# Opis przedmiotu zamówienia

## 1. Wstęp

Przedmiotem niniejszego postępowania jest dostarczenie kompletnego rozwiązania dla Centrum Dystrybucji (CD), będącego zapleczem dla profesjonalnego udostępniania plików za pomocą platformy VOD WFDiF. Udostępniane w nim materiały będą bezpośrednio przygotowane w projekcie jak również przetworzone przez platformę transkodującą. CD będzie wyposażone w system przechowywania danych (operacyjna biblioteka taśmowa), przestrzeń roboczą (wydajna macierz), platformę transkodującą (transkoder + stacja masteringowa), oprogramowanie (do sterowania zarządzaniem i przetwarzaniem danych), infrastrukturę sieciową wraz z jej ochroną, stanowiska wpisu i opisu materiałów. Rozwiązanie ma także pozwalać na udostępnianie fragmentów filmów i posiadać na to stosowną przestrzeń

## 2. Słownik pojęć

Projekt – zadania realizowane w ramach programu operacyjnego POPC.02.03.02-00-0007/17 o nazwie „Cyfrowa rekonstrukcja i digitalizacja polskich filmów fabularnych, dokumentalnych i animowanych w celu zapewnienia dostępu na wszystkich polach dystrybucji (kino, telewizja, Internet, urządzenia mobilne) oraz zachowania dla przyszłych pokoleń polskiego dziedzictwa filmowego”

Centrum Dystrybucyjne (CD) – planowana jednostka w WFDiF utworzona na potrzeby projektu

Rozwiązanie – kompletny system umożliwiający przechowywanie, przetwarzanie i udostępnianie materiałów audiowizualnych przez WFDiF klientom w skład, którego wchodzą między innymi elementy takie jak: biblioteka taśmowa, macierz robocza, transkodery, oprogramowanie zarządzające mediami i kontroli jakości, infrastruktura sieciowa. Całość ma stanowić spójny system.

Partner zewnętrzny – członek konsorcjum realizujący projekt. W obecnej chwili: PISF (Polski Instytut Sztuki Filmowej) i SFR (Studio Filmów Rysunkowych)

Oprogramowanie do zarządzania mediami (MAM) – oprogramowanie zapewniające kontrolę nad archiwizacją, przetwarzaniem i udostępnianiem materiałów audiowizualnych przez CD a także umożliwiające opis materiałów za pomocą metadanych.

System – zestaw urządzeń i oprogramowania realizujący określone założenia.

DCP – kinowa paczka dystrybucyjna

DCDM – bezkompresyjny wzorzec filmu w jakości kinowej

IMF – wzorzec filmu w jakości telewizyjnej

KDM – plik klucz umożliwiający odtworzenie zaszyfrowanego DCP

Stacja masteringowa – system umożliwiający przetwarzanie formatów plików audiowizualnych a także tworzenie i edycje kinowych paczek dystrybucyjnych.

Rewrapping – proces ponownej edycji kinowych paczek dystrybucyjnych.

Transkoder – urządzenie bądź urządzenie plus oprogramowanie służące do przetwarzania formatów plikowych w sposób automatyczny wg wskazanych reguł.

Automatyczna kontrola jakości – pobieżna kontrola stanu skopiowanych materiałów archiwizacyjnych potwierdzająca zgodność dostarczonych materiałów z parametrami dla materiałów archiwizacyjnych oraz wykrywająca błędy związane z kopiowaniem.

Ręczna kontrola jakości –kontrola jakości polegająca na dokładnej analizie materiałów, służąca wykryciu błędów związanych ze stworzeniem materiałów archiwizacyjnych.

Proxy – pliki poglądowe o obniżonej jakości.

Platforma VOD WFDiF – portal internetowy udostępniający zasoby CD.

## 3. Opis wymagań ogólnych

3.1. Urządzenia muszą być fabrycznie nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz nieużywane.

3.2. Całość dostarczanego sprzętu musi pochodzić z autoryzowanego kanału sprzedaży producentów zaoferowanego sprzętu.

3.3. Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich. W wypadku powzięcia wątpliwości, co do zgodności oferowanych produktów z opisem przedmiotu zamówienia, w szczególności w zakresie legalności oprogramowania, Zamawiający jest uprawniony do:

   a. zwrócenia się do producenta oferowanych produktów o potwierdzenie ich zgodności (w tym także do przekazania producentowi niezbędnych danych umożliwiających weryfikację),

   b. zlecenia producentowi oferowanych produktów lub wskazanemu przez producenta podmiotowi, inspekcji produktów pod kątem ich zgodności oraz ważności i zakresu uprawnień licencyjnych.

3.4. Jeżeli inspekcja, o której mowa w pkt. 3.3 wykaże niezgodność produktów z opisem przedmiotu zamówienia lub stwierdzi, że korzystanie z produktów narusza majątkowe prawa autorskie producenta, koszt inspekcji zostanie pokryty przez Wykonawcę, według rachunku przedstawionego przez podmiot wykonujący inspekcję, w kwocie nie przekraczającej 30% wartości zamówienia (ograniczenie to nie dotyczy kosztów poniesionych przez Zamawiającego w wyniku inspekcji, jak np. konieczność zakupu nowego oprogramowania). Prawo zlecenia inspekcji nie ogranicza ani nie wyłącza innych uprawnień Zamawiającego, w szczególności prawa do żądania dostarczenia produktów zgodnych z umową oraz roszczeń odszkodowawczych.

3.5. Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji.

3.6. Wszystkie urządzenia, które tego wymagają, muszą posiadać oznakowanie CE (Conformité Européenne) produktu albo spełniać normy równoważne.

3.7. Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz., jednofazowo i być wyposażone w przewody zasilające.

## 4. Idea działania

W pierwszej kolejności, rozwiązanie zostanie zasilone materiałami wykonanymi w trakcie prac digitalizacyjnych. Materiały trafią do WFDiF na przenośnych macierzach dyskowych bądź na taśmach LTO. Zostaną one przepisane na macierz roboczą, aby mogły być zaimportowane do oprogramowania do zarządzania mediami. Po zakończeniu kopiowania automatycznie uruchomiony zostanie proces automatycznej kontroli jakości materiałów. Następnie materiał zostanie skontrolowany ręcznie. W przypadku zbyt dużej liczby błędów zostanie zwrócony do poprawy przez dostarczającego. Materiał bezbłędny zostanie przekazany do wprowadzenia, opisu oraz archiwizacji. Równolegle zostaną stworzone pliki proxy dla MAM/DAM.
W przypadku udostępniania materiałów, zlecenie na wybrany film przychodzi z platformy VOD WFDiF. Wybrany materiał jest wyciągany z biblioteki taśmowej, transkodowany na przestrzeni roboczej do formatu określonego przez zamawiającego, udostępniony na wydzielonej przestrzeni do udostępniania. Dla zamawiającego zostaje wygenerowany link do pobrania materiału.

## 5. Materiały archiwizacyjne

Prace digitalizacyjno-rekonstruktorskie kończą się następującymi formatami:

5.1. Master archiwizacyjny, zawierający możliwie najwięcej informacji o rozdzielczości i kolorach. Zapisany w postaci sekwencji klatek w maksymalnej rozdzielczości rekonstrukcji - w formacie DPX RGB lub TIFF, głębia kolorów 10 bit/kanał w skali logarytmicznej lub 16/bit na kanał - w skali liniowej;

5.2. Rec. 709 jako master dla HDTV i pochodnych, cały film zapisany w formacie Apple QuickTime ProRes 422 HQ lub w formacie otwartym DNxHD 185x/365x, w rozdzielczości 1920x1080 pikseli, głębia kolorów 10 bit/kanał, prędkość odtwarzania 25 kl/s, ze ścieżką dźwiękową (opisaną w pkt 5.6 C), obraz w parametrach zgodnych z ITU-R BT.709. Plik musi posiadać planszę kontrolną, dodaną jako ostatnia klatka materiału, będącą wzorcem do poprawnej interpretacji formatu ProRes. Jako planszę kontrolną należy stosować planszę zgodną ze standardem ARIB STD-B28 v1.0;

5.3. DCDM – wykonany zgodnie z normą SMPTE 428-1-2006, zapisany w postaci sekwencji skadrowanych klatek całego filmu w modelu przestrzeni barw X'Y'Z', w formacie TIFF, głębia kolorów 16 bit/kanał, zawierające tylko aktywne piksele (bez dopełniania czernią);

5.4. DCP – nieszyfrowana kopia DCP, w rozdzielczości nie mniejszej niż rozdzielczość rekonstrukcji filmu, lecz nie mniej niż DCI 2K, prędkość odtwarzania 24 kl/s;

5.5. Dźwięk zapisany w formacie Broadcast Wave PCM, w rozdzielczości 24 bit i próbkowaniu 48 kHz, plik w formacie wielokanałowym (dla 5.1 układ LRCLfeLsRs). Układ kanałów powinien być oznaczony w nazwie pliku.

5.6. Mastery dźwięku przygotowane dla następujących pól eksploatacji:

A. zrekonstruowany RR (do DCDM i do mastera archiwizacyjnego),
B. master kinowy (do DCP i DCDM),
C. master TV 5.1 + 2.0,
D. master do Blu-ray 5.1

5.7. Pliki audio deskrypcji w formacie Broadcast Wave PCM, w rozdzielczości 24 bit i próbkowaniu 48 kHz

5.8. Napisy angielskie oraz dla niesłyszących w formacie EBU STL

Wszystkie formaty obrazu po rekonstrukcji, zapisane jako sekwencje klatek, będą podzielone na foldery nazwane numerem aktu, z którego pochodzą. Nazewnictwo klatek zawiera informacje o tytule, numerze aktu/rolki oraz informacje o klatce i jest zgodne z konwencją nazewniczą opublikowanej na stronie FInA.

W ramach projektu rekonstruowane zostanie około:

- 160 filmów fabularnych (15 973 minut),
- 200 krótkometrażowych animacji (4300 minut),
- 3000 kronik filmowych (tylko digitalizacja do mov – 36 000 minut),
- 70 filmów dokumentalnych (1 819 minut).

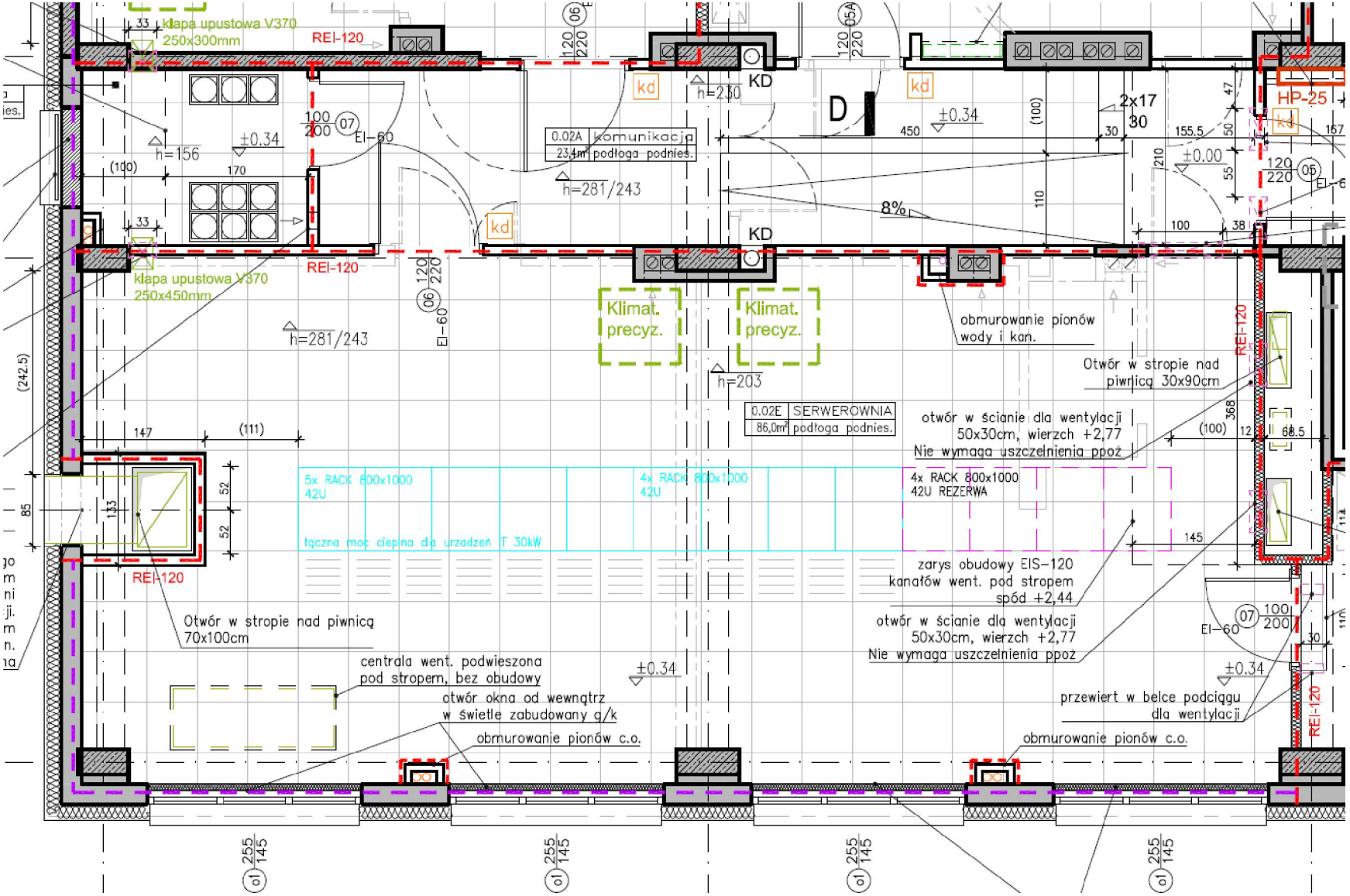
Należy pamiętać, że 100 minutowy film, to 144 000 klatek co w przypadku przechowywanych materiałów archiwizacyjnych będzie oznaczało dla każdego filmu fabularnego około 290 000 plików. Oferowane rozwiązanie musi więc działać poprawnie z ponad 100 mln plików.

Przykładowe wielkości materiałów:

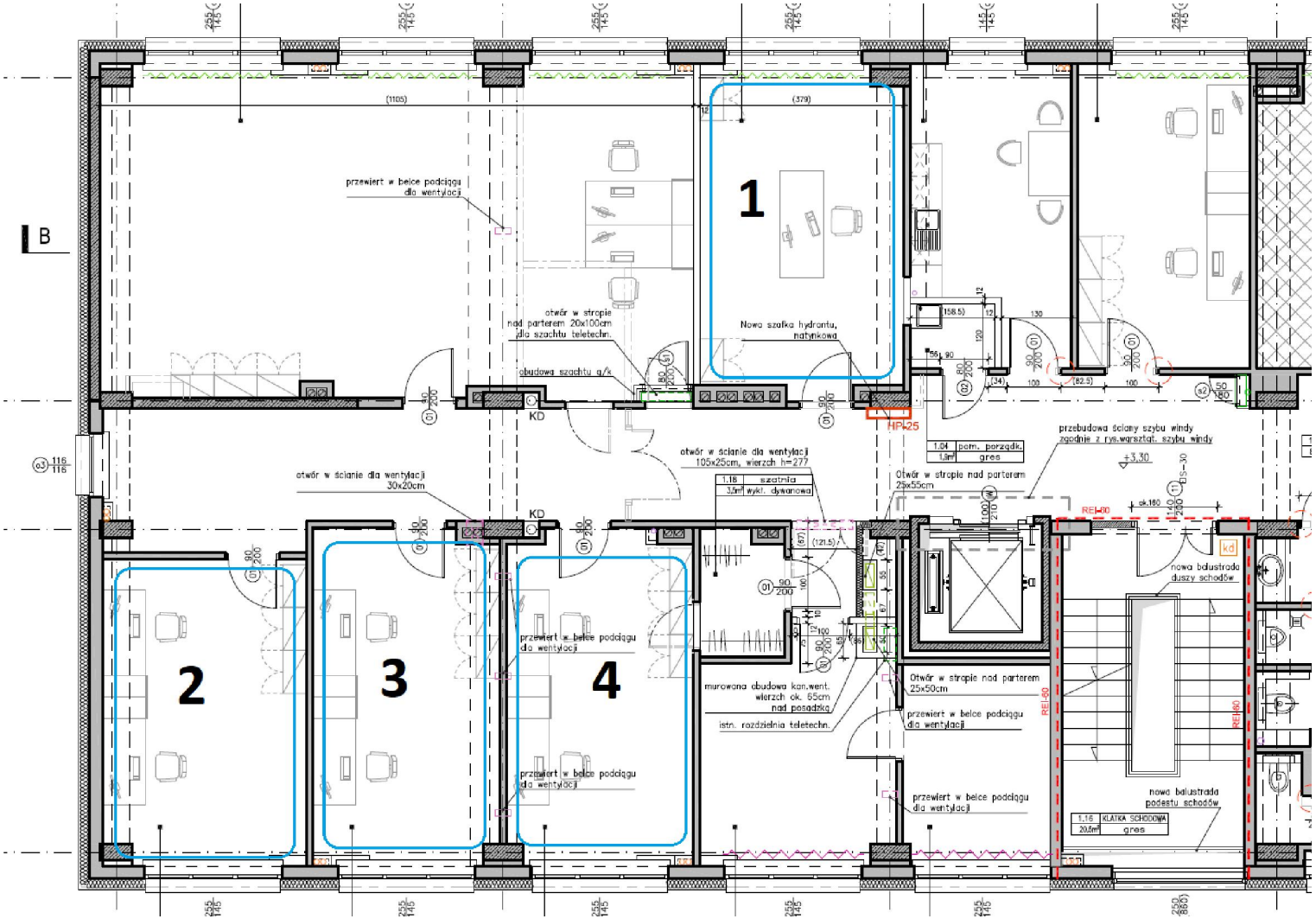
- Klatka filmu (tiff, dpx) – ok 50-80 MB
- Plik MOV (ProRes, DNxHD) – ok 120 GB
- DCP – ok 120 GB (pliki sterujące dziesiątki kB, MXF z treścią – kilkadziesiąt GB)
- WAVE – pojedyncze GB.

## 6. Istniejąca infrastruktura

Rozwiązanie dla Centrum Dystrybucyjnego zostanie zainstalowane w serwerowni na parterze budynku 21 (pomieszczenie B) jako zupełnie nowy system. Zamawiający nie wymaga jego integracji z posiadanymi urządzeniami. Nie przewiduje także prowadzenia prac, na urządzeniach CD, wykraczających poza jego opisane zadania. Serwerownia jest przygotowana tj. wyposażona jest w systemy: gaśniczy, klimatyzacji precyzyjnej, monitoringu środowiska, dozoru. Instalacja doprowadzona do pomieszczenia jest zabezpieczona przed zanikiem prądu (system UPS) oraz podłączona pod awaryjny agregat. Pracownie znajdują się bezpośrednio nad pomieszczeniem serwerowni, na pierwszym piętrze. Poniżej przedstawiono układ pomieszczeń.




**Rysunek 1 – Parter Serwerownia B**




**Rysunek 2 - I piętro Pomieszczenia CD**

Pomieszczenia CD wymagające połączenia z serwerownią

6.1. Instalacja elektryczna i podtrzymania zasilania

Na potrzeby zasilania rezerwowego zostały przewidziane dwa urządzenia UPS firmy GTec Europe typu Saturn 160kVA, o poniższych parametrach technicznych:

| | |
|---|---|
| WEJŚCIE: | |
| Moc znamionowa [kVA] | 160 |
| Napięcie [V] | 400 |
| Tolerancja napięcia: | ±20% |
| WYJŚCIE: | |
| Moc znamionowa [kVA] | 160 |
| Moc czynna [kW] | 160 |
| Prąd wyjściowy [A] | 232 |
| Liczba faz | 3 |
| Współczynnik szczytu | 3:1 |
| Częstotliwość [Hz] | 50/60 selektywna |
| Przeciążenie [%] | 125/150/168 dla 10'/1'/5" |

wraz z zestawem baterii, pozwalających na 60 minut pracy.

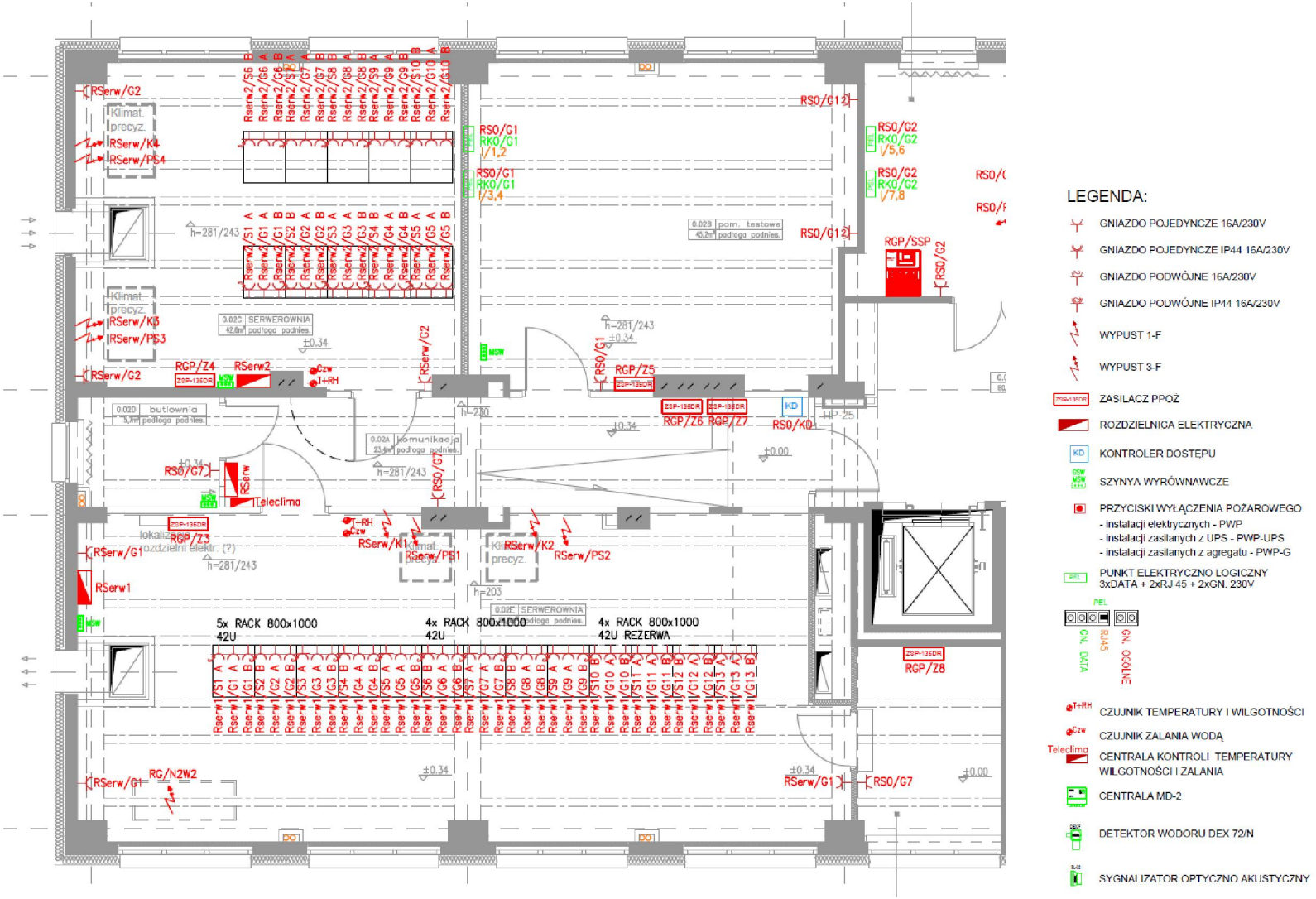
1.1. Agregat prądotwórczy

Zespół prądotwórczy wyposażone jest w silnik wysokoprężny Doosan, prądnica Leroy Sommer i panel sterowania Comap o poniższych parametrach technicznych:

| Silnik | | Prądnica | |
|---|---|---|---|
| Producent silnika | Doosan | Napięcie znamionowe [V] | 400 |
| Typ silnika | P126TI | Współczynnik mocy (cos ϕ) | 0,8 |
| Kraj produkcji | Korea Płd. | Temperatura, wysokość | 40°C 1000m n.p.m. |
| Moc silnika netto [kW] | 234,0 | Moc znamionowa [kVA] | 275,0 |
| Emisja spalin | Non-emission | Ochrona | IP 23 |
| Obroty [obr/min] | 1500 | Podłączenie z silnikiem | jednołożyskowe |
| Regulacja obrotów | Elektroniczna | Technologia | bezszczotkowa |
| Klasa wykonania | G3 | Podtrzymanie prądu zwarciowego | 270% 10s |
| Pojemność silnika [l] | 11,1 | Sprawność [%] | 93,1 |
| Liczba cylindrów | 6 | Klasa izolacji | H |
| Układ paliwowy | Wtrysk bezpośredni | Zawartość harmonicznych THD[%] | 2,5 |
| Instalacja [V] | 24 | Reaktancja $X_d''$[%] | 10,8 |
| Pojemność cieczy chłodzącej [l] | 51,0 | Regulacja napięcia | DVR, cyfrowy |
| Pojemność miski olejowej [l] | 23,0 | Pomiar napięcia | 3 fazy |
| Rodzaj paliwa | Diesel (EN 590) | Dokładność regulacji [%] | +/- 0,25 |
| | | Zasilanie AVR | uzwojenie pomocnicze |
| | | Zasilanie AVR (opcjonalne) | PMG |
| | | Miejsce produkcji | EU |

1.2. Instalacja elektryczna i teletechniczna

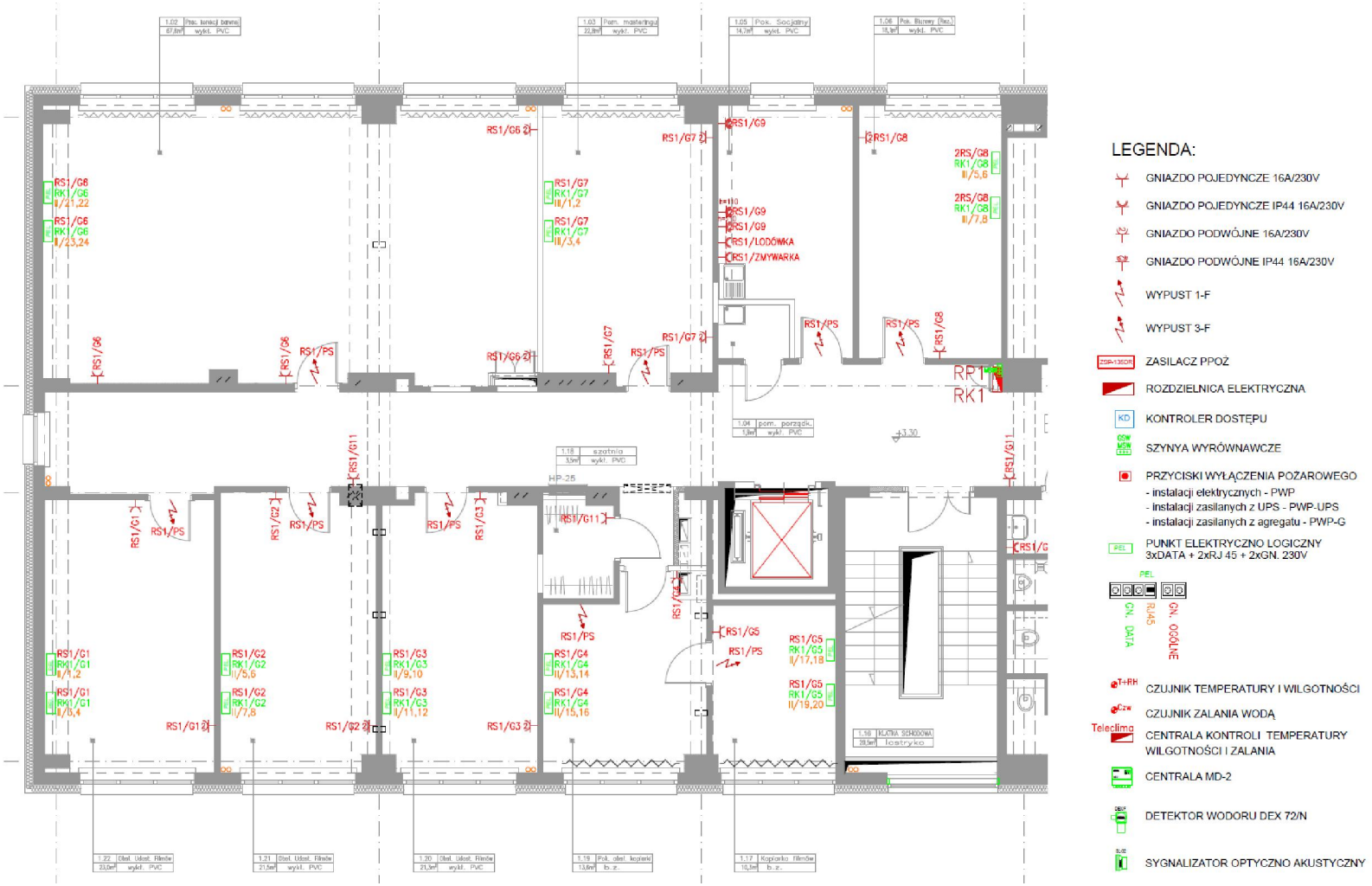
Instalacja elektryczna i teletechniczna została wykonana wg poniższego schematu. W przypadku teletechniki zastosowano okablowanie S/FTP Cat 7. Pomieszczenia 2,3,4 podłączone są bezpośrednio do serwerowni B, pomieszczenie 1 do Serwerowni A




LEGENDA:

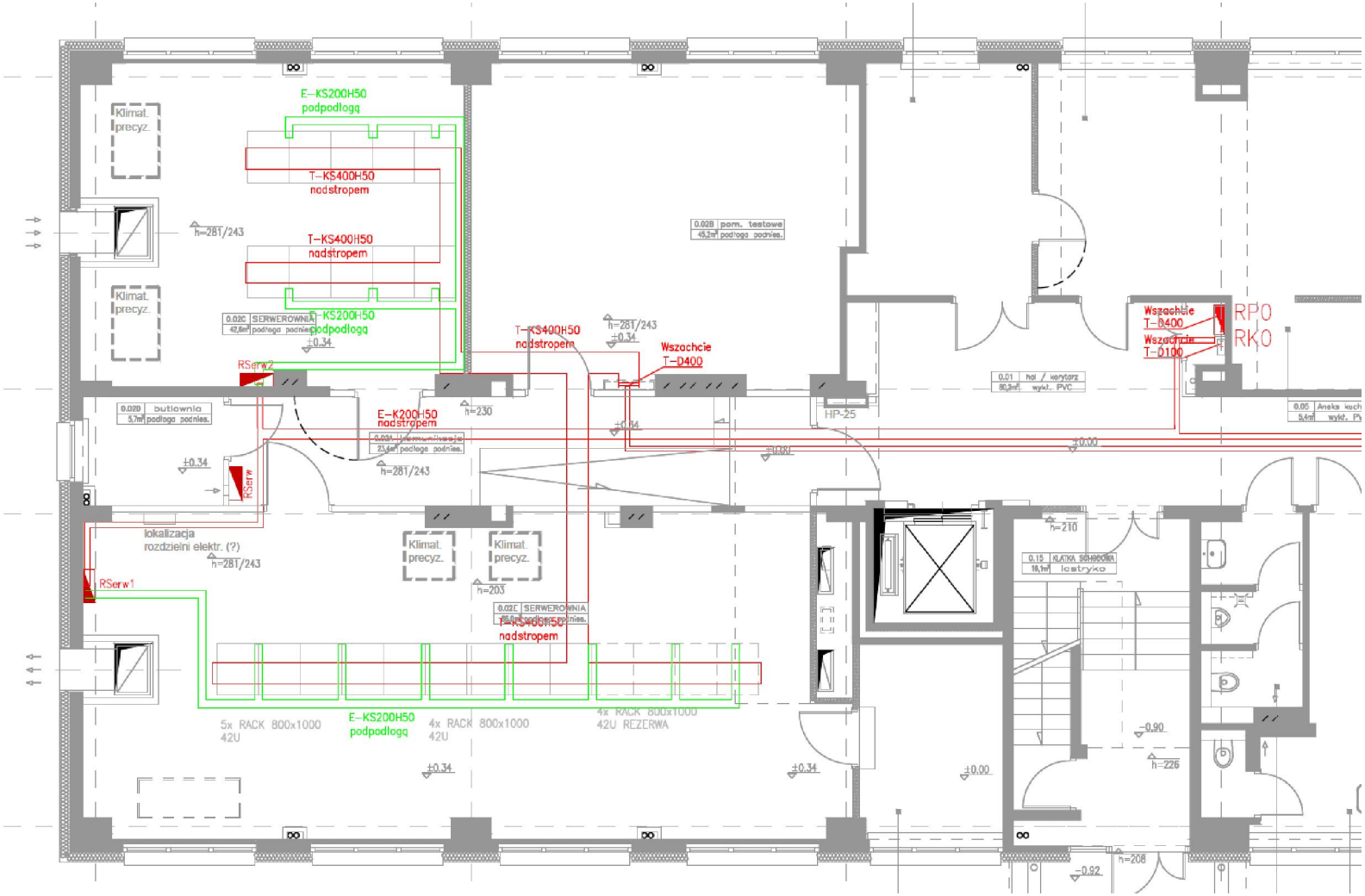
- GNIAZDO POJEDYNCZE 16A/230V
- GNIAZDO POJEDYNCZE IP44 16A/230V
- GNIAZDO PODWÓJNE 16A/230V
- GNIAZDO PODWÓJNE IP44 16A/230V
- WYPUST 1-F
- WYPUST 3-F
- ZASILACZ PPOŻ
- ROZDZIELNICA ELEKTRYCZNA
- KONTROLER DOSTĘPU
- SZYNYA WYRÓWNAWCZE
- PRZYCISKI WYŁĄCZENIA POŻAROWEGO
  - instalacji elektrycznych - PWP
  - instalacji zasilanych z UPS - PWP-UPS
  - instalacji zasilanych z agregatu - PWP-G
- PUNKT ELEKTRYCZNO LOGICZNY
  3xDATA + 2xRJ 45 + 2xGN. 230V
- CZUJNIK TEMPERATURY I WILGOTNOŚCI
- CZUJNIK ZALANIA WODĄ
- CENTRALA KONTROLI TEMPERATURY WILGOTNOŚCI I ZALANIA
- CENTRALA MD-2
- DETEKTOR WODORU DEX 72/N
- SYGNALIZATOR OPTYCZNO AKUSTYCZNY

**Rysunek 3 - Parter Serwerownia A i B**

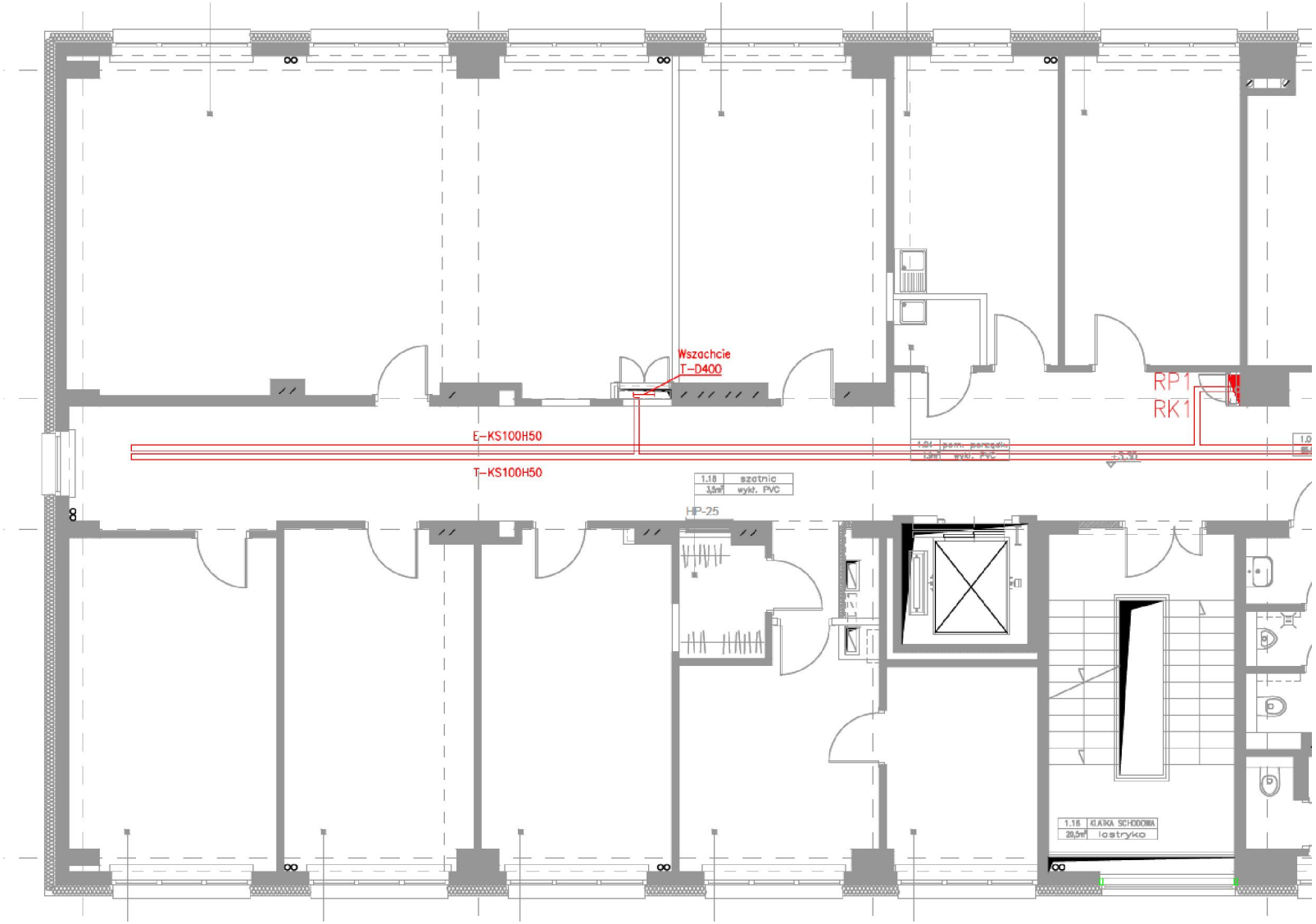



**Rysunek 4 - I piętra**

1.3. Schemat tras kablowych




**Rysunek 5 - Trasy kablowe parter**




**Rysunek 6 - Trasy kablowe I piętro**

# 2. Wymagania dla biblioteki taśmowej

System składowania danych w CD WFDiF opierał się będzie na dwóch połączonych ze sobą rodzajach urządzeń: bibliotece taśmowej i macierzy roboczej. Produktem projektu będą zdigitalizowane i zrekonstruowane filmy fabularne, dokumentalne, animacje i wydania Polskiej Kroniki Filmowej

W systemie składowane będą:

- sekwencje klatek (DPX, TIFF),
- pliki ciągłe o dużej wielkości (MOV 120-150 GB/szt.),
- pliki ciągłe o średniej wielkości (WAV),
- pliki dystrybucyjne (cyfrowe kopie dystrybucyjne – DCP, IMF, obrazy ISO).

W momencie uruchomienia, rozwiązanie musi być gotowe przyjąć w sumie około 2 PB ww. materiałów

## 2.1. Skalowalna biblioteka taśmowa.

W przypadku tego zamówienia biblioteka taśmowa, ta musi spełniać następujące, minimalne wymagania:

A. Pojemność netto biblioteki – 5,4 PiB;
B. Biblioteka może być zrealizowana przez jedno bądź dwa skalowalne urządzenia, tak aby została zachowana pełna redundancja (odporność na awarię: napędu, zasilania, robota, elektroniki sterującej);
C. Powinna posiadać minimum 5 napędów;
D. Powinna posiadać minimum 2 roboty;
E. Powinna posiadać funkcjonalność weryfikacji stanu danych na taśmach, realizowaną w tle, przez minimum jeden napęd w każdym urządzeniu. Weryfikacja musi polegać na sprawdzeniu poprawności odczytu danych na taśmie;
F. Biblioteka musi działać w oparciu o technologię LTO-8 lub lepszą;
G. Wyposażona musi być w taśmy wielokrotnego zapisu tej samej generacji co napędy;
H. Liczba slotów w bibliotece jest wynikowa dla wybranej technologii, nie mniej musi zawierać dodatkowy slot na taśmę czyszczącą na każde urządzenie biblioteczne;
I. Skalowalność biblioteki powinna umożliwiać dostawienie modułów zwiększającą dwukrotnie liczbę slotów;
J. Ze względu na specyfikę przechowywanych danych – format klatkowy, zamawiający oczekuje liniowego zapisu danych na taśmach w kolejności numerycznej;
K. Biblioteka powinna zapisywać sekwencyjne materiały archiwizacyjne w systemie plików innym niż LTFS;
L. Posiadać przestrzeń na tymczasowe dane, minimum dwukrotność pojemności zastosowanych taśm służącą np. do defragmentowania taśm.

## 2.2. Macierze robocze

W przypadku macierzy roboczych spełnione powinny być następujące wymagania:

A. Macierz dyskowa musi mieć możliwość zainstalowania w szafie stelażowej 19” (dołączony zestaw montażowy).

B. Musi być wyposażona we wszystkie niezbędne kable połączeniowe (zasilające i logiczne).
C. Powinna mieć możliwość rozbudowy (bez wymiany kontrolerów macierzy). Rozbudowa musi być możliwa w ramach oferowanego modelu macierzy bez stosowania dodatkowych przełączników lub koncentratorów.
D. Pojemność netto macierzy – minimum 224 TiB w trybie pracy RAID6 wyposażoną w dyski HDD (Hot Swap).
E. Wydajność macierzy przy odczycie 4 strumienie 4K (4096x2160) dla plików 16 bit RGB dla 25 kl/s (1 strumień - 1,7 GB/s).
F. Prędkość w odczycie musi być zachowana dla zajętości macierzy na poziomie 75%.
G. Macierz musi być przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączania. Brak pojedynczego punktu awarii, który powodowałby brak dostępu do danych.
H. Pełna redundancja macierzy, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Możliwość wykonywania aktualizacji oprogramowania macierzy w trybie online bez wyłączania jakiejkolwiek ścieżki dostępu hostów do macierzy. Wymiana elementów systemu w trybie „Hot-Swap", a w szczególności takich, jak: kontroler(y), zasilacz(e), wentylatory.
I. Możliwość zasilania z dwóch niezależnych źródeł zasilania –odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
J. Skalowalność wydajności i objętości.
K. W przypadku awarii dysku wydajność macierzy nie powinna ograniczyć jej wydajności poniżej 75% (zapis – odczyt).
L. Wymagane jest dostarczenie odpowiednich licencji dla wymienionych wcześniej funkcjonalności.

### 2.3. Dodatkowe wymagania

Dodatkowo system składowania danych w CD powinien umożliwiać:

A. Zdefragmenowanie taśm.
B. Podział przestrzeni taśmowej na kategorie
C. Kasowanie, duplikowanie, kopiowanie obiektów.
D. Posiadać funkcjonalność fragmentarycznego wykopiowania danych z taśm dla plików DPX (po zakresie klatek) i MOV (po TC)
E. Powinien być dostarczony z dyskami zapasowymi i 4 kasetami czyszczącymi

# 3. Wymagania dla platformy transkodującej, stacji masteringowej oraz oprogramowania do kontroli jakości.

### 3.1. Transkodery

Transkodery w CD powinny posiadać następujące właściwości:

A. Skalowalność pod względem wydajności;
B. Odczytywać materiały z kontenerów: dpx, mov, wave, mxf;
C. Eksportować dane w kontenerach: mxf, mov, mp4, wav;
D. Obsługiwać kompresję kodekami: Prores, DNxHD, H.264, H.265, XDCAM HD 422;
E. Posiadać funkcję forensic watermarking;

F. Posiadać funkcję wbijania logo i statycznego tekstu (burn in);
G. Posiadać funkcję wbijania napisów do wersji językowych (burn in);
H. Posiadać opcję skalowania obrazu o niższej rozdzielczości do rozdzielczości minimum UHD (4096x2160);
I. Posiadać funkcję skalowania obrazu do niższych rozdzielczości (np. skalowanie z 2K do HD);
J. Powinien działać w sposób automatyczny, działać pod kontrolą MAM, z wyjątkiem masteringu DCP i IMF;
K. Umożliwiać kodowanie materiałów do formatów VOD wg profili

| Profil | Video Bitrate | Video Resolution | Video Profil | Level | GOP Lenght | Audio Codec | Audio Bitrate |
|---|---|---|---|---|---|---|---|
| MP4-250 | 300 kbps | 416x234 | Main | 2.1 | 50 | AAC LC | 64 kbps |
| MP4-500 | 550 kbps | 640x360 | Main | 3.0 | 50 | AAC LC | 64 kbps |
| MP4-1000 | 950 kbps | 960x540 | High | 3.1 | 50 | AAC LC | 96 kbps |
| MP4-1500 | 1550 kbps | 1024x576 | High | 4.1 | 50 | AAC LC | 128 kbps |
| MP4-2500 | 2550 kbps | 1280x720 | High | 4.1 | 50 | AAC LC | 128 kbps |
| MP4-4000 | 3950 kbps | 1920x1080 | High | 4.1 | 50 | AAC LC | 128 kbps |

### 3.2. Stacja masteringowa

Dostarczona stacja masteringowa powinna spełniać następujące minimalne wymagania:

A. Odsługiwać wszystkie materiały archiwizacyjne;
B. Umożliwiać zmianę wymiarów oglądanego obrazu (pan&scan, aspect, down-sampling) w trakcie odtwarzania;
C. Konforming materiałów filmowych na podstawie list montażowych w formatach: XML (Final Cut Pro), AAF i OMF, EDL (CMX3600);
D. Synchronizacja dźwięku z obrazem;
E. Edycja obrazu z zastosowaniem typowych standardowych efektów (zooming, cropping, rotation, flip-flop,);
F. Możliwość użycia na tej samej linii czasu obrazu o różnych formatach, rozdzielczościach, o różnych przestrzeniach kolorystycznych z ustawianiem odpowiednich „3D LUT", w czasie rzeczywistym;
G. Wstawianie w obraz wyjściowy (burn-in) kodu czasowego;
H. Renderowanie różnych wersji materiałów wyjściowych co najmniej w formatach (kontenerach) DPX, TIFF, MXF, QT;
I. Odtwarzanie, mastering, transkodowanie, konwersja formatów emisyjnych (Broadcast) (zapis i odczyt) w tym:
    a. nieskompresowane pliki graficzne DPX i TIFF, JPEG2000;
    b. SONY XDCAM;
    c. Apple ProRes (444, 422, HQ);
    d. MXF DNxHD i DNxHR;
    e. MPEG-2, MPEG-4, H264, AVC-Intra (pliki DVD, Blu-ray itd.);
    f. kodeki H264 i H265 (zapis i odczyt);
    g. JPEG2000 MXF, DCP.

J. Mastering DCP w zakresie:
    a. przeglądanie materiałów źródłowych: obrazu, dźwięku, napisów w pełnej natywnej jakości odtwarzania;
    b. generowanie paczek DCP w standardach Interop i SMPTE;
    c. konforming otrzymanych materiałów źródłowych;
    d. odtwarzanie kodowanych i niekodowanych DCP w czasie rzeczywistym w rozdzielczości 2K i 4K;
    e. dodawanie innych wersji do DCP (suplementy);
    f. „Rewrapping" DCP z kluczem DKDM;
    g. szybkie renderowanie plików JPEG2000 ze wspomaganiem sprzętowym (GPU lub dedykowany hardware);
    h. edycja napisów dialogowych (subtitles): tekst, wielkość, zmiana czcionki, położenie. Obsługiwane formaty napisów: MXF, PNG, XML, CineCanvas, D-Cinema SMPTE 428-7;
    i. generowanie kluczy KDM;
    j. synchronizowanie dźwięku z obrazem;
    k. możliwość tworzenia paczek DCP z dźwiękiem ATMOS.
K. Mastering IMF w zakresie:
    a. wsparcie dla Application 2/2e Studio Profile;
    b. wsparcie profili JPEG 2000 w tym profili Broadcast BPC L7 i profili IMF 16 bit;
    c. wsparcie standardu DPP dla IMF Broadcast;
    d. import i odtwarzanie pakietów IMF o rozdzielczości do 4K w czasie rzeczywistym;
    e. możliwość edytowania napisów dialogowych;
    f. kontrola, weryfikacja i ocena pakietów IMF;
    g. możliwość synchronizacji dźwięku z obrazem.
L. Mastering HDR w zakresie:
    a. wsparcie dla zaleceń ITU BT-2100: Dolby Vision, HDR10 i HLG;
    b. możliwość konwersji materiałów do różnych standardów;
    c. konwersja SDR – HDR (w obu kierunkach).

Stanowisko musi być wyposażone w urządzenia do przeglądania materiałów filmowych w następującej konfiguracji:

A. Telewizor o wielkości minimum 65 cali o parametrach podobnych lub lepszych niż LG C9 OLED
B. System dźwięku dookólnego 5.1 (głośniki i wzmacniacze) umożliwiające odsłuch dźwięku o dynamice kinowej
C. Odtwarzacz zakodowanych DCP.

Dodatkowo w związku z wymogiem obsługi standardów zgodnych z wymaganiami dla systemów teleinformatycznych w tym wymaganiami w zakresie interoperacyjności, transkoder lub stacja masteringowa powinna umożliwiać eksport danych do kontenerów: wav, mp3, avi, mpg/mpeg, mp4/m4a/mpeg4, ogg, ogv. Dopuszcza się zastosowanie do tego celu dodatkowego oprogramowania.

### 3.3. Kontrola jakości

Aplikacja do kontroli jakości w CD musi działać w sposób automatyczny i ręczny. Po skopiowaniu danych na macierze robocze uruchamiany jest pierwszy test, którego zadaniem jest zgrubna ocena jakości materiałów. Po kontroli automatycznej dokonywana będzie kontrola ręczna.

Odtwarzacz (player) i oprogramowanie do automatycznej kontroli jakości ma mieć co najmniej takie funkcjonalności:

A. Obsługiwać następujące formaty:
   a. Kontenery: MXF, MPEG-2 TS, MPEG-2 PS, MP4, MOV, ASF, AVI, MKV, IMF, sekwencja DPX, sekwencja TIFF, encrypted DCP.
   b. Kodeki video: MPEG-2, DV/DVCPro 25/50/100, MPEG-4, AVC/H.264 (wszystkie profile), HEVC/H.265, WMV/VC-1, ProRes (wszystkie profile), ProRes 4444 XQ, DNxHR, DNxHD, MJPEG, MJPEG2000, DPX.
   c. Formaty obrazu: JPEG, JPEG2000, TIFF
   d. Kodeki audio: MPEG1/2, PCM, AAC, AES3, WAV, MP3, WMA, DV, AC-3, Dolby Digital, Dolby-E, DTS Audio, Dolby Atmos.
   e. Tekstowe (napisy dialogowe): EBU STL, CineCanvas, SRT, Timed Text.

B. Posiadać detekcję:
   a. zatrzymanych klatek
   b. czarnych klatek
   c. pustych klatek (media offline)
   d. macroblokizacje
   e. utratę ostrości
   f. szum video
   g. prędkości odtwarzania
   h. prędkości strumienia
   i. proporcji obrazu
   j. długości
   k. rozdzielczości
   l. formatu koloru
   m. poziomu luminancji/chrominancji
   n. poziomu czerni
   o. migotania

C. Automatyczna kontrola jakości powinna obejmować sprawdzanie i raportowanie co najmniej następujących parametrów:
   a. sprawdzenie kontenera: układ, długość, rozmiar pliku, różnica długości dźwięku i obrazu, timecode, techniczne parametry obrazu i dźwięku (rozdzielczość, ilość kanałów, bitrate, częstotliwości próbkowania, itp.) napisy, metadane.
   b. sprawdzanie zgodności pakietów DCP i IMF.
   c. sprawdzanie i wykrywanie wad plików video
   d. sprawdzanie i wykrywanie wad plików audio
   e. sprawdzanie dodatkowych cyfrowych informacji zawartych w materiale filmowym np.: napisy jako plik, napisy w obrazie (burn-in) itp.

# 4. Wymagania dla oprogramowania zarządzającego mediami w CD

Oprogramowanie instalowane w WFDiF powinno pozwalać na archiwizację, odzyskiwanie oraz opisywanie metadanymi materiałów różnego typu (w tym video). Powinno spełniać następujące funkcjonalności.

## 4.1. Wymagania ogólne:

A. Uniwersalny interface użytkownika;
B. Wysoka wydajność i bezpieczeństwo;
C. Możliwość skalowania;
D. Poglądowe proxy zabezpieczone znakiem wodnym z każdego z archiwizowanych materiałów;
E. Interface w języku polskim i/lub angielskim;
F. Zarządzanie procesami przetwarzania (np. kopiowanie, przenoszenie, duplikowanie, oznaczanie, subskrybowanie, komentowanie, inicjowanie transkodowania sekwencji zadań);
G. Możliwość graficznego budowania własnych procesów przetwarzania;
H. Możliwość zarządzania pracami i zadaniami dla systemu oraz poszczególnych osób/grup;
I. Możliwość kolejkowania procesów oraz nadawanie i zmiana im priorytetów;
J. Współpraca i zarządzanie programami do automatycznej kontroli jakości;
K. Integracja z transkoderem;
L. Integracja z posiadaną przestrzenią roboczą;
M. Możliwości założenia dowolnej ilości kont unikatowym użytkownikom (ew. możliwość dokupienia licencji);
N. Możliwości konfiguracji i administracji przez obsługę techniczną Zamawiającego interfejsu i funkcjonalności, w szczególności w zakresie: organizacji interfejsu wprowadzania danych, edycji etykiet, dodawania i usuwania pól i grup pól;

## 4.2. Katalogowanie, wyszukiwanie i sortowanie

A. Grupowanie materiałów archiwizowanych w struktury. Oprogramowanie ma umożliwiać przechowywanie różnych typów plików powiązanych logicznie w obrębie pojedynczego obiektu, na przykład dla pojedynczego tytułu filmu:
    a. Master archiwizacyjny (sekwencja DPX),
    b. DCDM (sekwencja TIFF),
    c. DCP,
    d. MOV,
    e. WAVE,
    f. itd.

B. Oprogramowanie ma pozwalać na grupowanie plików, stanowiących jedną logiczną całość, w formie pozwalającej na ich wygodne zarządzanie (np.: sekwencje DPX składające się na jeden materiał filmowy powinny być zgrupowane);
C. Na grupach można wykonywać zbiorczo takie operacje jak:

a. transkodowanie,
b. eksport,
c. edycja metadanych,
d. usuwanie plików,

D. Wyszukiwanie zgormadzonych materiałów, zapewniając co najmniej funkcjonalność:

a. wyszukiwania prostego – wyszukiwanie pełnotekstowe po wszystkich polach opisujących materiał;
b. wyszukiwanie zaawansowane – wyszukiwanie pozwalające na tworzenie złożonych kwerend składających się z zapytań o ciągi znaków występujące w wybranych polach w schemacie metadanych połączonych operatorami: AND, OR, NOT;
c. wyszukiwanie zaawansowane powinno pozwalać na wyszukiwanie materiałów poprzez powiązane z nimi obiekty (np.: wyszukaj seriale, które w powiązanych z nimi odcinkach mają w polu opis wartość…);
d. oprogramowanie powinno pozwalać na definiowanie kryteriów grupujących (np.: pola: „tytuł oryginalny”, „tytuł polski”, „tytuł pełny”, „tytuł pierwowzoru”, itp. można zgrupować pod wspólnym atrybutem „tytuł” – wyszukiwania po tak utworzonym polu powoduje wyszukanie treści po wszystkich polach wchodzących w jego skład);

E. Zarządzanie wyszukiwaniem materiałów i ich filtrowaniem pod kątem określonych kryteriów;
F. Powinno podpowiadać frazy możliwe do wyszukania;
G. W wyszukiwaniu zaawansowanym oprogramowanie powinno podpowiadać frazy możliwe do wyszukania w kontekście pola, po którym szukana jest dana fraza;
H. Powinno pozwalać na filtrowanie wyników wyszukiwania po zawartości dowolnego pola metadanych;
I. Powinno pozwalać na zapisanie wyników wyszukiwania do późniejszej obróbki;
J. Powinno pozwalać na zapisanie kryteriów wyszukiwania do późniejszego ich wykorzystania;
K. Powinno prezentować wyniki wyszukiwania w formie tabelarycznej lub kafelkowej;
L. Oprogramowanie powinno umożliwiać skonfigurowanie jakie pola metadanych mają być prezentowane w wynikach wyszukiwania;
M. Wyniki wyszukiwania materiałów wideo powinny zawierać klatki kluczowe;
N. Sortowanie wg polskich znaków diakrytycznych;
O. Powinno pozwalać na stronicowanie wyników wyszukiwania;

### 4.3. Użytkownicy i uprawnienia

A. Udostępnianie funkcjonalności dla zewnętrznych partnerów (użytkownik);
B. Rozbudowany system uprawnień (użytkownik, archiwista, kontroler jakości administrator);
C. Uprawnienia w oprogramowaniu mają pozwolić definiować dostęp użytkowników na poziomie:
   a. typów obiektów (np.: film fabularny, film dokumentalny);
   b. prawa własności plików (np. filmy SFR są prezentowane tylko pracownikom SFR);

c. poszczególnych pól opisujących obiekt (np.: dane o licencjach mogą być widoczne tylko dla ograniczonej grupy użytkowników);
d. typu plików przypisanych do obiektów (np. HiRes, proxy, other);

D. Uprawnienie mają być zależne od statusu obiektu (np.: obiekt o statusie „nowy" może być edytowany, a o statusie „zamknięty" może być już tylko przeglądany);
E. Możliwości interfejsu i uprawnienia użytkowników powinny być zależne od ich przynależności do grupy użytkowników i uprawnień nadanych tym grupom;

### 4.4. Odtwarzacz

A. Podstawowe funkcje:
   a. odtwarzanie,
   b. stop,
   c. przewijanie w tył i przód,
   d. skok do wybranego timecode'u,
   e. skok o jedną klatkę w tył i przód
B. Zaawansowany edytor przeglądania wideo:
   a. wsparcie procesu dodawania opisu (metadanych) do materiału cyfrowego (w tym przygotowania i wykorzystania gotowych słowników dziedzinowych do szybkiego dodawania metadanych zgodnie z zawartością materiału filmowego, np. scen z konkretnymi aktorami, wydarzeniami, itp.). Zapis dokładnego czasu (frame accurate) dla metadanych;
   b. oprogramowanie umożliwia odzyskanie wskazanej za pośrednictwem znaczników czasowych części materiału wideo - partial restore (nie jest wymagany odzysk frame-accurate, lecz dokładność powinna być nie mniejsza niż +/- 2 ramki);
   c. wskazanie znaczników czasowych dla materiału wideo powinno być możliwe z poziomu player'a wideo, zawartego w interfejsie użytkownika;
   d. tworzenie frame accurate video proxy oraz kopii materiału na potrzeby podglądu, edycji, pracy grupowej, współdzielenia, itp.
   e. tworzenie rough cuts, EDL (edit decision lists) i klipów (fragmentów) materiału cyfrowego (jako nowa kopia i jako subclip).

### 4.5. Metadane

A. Schemat metadanych zgodny z EN15744 i EN15907;
B. Możliwość importu metadanych z chmury za pomocą protokołu S3;
C. Drzewiasta struktura metadanych;
D. Swobodne dodawanie, usuwanie, podgląd, edycja metadanych, wersjonowanie, import, eksport, współdzielenie, określanie praw dostępu do metadanych;
E. Automatyczne pozyskiwanie metadanych zawierających dane techniczne;
F. Edycja metadanych pojedynczo i masowo;
G. Istnieje możliwość zarządzania metadanymi obiektów za pośrednictwem API;
H. Wprowadzanie metadanych w różnych wersjach językowych;
I. Możliwość zdefiniowania, które metadane mają tą samą wartość dla wszystkich języków (np.: daty, nazwy własne, dane teleadresowe, itp.) i ich modyfikacja w ramach dowolnego języka powoduje zmianę we wszystkich pozostałych językach;
J. Możliwość zdefiniowania, które pola w obiekcie są polami obowiązkowymi (bez ich wypełnienia nie można zapisać obiektu);

K. Oprogramowanie ma umożliwiać dodanie dowolnej ilości słowników kontrolowanych i powiązanie ich ze schematem metadanych;
L. Dodanie nowego słownika powinno być czynnością konfiguracyjną, możliwą do wykonania w interfejsie użytkownika, nie wymagającą żadnych zmian o charakterze programistycznym.

4.6. Udostępnianie:

A. Wspomaganie udostępniania treści:
    a. bezpieczny transfer (szyfrowanie);
    b. wsparcie ponawiania transferu w razie jego zerwania;
    c. konfiguracja parametrów transmisji;
    d. kontrola zaawansowania transferu (progres);
    e. integracja z interfejsem użytkownika repozytorium.

4.7. API - Interface programistyczny umożliwiający integrację z platformą VOD WFDiF:

A. Oprogramowanie ma udostępniać komplet funkcjonalności za pośrednictwem dobrze udokumentowanego API;
B. W oprogramowaniu nie mogą istnieć funkcje, które można wywołać z poziomu GUI, a nie istnieją ich odpowiedniki w API;
C. API jest dostępne w formie web-serwisów REST.

4.8. Raportowanie i logowanie:

A. Dynamiczne generowanie różnego rodzaju raportów w oparciu o zarejestrowane dane;
B. Raportowanie statystyk z realizacji zadań realizowanych za pomocą zdefiniowanych mechanizmów automatycznych w oprogramowaniu (tj. liczba zadań wykonanych przez poszczególne serwery, średni czas realizacji zadań, czas przetwarzania w stosunku do czasu trwania materiału);
C. Raportowanie statystyk związanych z obiektami w oprogramowaniu (tj. procent wykorzystania obiektów przez użytkownika, liczba tytułów w poszczególnych kategoriach / statusach);
D. Raportowanie statystyk związanych z aktywnościami Użytkowników (tj. liczba i daty logowań, czas trwania sesji).

4.9. Dodatkowe

A. Inicjowanie sesji online pracy grupowej nad materiałem cyfrowym (podgląd, adnotacje, listy zadań do wykonania, statusy, itp.);
B. Możliwość utworzenia sesji online dla wybranej grupy osób (tzw. sesja creative review), podczas której dany materiał cyfrowy może być:
    a. oglądany (wersja proxy w przeglądarce internetowej);
    b. adnotowany (z zapisem czasu, frame) – np. konieczność wykonania korekty materiału;
    c. komentowany;

d. tworzenie zadań do wykonania, ich priorytetu, deadline'u, itp. dla osób uczestniczących w sesji review;
e. zapis sesji w postaci raportu (np. PDF);
f. zmiana statusu (metadanych) materiału w zależności od statusu zadań utworzonych w ramach sesji creative review

# 5. Firewall

## 5.1. 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 trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- firewall,
- ochrony w warstwie aplikacji,
- protokołów routingu dynamicznego,

## 5.2. Redundancja, monitoring i wykrywanie awarii

A. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
B. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
C. Monitoring stanu realizowanych połączeń VPN.
D. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

## 5.3. Interfejsy, zasilanie:

A. System realizujący funkcję Firewall musi dysponować minimum:
   - 16 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.

- 2 gniazdami SFP+ 10 Gbps.

B. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
C. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
D. System musi być wyposażony w zasilanie AC.

5.4. Parametry wydajnościowe:

A. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 50.000 nowych połączeń na sekundę.
B. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps.
C. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
D. Wydajność szyfrowania IPSec VPN: nie mniej niż 10 Gbps.
E. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
F. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
G. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 900 Mbps.

5.5. 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:

A. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
B. Kontrola Aplikacji.
C. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
D. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
E. Ochrona przed atakami - Intrusion Prevention System.
F. Kontrola stron WWW.
G. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
H. Zarządzanie pasmem (QoS, Traffic shaping).
I. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
J. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
K. Analiza ruchu szyfrowanego protokołem SSL.
L. Analiza ruchu szyfrowanego protokołem SSH.

5.6. Polityki, Firewall

A. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
B. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    - Translację jeden do jeden oraz jeden do wielu.
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
C. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

5.7. Połączenia VPN

A. 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 w trybie pracy Galois/Counter Mode (GCM).
    - Obsługa protokołu Diffie-Hellman grup 19 i 20.
    - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
    - Tworzenie połączeń typu Site-to-Site oraz Client-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, DPD, Xauth.
    - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
B. 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. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
    - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

5.8. Routing i obsługa łączą WAN

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

5.9. Zarządzanie pasmem

A. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
B. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
C. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

5.10. Kontrola Antywirusowa

A. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
B. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
C. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
D. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

5.11. Ochrona przed atakami

A. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
B. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
C. Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
D. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
E. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
F. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
G. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

5.12. Kontrola aplikacji

A. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
B. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
C. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

D. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
E. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

5.13. Kontrola WWW

A. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
B. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
C. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
D. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
E. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

5.14. Uwierzytelnianie użytkowników w ramach sesji

A. 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, RSA SecurID) w oparciu o zewnętrzne bazy danych.
B. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
C. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

5.15. Zarządzanie

A. 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.
B. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
C. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
D. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

E. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
F. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

5.16. Logowanie

A. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
B. W przypadku, kiedy usługa logowania i raportowania realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.
C. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
D. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
E. Musi istnieć możliwość logowania do serwera SYSLOG.

5.17. Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

A. ICSA lub EAL4 dla funkcji Firewall.
B. ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
C. ICSA dla funkcji SSL VPN.

5.18. Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

A. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.
B. Logowanie do usługi realizowanej w chmurze na okres 60 miesięcy.
C. Możliwość weryfikacji poziomu bezpieczeństwa dla co najmniej 6 stacji klienckich na okres 60 miesięcy.

5.19. Gwarancja oraz wsparcie

A. 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 24x7.

5.20. Rozszerzone wsparcie serwisowe AHB/SOS

A. 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 60 miesięcy.
B. 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 24x7. 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.

# 6. Wymagania infrastruktury

Powstała w CD infrastruktura ma za zadanie realizować zadania w oparciu o sieć o przepustowości minimum 10 GbE

Do budynku zostaną podłączona łącze dostawcy internetowego o przepustowości min 2x10 Gb/s.

Dostawca w ramach instalacji systemu musi zapewnić:

6.1. Przełączniki sieciowe zgodne z oferowanym systemem
6.2. Przełączniki i sieć muszą być odporne na awarię i zapewnić pełną redundancję. Ma ona dotyczyć urządzeń i połączeń. Sieć powinna być odporna na awarię jednego przełącznika sieciowego
6.3. Komplet urządzeń stanowiących rozwiązanie powinien posiadać jeden zgodny kierunek przepływu powietrza. Wlot powietrza chłodzącego powinien znajdować się na froncie, wylot z tyłu. Dotyczy to zarówno modułów chłodzących jak i zasilaczy.
6.4. Napędy biblioteki powinny być podłączone 2 liniami, transfer danych z napędów na macierz roboczą musi być zrealizowany w technologii minimum FC 8 Gb/s.
6.5. Utworzenie przestrzeni dedykowanej udostępnieniu materiałów o wielkości minimum 50 TiB netto z możliwością skalowania. Minimalna wydajność zasobu to 10 Gb/s
6.6. System udostępniania danych musi być wyposażony w rozwiązanie umożliwiające automatyczne kasowanie danych po upływie określonego czasu

6.7. System udostępniania powinien umożliwiać pobranie danych, do których dostęp ograniczony jest hasłem generowanym dla konkretnego klienta.
6.8. Udostępniane sekwencje plikowe muszą być ściągane jako paczka
6.9. Infrastruktura powinna zawierać KVM IP wraz z dodatkową konsolą w serwerowni do obsługi zgromadzonych tam urządzeń
6.10. Dostęp do systemu z zewnątrz dla partnerów z wykorzystaniem VPN
6.11. Szafy aparaturowe o wymiarach minimalnych 800/1200/1980, szer./gł./wys. mm., wyposażone w drzwi przednie i tylne perforowane, o kolorze RAL 9005 czarny, konstrukcja spawana, wyposażone w PDU z monitoringiem oraz niezbędne akcesoria potrzebne do prowadzenia i upięcia okablowania. Przestrzenie niewykorzystane przez urządzenia muszą być zaślepione od frontu szafy. Szafy muszą być wyposażone w środkowe belki montażowe.
6.12. Okablowanie w serwerowni
6.13. Okablowanie do pomieszczeń CD (jeśli proponowane rozwiązanie nie umożliwia realizacji zadań w oparciu o istniejące okablowanie – do każdego pomieszczenia doprowadzone są 4 przewody UTP kategorii 7)
6.14. Połączenie serwerowni B z szafą krosową w serwerowni A (48 przewody S/FTP Cat 7. zakończone patchpanelem 48xRJ45 Cat. 6a (gniazda) oraz 96 włókna światłowodowe kategorii OM-4 – przewodem 4x24 włóknowym multimode, zakończone patchpanelem 48xLC-Duplex) oraz przewodem 12 włóknowym singlemode OS-2, zakończone patchpanelem 6xLC-Duplex
6.15. W przypadku stosowania extenderów dla obrazu, jego przesyłanie musi odbywać się bezstratnie.

**UWAGA! Serwerownia jest zabezpieczona przeciwpożarowo. W przypadku prac instalacyjnych naruszających te zabezpieczenia, wykonawca zobowiązany jest do przywrócenia ich stanu wraz uzyskaniem stosownego certyfikatu**

# 7. Stacje robocze do przepisywania materiałów filmowych i kontroli jakości:

Wymagania minimalne:

| | |
|---|---|
| **System operacyjny:** | Mac OS lub Windows |
| **CPU minimum:** | Intel Core i9-9xxx seria X, dual Intel Xeon GOLD 6xxx (min. 8 rdzeni/procesor) |
| **Pamięć dyskowa:** | 1 TB M2 NVMe plus 2 x 1 TB SSD RAID0 (min 2 mln. h. bezawaryjnej pracy SSD) |
| **RAM:** | 64GB |
| **Grafika/VRAM:** | QUADRO lub CUDA compliant GPU minimum 8GB graphics RAM |

Minimalne warunki dla 6 stacji roboczych:

7.1. Monitory 4K (4096x2160 z pokryciem przestrzeni DCI-P3: minimum 98% oraz rozmiarem ekranu zawartym w przedziale 30-40”). Ustawienia koloru: REC2020, REC709, DCI, PQ_DCI,

PQ_REC2100, HLG_REC2100, sRGB i kalibrowany. Częstotliwość odświeżania ramki minimalny zakres 24 – 60 Hz.

7.2. Odsłuch indywidualny do każdej stacji roboczej: słuchawki plus głośniki 2.0
7.3. Interface USB 3.2, Thunderbolt 3, eSATA
7.4. Możliwość obsługi systemów plików dla podłączanych urządzeń zewnętrznych (NTFS, ExFAT, HSF+, APFS, Ext2 i Ext3
7.5. Zewnętrzne napędy LTO-8 1 szt. i LTO-7 1 szt. podłączone do dwóch różnych stacji roboczych.
7.6. Możliwość odtwarzania archiwizowanych formatów filmowych w czasie rzeczywistym i w pełnej oryginalnej rozdzielczości (max. 4096 x 2160).
7.7. Klawiatura multimedialna (dodatkowa z pokrętłem Jog/Shuttle).

# 8. Wymagania dla dokumentacji

8.1. Wymagania Ogólne:

A. Dokumentacja musi być sporządzona w języku polskim, chyba że dotyczy oprogramowania narzędziowego obcego pochodzenia, wykorzystywanego w Rozwiązaniu, dla którego nie ma Dokumentacji w języku polskim, w takim przypadku Dokumentacja może zostać przekazana w języku angielskim.
B. Każda Dokumentacja z wyłączeniem dokumentacji technicznej, powstała w wyniku realizacji zamówienia i przekazana Zamawiającemu przez Wykonawcę stanowi własność Zamawiającego. Zamawiający ma prawo udostępniać Dokumentację osobom trzecim w sposób nie naruszający praw autorskich.
C. Aktualizacja Dokumentacji następuje każdorazowo po wprowadzeniu przez Wykonawcę zmian w Rozwiązaniu. W przypadku wprowadzenia zmian do Rozwiązania, wymagających odzwierciedlenia w Dokumentacji, zarówno wskutek pojawienia się aktualizacji Rozwiązania, jak i poprawy Błędów lub zmiany Konfiguracji, Wykonawca dostarczy zaktualizowaną Dokumentację (lub tę jej część, której zmiana dotyczy) w terminie nie przekraczającym 15 Dni od daty dokonania zmian w Rozwiązaniu, chyba że ustalony zostanie inny termin.
D. Wykonawca dostarczy szczegółową Dokumentację komponentów firm trzecich użytych w dostarczanym Systemie, w tym także dostarczaną przez ich producentów. Dokumentacja ta może występować w języku angielskim, jeśli nie ma tłumaczenia na język polski.
E. Dokumentacja musi być dostarczona w jednym egzemplarzu w formie papierowej lub elektronicznej (.pdf, .docx) na nośniku elektronicznym, w postaci umożliwiającej uzyskanie jej wydruku przy pomocy powszechnie używanych narzędzi.
F. Dokumentacja musi gwarantować kompletność dokumentu rozumianą jako pełne, bez wyraźnych i ewidentnych braków, przedstawienie omawianego problemu obejmujące całość z danego rozpatrywanego zakresu zagadnienia.
G. Dokumentacja musi zapewniać spójność i niezaprzeczalność dokumentu, rozumianych jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w Dokumentacji powykonawczej, jak i brak logicznych sprzeczności pomiędzy informacjami zawartymi w całej Dokumentacji oraz we fragmentach tego samego dokumentu.

H. Zawartość Dokumentacji musi być zgodna z wytworzonym Rozwiązaniem.

8.2. Dokumentacja szkoleniowa powinna odzwierciedlać przebieg szkolenia, wykorzystane materiały szkoleniowe i zawierać m. in. ścieżki postępowania i odpowiadające im zrzuty z ekranów.

8.3. Dokumentacja Administratora Oprogramowania.

A. Dokumentacja Administratora Oprogramowania Aplikacyjnego musi opisywać kolejność czynności i zakres możliwych danych do wprowadzenia oraz sposób postępowania w sytuacjach szczególnych i awaryjnych.
B. Dokumentacja Administratora Oprogramowania Aplikacyjnego powinna być dostępna w postaci elektronicznej umożliwiającej przeszukiwanie oraz odnajdywanie konkretnych tematów, zarówno z poziomu Oprogramowania Aplikacyjnego, jak i w postaci umożliwiającej jej wydruk.
C. Dokumentacja Administratora Oprogramowania Aplikacyjnego obejmować będzie, co najmniej:
    1. szczegółową (krok po kroku) instrukcję Instalacji i Konfiguracji Oprogramowania Aplikacyjnego,
    2. pełny opis parametrów instalacyjnych i Konfiguracyjnych Oprogramowania Aplikacyjnego wraz z opisem dopuszczalnych wartości i ich wpływem na działanie Oprogramowania Aplikacyjnego, obejmujący także wartości zalecanych ustawień,
    3. szczegółową (krok po kroku) instrukcję wgrywania nowych Wersji Systemu,
    4. szczegółowy opis możliwych do zastosowania Ról i uprawnień wraz z ich wpływem na działania Oprogramowania Aplikacyjnego,
    5. szczegółowy (krok po kroku) opis nadawania Ról i uprawnień,
    6. wykaz komunikatów błędów i ostrzeżeń.

8.4. Dokumentacja Użytkownika.

A. Wykonawca dostarczy Dokumentację użytkownika oraz opis Ścieżek Postępowania.
B. Dokumentacja użytkownika musi zawierać opis pełnej funkcjonalności Oprogramowania Aplikacyjnego w sposób przejrzysty umożliwiający samodzielne użytkowanie Oprogramowania Aplikacyjnego.
C. Dokumentacja musi opisywać kolejność czynności i zakres możliwych danych do wprowadzenia oraz sposób postępowania w sytuacjach szczególnych.
D. W zakresie kluczowych funkcji użytkowych (funkcji biznesowych) Dokumentacja użytkownika zawierać będzie Ścieżki Postępowania - jak wykonać określoną operację w Systemie opisaną krok po kroku wraz z zrzutami ekranów.
E. Dostarczona przez Wykonawcę Dokumentacja użytkownika, w tym „Ścieżki Postępowania” zostaną przygotowane w sposób umożliwiający Zamawiającemu dodanie ich jako odrębnych artykułów do bazy wiedzy.

8.5. Dokumentacja powykonawcza techniczna

A. Wykonawca jest zobowiązany dostarczyć w ramach zamówienia Dokumentację powykonawczą i techniczną Rozwiązania.
B. Dokumentacja powykonawcza musi być sporządzona w języku polskim, chyba że dotyczy oprogramowania narzędziowego obcego pochodzenia, wykorzystywanego w Rozwiązaniu, dla którego nie ma dokumentacji w języku polskim, w takim przypadku Dokumentacja może zostać przekazana w języku angielskim.
C. Aktualizacja Dokumentacji powykonawczej następuje w okresie przewidzianym dla asysty technicznej każdorazowo po wprowadzeniu przez Wykonawcę zmian w Rozwiązaniu.
D. W przypadku wprowadzenia zmian w elementach Oprogramowania i Oprogramowania Aplikacyjnego, wymagających odzwierciedlenia w Dokumentacji powykonawczej, zarówno na skutek pojawienia się aktualizacji Oprogramowania i Oprogramowania Aplikacyjnego, jak i poprawy błędów lub zmiany konfiguracji, Wykonawca dostarczy zaktualizowaną Dokumentację powykonawczą (lub tę jej część, której zmiana dotyczy) w terminie nie przekraczającym 15 Dni od daty dokonania zmian w Systemie, chyba, że ustalony zostanie inny termin.
E. Załącznikiem do Dokumentacji powykonawczej musi być Dokumentacja Kodu źródłowego.
F. Wykonawca jest zobowiązany dostarczyć Dokumentację techniczną dla Oprogramowania w zakresie administrowania, która została stworzona przez producenta danego elementu Oprogramowania.
G. Dokumentacja techniczna, o ile to możliwe, powinna zostać dostarczona w języku polskim. W przypadku, gdy producent komponentu (elementu) Oprogramowania nie opracował dokumentacji w języku polskim Dokumentacja techniczna musi być w języku angielskim.
H. Dokumentacja techniczna stanowić będzie uzupełnienie Dokumentacji powykonawczej.
I. Wykonawca jest zobowiązany dostarczyć Dokumentację powykonawczą, która musi być sporządzona zgodnie z poniższym szablonem, przy czym szablon może zostać uzupełniony o dodatkowe elementy przez Wykonawcę:

    1. Wstęp.
    2. Cel dokumentu.
    3. Słowniki.
    4. Terminy i skróty specyficzne dla Rozwiązania.
    5. Używane skróty technologiczne.
    6. Używane terminy.
    7. Symbole graficzne.
    8. Rodzaje środowisk Rozwiązania.
    9. Projekty poszczególnych środowisk.
    10. Projekt danego środowiska Rozwiązania.
    11. Architektura Rozwiązania (opisy wraz ze szczegółowymi schematami graficznymi).
        a. Architektura sieciowa Rozwiązania.
        b. Wymagania komunikacyjne dla sieci LAN.

c. Adresacja interfejsów sieciowych komponentów Rozwiązania.
d. Połączenia wymagane podczas eksploatacji Rozwiązania.
e. Obciążenia połączeń sieciowych w Rozwiązania.
f. Architektura sieci SAN Rozwiązania.
g. Wymagania komunikacyjne dla sieci SAN.
h. Platforma aplikacyjna Rozwiązania.
i. Pojemność Rozwiązania.
j. Zależność pomiędzy wszystkimi elementami Rozwiązania.

12. Usługi:
    a. aplikacyjne,
    b. bazodanowe,
    c. systemy operacyjne.
13. Opis każdego z WebSerwisów i/lub plików wymiany wraz ze wskazaniem danych wejściowych oraz danych wyjściowych.
14. Opis przepływu danych pomiędzy poszczególnymi Modułami wraz ze schematami graficznymi.
15. Wykaz wszystkich słowników Systemu.
16. Wykaz parametrów dla wszystkich Modułów Systemu wraz z podaniem możliwych wartości i konsekwencji ich ustawienia.
17. Dodatkowe oprogramowanie wymagane w Rozwiązaniu:
    a. urządzenia klienckie i peryferyjne w Rozwiązaniu
    b. rodzaje użytkowników Rozwiązania,
    c. stacje klienckie,
    d. oprogramowanie,
    e. urządzenia peryferyjne.
18. System backup'u:
    a. koncepcja rozwiązania,
    b. wymagania środowiska dla systemu backupowego,
    c. wymagania na polityki tworzenia kopii bezpieczeństwa,
    d. zabezpieczane elementy środowiska,
    e. system zabezpieczeń danych,
    f. koncepcja rozwiązania,
    g. wymagania środowiska dla systemu zabezpieczeń danych,
    h. sposób odtwarzania poszczególnych składników Rozwiązania.
19. Sposób instalacji i konfiguracji Rozwiązania:
    a. wykaz parametrów Systemu wraz z podaniem możliwych ich wartości z określeniem konsekwencji ich ustawienia,
    b. szczegóły ustawień parametrów środowiska dla Rozwiązania,
    c. sposób zmiany ustawień parametrów środowiska Rozwiązania.
20. Wymagania środowiska dla systemu wirtualizacji zasobów:

a. koncepcja rozwiązania wirtualizacji zasobów,
b. wykaz wymaganych maszyn wirtualnych,
c. wymagania środowiska dla systemu antywirusowego,
d. wymagania środowiska dla systemu usług katalogowych,
e. wymagania środowiska dla systemu zarządzania infrastruktury serwerowej oraz aplikacyjnej.

21. Wymagania Rozwiązania dla systemu rejestrowania monitorowania i audytu zdarzeń.
22. Sposób realizacji Rozwiązania dla systemu monitorowania usług.
23. Opis przypadków użycia niezbędnych do zarządzania Rozwiązaniem (Opis w tym punkcie jest odrębnym opisem przygotowanym przez Wykonawcę, w którym może odwoływać się zapisów dokumentacji technicznej).
24. Wymagania środowiska dla mechanizmów zarządzania awarią łącznie z rozwiązaniami DisasterRecovery:
    a. architektura rozwiązania DisasterRecovery dla Rozwiązania,
    b. koncepcja odtworzenia środowiska po katastrofie,
    c. procedury DisasterRecovery.
25. Infrastruktura fizyczna:
    a. serwery,
    b. macierze,
    c. biblioteki,
    d. inne urządzenia.
26. Możliwości współpracy systemu z platformami sprzętowymi i systemowymi.
27. Wymagane licencje - wykaz niezbędnych licencji.
28. Model danych Systemu.
29. Pełny opis interfejsu użytkownika.
30. Wykaz wszystkich komunikatów diagnostycznych.

# 9. Gwarancja

**Definicje:**

Awaria – uszkodzenie systemu/urządzenia, elementu systemu/urządzenia (sprzętowe lub programowe) lub poważne zakłócenie pracy systemu/urządzenia, którego skutkiem jest brak możliwości korzystania z niego lub jego części. Za Awarię uważane jest również jednoczesne wystąpienie szeregu usterek, w przypadku, gdy można wykazać, że występujące jednocześnie usterki mają ten sam skutek, co opisane powyżej Awarie.
Usterka – uszkodzenie elementu systemu/urządzenia (sprzętowe lub programowe), której skutkiem jest brak dostępu do określonej funkcjonalności systemu/urządzenia, niemającej wpływu na realizację podstawowych jego funkcjonalności.

**Warunki gwarancji**

1. Wykonawca gwarantuje, że dostarczony sprzęt jest fabrycznie nowy, jest w 100% sprawny, jest dobrej jakości i nie ma wad.
2. Wykonawca gwarantuje, że od dnia podpisania Protokołu Odbioru Technicznego sprzęt będzie działać zgodnie z opisem zawartym w dokumentacji.
3. Na dostarczony sprzęt Wykonawca udziela Kupującemu gwarancji od dnia podpisania Protokołu Odbioru Technicznego, na okres **60 miesięcy**. Gwarancją objęte są wszystkie bez wyjątku elementy zamawianego sprzętu. Gwarancja obejmuje wsparcie techniczne i aktualizację oprogramowania.
4. Zamawiający wymaga, aby serwis dla urządzeń fizycznych był autoryzowany przez producenta tych urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta.
5. Wszelkie koszty napraw i obsługi gwarancyjnej, w tym koszty transportu, ponosi Wykonawca.
6. Wykonawca zobowiązuje się do zwrotu kosztów naprawy gwarancyjnej zrealizowanej przez Zamawiającego w przypadku, gdy dwukrotnie bezskutecznie wzywał Wykonawcę do jej wykonania.
7. Zgłaszania awarii i usterek Zamawiający będzie mógł dokonywać za pośrednictwem telefonu, lub poczty elektronicznej.
8. Czas reakcji:
    - na zgłoszoną awarię (rozumianą jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć 4 godzin; usunięcie awarii (naprawa lub wymiana wadliwego podzespołu lub urządzenia lub oprogramowania) musi zostać wykonane w przeciągu 24 godzin od momentu zgłoszenia awarii
    - na zgłoszoną usterkę (rozumianą jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć 24 godzin; usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia lub oprogramowania) musi zostać wykonane w przeciągu 3 dni roboczych od momentu zgłoszenia usterki
9. Serwis gwarancyjny jest świadczony w miejscu instalacji urządzeń w siedzibie Kupującego lub w serwisie Wykonawcy (Producenta).
10. W przypadku Sprzętu, dla którego jest wymagany dłuższy czas na naprawę, Zamawiający dopuszcza podstawienie na czas naprawy sprzętu o nie gorszych a porównywalnych parametrach funkcjonalnych.
11. O ile naprawa w miejscu zainstalowania okaże się niemożliwa, Wykonawca dokona naprawy w punkcie serwisowym, a wszelkie dodatkowe koszty związane z takim sposobem naprawy obciążają Wykonawcę.
12. W przypadku, jeśli naprawy gwarancyjne wykonywane będą w imieniu Wykonawcy przez stronę trzecią to Wykonawca ponosi pełną odpowiedzialność z tytułu niewykonania lub nienależytego wykonania usług przez tę stronę.
13. Wykonawca poda adres serwisu gwarancyjnego (w tym: numery telefonów, faksu, adres poczty elektronicznej), pod który Zamawiający będzie wysyłał zgłoszenia o stwierdzonych usterkach i wadach. W przypadku zmiany adresu zgłoszeń serwisowych, Wykonawca jest zobowiązany niezwłocznie powiadomić o tym fakcie Zamawiającego. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego), e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń.
14. Gwarancja nie obejmuje zwykłego zużycia materiałów oraz uszkodzeń powstałych wskutek zdarzeń objętych „siłą wyższą” lub innych okoliczności niezależnych od Wykonawcy, np. nieprawidłowego lub niefachowego posługiwania się sprzętem przez personel

Zamawiającego, stosowania nieprawidłowych metod obsługi, nadmiernego przeciążenia, lub jakichkolwiek innych spowodowanych przez Zamawiającego.

## 10. Szkolenie

Sprzedawca przeprowadzi szkolenia w zakresie użytkowania, obsługi sprzętu i oprogramowania, podstawowego serwisu urządzeń wykonywanego przez użytkownika dla każdego z elementów rozwiązania minimum według poniższego zakresu.

10.1. Szkolenia ogólne z architektury rozwiązania oraz funkcjonalności każdego z elementów - minimum 8 godzin;
10.2. Szkolenia z obsługi i podstawowej administracji i konfiguracji biblioteki taśmowej oraz macierzy roboczej - minimum 2x8 godzin;
10.3. Szkolenia z obsługi i podstawowej administracji i konfiguracji systemu transkoderów - minimum 8 godzin;
10.4. Szkolenia z obsługi stacji masterningowej - minimum 8 godzin;
10.5. Szkolenia z obsługi stanowisk do ingestu oraz oprogramowania do kontroli jakości - minimum 8 godzin;
10.6. Szkolenia z obsługi oprogramowania zarządzającego mediami w CD:
a) dla osób administrujących - minimum 3x8 godzin;
b) dla użytkowników - mini- minimum 2x8 godzin;
10.7. Szkolenia z zakresu konfiguracji firewall oraz administracji infrastruktury sieciowej - - minimum 2x8 godzin.