznikami 2
- Temperatura pracy (patrz instrukcja obsługi) -25…+55°C; 75°C przez 2h
- Stopień ochrony PN-EN 60529:2003 IP 44
- Klasa funkcjonalna PN-EN 12101-10:2007 A
- Klasa środowiskowa PN-EN 12101-10:2007 1
- Klasa środowiskowa VdS 2593 III
- Klasa ochronności PN-EN 60950-1:2007/A11:2009/A1:2011 I
- Parametry indywidualne: Maksymalny prąd wyjściowy Imax b / Nominalny prąd wyjściowy Imax a / Maks.
Pojemność baterii akumulatorów: 3A/2A/18Ah.

15. Komplet materiałów montażowych innych
(skrzynki, rozdzielnice, zabezpieczenia, itp. niezbędnych do wykonania instalacji zgodnie z dokumentacją projektową).

16. Komplet materiałów do wykonania tras kablowych
Listwy instalacyjne, uchwyty, złączki, puszki połączeniowe, itp. zgodnie z dokumentacją projektową.

17. Komplet okablowania instalacji
Przewody zasilające, sterujące, sygnałowe, systemowe zgodnie z dokumentacją projektową.

18. WYKAZ WAŻNIEJSZYCH AKTÓW PRAWNY, NORM I PRZEPISÓW OBOWIĄZUJĄCYCH W POLSCE DOTYCZĄCYCH PRZEDSIĘWZIĘCIA

a). Ustawa z dnia 7 lipca 1994r. Prawo budowlane (Dz.U. 2016 poz.290 z późn. zm.),
b). Rozporządzenie Ministra Infrastruktury z dn. 12 kwietnia 2002r w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz.U. Nr 75, poz.690, z 2003r. Nr 33, poz.270, z 2004r. Nr 109, poz.1156 z 2008r. Nr 201, poz.1238 i Nr 228, poz.1514; z 2009r. Nr 56, poz.461 z późn. zm.),
c). Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 roku w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. Nr 109, poz.719 z późn. zm.);
d). Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 16 czerwca 2003r. w sprawie uzgadniania projektu budowlanego pod względem ochrony przeciwpożarowej (Dz.U. Nr 121, poz.1137 z późn. zm.);
e). Specyfikacja techniczna PKN-CEN/TS 54-14 Systemy sygnalizacji pożarowej. Cześć 14: Wytyczne planowania, projektowania, instalowania, odbioru, eksploatacji i konserwacji;
f). PN-EN 54-16:2011 - Systemy sygnalizacji pożarowej -- Część 16: Centrale dźwiękowych systemów ostrzegawczych;
g). PN-EN 54-4:2001 - Systemy sygnalizacji pożarowej -- Część 4: Zasilacze;
h). PN-EN 54-24:2008 - Systemy sygnalizacji pożarowej -- Część 24: Dźwiękowe systemu ostrzegawcze – Głośniki;
i). PN-EN 60849:2001 - Dźwiękowe systemy ostrzegawcze;
j). Instrukcje, DTR i wytyczne producentów instalowanych urządzeń;
k). Obowiązujące normy i przepisy budowy urządzeń elektrycznych.
15. System powinien być objęty integracją z innymi systemami kontroli i nadzoru technicznego (systemem KD, SSWiN, PPOŻ, CCTV, system SUG, systemami klimatyzacji).

## 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 typy 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 posadowić 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 akredytacje 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 pobyty 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 ścisłe 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 rozprowadzenie 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 ustali 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 podrzędnego (obecnego) (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 producenckich 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 wyższej, 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 [rozszytych na panelach krosowych], należy przeliczyć to jako 80*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. W sieci typu core zastosowanie przełączników o większej ilości portów 40/100GE w celu podłączenia przełączników serwerowych. Przyjmuje się zasadę redundancji wszystkich urządzeń pracujących w sieci core (przełączniki typu core, UTM/Firewall, kontrolery).
8. Należy uzgodnić z Działem Informatyki liczbę oraz rodzaj/model przełączników sieciowych odpowiednich do danego projektu.
9. 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
10. 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
11. Dla sieci CCTV wymagane są oddzielne przełączniki sieciowe, również wyposażone w porty typu uplink standardu 10G SFP+.

12. Do sieci CCTV, telefonii IP (VoIP), sieci bezprzewodowej WLAN należy stosować przełączniki 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 rozdzielenia sieci przełącznikiem biurkowym, przełącznik ten musi być zarządzalny i posiadać porty standardu co najmniej 10G.
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.
17. Każdy z instalowanych aktywnych urządzeń infrastruktury powinien zostać zintegrowany z obecnym w infrastrukturze Spółki systemem jej monitorowania (w zależności od rodzaju i klasy urządzenia). Integracja ta powinna być nieograniczana zakresowo jakimkolwiek zobowiązaniem licencyjnym, a jeśli takie ograniczenie zachodzi, wykonawca (dostawca) powinien dostarczyć na swój koszt wraz z tym urządzeniem komplet pełnych licencji pozwalających na realizację takiego monitoringu na okres do 5 lat od chwili podpisania protokołu odbioru inwestycji.
18. Przyjęcie minimalnych wymagań technicznych oraz technologicznych dla określonych klas urządzeń aktywnych:

## 5.1. PUNTY DOSTĘPOWE (AP)

- urządzenie sieciowe, punkt dostępowy dwuradiowy, w zamkniętej architekturze przeznaczone do montażu na ścianie, suficie podwieszanym lub suficie trwałym w obudowie ognioodpornej z tworzywa sztucznego zgodnego ze standardem UL94-5VB;
- urządzenie musi być w 100% kompatybilne z wyspecyfikowanym kontrolerem sieci bezprzewodowej;
- równoczesna praca na częstotliwościach 2.4GHz oraz 5GHz;
- wsparcie dla 802.11ac 3x3 MIMO z prędkością przesyłania danych do 1300Mbps
- zasilanie: Power over Ethernet IEEE 802.3at (pobór mocy max. 17W);
- praca w trybie pojedynczego AP lub razem z kontrolerem;
- obsługa do 16 ESSID na radio z obsługą 802.1q VLAN;
- w trybie pracy z kontrolerem obsługa co najmniej następujących funkcjonalności: wykrywanie obcych AP, AP load balancing, szybki roaming L2/L3, captive portal, obsługa gości;
- minimum 1 port 10/100/1000Base-T;
- maksymalne wymiary: 180mm x 180mm x 44mm;
- maksymalna waga: 0,61kg;
- temperatura pracy: -10$^{o}$C do 50$^{o}$C;
- względna wilgotność pracy: 10%-90%;
- niepalność obudowy zgodna z UL94-5VB;
- wbudowane anteny o następujących minimalnych parametrach: 3x2,4GHz, 3x5GHz, 3dBi dla 2,4GHz, 5dBi dla 5GHz;
- przystosowane do montażu na suficie oraz na ścianie;
- obsługa standardów radiowych: 802.11 a/b/g/n/ac;
- ilość obsługiwanych strumieni przestrzennych: minimum 3;
- obsługa szerokości kanałów: 20MHz, 40MHz, 80MHz;
- zakres częstotliwości: 2,412-2,472GHz, 5,180-5,825GHz;
- wspierane kanały: dla 2,4GHz: 1-13 (Europa); dla 5GHz: 36-140 (Europa);
- obsługa ESSID: 16 na radio (sumarycznie 32);
- szybkość transmisji: do 450Mbps dla 2,4GHz, do 1300Mbps dla 5GHz;

- obsługa użytkowników: min. 350
- obsługa QoS: 802.11e/WMM, DSCP 802.1p, Airtime Fairness, Band Steering, konwersja multicast do unicast;
- funkcje bezpieczeństwa: (niezalecane - WEP, WPA/WPA2 mixed, WPA2-Personal), wymagane - WPA2-Enterprise (802.1x), WPA3, enkrypcja TKIP oraz AES, tagowanie 802.1q, izolacja stacji bezprzewodowych, DHCP snooping, firewall warstwy L2;
- tryby pracy: pojedynczy AP, tunelowane zarządzanie z centralnego kontrolera;
- zarządzanie: WEB (HTTP/HTTPS), SNMP v1, v2c, v3;
- funkcje mobilności: fast roaming L2 oraz L3;
- minimum 3 lata gwarancji;
- nie dopuszcza się instalacji, gdzie w danym miejscu są widoczne więcej niż 3 AP (brak zachodzenia na siebie kanałów 40MHz).

## 5.2 KONTROLER AP

- urządzenie sieciowe w zamkniętej architekturze o wysokości co najmniej 1U;
- minimum 4 porty LAN 10/100/1000Base-T;
- minimum 1 port szeregowy konsoli (interfejs RJ-45);
- wskaźniki LED co najmniej: Status, Zasilanie, HDD;
- wyświetlacz LCD na przednim panelu
- możliwość jednoczesnej obsługi minimum 300 punktów dostępowych, bez konieczności dokupowanie dodatkowych licencji;
- możliwość jednoczesnej obsługi lokalnych kont (Local Accounts) minimum 10000;
- możliwość jednoczesnej obsługi kont „na żądanie" (On-Demand Accounts) minimum 10000;
- obsługa następujących typów autentykacji: 802.1X, UAM (w przeglądarce), IP lub MAC;
- obsługa następujących serwerów autentykacji: serwer kont lokalnych, serwer kont na żądanie, serwer kont gości, RADIUS, LDAP, NT Domain, SIP, POP3;
- wbudowany Captive Portal, z możliwością pełnej konfiguracji i dynamicznej rekonfiguracji portalu z poziomu kontrolera, wraz z możliwością dynamicznej zmiany metod autentykacji; obsługa różnych portali dla różnych stref usługowych;
- obsługa stref usługowych bazujących na porcie fizycznym lub VLANie;
- obsługa dynamicznie generowanych kont na żądanie za pomocą następujących metod: rejestracja SMS, zakup przez PayPal, integracja z PMS, zestaw przenośnej klawiatury i drukarki (autentykacja za pomocą kodów QR);
- obsługa kont gości: ograniczenie czasowe, konfiguracja czasu reaktywowania konta gościa, rejestracja i aktywacja poprzez email;
- wbudowana obsługa kont portali społecznościowych: Facebook, Google+;
- obsługa następujących typów połączeń VPN: zdalne, lokalne, Site-to-Site;
- obsługa protokołów tunelowania: IPSec, PPTP;
- obsługa izolacji sieci: Intra-VLAN or port, Inter-VLAN or port;
- wykrywanie obcych AP (Rouge AP Detection): tak;
- obsługa funkcjonalności zwiększonej mobilności użytkowników, minimum: Fast Roaming, Cross Gateway Roaming, WISPr Smart Client, rozpoznanie typu urządzenia mobilnego w celu optymalizacji captive portalu, logowanie wielu urządzeń w obrębie jednego konta oraz możliwość limitowania ilości urządzeń, Automatyczne logowanie z użyciem kodu QR;
- pełna konfiguracja wszystkich usług za pomocą interfejsu WEB, wiele poziomów uprawnień kont administratorskich;
- synchronizacja czasu: NTP, ręczna;
- obsługa SNMP: minimum v2c;
- obsługa i zarządzanie punktami dostępowymi: automatyczne wykrycie AP, automatyczna konfiguracja AP z możliwością określenie różnych szablonów, dla różnych modeli AP, konfiguracja, backup oraz odtworzenie dla AP z poziomu kontrolera, firmware batch upgrade dla AP z poziomu kontrolera, zarządzanie AP zarówno w warstwie L2 jak i w warstwie L3, zarządzanie równomiernym obciążeniem punktów dostępowych (tzw. AP Load Balancing);

- obsługa i zarządzanie użytkownikami: tworzenie polityk w zależności od roli jak i czasu i lokalizacji, limitowanie pasma dla użytkowników, klasyfikacja ruchu w oparciu o 802.1P / DSCP, limitowanie równoległych sesji, obsługa ponownego przypisania IP po ponownej autentykacji;
- obsługa redundancji N+1 z automatyczną synchronizacją;
- wspierane protokoły IP: IPv4, IPv6;
- wbudowane mechanizmy sieciowe: DHCP Server, DHCP relay, NAT, wbudowany http Proxy Server, WAN port load balancing, obsługa dynamicznego routingu, lokalne rejestry DNS, wbudowana integracja z systemem PMS, wbudowany system tworzenia i rozliczenia kont, obsługa kont w wariantach czasowym oraz ilości transferu;
- obsługa logów aktywności sieciowej: SYSLOG, CAPWAP log, log zmiany konfiguracji, RADIUS Server log, logowanie zdarzeń użytkowników, Firewall log, DHCP Server/Lease Log, PMS Interface log, raport rozliczenia kont na żądanie, notyfikacja e-mail na temat statusu AP, logowanie na zewnętrzny serwer FTP;
- zasilanie: wbudowany zasilacz 230V AC, maksymalny pobór mocy 35W;
- minimum 3 letniej gwarancji producenta obejmującej sprzęt i oprogramowanie, wymiana na następny dzień roboczy, z dostępem do nowych funkcjonalności oraz nieodpłatnej aktualizacji oprogramowania, zgodnie z ofertą.

## 5.3. UTM/FIREWALL

A. Wymagania ogólne
- Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.
- Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
- System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
- W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość konfiguracji: Routingu, Firewall'a, IPSec VPN, IPS, Antywirus.
- System musi wspierać IPv6 oraz IPv4 w zakresie funkcji firewall i protokołów routingu dynamicznego.

B. Redundancja, monitoring i wykrywanie awarii
- W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Passive. Powinna istnieć funkcja synchronizacji sesji firewall.
- Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
- Monitoring stanu realizowanych połączeń VPN.
- System musi umożliwiać agregację linków w oparciu o protokół LACP.

C. Interfejsy, dyski, zasilanie
- System realizujący funkcję Firewall musi dysponować minimum: 10 portami Gigabit Ethernet RJ-45; 8 gniazdami SFP 1 Gbps; 4 gniazdami SFP+ 10 Gbps.
- System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
- W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- System realizujący funkcję Firewall musi być wyposażony w dysk SSD o pojemności minimum 120GB.
- System musi być wyposażony w zasilanie AC.

D. Parametry wydajnościowe
- W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 90.000 nowych połączeń na sekundę.

- Przepustowość Stateful Firewall: nie mniej niż 30 Gbps dla pakietów 1518 B.
- Wydajność szyfrowania VPN IPSec, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256: nie mniej niż 4 Gbps.
- Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 11 Gbps.
- Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3,2 Gbps.

E. Funkcje systemu bezpieczeństwa - w ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
- Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
- Kontrola Aplikacji.
- Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
- Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS.
- Ochrona przed atakami - Intrusion Prevention System.
- Kontrola stron WWW.
- Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
- Zarządzanie pasmem (QoS, Traffic shaping).
- Analiza ruchu szyfrowanego protokołem SSL.
- Analiza ruchu szyfrowanego protokołem SSH.

F. Polityki Firewall
- Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
- System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz translację jeden do jeden oraz jeden do wielu.
- W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

G. Połączenia VPN - system musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
- Wsparcie dla IKE v1 oraz v2.
- Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów.
- Obsługa protokołu Diffie-Hellman grup 19 i 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
- Tworzenie połączeń typu Client-to-Site oraz Site-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal.
- Mechanizm „Split tunneling” dla połączeń Client-to-Site.
- System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki oraz pracę w trybie Tunnel przy zastosowaniu dedykowanego klienta.

H. Routing i obsługa łączy WAN
- W zakresie routingu rozwiązanie powinno zapewniać obsługę: routingu statycznego oraz Policy Based Routingu.
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP.
- System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

I. Zarządzanie pasmem
- System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
- Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

J. Kontrola Antywirusowa
- Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
- System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
- Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.

K. Ochrona przed atakami
- Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
- Baza sygnatur ataków powinna zawierać minimum 1500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
- System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS.
- Mechanizmy ochrony (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL.
- Wykrywanie i blokowanie komunikacji do sieci botnet.

L. Kontrola aplikacji
- Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu nie bazując jedynie na wartościach portów TCP/UDP.
- Baza Kontroli Aplikacji powinna zawierać minimum 300 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- Powinny być kontrolowane aplikacje chmurowe co najmniej: Google Docs, Facebook, Dropbox.
- Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
- Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

M. Kontrola WWW
- Moduł kontroli WWW musi korzystać z bazy zawierającej miliony adresów URL pogrupowanych w kategorie tematyczne.
- W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, proxy avoidance.
- Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
- Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
- Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

N. Uwierzytelnianie użytkowników w ramach sesji
- System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu; Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP; Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych.
- Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego w kliencie VPN.
- Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory.

O. Zarządzanie
- Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

- Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
- System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3.
- System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
- Zgodność ze stosowanym w Spółce systemem centralnego zarządzania i monitorowania podsystemami urządzeń typu Firewall.

P. Logowanie
- System musi mieć możliwość logowania do aplikacji (logowania i raportowania), lub w ramach postępowania musi zostać dostarczony dedykowany komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, dedykowanej komercyjnej platformy sprzętowej lub programowej.
- W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
- Zamawiający nie dopuszcza możliwości wysyłania logów i raportów do chmury.
- Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
- Musi istnieć możliwość logowania do serwera SYSLOG.

Q. Certyfikaty
- Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall oraz ICSA lub EAL4 dla funkcji VPN.

R. Serwisy i licencje
- W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: kontrole aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres 60 miesięcy.

S. Gwarancja oraz wsparcie
- Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

T. Rozszerzone wsparcie serwisowe i inne wymagania
- System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym dniu roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres min. 60 miesięcy.
- Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5.

U. Oferent winien przedłożyć dokumenty:
- Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
- Certyfikat ISO 9001 podmiotu serwisującego.
- W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz.

2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

## 5.4. FIREWALL DB

System zabezpieczeń musi składać się z modułu wykonawczego działającego w warstwie sieciowej oraz zewnętrznego modułu zarządzającego.

A. Moduł wykonawczy:

1. System ochrony baz danych musi posiadać nie mniej niż następujące funkcje:
- Wyszukiwanie i klasyfikacja usług bazodanowych w sieci klienta
- Wyszukiwanie i klasyfikacja informacji w bazach danych. Klasyfikacja odbywać się musi zarówno poprzez wykorzystanie wbudowanych wzorców danych (jak numery kart kredytowych, dane personalne, dane finansowe, identyfikatory bankowe, dane medyczne etc.) jak i przez definiowanie własnych wyrażeń. Definicja uwzględniać musi nazwy tabel, kolumn oraz rekordy w tabelach przy użyciu wyrażeń regularnych. Musi istnieć możliwość wykorzystania wykrytych informacji przy definiowaniu reguł monitoringu.
- Testowanie podatności systemów bazodanowych, przy uwzględnieniu analizy podatności systemu operacyjnego oraz baz danych na znane typy ataków, błędy konfiguracyjne, brak aktualizacji oprogramowania, weryfikacja zabezpieczenia kont użytkowników bazodanowych. Rozwiązanie musi posiadać funkcję uwierzytelnienia w systemie operacyjnym oraz w bazie danych w celu wykonania powyższych testów. Uwierzytelnienie w systemie operacyjnym obsługiwać powinno nie mniej niż protokoły SSH oraz NTLM. W proponowanym rozwiązaniu zawarta musi być licencja na testowanie podatności nie mniej niż 100 instancji bazodanowych.
- Monitoring dostępu do informacji (ang. Database Activity Monitoring, zwany dalej DAM) w bazach danych (z uwzględnieniem języków DCL, DML, DDL, TCL, procedur składowanych). Definiowanie polityki monitoringu musi uwzględniać nie mniej niż następujące kryteria: użytkownik bazodanowy oraz aplikacyjny, tabele, kolumny, typ danych, schemat bazy danych, ilość wystąpień, dostęp do danych wrażliwych (zdefiniowanych poprzez system wykrywania danych z punktu 1.a) oraz dane pobrane z zewnętrznych systemów (wymagana jest w tym celu integracja z Active Directory, serwerów LDAP, pobranie danych z pliku oraz z baz danych przy wykorzystaniu zapytań SQL).
- Aktywna ochrona baz danych – Database Firewall

2. Opisana w punkcie 1.e ochrona baz danych oznacza:
- Definiowanie reguł dostępu użytkowników bazodanowych do poszczególnych obiektów w bazie danych poprzez automatyczne tworzenie (na podstawie analizy ruchu sieciowego) listy użytkowników oraz listy zapytań sql, jakie użytkownik może wykonać w odniesieniu do tabel baz danych. Musi istnieć możliwość definiowania oddzielnych reguł dostępu w odniesieniu do tabel z danymi wrażliwymi, sklasyfikowanymi przez moduł opisany w punkcie 1.b. System musi posiadać dodatkowo możliwość automatycznego tworzenia list: źródłowych adresów IP, nazw aplikacji klienckich oraz nazw systemu operacyjnego, z których użytkownik ma dostęp do zasobów. Na podstawie powyższych list definiowane są reguły polityki bezpieczeństwa.
- Tworzenie list tabel, do których poszczególni użytkownicy bazodanowi nie mogą mieć dostępu. Musi istnieć również możliwość definiowania dni tygodnia oraz godzin, w jakich dany użytkownik może nawiązać połączenie z bazą danych.
- W logach dotyczących zarejestrowanych naruszeń / anomalii wymagane są co najmniej następujące informacje: nazwa użytkownika bazodanowego, dodatkowe dane o użytkowniku pochodzące z zewnętrznych systemów (moduł opisany w punkcie 1.d), źródłowy adres IP, pełne zapytanie SQL wykonane przez użytkownika.
- Możliwość zablokowania ruchu wykorzystującego podatności wykryte w bazach danych poprzez moduł opisany w punkcie 1c.
- Wykrywanie znanych ataków SQL Injection oraz ataków na niższych warstwach sieciowych skierowanych na usługę bazy danych. Aktualizacje sygnatur muszą być dostarczone przez producenta co najmniej raz w miesiącu.

3. System DAM musi działać niezależnie od opisanego w punkcie 2 modułu aktywnej ochrony baz danych, zatem możliwe jest zdefiniowanie bardzo szczegółowych reguł monitoringu dostępu do danych, zapewniając jednocześnie odpowiedni poziom ochrony dla całości ruchu do bazy.
4. System DAM musi wykrywać komendy wykonywane na system zarządzania bazą danych, a także identyfikować próby eksportu danych z tabel bezpośrednio do plików.
5. Archiwizowane logi dotyczące aktywności użytkowników muszą być zapisywane w postaci zaszyfrowanej oraz muszą zostać skompresowane
6. Musi istnieć możliwość zmiany wszystkich haseł użytkowników systemu ochrony baz danych.
7. Rozwiązanie musi posiadać funkcję wysyłania informacji o zdarzeniach poprzez protokół SNMP, syslog, wiadomość e-mail oraz uruchomienia skryptu
8. System musi posiadać gotowe szablony raportów dotyczące:
- Alarmów bezpieczeństwa
- Zdarzeń systemowych
- Zmian w profilach baz danych
- Monitorowania aktywności użytkowników na bazach
- Wykonanych testów podatności systemów, klasyfikacji usług oraz informacji w bazach danych.
- Zgodności z wymaganiami regulacji, m.in.: PCI, SOX,
9. Musi istnieć możliwość wykorzystania informacji z zewnętrznych źródeł (opisanych w punkcie 1.d) w raportach.
10. Musi istnieć możliwość tworzenia własnych raportów, zarówno w formie tekstowej jak i reprezentacji graficznej, a także automatycznego, cyklicznego wysyłania raportów wiadomością e-mail.
11. Producent musi zapewnić aktualizację systemu, uwzględniając co najmniej: sygnatury ataków, listę reguł polityki bezpieczeństwa oraz monitorowania aktywności użytkowników na bazach danych, listę testów podatności baz danych oraz listę raportów.
12. System musi monitorować oraz zabezpieczać co najmniej następujące systemy baz danych: Oracle, MSSQL, MySQL, Sybase, Informix, IBM DB2, Netezza, Teradata. Jako zabezpieczenie rozumiane jest zarówno monitorowanie aktywności (audyt) jak i analiza behawioralna całości ruchu nawet nie poddanego audytowi
13. Proponowane rozwiązanie musi zostać dostarczone wraz z licencjami na funkcje automatycznego logowania do baz danych i pobierania wykazu uprawnień użytkowników do poszczególnych obiektów bazy danych, tak aby możliwe było zwizualizowanie ścieżki za pośrednictwem której użytkownik posiada dostęp do konkretnego obiektu. Moduł ten musi być dostarczony do obsługi co najmniej 25 baz oraz musi pozwalać na diagnozowanie wypadków zbyt rozległych praw lub niewykorzystywanych uprawnień.
14. Proponowane rozwiązanie musi zostać dostarczone (wraz z licencjami) wraz z aplikacjami monitorującymi ruch lokalnie na serwerach bazodanowych (zwanymi dalej aplikacją agent). W cenie zakupionego systemu dostarczonych powinno być nie mniej niż 25 aplikacji agent. Wspierane muszą być następujące systemy operacyjne: AIX, HP-UX, RedHat, SUSE, OEL, Solaris, Windows. Aplikacja agent ma na celu wysyłanie informacji o lokalnej aktywności użytkowników do modułu wykonawczego. Moduł wykonawczy musi posiadać możliwość weryfikacji stanu działania agenta.
15. Agent musi posiadać możliwość pracy w trybach – sniffing oraz inline. Jako sniffing rozumiany jest tryb pracy bez opóźnień z możliwością terminacji sesji w przypadku wykrycia nadużycia. Tryb inline rozumiany jest jako wstrzymywanie ruchu od użytkownika do systemu bazodanowego, przesyłanie ruchu do jednostki wykonawczej oraz oczekiwanie na decyzję czy zapytanie jest zgodne z polityką bezpieczeństwa. Agent musi posiadać możliwość blokowania ruchu w przypadku wykrycia incydentu.
16. Agent musi wykrywać nowo zdefiniowane interfejsy bazy danych i automatycznie dodawać je do reguł monitorowania
17. Agent musi posiadać możliwość definiowania reguł, zgodnie z którymi aplikacja wybierać będzie ruch który ma być wysyłany do jednostki wykonawczej
18. Agent musi posiadać możliwość kompresji ruchu przesyłanego do urządzeń
19. Wymagane jest wsparcie techniczne obejmujące naprawę sprzętu w przypadku awarii, obsługę problemów technicznych w godzinach pracy oraz dostęp do aktualizacji oprogramowania oraz dokumentacji technicznej ważne przez co najmniej 36 miesięcy w ramach gwarancji.
20. System musi zostać zainstalowany jako maszyna wirtualna w posiadanym przez zamawiającego systemie Vmware Vsphere.

<u>B. Moduł zarządzający – 1 szt. dla systemu złożonego z kilku modułów wykonawczych:</u>

W ramach realizacji Zamówienia dostawca dostarczy i uruchomi centralny system zarządzania zarówno Database Firewall oraz Web Appliaction Firewall zapewniający wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza Internet.
1. Centralny serwer zarządzający systemu zabezpieczeń musi być dostarczony w formie gotowej maszyny wirtualnej działającej w środowisku witalizacyjnym w infrastrukturze zamawiającego lub w zakresie aplliance systemu bazodanowego.
2. Serwer zarządzający oferowanego rozwiązania musi być dostępny poprzez interfejs przeglądarki Web w celu eliminacji konieczności instalacji dodatkowego oprogramowania na stacji administratora. Konfiguracja wstępna poprzez terminal i linię komend, zarządzanie musi odbywać się poprzez interfejs przeglądarki internetowej.
3. Wymagane jest zarządzanie zorientowane zadaniowo. Oznacza to, iż musi istnieć mechanizm informowania administratora o wykonaniu/nie wykonaniu na czas zadania zleconego innym użytkownikom systemu.
4. Wszystkie zamawiane elementy systemu zabezpieczeń muszą być dostarczone przez jednego producenta i zarządzane z pojedynczego centralnego serwera zarządzania.
5. Serwer zarządzający musi oferować interfejs API pozwalający na odczyt i zmianę konfiguracji
6. Rozwiązanie musi umożliwiać dostęp do bazowego systemu operacyjnego na najwyższych uprawnieniach
7. Uwierzytelnianie użytkowników oferowanego rozwiązania musi być możliwe za pomocą protokołu RADIUS oraz poprzez integrację z Active Directory
8. Serwer zarządzający musi posiadać wbudowany mechanizm RBAC który umożliwia integrację z Active Directory poprzez przypisanie roli w zależności od przynależności do określonej grupy w Active Directory
9. Całość konfiguracji oraz repozytorium logów musi być przechowywane na centralnym serwerze zarządzania
10. Zbudowane profile muszą być przechowywane na centralnym serwerze zarządzania
11. Wymagane jest wsparcie techniczne producenta, ważne przez 36 miesięcy obejmujące obsługę problemów technicznych w godzinach pracy oraz dostęp do aktualizacji oprogramowania oraz dokumentacji technicznej w ramach gwarancji.
12. W przypadku niemożności umieszczenia modułu zarządzania w przestrzeni wirtualnej, wykonawca musi dostarczyć odpowiedni serwer fizyczny.

## 5.5. SYSTEM DO ZARZĄDZANIA SPRZĘTEM INFORMATYCZNYM I OPROGRAMOWANIEM

A. Zarządzanie sprzętem
1. Zdalne wykrywanie komputerów w sieci
2. Skaner sieci umożliwia wykrycie aktywnych urządzeń sieciowych z wykorzystaniem protokołu SNMP
3. Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o aktualizacji
4. Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy
5. Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu
6. Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM
7. Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany
8. Wykorzystanie Active Directory do tworzenia drzewa sieci
9. Pełna synchronizacja rekordów komputerów (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)
10. Możliwość pogrupowania wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów, lokalizacji, statusów)
11. Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc. )
12. Możliwość tworzenie własnych typów elementów wyposażenia

13. Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: Switch, Router, Access Point, Bridge, Modem, NAS, UPS, itd.)
14. Automatyczne wykrywanie monitorów
15. Automatyczne tworzenie zestawów: Komputer + Monitor
16. Automatyczne tworzenie zestawów: host+ maszyny wirtualne
17. Automatyczne wykrywanie typu komputera (Desktop\Notebook\Serwer\Kontroler domeny) na podstawie wyników skanowania sprzętu
18. Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.)
19. Możliwość wiązania elementów wyposażenia w zestawy
20. Możliwość użycia makrodefinicji w celu spersonalizowania nazw elementów w drzewku wyposażenia.
21. Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach
22. Możliwość podpinania dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików
23. Raport dodanych załączników
24. Możliwość przypisania sprzętu do konkretnych osób
25. Możliwość przypisania sprzętu do wybranej firmy
26. Automatyczne wyznaczanie 'Głównego użytkownika' komputera
27. Możliwość tworzenia wielu powiązań wyposażenia z użytkownikiem.
28. Możliwość przypisania sprzętu do dowolnej lokalizacji
29. Możliwość definiowania własnych, dowolnych atrybutów sprzętu
30. Możliwość przypisania stałego atrybut COA, który będzie uwzględniany na raportach wyposażenia i audytu
31. Możliwość określenia informacji o wykorzystywanej wirtualizacji
32. Automatyczne wykrywanie, czy komputer jest maszyną wirtualną
33. Wykrywanie maszyn wirtualnych typu: Parallels Virtual Platform
34. Wykrywania komputerów typu All-In-One
35. Automatyczne wykrywanie typów stacji roboczej (Tower\Desktop\SFF\uSFF)
36. Możliwość definiowania statusów dla sprzętu (Nowy, Do kasacji, W serwisie, itd. )
37. Aktywnym komputerom (bez określonego statusu) przydzielany jest status 'W użyciu'
38. Możliwość definiowania szczegółowych informacji finansowych
39. Obsługa walut w danych finansowych
40. Definiowanie bazy dostawców sprzętu i oprogramowania
41. Automatyczne tworzenie historii zmian sprzętu
42. Raport zbiorczy historii zmian w sprzęcie
43. Ewidencja zdarzeń serwisowych
44. Możliwość dodawania notatek\komentarzy dla zdefiniowanych obiektów zasobów
45. Informacja na temat pojemności dysków twardych oraz wolnego miejsca
46. Generowanie protokołów przekazania\zwrotu\utylizacji sprzętu.
47. Możliwość generowania Karty informacyjnej dla elementu wyposażenia
48. Generowanie etykiet z kodami kreskowymi do inwentaryzacji wyposażenia
49. Drukowanie lub zapisywanie do pliku raportów ze szczegółami sprzętu
50. Możliwość określenia loga firmy oraz użycia go na wydrukach.
51. Możliwość cyklicznego wykonywania skanowania sprzętu z różnymi ustawieniami
52. Możliwość porównywania wyników skanowania sprzętu.
53. Skanowanie WMI w skanerze "dyskietkowym" (Pen Drive)
54. Funkcjonalności monitorowania dziennika zdarzeń systemu Windows
55. Automatyczne monitorowanie i raportowanie zmian w podzespołach sprzętu
56. Możliwość zdalnego wykonania skryptów (batch) - Obsługa zadań jednorazowych i cyklicznych. Możliwość wykonania zadania dla wszystkich komputerów (uwzględnia komputery, które zostaną dodane w przyszłości)
57. Edytor skryptów (batch) z funkcją kolorowania składni.
58. Możliwość wykorzystania predefiniowanych skryptów (batch)
59. Możliwość importu informacji o wyposażeniu z pliku CSV
60. Mechanizm automatycznej ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu)

61. Mechanizm automatycznego tworzenia rekordów producenta sprzętu (na podstawie wyników skanowania sprzętu).
62. Obsługa kodów QR.
63. Możliwość powiązania wyposażenia z działem.
64. Funkcjonalność przeniesienia utylizowanego wyposażenia do archiwum
65. Automatyczna aktualizacji adresów IP komputerów bez zainstalowanego agenta.
66. Agent odczytuje identyfikator SID komputera
67. Możliwość zarządzania sprzętem przez aplikacje mobilną (Android, Windows Phone)

B. Zarządzanie oprogramowaniem

1. Inwentaryzacja licencji
2. Kompletna informacja na temat posiadanych licencji (typ, producent, czas ważności, informacje finansowe)
3. Możliwość przypisania licencji do komputera
4. Podpinanie załączników w dowolnym formacie
5. Definiowanie wymaganych atrybutów legalności (faktura, nośnik, COA, etc.)
6. Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecania skanów
7. Zdalny skan komputerów (bieżący lub okresowy)
8. Możliwość zmiany priorytetu skanowania oprogramowania.
9. Szablony ustawień skanowania
10. Identyfikacja zainstalowanych aplikacji
11. Możliwość rozliczania pakietów aplikacji
12. Możliwość rozliczania systemów operacyjnych
13. Rozliczanie licencji typu „Downgrade”
14. Możliwość cyklicznego wykonywania skanowania plików z różnymi ustawieniami
15. Prawidłowe rozpoznawanie aplikacji nawet mimo zmiany jej nazwy
16. Możliwość określania masek plików dla publikacji elektronicznych (e-book).
17. Skanowanie plików skompresowanych
18. Możliwość skanowania oraz identyfikacji zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lzh, lzma, msi, nrg, rar, tar, taz
19. Możliwość predefiniowanie profili skanowania (np. profil wzorcowy)
20. Skanowanie komputerów niepodłączonych do sieci
21. Możliwość wysyłania wyników skanowania offline na serwer FTP (Audyt)
22. Możliwości przekazanie konfiguracji wzorcowej dla skanera offline
23. Śledzenie zmian w stanie zainstalowanego oprogramowania
24. Możliwość porównania wyników skanowania oprogramowania
25. Audyt oprogramowania rozliczany automatycznie - informacja o stanie posiadanych licencji i faktycznie zainstalowanych programach
26. Historia audytów (Wyniki audytów są przechowywane w bazie danych - można do nich wracać w dowolnej chwili, porównywać je i generować stosowne raporty)
27. Wykrywanie plików multimedialnych
28. Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika)
29. Odczytywane są informacje o składnikach aplikacji, których programy instalacyjne nie są zgodne ze standardem MSI
30. Jeśli aplikacja została zainstalowana dla konkretnego użytkownika, odczytywany jest jego SID
31. Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji\pakietów\systemów operacyjnych
32. Mechanizm informujący o nowej bazie wzorców oprogramowania
33. Możliwością definiowania własnych wzorców oprogramowania
34. Wsparcie procesu Audytu przez zaimportowanie materiału zdjęciowego i jego obróbkę
35. Wykrywanie kluczy/identyfikatorów programów
36. W przypadku aktywacji systemu Windows z użyciem serwera KMS, klucza MAK (Multiple Activation Keys) lub VLK (Volume License Keys) odczytywane jest 5 ostatnich znaków klucza
37. Odczytywanie informacji o częściowych kluczach pakietów Microsoft Office
38. Definiowanie licencji przeznaczonych do przyszłego zakupu
39. Definiowanie kluczy seryjnych i przypisywanie do licencji
40. Gotowe metryki audytowanego komputera - załącznik do protokołu przekazania stanowiska komputerowego (sprzęt + oprogramowanie)
41. Drukowanie lub zapisywanie do pliku raportów ze szczegółami oprogramowania

42. Zbiorcze raporty wyników skanowania oprogramowania - Pakiety, pliki, systemy operacyjne, kluczy zainstalowanych aplikacji
43. Raport z informacjami o pakietach oprogramowania uwzględniający parametry: przybliżona wielkość, adres strony internetowej, lokalizacja pliku instalacyjnego, architektura aplikacji, itd.
44. Raport z informacjami o systemach operacyjnych uwzględniający parametry: Data instalacji, Architektura systemu, Wersja kompilacji, itd.
45. "Wielkie raporty" (Możliwość utworzenia zbiorczych raportów obejmujących np. wszystkie przeskanowane pliki)
46. Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (*.msi)
47. Możliwość utworzenia harmonogramu deinstalacji oprogramowania
48. Możliwości wygenerowania skryptu deinstalacji aplikacji na podstawie otrzymanych wyników skanowania oprogramowania
49. Automatyczne tworzenie wzorców oprogramowania dla systemów operacyjnych.
50. Automatyczne dodawanie informacji o wydawcy oprogramowania dla nowych wzorców, tworzonych na podstawie wyników skanowania

C. Kontrola wykorzystania sprzętu i oprogramowania

1. Dane gromadzone dla konkretnych użytkowników (na bazie loginów) - jeden użytkownik może mieć przypisanych wiele loginów i pracować na różnych komputerach
2. Możliwość pogrupowania pracowników z podziałem na jednostki organizacyjne w firmie (np. względem działów)
3. Możliwość określenia firmy do której należy pracownik
4. Możliwość określenia przełożonego dla pracownika
5. Możliwość prezentacji 'stanu pracownika' (obecny, nieobecny, nowy).
6. Możliwość prezentacji 'statusu pracownika' (Zatrudniony, zwolniony, itd.)
7. Możliwość przeniesienia rekordu pracownika do archiwum
8. Funkcjonalności automatycznego generowania zmian rekordu pracownika – Historia pracownika
9. Raport zbiorczy historii zmian w rekordach pracowników
10. Analiza aktywności użytkowników
11. Analiza zdarzeń sesji użytkownika (Logowanie, Wylogowanie, Zablokowanie, Odblokowanie, Nawiązanie połączenia RDP, Zakończenie połączenia RDP )
12. Analiza przerw w pracy
13. Analiza jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków)
14. Analiza wykorzystania poszczególnych aplikacji w czasie
15. Analiza czasu działania aplikacji na pierwszym planie i sumarycznie
16. Statystyki najczęściej wykorzystywanych aplikacji
17. Statystyki wykorzystania komputerów przez poszczególnych użytkowników
18. Statystyki aktywności pracownika i grup pracowników
19. Możliwość generowania raportów z monitoringu pracowników dla wybranego zakresu godzin
20. Możliwość utworzenia działów firmy oraz określenia stawek godzinowych dla pracowników.
21. Kontrola wydruków - historia zadań drukowania zainicjowanych przez poszczególnych użytkowników
22. Kontrola wydruków - Monitoring wydruków obejmuje szczegółowe parametry (np. format papieru, orientacje, skalowanie, itd.)
23. Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz-b/kolor, dpi)
24. Monitorowanie wydruków na drukarkach sieciowych.
25. Monitorowanie użytkowników stacji terminalowych
26. Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.)
27. Blokowania niepożądanych aplikacji. Programy mogą być blokowane dla całej firmy lub tylko dla wybranych użytkowników.
28. Możliwość autoryzacji nośników zewnętrznych
29. Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych
30. Możliwość określenia praw dostępu w zależności od typu urządzenia, np. Pendrive, CD/ROM.
31. Możliwość blokowania dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.)
32. Definiowanie bazy informacji o napędach zewnętrznych.
33. Komunikacja z użytkownikami (Skype, mail) bezpośrednio z zakładki Pracownicy
34. Odczytywanie informacji o użytkownikach z Active Directory

35. Pełna synchronizacja rekordów użytkowników (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)
36. Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień
37. Możliwość podglądu zdjęcia przypisanego do pracownika.
38. Możliwość przypisania do pracownika załączników (pliki).
39. Możliwość przypisania do pracownika notatek.
40. Ewidencja zdarzeń przypisanych do użytkowników
41. Powiadomienia przesyłane w czasie rzeczywistym o zdarzeniach, które miały miejsce w obrębie infrastruktury, systemu lub użytkowników
42. Powiadomienia o kończącej się gwarancji\umowie serwisowej dla zasobu.
43. Możliwości określenia typu gwarancji dla zasobu
44. Powiadomienia o utworzeniu monitora, wykryciu maszyny wirtualnej
45. Informacje o awariach, poczynaniach użytkowników: zakończonej aktualizacji, akcji podpięcia przenośnych dysków, włożenia płyt do napędów CD/DVD, śledzenie uruchomienia aplikacji przez użytkownika, monitorowanie o małej ilości miejsca
46. Informacje o ostatnio zalogowanych osobach na stacjach klienckich.
47. Możliwość centralnego zarządzania wynikami skanowania sprzętu i oprogramowania
48. Funkcja automatycznego tworzenia działów na podstawie informacji odczytanych z Active Directory.

D. Kontrola wykorzystania Internetu

1. Raporty dotyczące aktywności użytkowników w Internecie oparte na loginach - jeden użytkownik może mieć przypisanych wiele loginów i pracować na różnych komputerach
2. Dokładna analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki )
3. Monitoring stron internetowych dla protokołu http\https (IE,Chrome, Firefox, Opera, Edge)
4. Analiza liczby wejść na poszczególne strony lub domeny
5. Blokowanie stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokowanie WWW po zawartości (ContentType)
6. Blokowanie stron internetowych dla protokołu http\https (Chrome, Firefox, Opera, Edge)
7. Analiza odwiedzanych domen i stron
8. Kategoryzowanie stron internetowych

E. Zdalny helpdesk

1. Możliwość rejestracji i obsługi incydentów.
2. Opis zgłoszenia w formacie HTML
3. Możliwość dodawania załączników do incydentów
4. Możliwość tworzenia własnych dodatkowych atrybutów dla zgłoszeń
5. Możliwość określania relacji pomiędzy incydentami (np.. Kopia, Incydent nadrzędny)
6. Możliwość tworzenia notatek dla incydentów
7. Możliwość wykorzystania funkcji monitoringu czasu pracy nad incydentem (time tracking)
8. Notyfikacje e-mail o utworzeniu\zmianie\usunięciu incydentu.
9. Możliwość określenia dodatkowych subskrybentów dla notyfikacji e-mail dotyczącej zmian w incydencie
10. Notyfikacje e-mail o zbliżających się terminach realizacji incydentu (DeadLine)
11. Automatyczny import wiadomości e-mail, jako zgłoszeń helpdesk
12. Obsługa wielu kont pocztowych (Import + notyfikację email)
13. Możliwość określania uprawnień do incydentów (Publiczne, Prywatne, dla określonych działów)
14. Możliwości personalizowania widoku raportu listy incydentów
15. Możliwość zarządzania filtrami zdefiniowanymi dla listy incydentów
16. Obsługa nazwy DNS oraz adresów IP (IPv4, IPv6) dla incydentów
17. Możliwość wydruku historii incydentu
18. Funkcjonalność kalendarza (Planowanie rozwiązania incydentów)
19. Możliwość powiązania incydentu z elementem zasobów
20. Zdalne operacje na plikach i katalogach
21. Zdalne zarządzanie procesami i rejestrem
22. Monitorowanie na odległość pracy wykonywanej na komputerze
23. Zdalny podgląd pulpitów wielu stacji ( Funkcja Company Online)
24. Możliwość wywołania Windows Remote Desktop na danej stacji z poziomu aplikacji
25. Możliwość wysyłania wiadomości do użytkowników

26. Możliwość uruchamiana na stacjach programów z wiersza poleceń Command Line
27. Możliwość zdalnego uruchamiania komputera za pomocą funkcji Wake-On-Lan
28. Możliwość zdalnego przejęcia kontroli nad stacją roboczą
29. Możliwość zablokowania klawiatury i myszki na stacji klienckiej w trakcie przejęcia kontroli pulpitu zdalnego.
30. Możliwość przesłania kombinacji klawiszy Ctrl + Alt + Delete w zdalnym pulpicie.
31. Możliwość wysłania pytania o zgodę na zdalny dostęp lub wysłania komunikatu z informacją o rozpoczęciu podglądu pulpitu.
32. Możliwości podglądu pulpitu zdalnego w osobnym oknie z opcją fullscreen
33. Obsługa wielu monitorów dla podglądu pulpitu.
34. Możliwość wyboru monitora, z którego ma być przekazywany obraz podglądu pulpitu
35. Możliwość nawiązania połączenia pulpitu zdalnego z wieloma komputerami jednocześnie
36. Możliwość połączenia pulpitem zdalnym w konfiguracji NAT-NAT
37. Funkcjonalności zdalnego zarządzania usługami systemu Windows

F. Pracownik

1. Możliwość przeglądania podstawowych informacji dotyczących aktywności pracy
2. Możliwość przeglądania ostatnio zgłoszonych incydentów
3. Dostęp webowy do statystyk monitoringu, zgłoszeń helpdesk oraz powiązanych z pracownikiem zasobów

G. Inne

1. Możliwość określania praw dostępu do grup zasobów lub pracowników
2. Aplikacja desktopowa służąca do zarządzania systemem może być zainstalowana na dowolnej liczbie komputerów ("Licencja pływająca")
3. Dodatkowa aplikacja webowa umożliwiająca dostęp do systemu i zarządzanie systemem
4. Wersja angielska (en-US) interfejsu użytkownika.
5. Możliwość wyboru silnika bazy danych - MS SQL (również darmowe dystrybucje) lub PostgreSQL (darmowy, bez limitów wielkości bazy danych)
6. Swobodna migracja danych pomiędzy MS SQL i PostgreSQL
7. Zdalna instalacja i deinstalacja agentów na stacjach roboczych
8. Odczytywanie struktury sieci z Active Directory
9. Mechanizm automatycznego tworzenia komputera na podstawie danych przesłanych przez agenta.
10. Mechanizm automatycznego tworzenia pracownika na podstawie danych przesłanych przez agenta.
11. Automatycznie dodane komputery\pracownicy są powiązane z odpowiednią grupą zgodną z OU w Active Directory.
12. Możliwość definiowania nieograniczonej liczby użytkowników systemu
13. Możliwość określenia ról dla kont systemu : Administratorzy, Menadżerowie, Zarządcy.
14. Indywidualny login i hasło dla poszczególnych użytkowników
15. Możliwość logowania z użyciem poświadczeń użytkownika systemu Windows.
16. Możliwość automatycznego logowania do systemu.
17. Zarządzanie uprawnieniami użytkowników - możliwość ograniczenia dostępu do poszczególnych funkcji programu
18. Zabezpieczenie Agentów przed nieautoryzowanym dostępem
19. Możliwość eksportowania danych do plików zewnętrznych (Excel, html, CSV, PDF, TXT, MHT, RTF, BMP)
20. Przystosowanie do pracy w sieciach WLAN
21. Możliwość podglądu aktualnych zadań serwera programu.
22. Centrum informacji - przekrojowy raport na temat zdarzeń oraz statusu monitorowanych komputerów i użytkowników
23. Wielopoziomowe drzewo lokalizacji
24. Możliwość wyszukiwania danych w tabelach raportów.
25. Możliwość dowolnego definiowania grup sprzętu i użytkowników
26. Możliwość tworzenia dowolnych raportów ad-hoc - sortowanie kolumn grupowanie, ukrywanie/odkrywanie kolumn, zaawansowane filtrowanie danych w oparciu o funkcje logiczne
27. Możliwość definiowania i zapamiętywania własnych widoków
28. Możliwość eksportu danych bezpośrednio do MS Excel
29. Budowanie zestawień metodą drag'n'drop

30. Budowa modułowa z możliwością przypisywania określonych wtyczek programu (funkcji) do poszczególnych Agentów
31. Obsługa protokołu SSL zapewniającego bezpieczną komunikację Master-Serwer oraz Agent-Server.
32. Mechanizm kompresji pakietów danych przesyłanych przez Agenta.
33. Możliwość automatycznego wykrywania lokalizacji serwera aplikacji (WS-Discovery)
34. Możliwość przekazania agentowi nowych parametrów połączenia z usługą programu server (serwer zapasowy)
35. Możliwość definiowania konfiguracji serwera proxy dla połączenia Agent-Server.
36. Mechanizm zdalnego pobierania bieżących aktualizacji do programu
37. Help kontekstowy wraz z podręcznikiem użytkownika w polskiej wersji językowej
38. Dostęp do bazy wiedzy systemu
39. System pomocy kontekstowej oraz tool-tips
40. Możliwość definiowania ustawień pracy Agentów (optymalizacja dla dużej liczby komputerów)
41. Możliwość wykorzystania dedykowanego narzędzia, dostarczanego z systemem, do wykonywania kopii bazy danych, niezależnie od wersji silnika bazy danych (MSSQL, PostgreSQL). Możliwość uruchomienia narzędzia backupu bazy w trybie wsadowym.
42. Automatyczna i manualna konserwacja bazy danych
43. Manualna i automatyczna konserwacja bazy danych - możliwość usuwania wyników skanowania oprogramowania.
44. Możliwość personalizacji pakietu instalacyjnego agenta.

H. Specyfikacja techniczna

1. Aplikacja Master\Server\Agent musi istnieć w wersji x86\x64.
2. Wymagana rozproszona architektura systemu: Serwer, Master, Agent (Możliwa praca każdego z komponentów na różnych komputerach )
3. Praca w oparciu zarówno o komercyjną bazę danych jak i darmową.
4. Obsługa systemów operacyjnych - Agent: minimum 2008 Server, 2008 Server R2, 2012 Server, Windows 7, Windows 8.x, Windows 10, Windows 11
5. Obsługa systemów operacyjnych - Master : Minimum 2008 Server, 2008 Server R2, 2012 Server, Windows 7, Windows 8.x, Windows 10, Windows 11
6. Obsługa systemów operacyjnych Serwer, minimum - Vista, 2008 Server, 2008 Server R2, 2012 Server, Windows 7, Windows 8.x, Windows 10, Windows 11

## 5.6. SYSTEM MONITORINGU INFRASTRUKTURY SIECIOWEJ

A. Moduł monitorowania infrastruktury:
1. Oprogramowanie powinno posiadać Wymagana możliwość uruchomienia na platformie linux lub windows.
2. Oprogramowanie powinno zapewniać mechanizm równoważenia obciążenia oraz zapewnienia redundancji elementów zbierających dane od agentów aplikacyjnych.
3. Oprogramowanie musi:
- monitorować wielowarstwowe aplikacje wykonane w technologii Java, działające na serwerach aplikacyjnych JBoss, WebSphere, Weblogic oraz innych zgodnych z technologią J2EE,
- wykrywać i ewidencjonować każdą transakcję wykonywaną w aplikacji bez potrzeby definiowania zależności pomiędzy komponentami.
- Prezentować wszystkie pojedyncza transakcje z dowolnie wybranego zakresu czasowego na wspólnym panelu (ang. dashboard)
- Ewidencjonować przebieg wszystkich transakcji pomiędzy wszystkimi komponentami aplikacji w monitorowanym środowisku z możliwością uzyskania następujących informacji o każdej z pojedynczych transakcji: drzewo wywołania kodu Java w ramach ścieżki wykonania – do poziomu nazwy wywoływanej metody. Oprogramowanie nie może ograniczać liczby monitorowanych klas i metod; czasach odpowiedzi serwera do aplikacji klienckiej jak i całkowitym czasie wykonania transakcji po stronie serwera (wątków synchronicznych oraz asynchronicznych); czasy wykonania pojedynczych metod; wartość parametrów wywołania wskazanych metod. Jeżeli parametr nie jest serializowany, oprogramowania powinno dostarczać mechanizm dynamicznego (bez potrzeby modyfikacji kodu i struktury aplikacji) zastosowania zewnętrznego deserializatora

- zbierać i monitorować wszystkie zapytania SQL wykonywane z poziomu monitorowanej aplikacji z możliwością ich powiązania z transakcjami, które dane zapytania wykonują,
- posiadać Wymagana możliwość prezentowania na wykresach dowolnych, konfigurowalnych wartości z transakcji
- pozwalać na tworzenie wykresów.
- umożliwiać analizę użycia pamięci aplikacji
- posiadać własny interfejs do tworzenia lub konfigurowania własnych wtyczek monitorujących,
- zapewnić mechanizmy bezpieczeństwa w zakresie dostępu do danych wrażliwych

4. Oprogramowanie musi wspierać definiowanie transakcji na podstawie dowolnych kryteriów, np.:
- URL,
- Wartość parametru z nagłówka HTTP,
- Wartość parametru z zapytania GET lub POST,
- Wartość atrybutu sesji HTTP,
- Wykonanie konkretnej metody w kodzie Java,
- Wykonanie konkretnego zapytania SQL,
- Wywołanie konkretnej usługi WebService.

5. Oprogramowanie ma umożliwiać monitoring podstawowych parametrów systemowych (CPU, pamięć, zajętość dysków, utylizacja interfejsów sieciowych), komponentów środowiska aplikacyjnego – zarówno tych, które hostują serwery aplikacyjne Java, jak i tych, które nie hostują aplikacji w technologii Java (np. serwery bazodanowe, serwery Nginx, serwery Apache działające w ramach systemów operacyjnych z rodziny Unix/Linux).
6. Oprogramowanie musi zbierać informacje o wszystkich wyjątkach (obsłużonych lub nie). Musi istnieć Wymagana możliwość zobaczenia szczegółowych informacji na temat transakcji, które wygenerowały wyjątek albo wpis do logu.
7. Oprogramowanie musi dawać Wymagana możliwość wyświetlenia transakcji dla każdego wybranego użytkownika, nawet jeśli nie wskazał/zgłosił/doświadczył on żadnych problemów wydajnościowych.
8. Oprogramowanie musi dawać Wymagana możliwość dynamicznej (bez potrzeby restartu serwera aplikacji) zmiany konfiguracji metryk (np. dodanie reguły monitorowania klasy, metody, parametru)
9. Oprogramowanie musi mieć Wymagana możliwość instalacji (dołączenia) do uruchomionej bez monitoringu wirtualnej maszyny Java – co najmniej dla Oracle JVM 1.6+ i zbierania danych o wydajności bez potrzeby restartu serwera aplikacji. (analogicznie do oprogramowania typu VisualVM).
10. Oprogramowanie musi monitorować serwery aplikacji min. HIS i ERP.
11. Oprogramowanie musi zostać zainstalowane jako serwer zwirtualizowany.
12. W przypadku braku możliwości instalacji jako serwer wirtualny, Wykonawca ma obowiązek dostarczenia serwera fizycznego RACK max 1U.
13. Oprogramowanie musi działać na własnej bazie danych nie wykorzystując baz danych wymagających dodatkowych licencji.
14. Dostarczone licencje nie mogą ograniczać liczby użytkowników końcowych korzystających z oprogramowania ani liczby przetwarzanych lub przechowywanych dokumentów, plików, rekordów, żądań, etc.
15. Licencje nie mogą być ograniczone czasowo.
16. System będzie monitorował każdy serwer aplikacyjny i klaster serwerów baz danych.
17. Licencje nie mogą ograniczać ich zastosowania. Zastosowanie rozumiane jest jako Wymagana możliwość ich stosowania w dowolnym środowisku (programistyczne, testowe, produkcyjne itp.)
18. Dla oprogramowania muszą być dostępne na terenie Polski autoryzowane szkolenia.
19. Dla oferowanego oprogramowania muszą istnieć na terenie Polski autoryzowani partnerzy usługowi.
20. Dla oferowanego oprogramowania musi istnieć wsparcie co najmniej w języku polskim.
21. Oferowane Oprogramowanie powinno być opisane na publicznie i powszechnie dostępnych stronach WWW producenta lub społeczności rozwijającej produkt.

B. Moduł wyświetlania:
1. System monitoringu wizyjnego musi zostać obsłużony przez panel wyświetlacza o wielkości minimum 40 cali w rozdzielczości minimum 4K.
2. Należy zastosować minimum dwa takie wyświetlacze po jednym na system monitoringi i zarządzania.
3. Monitoring musi zostać połączony z serwerem poprzez okablowanie HDMI przenoszące sygnały 4K.
4. Dopuszcza się stosowania modułów PC jako urządzenia pośredniczące w wyświetlaniu, zarówno jako wtyczki HDMI/USB jak i pełne stacje robocze.
5. Częstotliwość wyświetlania minimum 25fps.

6. Zasilacz 230V
7. Gwarancja i serwis minimum 3 lata.

## 5.7. PRZEŁĄCZNIK SIECIOWY

1. Porty przełącznika: minimum 24 lub 48*10/100/1000Base-T, minimum 2 porty 10GE SFP+; Porty SFP+ 10GE obsługujące moduły 1GE SFP (w zależności od wymagań i uzgodnień z Działem Informatyki Spółki);
2. Wkładki: wszystkie porty przełącznika wyposażone we odpowiednie wkładki dla okablowania single mode, wkładki muszą być autoryzowane do użycia przez producenta sprzętu
3. Stackowanie: możliwość połączenia minimum 4 przełączników w stos za pomocą portów SFP+ bez dedykowanego okablowania
4. Obsługa PoE: Obsługa standardów IEEE 802.3af oraz IEEE 802.3at na minimum 48 portach urządzenia
5. Matryca przełączająca: minimum 176 Gbps
6. Przepustowość pakietów: minimum 105 Mpps (dla pakietów 64Kb)
7. Pojemność tablicy MAC: minimum 16000
8. Ilość wpisów tablicy ACL: minimum 1000
9. Ilość kolejek sprzętowych dla portów GE: 8
10. Ilość aktywnych IEEE802.1Q VLAN: minimum 4092
11. Zasilanie urządzenia: 230V AC zasilacz wbudowany w urządzenie, wbudowany zasilacz dla funkcji PoE z budżetem mocy minimum 740W, redundantny zasilacz 48V DC wbudowany w urządzenie
12. Oszczędzanie energii: zgodność ze standardem IEEE 802.3az (Energy Efficient Ethernet); funkcja LED Shut-off oraz Auto Fan Speed Control;
13. Certyfikaty bezpieczeństwa: CE, RoHS
14. Zabezpieczenie przed wyładowaniami atmosferycznymi: 6KV
15. Algorytm pracy: Storage and forwarding
16. Routing L3: routing statyczny, minimum 128 statycznych tras routingu; RIP
17. Obsługa VLAN: IEEE 802.1Q, QinQ, selektywne QinQ, elastyczne QinQ
18. Wsparcie dla zdefiniowanych typów VLANów: Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation
19. Obsługa protokołów IP: IPv4 oraz IPv6
20. Obsługa spanning tree: IEEE 802.1D STP, IEEE 802.1W RSTP, IEEE 802.1S MSTP, Root guard, BPDU guard, BPDU forwarding, BPDU tunel
21. Obsługa protokołów redundantnego ringu: MRPP, ITU-T G.8032, Loopback Detection, Fast Link
22. Agregacja LACP: zgodne z IEEE 802.3ad, minimum 128 grup po 8 portów, Load Balance
23. Inne funkcje L1 i L2: DAI, limitowanie adresów MAC na porcie oraz VLANie, kontrola sztormów w oparciu o pakiety i bajty, Virtual Cable Testing, DDM, UDLD, LLDP, LLDP-MED, Port Mirror, CPU Mirror, sFlow, Dying GASP, VSF
24. Obsługa Openflow: OpenFlow 1.0, wsparcie dla Opendaylight, Floodlight, Ryu, Pox,
25. Funkcje QoS: Klasyfikacja ruchu w oparciu o IEEE 802.1p CoS, DSCP, ACL, VLAN ID, IPv6 Flow Label, wsparcie kolejkowania SP, WRR, SWRR, DWRR, Bandwidth Control, Flow Redirect,
26. Bezpieczeństwo: Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, ND Snooping, DAI, IEEE 802.1x, Web Portal, Authentication, Authorization, Accounting, Radius, TACACS+
27. Listy kontroli dostępu: minimum 1000 wpisów typu IP ACL, MAC ACL, MAC-IP ACL, User-Defined ACL, Czasowe ACL, ACL na interfejsie VLAN
28. Multicast: IGMP v1/v2/v3 snooping, IGMP fast leave, IPv6 MLD v1/v2 snooping, MVR, IPv4/IPv6 DCSCM(D)
29. Zarządzanie: XModem/TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMPv1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Ping, Trace Route, Radius Authentication, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files
30. Firmware oraz konfiguracja: oprogramowanie przełącznika (firmware) dostępny bez ograniczeń czasowych, przez cały okres cyklu życiowego urządzenia poprzez internet, wsparcie techniczne producenta lub dystrybutora bez konieczności wykupu dodatkowych usług, możliwość wgrania kilku plików z obrazem lub konfiguracją systemu, możliwość wgrania oprogramowania oraz konfiguracji poprzez TFTP/FTP,

31. Obsługa DHCP: IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP, Snooping,IPv4/IPv6 DHCP Server
32. Sposób podłączenia: po jednym połączeniu 10GE z minimum dwoma przełącznikami core.
33. Wymiary: max. 1 Rack Unit o głębokości nie większej niż 450 mm
34. Rodzaj gwarancji: lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat.

## 5.8. PRZEŁĄCZNIK TYPU CORE

1. Porty przełącznika: minimum 24 lub 48*10G (SFP+), minimum 6*40G zamiennie z 100G (QSFP+) (z możliwością rozszycia każdego portu 40G na 4x10G) (w zależności od wymagań i uzgodnień z Działem Informatyki Spółki)
2. Wkładki: wszystkie porty przełącznika wyposażone we odpowiednie wkładki dla okablowania single mode, wkładki muszą być autoryzowane do użycia przez producenta sprzętu
3. Stackowanie: możliwość połączenia minimum 4 przełączników w stos za pomocą portów QSFP+ bez dedykowanego okablowania
4. Port zarzadzania: minimum 1x 10/100/1000Mbps RJ45 Ethernet Management port, minimum 1x USB 2.0 management port
5. Matryca przełączająca: minimum 1280 Gbps
6. Przepustowość pakietów: minimum 960 Mpps (dla pakietów 64Kb)
7. Pojemność tablicy MAC: minimum 96000
8. Ilość kolejek sprzętowych dla portów GE: minimum 8
9. Ilość aktywnych IEEE802.1Q VLAN: minimum 4096
10. Zasilanie urządzenia: minimum dwa modularne, w pełni redundantne zasilacze 100-240VAC
11. Chłodzenie urządzenia: aktywne, redundantne, minimum 4 hot-swappowe wentylatory
12. Certyfikaty bezpieczeństwa: CE, RoHS
13. Ruting L3: Ruting statyczny, RIPv1/v2, OSPFv2, RIPng, OSPFv3, BGP4, Ruting LPM, Ruting PBR dla IPv4/IPv6, DVMRP, PIM-DM, PIM-SM, PIM-SSM, Static multicast route
14. Obsługa VLAN: 802.1Q
15. Wsparcie dla zdefiniowanych typów VLANów: MAC VLAN, Voice VLAN, PVLAN, Protocol VLAN, Multicast VLAN, N:1 VLAN Translation
16. Obsługa protokołów IP: IPv6 oraz IPv4
17. Obsługa spanning tree: IEEE 802.1D STP, IEEE 802.1W RSTP, IEEE 802.1S MSTP, Root guard, BPDU guard, BPDU forwarding, BPDU tunnel
18. Obsługa protokołów redundantnego ringu: MRPP lub równoważne
19. Agregacja LACP: zgodne z IEEE 802.3ad, minimum 128 grup po 8 portów, LACP Load Balance
20. Inne funkcje L1 i L2: unicast/broadcast/multicast storm-control, GVRP DDM, UDLD, LLDP, LLDP-MED, sFlow Traffic Analysis
21. Inne funkcje L3: VRRP, URPF, ECMP, BFD
22. Funkcje Data Center: IEEE VEPA, TRILL, VXLAN
23. Obsługa Openflow: Openflow 1.0, Opendaylight, Floodlight, Ryu, Pox
24. Funkcje QoS: 8 kolejek na port, SWRR, SP, WRR, DWRR, SDWRR, WRED, traffic shaping, klasyfikacja ruchu w oparciu o: CoS, ToS, DiffServ DSCP, ACL, port
25. Bezpieczeństwo: IEEE 802.1x AAA, Port, MAC based authentication, RADIUS, TACACS+, Guest VLAN, Auto VLAN, DHCP/DHCPv6 snooping, port security, ARP Guard, Local ARP Proxy, ARP binding, Anti ARP/NDP cheat, Anti ARP/NDP scan
26. Listy kontroli dostępu: minimum typu IP ACL, MAC ACL, IP-MAC ACL, time ranged ACL, VLAN based ACL. ACL konfigurowane na porcie, VLANie lub interfejsie VLAN.
27. Multicast: IGMP v1/v2/v3, IGMP snooping v1/v2/v3, IGMP L2 Query, ND snooping, MLD snooping
28. Zarządzanie: CLI, Web/SSL, Telnet, SSH, IPv4/IPv6 SNMP v1/v2c/v3, SNMP Trap, RMON 1,2,3,9, Dual firmware images/configuration files, 802.3ah, HTTP SSL
29. Firmware oraz konfiguracja: oprogramowanie przełącznika (firmware) dostępny bez ograniczeń czasowych, przez cały okres cyklu życiowego urządzenia poprzez internet, wsparcie techniczne producenta lub dystrybutora bez konieczności wykupu dodatkowych usług, możliwość wgrania kilku

plików z obrazem lub konfiguracją systemu, możliwość wgrania oprogramowania oraz konfiguracji poprzez TFTP/FTP,
30. Obsługa DHCP: DHCP client/server/relay, DHCPv6 relay/server, DHCP snooping, DHCP Option 82
31. Sposób podłączenia: po jednym połączeniu 10GE z każdym przełącznikiem dostępowym, minimum 2 połączenia 40/100GE z każdym kolejnym przełącznikiem core, po jednym połączeniu 40/100GE z każdego przełącznika core z przełącznikiem serwerowym.
32. Wymiary: max. 1 Rack Unit o głębokości nie większej niż 1000 mm
33. Rodzaj gwarancji: lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat.

## 5.9. PRZEŁĄCZNIK SERWEROWY

1. Porty przełącznika: minimum 24 lub 48*1/10G (SFP-SFP+) definiowane wkładką, minimum 6*40G zamiennie z 100G (QSFP+) (z możliwością rozszycia każdego portu 40G na 4x10G) (w zależności od wymagań i uzgodnień z Działem Informatyki Spółki)
2. Wkładki: wszystkie porty przełącznika wyposażone we odpowiednie wkładki dla okablowania multi mode do serwerów, wkładki muszą być autoryzowane do użycia przez producenta sprzętu
3. Stackowanie: możliwość połączenia minimum 4 przełączników w stos za pomocą portów QSFP+ bez dedykowanego okablowania
4. Port zarzadzania: minimum 1x 10/100/1000Mbps RJ45 Ethernet Management port, minimum 1x USB 2.0 management port
5. Matryca przełączająca: minimum 1280 Gbps
6. Przepustowość pakietów: minimum 960 Mpps (dla pakietów 64Kb)
7. Pojemność tablicy MAC: minimum 96000
8. Ilość kolejek sprzętowych dla portów GE: minimum 8
9. Ilość aktywnych IEEE802.1Q VLAN: minimum 4096
10. Zasilanie urządzenia: minimum dwa modularne, w pełni redundantne zasilacze 100-240VAC
11. Chłodzenie urządzenia: aktywne, redundantne, minimum 4 hot-swappowe wentylatory
12. Certyfikaty bezpieczeństwa: CE, RoHS
13. Ruting L3: Ruting statyczny, RIPv1/v2, OSPFv2, RIPng, OSPFv3, BGP4, Ruting LPM, Ruting PBR dla IPv4/IPv6, DVMRP, PIM-DM, PIM-SM, PIM-SSM, Static multicast route
14. Obsługa VLAN: 802.1Q
15. Wsparcie dla zdefiniowanych typów VLANów: MAC VLAN, Voice VLAN, PVLAN, Protocol VLAN, Multicast VLAN, N:1 VLAN Translation
16. Obsługa protokołów IP: IPv6 oraz IPv4
17. Obsługa spanning tree: IEEE 802.1D STP, IEEE 802.1W RSTP, IEEE 802.1S MSTP, Root guard, BPDU guard, BPDU forwarding, BPDU tunnel
18. Obsługa protokołów redundantnego ringu: MRPP lub równoważne
19. Agregacja LACP: zgodne z IEEE 802.3ad, minimum 128 grup po 8 portów, LACP Load Balance
20. Inne funkcje L1 i L2: unicast/broadcast/multicast storm-control, GVRP DDM, UDLD, LLDP, LLDP-MED, sFlow Traffic Analysis
21. Inne funkcje L3: VRRP, URPF, ECMP, BFD
22. Funkcje Data Center: IEEE VEPA, TRILL, VXLAN
23. Obsługa Openflow: Openflow 1.0, Opendaylight, Floodlight, Ryu, Pox
24. Funkcje QoS: 8 kolejek na port, SWRR, SP, WRR, DWRR, SDWRR, WRED, traffic shaping, klasyfikacja ruchu w oparciu o: CoS, ToS, DiffServ DSCP, ACL, port
25. Bezpieczeństwo: IEEE 802.1x AAA, Port, MAC based authentication, RADIUS, TACACS+, Guest VLAN, Auto VLAN, DHCP/DHCPv6 snooping, port security, ARP Guard, Local ARP Proxy, ARP binding, Anti ARP/NDP cheat, Anti ARP/NDP scan
26. Listy kontroli dostępu: minimum typu IP ACL, MAC ACL, IP-MAC ACL, time ranged ACL, VLAN based ACL. ACL konfigurowane na porcie, VLANie lub interfejsie VLAN.
27. Multicast: IGMP v1/v2/v3, IGMP snooping v1/v2/v3, IGMP L2 Query, ND snooping, MLD snooping
28. Zarządzanie: CLI, Web/SSL, Telnet, SSH, IPv4/IPv6 SNMP v1/v2c/v3, SNMP Trap, RMON 1,2,3,9, Dual firmware images/configuration files, 802.3ah, HTTP SSL

29. Firmware oraz konfiguracja: oprogramowanie przełącznika (firmware) dostępny bez ograniczeń czasowych, przez cały okres cyklu życiowego urządzenia poprzez internet, wsparcie techniczne producenta lub dystrybutora bez konieczności wykupu dodatkowych usług, możliwość wgrania kilku plików z obrazem lub konfiguracją systemu, możliwość wgrania oprogramowania oraz konfiguracji poprzez TFTP/FTP,
30. Obsługa DHCP: DHCP client/server/relay, DHCPv6 relay/server, DHCP snooping, DHCP Option 82
31. Sposób podłączenia: minimum 1 połączenie 40/100GE z każdym przełącznikiem core
32. Wymiary: max. 1 Rack Unit o głębokości nie większej niż 1000 mm
33. Rodzaj gwarancji: lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat.

# 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 złączek rozłącznych,
2. reflektogramów (format *.pdf),
3. reflektogramów wygenerowanych przez urządzenie pomiarowe.

c. Trakty bezprzewodowe – przygotowanie dokumentacji projektowej na potrzeby budowy sieci bezprzewodowej WiFi obejmuje:

a) Rozmieszczenie punktów dostępowych z pokryciem sygnału (min. parametry siła sygnału odbieranego -60dBm do -70dBm),

b) Pomiar parametru Sygnał/Szum (parametr Sygnał/Szum – min. 27 dB, zalecane 35 dB),

c) Analiza zajętości kanałów w obu pasmach,

d) Pomiar widma częstotliwości 2,4 GHz i 5 GHz (w celu wykrycia potencjalnych zakłóceń/kolizji generowanych przez inne urządzenia),

e) Zaproponowanie przydziału kanałów do punktów dostępowych,

f) Inne zalecenia techniczne i obserwacje powstałe w czasie pomiarów,

Wg przyjętych założeń:

a) Sieć WLAN musi zapewniać dostęp dla klientów sieci bezprzewodowej w technologiach 802.11a/b/g/n i 802.11ac oraz zapewnić funkcjonalność roamingu urządzeń bezprzewodowych pomiędzy Access Pointami,

b) Punkty AP montowane będą w korytarzach na sufitach właściwych lub podwieszanych, zasilane AP wykonać po skrętce z PoE, kategoria okablowania 6A,

c) Rozmieszczenie punktów dostępowych tak by zasięg dla poszczególnych punktów dostępowych spełniał warunek (zasięgi poszczególnych AP muszą się nakładać w min. 15% tak aby zapewnić funkcjonalność roamingu).

# 7. DOKUMENTACJA POWYKONAWCZA

Dokumentacja powykonawcza musi zawierać w szczególności:
1. raporty z pomiarów dynamicznych okablowania oraz pomiary propagacji sygnału sieci bezprzewodowej dla standardów 802.11 g/n i ac w zakresie częstotliwości 2.4GHz oraz 5GHz i wykonanie dokumentacji projektowej sieci WLAN wraz z mapami pokrycia siecią poszczególnych pięter budynków zawierających rozkład pomieszczeń;
2. rzeczywiste trasy prowadzenia kabli transmisyjnych na rzutach budynków w skali nie mniejszej niż 1:100 (w formacie pdf oraz wektorowej – najlepiej format AutoCAD);
3. oznaczenia poszczególnych szaf, gniazd, kabli i portów w panelach krosowych;
4. lokalizację przebić 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 wchodzą 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 serwerownie), 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-letnia gwarancją producencką (certyfikacją),
- sporządzenie dokumentacji powykonawczej dla odtworzonej infrastruktury sieciowej,
- objęcie odtworzonej infrastruktury co najmniej 5-letnia gwarancja,
- 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 punktu 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 łączeń 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 przeciążania 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 sjest 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 jakiejkolwiek 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. niezmniejszonej 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 należytego 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 opóźnieni 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 wariancie 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, uniemożliwiające 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 budowalnych 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 przełącznice,
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 Leczniczych.
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 Leczniczym. Komponent może być dedykowany dla wszystkich Podmiotów Leczniczych 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 wpływającą 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 Sieć 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 przekaże 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 wariancie) 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 wariancie) 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 | pomiar | 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 | pomiar | 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) | pomiar | 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) | pomiar | 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 realizacje 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@szpitalepomorskie.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 zarzadzania 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 umożliwia 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 Orchestration, 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.
- Aprowizowanie 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 aprowizacji 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 wewnętrznie 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 protokół 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 protokół 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 protokół 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 wymienialne 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 dyskowych/modułach 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. Odzyskiwania 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 dokonywania 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 rozbiciem na odczyty i zapisy; historii i trendu zajętości),
  - maszyn wirtualnych (średnia: zajętość, wykorzystanie vCPU, vMEM, przepustowość MB/s oraz IO/s w rozbiciu 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 rozbiciu na zapisy i odczyty w ciągu ostatnich 24h, histogramu czasu obsługi z rozbiciem 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 zapewni 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 20xC13.

**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 wynoszenia 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 umożliwiająca 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 slocie 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 DNA
- 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.