

PROGRAM FUNKCJONALNO-UŻYTKOWY

Numer/nazwa zadania inwestycyjnego:

PROGRAM FUNKCJONALNO-UŻYTKOWY ORAZ KONCEPCJA KONIECZNYCH DO WDROŻENIA ROZWIĄZAŃ TECHNICZNYCH W ZAKRESIE DOSTOSOWANIA POMIESZCZEŃ OSTATNIEJ KONDYGNACJI BUDYNKU SIEDZIBY ZAMAWIAJĄCEGO DLA POTRZEB INSPEKTORATU WEWNĘTRZNEGO SŁUŻBY WIĘZIENNEJ ORAZ PRZEBUDOWANIE POMIESZCZEŃ RECEPCJI I WEJŚCIA GŁÓWNEGO ZNAJDUJĄCEGO SIE NA PARTERZE BUDYNKU W SPOSÓB POPRAWIAJĄCY ICH BEZPIECZEŃSTWO I FUNKCJONALNOŚĆ PRZY UL. RAKOWIECKIEJ 37A W WARSZAWIE

Adres obiektu:

**UL. RAKOWIECKA 37A, 02-521 WARSZAWA, DZIELNICA MOKOTÓW
DZIAŁKA EWIDENCYJNA NR 31/1 Z OBRĘBU 10110, JEDNOSTKA EWIDENCYJNA 146505_8**

Nazwa i adres Zamawiającego:

**CETRALNY ZARZĄD SŁUŻBY WIĘZIENNEJ
AL. RAKOWIECKA 37A, 02-521 WARSZAWA**

Wykonawca:

**SILTEC Sp. z o.o.
Ul. Parzniewska 12
05-800 Pruszków**



Opracował:

P. Radosław Lenart
upr. branża architektoniczna 17/WMOKK/2018
upr. branża konstrukcyjno-budowlana MAZ/0937/PWBkB/17

P. Arkadiusz Wild
upr. branża niskoprądowa PISA 6143/P/2021
P. Tadeusz Figat upr. branża sanitarna Wa-375/90

KODY Wspólnego Słownika Zamówień CPV:

71000000-8 : Usługi architektoniczne, budowlane, inżynieryjne i kontrolne.
71221000-3 : Usługi architektoniczne w zakresie obiektów budowlanych.
45111300-1 : Roboty rozbiórkowe.
45000000-7 : Roboty budowlane.
45311200-2 : Roboty w zakresie instalacji elektrycznych.
45262500-6 : Roboty murarskie i murowe.
45410000-4 : Tynkowanie.
45320000-6 : Roboty izolacyjne.
45400000-1 : Roboty wykończeniowe.
39150000-8 : Różne meble i wyposażenie.
45331000-6 : Instalowanie urządzeń grzewczych, wentylacyjnych i klimatyzacyjnych.
45232460-4 : Roboty sanitarne.

Warszawa, kwiecień 2023 r.

SPIS TREŚCI

DZIAŁ I - CZĘŚĆ OPISOWA	4
ROZDZIAŁ 1 – OPIS OGÓLNY PRZEDMIOTU ZAMÓWIENIA.....	4
ROZDZIAŁ 2 - CHARAKTERYSTYCZNE PARAMETRY OKREŚLAJĄCE WIELKOŚĆ OBIEKTU I ZAKRES PLANOWANYCH ROBÓT.	5
ROZDZIAŁ 3 - AKTUALNE UWARUNKOWANIA WYKONANIA PRZEDMIOTU ZAMÓWIENIA	10
ROZDZIAŁ 4 – PRZEWIDYWANY ZAKRES PRAC PROJEKTOWYCH I ROBÓT BUDOWLANYCH DO WYKONANIA.	10
ROZDZIAŁ 5 - WYMAGANIA INWESTORA W STOSUNKU DO PRZYGOTOWANIA TERENU BUDOWY.....	11
ROZDZIAŁ 6 - WYMAGANIA INWESTORA W STOSUNKU DO OPRACOWANIA PROJEKTÓW WYKONAWCZYCH.....	12
ROZDZIAŁ 7 – WARUNKI WYKONANIA I ODBIORU ROBÓT.	14
DZIAŁ II – KONCEPCJA REALIZACJI ZADANIA	20
PRZEDMIOT OPRACOWANIA.....	21
PRZEZNACZENIE I UKŁAD FUNKCJONALNY POZIOM 0 - MODERNIZACJA POMIESZCZEŃ.....	23
INSTALACJA WENTYLACJI MECHANICZNEJ.	24
SYSTEM BEZPIECZEŃSTWA I DEPONOWANIA BRONI.....	24
PODSTAWOWE ZAŁOŻENIA.	24
SYSTEMY BEZPIECZEŃSTWA.	25
SYSTEM INTERKOMOWY.	28
TELEWIZYJNY SYSTEM NADZORU.	28
BMS INTEGRACJA SYSTEMÓW.....	28
DEPOZYTOR.	29
INSTALACJA GNIAZD NAPIĘCIA 230V/AC.....	29
INSTALACJA OŚWIETLENIA.	29
ARANŻACJA WNĘTRZA POZIOM 0	30
PRZEZNACZENIE I UKŁAD FUNKCJONALNY POZIOM 4 – MODERNIZACJA POMIESZCZEŃ.....	33
ODDYMIANIE KLATEK SCHODOWYCH:.....	35
PRACE BUDOWLANE I ELEKTROINSTALACYJNE - ZWIĘKSZENIE TŁUMIENNOŚCI ELEKTROMAGNETYCZNEJ PRZEGRODY BUDOWLANEJ.....	35
OCHRONA ELEKTROMAGNETYCZNA.	37
OCHRONA BEZPIECZEŃSTWA EMISJI – UZIOM „RED”.....	37
INSTALACJA WENTYLACJI MECHANICZNEJ I KLIMATYZACJI	37
INSTALACJA GNIAZD NAPIĘCIA 230V/AC, GNIAZD INSTALACJI TELETECHNICZNYCH.....	38
INSTALACJA OŚWIETLENIA.	39
SYSTEM TELEINFORMATYCZNY RED	39
ARCHITEKTURA SYSTEMU	43
SERWERY DOSTĘPOWE - VDI	45

MACIERZ DYSKOWA – PRODUKCYJNA	47
PRZEŁĄCZNIKI SAN	49
PRZEŁĄCZNIK LAN – CORE	52
PRZEŁĄCZNIK LAN – ACCESS	52
ARCHITEKTURA ROZWIĄZANIA – SYSTEM KOPII ZAPASOWYCH	56
OPROGRAMOWANIE SYSTEMU KOPII ZAPASOWYCH	57
WYMOGI PODSTAWOWE	57
WYMOGI DLA LICENCJONOWANIA	72
CENTRALNY SERWER KOPII ZAPASOWYCH	73
SERWER KOPII ZAPASOWYCH – MEDIA AGENT	75
REPOZYTORIUM DYSKOWE KOPII ZAPASOWYCH	77
OPROGRAMOWANIE	80
SYSTEMY OPERACYJNE	80
WIRTUALIZACJA	80
OPROGRAMOWANIE DOSTĘPOWE – VDI	85
SYSTEM BEZPIECZEŃSTWA I DEPONOWANIA KLUCZY I MATERIAŁÓW NIEJAWNYCH	87
PODSTAWOWE ZAŁOŻENIA	87
SYSTEMY BEZPIECZEŃSTWA	88
SYSTEM INTERKOMOWY	91
TELEWIZYJNY SYSTEM NADZORU	91
BMS INTEGRACJA SYSTEMÓW	91
DEPOZYTORY	92
SEJFY DO PRZECHEWYWANIA MATERIAŁÓW NIEJAWNYCH	92
SYSTEM SYGNALIZACJI POŻARU	93
OCHRONA PRZECIWPORAŻENIOWA	93
OZNACZENIA	93
SERWISOWALNOŚĆ URZĄDZEŃ, BADANIA I POMIARY	93
PRZYGOTOWANIE PRZEZ WYKONAWCĘ WZORU DOKUMENTÓW NIEZBĘDNYCH DO UZYSKANIA AKREDYTACJI SYSTEMÓW TELEINFORMATYCZNYCH	94

DZIAŁ I - CZĘŚĆ OPISOWA

ROZDZIAŁ 1 – Opis ogólny przedmiotu zamówienia.

Przedmiot, cel i zakres opracowania.

Podstawą opracowania PFU oraz dokumentacji technicznej koncepcyjnej jest podpisana umowa nr 27/2023 z dnia 12.04.2023 r. na wykonanie zadania występującego pn.: „Dostosowanie pomieszczeń ostatniej kondygnacji budynku siedziby Zamawiającego dla potrzeb Inspektoratu Wewnętrznego Służby Więziennej oraz przebudowanie pomieszczeń recepcji i wejścia głównego znajdującego się na parterze budynku w sposób poprawiający ich bezpieczeństwo i funkcjonalność przy ul. Rakowieckiej 37a w Warszawie” wraz z wprowadzonymi rozwiązaniami wynikającymi z uzgodnień z Zamawiającym oraz obowiązującymi przepisami, aktami prawnymi i normami.

Zakres inwestycji przewiduje zmiany architektoniczne i instalacyjne na poziomie parteru wynikające ze śluzowania korytarza dostępowego celem uzyskania zwiększonego bezpieczeństwa pracy na terenie jednostki organizacyjnej oraz zmian architektonicznych i instalacyjnych na poziomie czwartego piętra celem utworzenia stref ochronnych zgodnie z Rozporządzeniem Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. poz. 683), Rozporządzeniem Rady Ministrów z dnia 22 lutego 2017 r. zmieniającym rozporządzenie w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. poz. 522) oraz Zarządzenia Ministra Sprawiedliwości w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych z dnia 23 stycznia 2014 r. (Dz.Urz.MS z 2014 r. poz.32). Opracowanie zostało przygotowane na podstawie prowadzonych konsultacji technicznych z Użytkownikiem związanych z wykonaniem modernizacji, ochroną elektromagnetyczną ww. pomieszczeń przeznaczonych do prowadzenia działań operacyjnych. Rozpowszechnianie informacji o koniecznych do wdrożenia zabezpieczeniach na terenie jednostki organizacyjnej struktur CZSW może doprowadzić do utraty poufności i integralności chronionych zasobów związanych z przetwarzanymi werbalizowanymi informacjami niejawnymi. Materiał może być wykorzystany do dalszych celów realizacji tylko tego zadania, wybudowania zespołu pomieszczeń stanowiących Strefy Ochronne.

Celem przedsięwzięcia jest:

- Obniżenie prawdopodobieństwa wystąpienia zdarzeń, które mogą powstać w wyniku działań terrorystycznych lub wandalizmu, poprzez modernizację architektoniczną i instalacyjną na poziomie parteru (pomieszczeń recepcji i wejścia głównego) oraz wdrożenie zabezpieczeń fizycznych i technicznych.
- Eliminacja zagrożeń mogących powstać w wyniku utraty dostępności, integralności i poufności informacji niejawnych na poziomie czwartego piętra poprzez modernizację architektoniczną i instalacyjną umożliwiającą utworzenie stref ochronnych, wdrożenie zabezpieczeń fizycznych i technicznych oraz systemu teleinformatycznego do przetwarzania informacji niejawnych do klauzuli POUFNE włącznie.

- Eliminacja zagrożeń mogących powstać w wyniku utraty dostępności, integralności i poufności informacji niejawnych na poziomie czwartego piętra poprzez modernizację architektoniczną i instalacyjną umożliwiającą utworzenie Kancelarii Tajnej, wdrożenie zabezpieczeń fizycznych i technicznych oraz autonomicznego systemu teleinformatycznego do przetwarzania informacji niejawnych do klauzuli ŚCIŚLE TAJNE włącznie.
- Eliminacja zagrożeń powstałych w wyniku ujawniającej emisji elektromagnetycznej przewodzonej oraz promieniowanej z obszaru serwerowni na poziomie czwartego piętra.

Po realizacji ww. zadania dla wdrożonego systemu teleinformatycznego i ustanowionych stref ochronnych należy uzyskać pozytywną opinię ABW w zakresie skuteczności zastosowanych rozwiązań i zabezpieczeń i wdrożonych systemów.

Wykonawca wykona kompletną dokumentację wraz ze wszystkimi wymaganymi prawem uzgodnieniami oraz uzyskaniem wszelkich niezbędnych pozwoleń na realizację inwestycji.

Wykonawca wykona przedstawione roboty budowlane wraz z niezbędnymi robotami niemożliwymi do uwzględnienia na danym etapie opracowania, które mają pozwolić na osiągnięcie celu.

Wykonawca dokumentacji projektowej zobowiązany będzie do pełnienia nadzoru autorskiego w czasie realizacji zadania oraz w okresie rękojmi za wady dla robót budowlanych.

ROZDZIAŁ 2 - Charakterystyczne parametry określające wielkość obiektu i zakres planowanych robót.

STAN ISTNIEJĄCY

Budynek administracyjny Centralnego Zarządu Służby Więziennej 5-kondygnacyjny, podpiwniczony, położony jest w Warszawie przy ul. Rakowieckiej 37a.

Od strony północnej usytuowany jest w ciągu zabudowań ulicy Rakowieckiej. Od wschodu przylega do budynku administracyjnego i drukarni Aresztu Śledczego w Warszawie-Mokotowie.

Od południa znajduje się wewnętrzny parking oraz budynki hotelu pracowniczego i stołówki. Od zachodu obiekt graniczy z budynkiem mieszkalnym usytuowanym na rogu Alei Niepodległości i ulicy Rakowieckiej oraz posesją należącą do tego budynku.

Status prawny nieruchomości:

- a) działka ewidencyjna nr 31/1 z obrębu 1-01-10, jednostka ewidencyjna 146505-8, przy ul. Rakowieckiej 37a w dzielnicy Mokotów m. st. Warszawy;
- b) właściciel: Skarb Państwa.

Układ konstrukcji obiektu w części objętej opracowaniem:

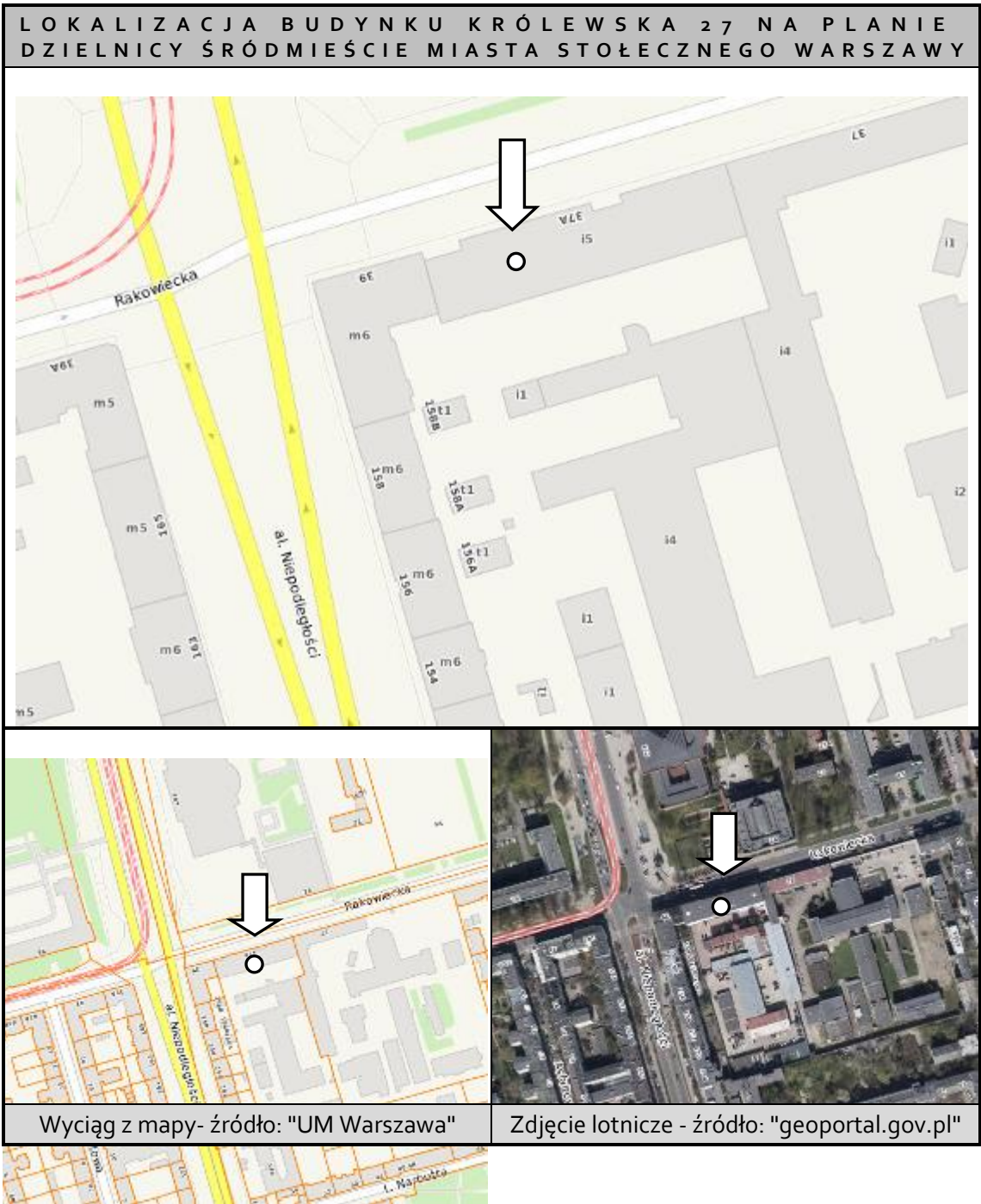
BUDYNEK UŻYTECZNOŚCI PUBLICZNEJ WARSZAWA UL. KRÓLEWSKA 27		
L.p.	ELEMENT	RODZAJ MATERIAŁU
1	Układ konstrukcyjny	podłużny – trzytraktowy ze ścianami konstrukcyjnymi murowanymi oraz betonowymi
2	Ściany zewnętrzne	murowane z cegły oraz wypełnienia z cegły kratówki i bloczków gazobetonowych, średnia grubość elementów 45-97cm
3	Ściany konstrukcyjne wewnętrzne	murowane z cegły oraz wypełnienia z cegły kratówki i bloczków gazobetonowych, średnia grubość 45-83cm
4	Szyb windy	lekka konstrukcja stalowa ocynkowana oszklona szkłem bezpiecznym, w piwnicy ścianki szybu z cegły kratówki wypełniającej płaszczyzny między słupami stalowymi szybu
5	Ściany działowe	murowane z cegły / wykonane z płyt G-K
6	Stropy	nad piwnicami odcinkowe, częściowo Kleina, nad parterem stropy Kleina, nad I, II i III piętrem stropy gęstożebrowe DZ-3, nad IV piętrem stropodach lekki z sufitem podwieszonym
7	Schody	biegi: żelbetowe spoczniki: żelbetowe

Powierzchnia obliczona dla pomieszczeń podlegających opracowaniu w związku z przebudową.

Obliczenia powierzchni:

- Długość budynku 69,90 m.
- Szerokość 15,90 m.
- Wysokość 18,30 m.
- Powierzchnia zabudowy 1111,41 m².
- Powierzchnia użytkowa 5243,63 m².
- Kubatura 22058 m³.

Lokalizację obiektu przedstawiono na ilustracji poniżej:



Program użytkowy pomieszczeń podlegający opracowaniu

Obecna powierzchnia pomieszczeń dla których prowadzona będzie ingerencja w zakresie robót budowlanych:

PARTER		
NR POM	NAZWA POM.	POW.[M2]
00/0.1	WIATROŁAP	3,26
00/0.2	HOL WEJŚCIOWY	29,19
00/0.3	POCZEKALNIA	9,63

00/0.4	POM. DODATKOWE	6,90
00/0.5	KLATKA SCHODOWA	26,74
00/0.6	RECEPCJA	4,10
00/0.7	WIATROŁAP	8,19
	SUMA	88,01

Obecna powierzchnia pomieszczeń dla których prowadzona będzie ingerencja w zakresie robót budowlanych:

IV PIĘTRO		
NR POM	NAZWA POM.	POW.[M2]
4/30	POKÓJ BIUROWY	18,59
4/32	POKÓJ BIUROWY	14,92
4/33	POKÓJ BIUROWY	15,04
4/33.1	POM. TECHNICZNE	3,25
4/34	POKÓJ BIUROWY	14,61
4/42	KORYTARZ	61,80
	SUMA	128,21

STAN PLANOWANY

Zgodnie z rozporządzeniem Rady Ministrów z 29 maja 2012r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych na etapie projektowym należy w uzgodnieniu z Użytkownikiem dokonać procesu analizy ryzyka - określenia poziomu zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą zgodnie z art. 49 ust. 1 ustawy z 5 sierpnia 2010r. o ochronie informacji niejawnych.

Inwestycja przewiduje zmiany architektoniczne i instalacyjne dla zapewnienia prawidłowego, bezpiecznego funkcjonowania zespołu pomieszczeń na poziomie parteru i czwartego piętra, w zakresie przeciwdziałania wandalizmowi, atakom terrorystycznym i inwigilacji elektronicznej. Na poziomie parteru wynikające z konieczności służowania korytarza dostępowego celem uzyskania zwiększonego bezpieczeństwa pracy na terenie jednostki organizacyjnej, przewiduje się doposażenie strefy wejścia w pomieszczenia ochrony tj. pomieszczenie osób dozoru oraz dyspozytorni, a także wprowadzenie kontroli dostępu w miejscach kluczowych pod względem bezpieczeństwa. Na poziomie czwartego piętra celem utworzenia stref ochronnych zgodnie z Rozporządzeniem Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. poz. 683), Rozporządzeniem Rady Ministrów z dnia 22 lutego 2017 r. zmieniającym rozporządzenie w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. poz. 522) oraz Zarządzenia Ministra Sprawiedliwości w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych z dnia 23 stycznia 2014 r. (Dz.Urz.MS z 2014 r. poz.32), przewiduje się doposażenie pomieszczeń czwartego piętra w zespół pomieszczeń ochronnych tj. kancelarii tajnej, czytelní, pomieszczenia BSK oraz pomieszczenia sejfów a także utworzenie serwerowni.

Planowana powierzchnia pomieszczeń, dla których prowadzona będzie ingerencja w zakresie robót budowlanych:

PARTER

NR POM	NAZWA POM.	POW.[M2]
00/0.1	WIATROŁAP	12,58
00/0.2	HOL WEJŚCIOWY	24,87
00/0.3	POM. OSÓB DOZORUJĄCYCH	11,43
00/0.4	POM. Z DEPOZYTOREM	7,71
00/0.5	KLATKA SCHODOWA	29,25
00/0.6	WIATROŁAP	8,19
	SUMA	94,03

Planowana powierzchnia pomieszczeń, dla których prowadzona będzie ingerencja w zakresie robót budowlanych:

IV PIĘTRO

NR POM	NAZWA POM.	POW.[M2]
4/30	POKÓJ BIUROWY	14,49
4/30.1	POM. DODATKOWE	3,64
4/32	POKÓJ BIUROWY	7,74
4/32.1	POM. BSK	5,52
4/33	POM. SEJFÓW	7,42
4/33.1	KANCELARIA	9,76
4/33.2	CZYTELNIA	7,28
4/34	SERWEROWNIA	10,44
4/34.1	POM. DODATKOWE	3,84
4/42	KORYTARZ	55,21
	SUMA	125,34

SPIS PLANOWANYCH GRUP ROBÓT

1. Prace projektowe, przygotowawcze i uzgodnieniowe.
2. Wykonanie robót rozbiórkowych i demontażowych.
3. Modernizacja zespołu pomieszczeń w zakresie robót budowlanych
4. Modernizacja instalacji elektrycznych.
5. Modernizacja instalacji sanitarnej.

Szczegółowa koncepcja zakresu prac i rozwiązań została przedstawiona w dziale II n/n opracowania.

Konstrukcja projektowana zakłada wykonanie otworów w ścianach konstrukcyjnych oraz замуrowania otworów konstrukcyjnych. W miejscach projektowanych otworów zakłada się wykonanie nowych nadproży, dla ścian działowych z elementów betonowych prefabrykowanych typu L-19/N, dla ścian nośnych z belek stalowych. Demontażom i ponownym montażom podlega istniejąca podwieszona konstrukcja sufitu podwieszanego wraz z instalacją wentylacyjną i oświetleniową. Planuje się wykonanie nowych ścian działowych lekkich oraz przed ścianek do ścian już istniejących, z bloczków z betonu komórkowego gr. od 6 do 25 cm. Wykończenie nowych ścian (nastąpi z wykorzystaniem tynku gipsowego dwukrotnie pomalowanego), wraz z przygotowaniem podłoża

i gruntowaniem. Istniejące drzwi drewniane w strefie ochronnej II wymienić na nowe drzwi stalowe RC2 z okleiną drewnopodobną w klasie ppoż. Istniejące rozsuwane drzwi wejściowe do budynku na parterze (zostaną wymienione) na nowe. Na poziomie parteru nastąpi wykonanie otworów w ścianach nośnych wewnętrznych wraz z montażem nowych drzwi i okien oraz wykonaniem nadproży z belek stalowych. Zostanie wymurowana przegroda budowlana na granicy strefy ochronnej III wraz z montażem drzwi dostępowych klasy RC4. Powyżej zainstalowanych drzwi zamontować kratę RC4 celem możliwości przewietrzania korytarza. Nastąpi doposażenie istniejących świetlików dachowych w korytarzu oraz okien w pomieszczeniach strefy ochronnej II w kratę stalową RC4 celem zabezpieczenia dostępu od strony dachu. Wykonane zostanie wzmocnienie konstrukcją stalową podłogi pomieszczeń dedykowanych dla potrzeb serwerowni oraz pomieszczenia sejfów. Wykonana zostanie przebudowa systemu oddymiania korytarzy.

GRUPY, KLASY, KATEGORIE ROBÓT

Określone w rozporządzeniu nr 2195/2002 z dnia 5 listopada 2002 r. w sprawie Wspólnego Słownika Zamówień (Dz. Urz. WE L 340 z 16.12.2002, z późn. zm.):

71000000-8 : Usługi architektoniczne, budowlane, inżynierskie i kontrolne

71221000-3 : Usługi architektoniczne w zakresie obiektów budowlanych

45111300-1 : Roboty rozbiórkowe

45000000-7 : Roboty budowlane

45311200-2 : Roboty w zakresie instalacji elektrycznych

45262500-6 : Roboty murarskie i murowe

45410000-4 : Tynkowanie

45320000-6 : Roboty izolacyjne

45400000-1 : Roboty wykończeniowe

39150000-8 : Różne meble i wyposażenie

45331000-6 : Instalowanie urządzeń grzewczych, wentylacyjnych i klimatyzacyjnych

45232460-4 : Roboty sanitarne

45331100-7 : Instalowanie centralnego ogrzewania

ROZDZIAŁ 3 - Aktualne uwarunkowania wykonania przedmiotu zamówienia

Zamawiającym jest: CZSW 02-521 Warszawa ul. Rakowiecka 37a.

ROZDZIAŁ 4 – Przewidywany zakres prac projektowych i robót budowlanych do wykonania.

1. Prace projektowe, przygotowawcze i uzgodnieniowe w tym:

- Opracowanie projektu budowlanego na przebudowę pomieszczeń wraz ze zmianą sposobu użytkowania w zakresie elementów konstrukcyjnych oraz wydzielenia ppoż..
 - Opracowanie projektu wykonawczego modernizacji zespołu pomieszczeń wraz z budową Stref Ochronnych z uwzględnieniem podziału na opracowania branżowe o stopniu szczegółowości pozwalającym na prawidłową realizację robót budowlanych.
 - Projekty budowlane – 3 egzemplarze w wersji papierowej oraz 3 egzemplarze w wersji elektronicznej.
 - Projekty wykonawcze wraz z inwentaryzacją stanu istniejącego dla wszystkich branż - 3 egzemplarze w wersji papierowej oraz 3 egzemplarze w wersji elektronicznej.
 - Specyfikacje techniczne wykonania i odbioru robót budowlanych dla zakresu dokumentacji projektowej w każdej branży - 2 egzemplarze w wersji papierowej oraz 2 egzemplarze w wersji elektronicznej.
 - Wersja elektroniczna powinna być przekazywana na nośnikach CD w plikach przygotowanych do druku typu *.pdf oraz komplet materiału w plikach edytowalnych – w formatach *.doc oraz *.dwg.
 - Uzyskanie ostatecznej decyzji pozwolenia na budowę oraz niezbędnych dokumentów formalno-prawnych umożliwiających osiągnięcie celu zadania.
2. Wykonanie robót budowlanych w oparciu o ww. dokumentację, prac rozbiórkowych i demontażowych, w tym:
- Opróżnienie pomieszczeń.
 - Demontaż i wykonanie przesunięcia pionów centralnego ogrzewania wraz z grzejnikami.
 - Demontaż stolarki drzwiowej.
 - Rozbiórka wytypowanych ścian działowych.
 - Zaślepienie poprzez zabetonowanie wybranych kanałów wentylacji grawitacyjnej.
 - Wykonanie otworów w ścianach i stropach niezbędnych do realizacji zadania.
 - Rozbiórka warstw posadzkowych w wytypowanych pomieszczeniach.
 - Rozbiórka wytypowanych fragmentów ścian oraz wycięcia otworów w ścianach.
 - Demontaż istniejącego okablowania instalacji elektrycznych i teletechnicznych – w zakresie wymaganej w inwestycji.

3. Modernizacja zespołu pomieszczeń zgodnie z przedstawioną w dziale II koncepcyjną realizacją zadania.

ROZDZIAŁ 5 - Wymagania inwestora w stosunku do przygotowania terenu budowy.

Przygotowanie terenu pod budowę oraz organizacja robót:

1. Wykonawca jest zobowiązany do zabezpieczenia terenu budowy w okresie trwania realizacji Kontraktu, aż do zakończenia i odbioru ostatecznego robót.

2. Prace prowadzone będą w obiekcie czynnym. Z tych powodów organizacja robót budowlanych, transport materiałów oraz praca sprzętu budowlanego nie mogą stanowić nadmiernego utrudnienia ani zagrożenia dla eksploatacji i bezpiecznego użytkowania obiektu.
3. Teren prac winien być zabezpieczony przed dostępem dla osób postronnych. Sposób zabezpieczenia budowy należy uzgodnić z przedstawicielami Inwestora.
4. Miejsce składowania materiałów w obrębie budowy wymaga uzgodnienia z Inspektorem nadzoru. Wykluczone jest składowanie i magazynowanie materiałów łatwopalnych bez właściwego zabezpieczenia.
5. Do dokonywania odbiorów robót zanikowych i ulegających zakryciu Zamawiający upoważni Inspektora nadzoru inwestorskiego.
6. Do dokonania końcowego odbioru wykonanych robót Zamawiający powoła Komisję odbiorową, w której uczestniczyć będą osoby wyznaczone przez Wykonawcę i Zamawiającego.

ROZDZIAŁ 6 - Wymagania inwestora w stosunku do opracowania projektów wykonawczych.

Dokumentacja wykonawcza obejmie zakres prac, budowlanych, elektroinstalacyjnych i rozwiązań technicznych elektronicznych systemów zabezpieczeń tym samym obniżając ryzyko prawdopodobieństwa wystąpienia zdarzenia i jego konsekwencji w odniesieniu do atrybutów bezpieczeństwa przedmiotowego budynku.

1. Zakres i forma projektów wykonawczych odpowiadać powinny zamówieniu w taki sposób, w jaki określił je Zamawiający. Odpowiadać powinny wymaganiom dotyczącym postępowania poprzedzającego rozpoczęcie robót budowlanych wynikające z ustawy z dnia 7 lipca 1994 r. Prawo budowlane (Dz. U. z 2022 r., poz. 2351 z późn. zm.) oraz wymogom określonym w Rozporządzeniu Ministra Rozwoju i Technologii z dnia 20 grudnia 2021 r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego (tj. Dz. U. 2021 r., poz. 2454), wydanym na podstawie delegacji art. 31 ust. 4 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj. Dz.U. z 2022 r. poz. 1710.).
2. Projekt wykonawczy powinien być opracowaniem, w którym wydzielone będą tomy zgodnie z przyjętą systematyką podziału robót budowlanych.
3. Nazwy i kody: grup robót, klas robót, kategorii robót powinny być podane zgodnie z nazewnictwem i numeracją określoną w rozporządzeniu nr 2195/2002 z dnia 5 listopada 2002 roku w sprawie Wspólnego Słownika Zamówień (Dz. Urz. WE L 340 z 16.12.2002 r., z późn. zm.)
4. Projekt budowlany oraz wykonawczy powinien być przekazany Zamawiającemu w formie wydruków i w postaci elektronicznej w ogólnie dostępnych formatach np. *pdf oraz w wersjach edytowalnych. W każdym tomie wszystkie strony powinny być opatrzone numeracją, a wydruki trwale spięte.
5. Strona tytułowa projektu budowlanego oraz wykonawczego powinna zawierać:
 - nazwę zamierzenia budowlanego;

- adres i kategorię obiektu budowlanego;
 - nazwę jednostki ewidencyjnej, nazwę i numer obrębu ewidencyjnego oraz numery działek ewidencyjnych, na których obiekt jest usytuowany;
 - imię i nazwisko lub nazwę inwestora oraz jego adres;
 - spis zawartości projektu budowlanego, w którym wymienia się jego elementy.
6. Projekty zawierać będą rysunki w skali uwzględniającej specyfikę zamawianych robót i zastosowanych skali rysunków w projekcie budowlanym wraz z wyjaśnieniami opisowymi, dotyczącymi:
- 6.1. Rozwiązań budowlano-konstrukcyjnych i materiałowych.
 - 6.2. Detali architektonicznych oraz urządzeń budowlanych.
 - 6.3. Instalacji i wyposażenia technicznego.
7. Oczekiwany zakres prac projektowych obejmuje w szczególności dokumentację wykonawczą wielobranżową modernizacji pomieszczenia:
- 7.1. Projekt wykonawczy architektoniczny obejmujący w szczególności: rozwiązania akustyczne i elektromagnetyczne obiektu, wzmocnienia przegród budowlanych i stropów, detale architektoniczne; zestawienie stolarki drzwiowej; projekt posadzki, projekt sufitu, rozmieszczenie oświetlenia, kolorystyka ścian.
 - 7.2. Projekt wykonawczy instalacji elektrycznych zasilającej.
 - 7.3. Projekt wykonawczy instalacji teletechnicznych światłowodowych.
 - 7.4. Projekt wykonawczy instalacji telewizji dozorowej CCTV.
 - 7.5. Projekt wykonawczy instalacji systemu sygnalizacji włamania i napadu SSWiN oraz kontroli dostępu SKD.
 - 7.6. Projekt wykonawczy instalacji systemu depozytory kluczy.
 - 7.7. Dostosowanie przeciwpożarowe w zakresie wydzielonej strefy.
 - 7.8. Analiza systemu oddymiania po wykonanej przebudowie parteru, wydzielenie strefy klatki schodowej drzwiami ppoż. dymoszczelnymi na wszystkich kondygnacjach klatki schodowej, weryfikacja powierzchni klapy oddymiającej i napowietrzania klatki lub wariantowo wykonanie systemu napowietrzenia klatki schodowej z posadowieniem centrali wentylacyjnej na dachu z wykonaniem podkonstrukcji stalowej na dachu z oparciem na ścianach klatki schodowej (wariant pożądanym w przypadku braku możliwości oddymiania metodą grawitacyjną), w przypadku braku możliwości dostosowania klatek do warunków ppoż. wymaga się wykonania nowej ekspertyzy ppoż. budynku z uzyskaniem niezbędnych odstępstw (dotyczy także strefy wejściowej parteru), jeśli na etapie projektu wyniknie brak możliwości spełnienia warunków ppoż. obiektu w zakresie przedmiotowej przebudowy należy wykonać ekspertyzę ppoż..

- 7.9. Uzyskanie niezbędnych zgód i pozwoleń na możliwość pracy pracowników służby dyżurnej na parterze w wyznaczonym pomieszczeniu przy wejściu głównym do budynku (brak obecnie wymaganego nasłonecznienia dziennego pomieszczenia), dotyczy między innymi decyzji sanepid.
- 7.10. Przebudowa systemu SSP i oddymiania klatek schodowych w budynku.
- 7.11. Zgodnie z ekspertyzą ppoż. istniejącą na budynku oraz dokumentami Inwestora na ostatnich kondygnacjach w celu oddymiania korytarzy wykonane są klapy oddymiające bez napowietrzania. W wyniku wydzielenia strefy chronionej wymagane jest wykonanie systemu oddymiania korytarzy np. poprzez zastosowanie krat zamiast ściany lub wykonanie dodatkowego okna oddymiającego korytarz w części wydzielonej. Decyzja w tym zakresie należy do Wykonawcy na etapie sporządzania projektu budowlanego i dostosowania przebudowanej części do przepisów ppoż. wraz z drogami ewakuacyjnymi.
8. Opracowania rysunkowe i tekstowe powinny być wzajemnie powiązane tak, aby każdy opisany rodzaj roboty budowlanej był łatwy do zlokalizowania na rysunkach.
9. Część rysunkowa powinna zawierać:
- 9.1. Rzuty, przekroje – w ramach projektu architektonicznego i branżowych.
 - 9.2. Rysunki detali – w ramach projektów architektonicznego i branżowych, w zakresie wynikającym z potrzeb.
 - 9.3. Schematy instalacyjne – opracowywane w ramach projektów branżowych, w zakresie wynikającym z potrzeb.
 - 9.4. Wykonanie symulacji oddymiania klatek schodowych (w razie potrzeby projektowej).
 - 9.5. Wizualizacja strefy wejściowej parteru budynku po przebudowie.
10. Rysunki powinny być sporządzone w skali:
- 1:100 i 1:50 w zakresie architektury, a także instalacji, technologii specjalistycznej i aranżacji wnętrz;
 - 1:20, 1:10, 1:5 i 1:2 w zakresie detali;
 - 1:1 w szczególnie uzasadnionych wypadkach.
11. Wykonawca ma obowiązek uzgodnienia projektów wykonawczych z Inwestorem w zakresie zastosowanych standardów wykończenia pomieszczeń oraz proponowanych aranżacji wnętrz. Uzgodnienia z Inwestorem wymagają zachowania formy pisemnej pod rygorem nieważności.

ROZDZIAŁ 7 – Warunki wykonania i odbioru robót.

Ogólne wymagania dotyczące robót

Wykonawca jest odpowiedzialny za jakość wykonania robót oraz ich zgodność z dokumentacją projektową, S.T.

(Specyfikacją Techniczną), poleceniami Inspektora Nadzoru oraz sztuką budowlaną. Podstawą wykonania robót jest dokumentacja projektowa, specyfikacja techniczna wykonania i odbioru robót, a wymagania zawarte choćby w jednej z nich są obowiązujące dla Wykonawcy. Wszystkie wykonane roboty i dostarczone materiały muszą być zgodne z dokumentacją projektową i specyfikacjami technicznymi, a także z innymi obowiązującymi przepisami. Przy wykonaniu robót należy uwzględnić instrukcje producenta materiałów oraz przepisy związane i obowiązujące, w tym również te, które uległy zmianie lub aktualizacji.

Ogólne zasady wykonania robót

Wykonawca jest odpowiedzialny za dokładne wytyczenie w planie i wyznaczenie wysokości wszystkich elementów robót z wymiarami i rzędnymi określonymi w dokumentacji projektowej lub przekazanymi na piśmie przez Inwestora. Następstwa jakichkolwiek błędów spowodowanych przez wykonawcę w wytyczeniu i wyznaczeniu robót zostaną poprawione przez Wykonawcę na jego koszt. Sprawdzenie wytyczenia robót lub wyznaczenia wysokości przez Inwestora nie zwalnia Wykonawcy od odpowiedzialności za ich dokładność. Decyzje Inwestora dotyczące akceptacji lub odrzucenia materiałów i elementów robót będą oparte na wymaganiach sformułowanych w kontrakcie, dokumentacji projektowej i S.T., a także w normach i wytycznych. Przy podejmowaniu decyzji Inwestor uwzględni wyniki badań materiałów i robót, rozrzuty normalnie występujące przy produkcji i przy badaniach materiałów, wyniki badań naukowych oraz inne czynniki wpływające na rozważną kwestię. Polecenia Inwestora będą wykonywane nie później niż w czasie przez niego wyznaczonym, po ich otrzymaniu przez Wykonawcę pod groźbą zatrzymania robót. Skutki finansowe z tego tytułu ponosi Wykonawca.

Wymagania w zakresie materiałów

Źródła uzyskania materiałów

Materiały zamienne w stosunku do zatwierdzonego przez Zamawiającego, wykonawca robót przedstawi do zatwierdzenia przez Inwestora. Propozycja zamiany powinna zawierać porównanie, które wskazuje jednoznacznie, że parametry proponowanego materiału są tożsame lub lepsze w stosunku do zatwierdzonych na etapie projektu. Zatwierdzenie pewnych materiałów z danego źródła nie oznacza automatycznie, że wszystkie materiały z danego źródła uzyskają zatwierdzenie. Wykonawca zobowiązany jest do udokumentowania, że materiały uzyskane z dopuszczonego źródła w sposób ciągły spełniają wymagania S.T. w czasie postępu robót. Wykonawca ponosi odpowiedzialność za spełnienie wymagań jakościowych i ilościowych materiałów z jakichkolwiek źródeł. Wykonawca poniesie wszystkie koszty, a w tym: opłaty, wynagrodzenia i jakiekolwiek inne koszty związane z dostarczeniem materiałów i urządzeń do robót.

Materiały nieodpowiadające wymaganiom

Materiały nieodpowiadające wymaganiom zostaną przez Wykonawcę wywiezione z terenu budowy. Każdy rodzaj robót, w którym znajdują się niezbadane i niezaakceptowane materiały, Wykonawca wykonuje na własne ryzyko, licząc się z jego nieprzyjęciem i niezapłaceniem.

Przechowywanie i składowanie materiałów

Wykonawca zapewni takie warunki tymczasowego składowania materiałów, aby do czasu, gdy będą one potrzebne do robót, były zabezpieczone przed zanieczyszczeniem, zachowały swoją jakość i właściwość do robót oraz były dostępne do kontroli Inspektora Nadzoru. Miejsca czasowego składowania będą zlokalizowane w obrębie terenu budowy w miejscach uzgodnionych z Inwestorem lub poza terenem budowy w miejscach zorganizowanych przez Wykonawcę.

Zasady kontroli jakości robót

Celem kontroli robót będzie takie sterowanie ich przygotowaniem i wykonaniem, aby osiągnąć założoną jakość robót. Wykonawca jest odpowiedzialny za pełną kontrolę robót i jakości materiałów.

Wykonawca zapewni odpowiedni system kontroli, włączając personel, laboratorium, sprzęt, zaopatrzenie i wszystkie urządzenia niezbędne do pobierania próbek i badań materiałów oraz robót.

Wykonawca będzie przeprowadzać pomiary i badania materiałów oraz robót z częstotliwością zapewniającą stwierdzenie, że roboty wykonano zgodnie z wymaganiami zawartymi w dokumentacji projektowej i S.T. Minimalne wymagania co do zakresu badań i ich częstotliwości są określone w normach, wytycznych i warunkach technicznych wykonania i odbioru robót. W przypadku, gdy nie zostały one tam określone, Inspektor Nadzoru ustali, jaki zakres jest konieczny, aby zapewnić wykonanie robót zgodnie z kontraktem. Wykonawca dostarczy Inspektorowi Nadzoru świadectwa, że wszystkie stosowane urządzenia i sprzęt badawczy posiadają ważną legitymację, zostały prawidłowo wykalibrowane i odpowiadają wymaganiom norm określających procedury badań. Wszystkie koszty związane z ograniczeniem i prowadzeniem badań materiałów ponosi Wykonawca.

Badania i pomiary

Wszystkie badania i pomiary będą przeprowadzone zgodnie z wymaganiami norm. W przypadku, gdy normy nie obejmują jakiegokolwiek badania wymaganego w ST, stosować można wytyczne krajowe albo inne procedury, zaakceptowane przez Inspektora Nadzoru. Przed przystąpieniem do pomiarów lub badań, Wykonawca powiadomi Inspektora Nadzoru o rodzaju, miejscu i terminie pomiaru lub badania. Po wykonaniu pomiaru lub badania, Wykonawca przedstawi na piśmie ich wyniki do akceptacji Inspektora Nadzoru.

Atesty jakości materiałów i urządzeń

Przed wykonaniem badań jakości materiałów przez Wykonawcę, Inspektor Nadzoru może dopuścić do użycia materiały posiadające atest producenta stwierdzający ich pełną zgodność z warunkami podanymi w ST. W przypadku materiałów, dla których atesty są wymagane przez ST, każda partia dostarczona do robót będzie posiadać atest określający w sposób jednoznaczny jej cechy. Produkty przemysłowe będą posiadać atesty wydane przez producenta, poparte w razie potrzeby wynikami wykonanych przez niego badań. Kopie wyników tych badań, będą dostarczone przez Wykonawcę Inspektorowi Nadzoru. Materiały posiadające atest, a urządzenia - ważne legitymacje mogą być badane w dowolnym czasie. Jeżeli zostanie stwierdzona niezgodność ich właściwości z ST, to takie materiały lub urządzenia zostaną odrzucone.

Wymagania w zakresie sprzętu, maszyn i urządzeń budowlanych

Wykonawca jest zobowiązany do używania jedynie takiego sprzętu, który nie spowoduje niekorzystnego wpływu na jakość wykonywanych robót. Sprzęt używany do robót powinien być zgodny z ofertą Wykonawcy i powinien odpowiadać pod względem typów i ilości wskazaniom zawartym w ST, w przypadku braku ustaleń w takich dokumentach sprzęt powinien być uzgodniony i zaakceptowany przez Inwestora. Liczba i wydajność sprzętu będzie gwarantować przeprowadzenie robót, zgodnie z zasadami ustalonymi w dokumentacji projektowej i ST i wskazaniach Inwestora w terminie przewidzianym Zleceniem. Sprzęt będący własnością Wykonawcy bądź wynajęty do wykonania robót ma być utrzymywany w dobrym stanie i gotowości do pracy. Będzie on zgodny z normami ochrony środowiska i przepisami dotyczącymi jego użytkowania. Jeżeli dokumentacja projektowa lub ST przewidują możliwość wariantowego użycia sprzętu przy wykonywanych robotach, Wykonawca powiadomi Inwestora o swoim zamiarze wyboru i uzyska jego akceptację przed użyciem sprzętu. Wybrany sprzęt, po akceptacji Inspektora Nadzoru nie może być później zmieniony bez jego zgody. Jakkolwiek sprzęt, maszyny, urządzenia i narzędzia niegwarantujące zachowania warunków Zlecenia, zostaną przez Inwestora zdyskwalifikowane i niedopuszczone do robót.

Wymagania w zakresie transportu

Wykonawca stosować się będzie do ustawowych ograniczeń nacisku na oś przy transporcie materiałów i sprzętu na i z terenu robót. Uzyska on wszelkie niezbędne zezwolenia od władz, co do przewozu nietypowych ładunków i w sposób ciągły będzie o każdym takim przewozie powiadamiał Inspektora Nadzoru. Wykonawca jest zobowiązany do stosowania jedynie takich środków transportu, które nie wpłyną niekorzystnie na jakość wykonywanych robót i przewożonych materiałów. Liczba środków transportu będzie zapewniać prowadzenie robót zgodnie z zasadami określonymi w dokumentacji projektowej, ST i wskazaniach Inspektora Nadzoru, w terminie przewidzianym kontraktem. Środki transportu nieodpowiadające warunkom dopuszczalnym naciskom na osie mogą być użyte przez Wykonawcę pod warunkiem przywrócenia do stanu pierwotnego użytkowanych odcinków dróg publicznych na koszt Wykonawcy. Wykonawca będzie usuwać na bieżąco, na własny koszt, wszelkie zanieczyszczenia spowodowane jego pojazdami na drogach publicznych oraz dojazdach do terenu budowy.

Wymagania w zakresie odbioru robót**Odbiory robót zanikających i ulegających zakryciu**

Odbiór robót zanikających i ulegających zakryciu polega na finalnej ocenie ilości i jakości wykonywanych robót, które w dalszym procesie realizacji ulegają zakryciu. Odbiór robót zanikających i ulegających zakryciu będzie dokonywany w czasie umożliwiającym wykonanie ewentualnych korekt i poprawek bez hamowania ogólnego postępu robót. Odbioru dokonuje Inspektor Nadzoru. Gotowość danej części robót do odbioru zgłasza Wykonawca powiadomieniem Inspektora Nadzoru. Odbiór będzie przeprowadzony niezwłocznie, nie później jednak niż w ciągu 3 dni od daty powiadomienia Inspektora Nadzoru. Jakość i ilość robót ulegających zakryciu ocenia Inspektor Nadzoru na podstawie dokumentów zawierających komplet wyników badań laboratoryjnych i w oparciu o przeprowadzone pomiary, w konfrontacji z dokumentacją projektową, S.T. i uprzednimi ustaleniami.

W przypadku, gdy roboty nie zostaną zgłoszone do odbioru przez kierownika budowy i nie zostaną odebrane przez Inspektora Nadzoru, Wykonawca zobowiązany jest do umożliwienia Inspektorowi Nadzoru sprawdzenia wykonania ww. robót poprzez np. odkrycie tych robót lub wykonanie otworów umożliwiających to sprawdzenie. Jeśli Inspektor Nadzoru potwierdzi, iż roboty zostały wykonane w sposób prawidłowy, Wykonawca zobowiązany jest do przywrócenia robót do stanu przed ich odkryciem.

Jeśli Inspektor Nadzoru stwierdzi, że ww. roboty zostały wykonane w sposób nieprawidłowy, Wykonawca zobowiązany jest do usunięcia nieprawidłowo wykonanych robót oraz do ponownego ich wykonania w należyty sposób. Odkrycie, zakrycie, rozebranie i ponowne wykonanie robót, o których mowa powyżej, Wykonawca zobowiązany jest wykonać na własny koszt.

Odbiór końcowy robót

Odbiór końcowy polega na finalnej ocenie rzeczywistego wykonania robót w odniesieniu do ich ilości, jakości i wartości. Całkowite zakończenie robót oraz ich gotowość do odbioru końcowego będzie stwierdzona przez Wykonawcę powiadomieniem na piśmie o tym fakcie Inspektora Nadzoru. Odbiór końcowy robót nastąpi w terminie ustalonym w umowie. Odbioru końcowego robót dokona Komisja Odbiorowa wyznaczona przez Zamawiającego w obecności Inwestora i Wykonawcy.

Komisja odbierająca roboty dokona ich oceny jakościowej na podstawie przedłożonych dokumentów, wyników badań i pomiarów, ocenie wizualnej oraz zgodności wykonania robót z dokumentacją projektową, S.T. W toku odbioru końcowego robót komisja zapozna się z realizacją ustaleń przyjętych w trakcie odbiorów robót zanikających i ulegających zakryciu, zwłaszcza w zakresie wykonania robót uzupełniających i robót poprawkowych.

W przypadku odbioru końcowego, Wykonawca:

1. Przeprowadzi przed czynnościami odbioru wymagane próby i sprawdzenia robót. O terminie ich przeprowadzenia Wykonawca zawiadomi Zamawiającego, nie później niż na 3 dni przed terminem wyznaczonym do dokonania prób i sprawdzeń.
2. Zakończy wszystkie roboty i przeprowadzi z wynikiem pozytywnym wymagane próby i sprawdzenia w trybie ustalonym w umowie oraz powiadomi na piśmie o tym fakcie Inspektora Nadzoru.

Dokumenty do odbioru końcowego robót

Podstawowym dokumentem do dokonania odbioru końcowego robót jest protokół odbioru końcowego robót sporządzony wg wzoru ustalonego przez Zamawiającego. Warunkiem potwierdzenia gotowości do odbioru końcowego jest dostarczenie przez Wykonawcę kompletnej i prawidłowo sporządzonej dokumentacji powykonawczej jak również innych dokumentów wymaganych w myśl umowy i obowiązujących przepisów. Kompletność dokumentów powykonawczych należy uzgodnić z Inspektorem Nadzoru.

W przypadku, gdy wg Komisji, roboty pod względem przygotowania dokumentacyjnego nie będą gotowe do odbioru końcowego, Komisja w porozumieniu z Wykonawcą wyznaczy ponowny termin odbioru końcowego robót.

Wymagania w zakresie zabezpieczenia terenu budowy

Wykonawca jest zobowiązany do zabezpieczenia terenu budowy w okresie trwania realizacji umowy, aż do zakończenia i odbioru ostatecznego robót.

Wymagania w zakresie ochrony środowiska

Wykonawca ma obowiązek znać i stosować w czasie prowadzenia robót wszelkie przepisy dotyczące ochrony środowiska naturalnego. W okresie trwania budowy i wykończania robót Wykonawca będzie, podejmować wszelkie uzasadnione kroki mające na celu stosowanie się do przepisów i norm dotyczących ochrony środowiska na terenie i wokół terenu budowy oraz będzie unikać uszkodzeń lub uciążliwości dla osób lub własności społecznej i innych, a wynikających ze skażenia, hałasu lub innych przyczyn powstałych w następstwie jego sposobu działania.

Stosując się do tych wymagań będzie miał szczególny wzgląd na środki ostrożności i zabezpieczenia przed:

- zanieczyszczeniem zbiorników i cieków wodnych pyłami lub substancjami toksycznymi,
- zanieczyszczeniem powietrza pyłami i gazami,
- możliwością powstania pożarów.

Wymagania w zakresie ochrony przeciwpożarowej

Wykonawca będzie przestrzegać przepisów ochrony przeciwpożarowej. Wykonawca będzie utrzymywać sprawny sprzęt przeciwpożarowy, wymagany przez odpowiednie przepisy. Materiały łatwopalne będą składowe w sposób zgodny z odpowiednimi przepisami i zabezpieczone przed dostępem osób trzecich. Wykonawca będzie odpowiedzialny za wszelkie straty spowodowane pożarem wywołanym jako rezultat realizacji robót albo przez personel Wykonawcy.

Wymagania w zakresie bezpieczeństwa i higiena pracy

Podczas realizacji robót Wykonawca będzie przestrzegał przepisów dotyczących bezpieczeństwa i higieny pracy oraz stosował się do zaleceń Planu Bezpieczeństwa i Ochrony Zdrowia opracowanego przez Kierownika Budowy. W szczególności Wykonawca ma obowiązek zadbać, aby personel nie wykonywał pracy w warunkach niebezpiecznych, szkodliwych dla zdrowia oraz niespełniających odpowiednich wymagań sanitarnych. Wykonawca zapewni i będzie utrzymywał wszelkie urządzenia zabezpieczające, socjalne oraz sprzęt i odpowiednią odzież dla ochrony życia i zdrowia osób zatrudnionych na budowie oraz dla zapewnienia bezpieczeństwa publicznego.

DZIAŁ II – KONCEPCJA REALIZACJI ZADANIA

NAZWA ZAMIERZENIA BUDOWLANEGO:

**KONCEPCJA PROGRAMOWO-PRZESTRZENNA
OPRACOWANIE BUDOWLANO-INSTALACYJNE
DLA ZADANIA**

występującego pn.: „dostosowanie pomieszczeń ostatniej kondygnacji budynku siedziby Zamawiającego dla potrzeb Inspektoratu Wewnętrznego Służby Więziennej oraz przebudowanie pomieszczeń recepcji i wejścia głównego znajdującego się na parterze budynku w sposób poprawiający ich bezpieczeństwo i funkcjonalność”

ADRES:

**UL. RAKOWIECKA 37A, 02-521 WARSZAWA, DZIELNICA MOKOTÓW
DZIAŁKA EWIDENCYJNA NR 31/1 Z OBRĘBU 10110,
JEDNOSTKA EWIDENCYJNA 146505_8**

INWESTOR:

**CENTRALNY ZARZĄD SŁUŻBY WIĘZIENNEJ
UL. RAKOWIECKA 37A 02-521 WARSZAWA**

Wykonawca:

**SILTEC Sp. z o.o.
Ul. Parzniewska 12
05-800 Pruszków**

Opracował:

P. Radosław Lenart
upr. branża architektoniczna 17/WMOKK/2018
upr. branża konstrukcyjno-budowlana MAZ/0937/PWBkB/17
P. Arkadiusz Wild
upr. branża niskoprądowa PISA 6143/P/2021
P. Tadeusz Figat
upr. branża sanitarna Wa-375/90

Warszawa, kwiecień 2023 r.

Przedmiot opracowania.

Przedmiotem opracowania jest dokumentacja koncepcyjna obejmująca konieczny do wdrożenia zakres prac budowlanych, elektroinstalacyjnych i rozwiązań technicznych na poziomie parteru wynikające ze służowania korytarza dostępowego celem uzyskania zwiększonego bezpieczeństwa pracy na terenie jednostki organizacyjnej oraz zmian architektonicznych i instalacyjnych na poziomie czwartego piętra, celem utworzenia stref ochronnych zgodnie z *Rozporządzeniem Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. poz. 683)*, *Rozporządzeniem Rady Ministrów z dnia 22 lutego 2017 r. zmieniającym rozporządzenie w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. poz. 522)* oraz Zarządzenia Ministra Sprawiedliwości w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych z dnia 23 stycznia 2014 r. (Dz.Urz.MS z 2014 r. poz.32), na terenie budynku CZSW w Warszawie, 02-521 Warszawa ul. Rakowiecka 37a, rozwiązań niezbędnych dla zapewnienia prawidłowego, bezpiecznego funkcjonowania zespołu pomieszczeń na poziomie parteru i czwartego piętra w zakresie przeciwdziałania aktom wandalizmu, atakom terrorystycznym i inwigilacji elektronicznej. Przedstawione w opracowaniu rozwiązania w zakresie ochrony elektromagnetycznej zwiększą tłumienność elektromagnetyczną przegrody budowlanej serwerowni, umożliwią bezpieczną pracę na stanowiskach teleinformatycznych (wdrożenie sprzętu teleinformatycznego ze zwiększonym zabezpieczeniem technicznym – poziom level B zgodnie z normą SDIP-27), obniżą prawdopodobieństwo pozyskania informacji niejawnych przetwarzanych i werbalizowanych, ograniczając emisję ujawniającą przewodzoną i promieniowaną z zastosowaniem rozwiązań pasywnych. W zakresie zwiększania izolacyjności akustycznej wybranych pomieszczeń, zabezpieczą je przed bezpośrednim podsłuchem akustycznym.

Opracowanie zostało przygotowane na podstawie prowadzonych konsultacji technicznych, związanych z wykonaniem modernizacji architektonicznej, ochroną elektromagnetyczną i akustyczną zespołu pomieszczeń przeznaczonych do prowadzenia działań operacyjnych i bezpiecznej pracy. Rozpowszechnianie informacji o koniecznych do wdrożenia zabezpieczeniach na terenie jednostki organizacyjnej struktur CZSW Warszawa może doprowadzić do utraty poufności i integralności chronionych zasobów związanych z przetwarzanymi werbalizowanymi informacjami. W konsekwencji bezsporne jest, iż przedmiotowy dokument zawiera informacje przede wszystkim o charakterze technicznym, technologicznym, organizacyjnym przedsiębiorstw oraz inne informacje posiadające wartość gospodarczą. Materiał może być wykorzystany przez przedstawicieli CZSW do dalszych celów realizacji tylko tego zadania, występującego pn.: „Dostosowanie pomieszczeń ostatniej kondygnacji budynku siedziby Zamawiającego dla potrzeb Inspektoratu Wewnętrznej Służby Więziennej oraz przebudowanie pomieszczeń recepcji i wejścia głównego znajdującego się na parterze budynku w sposób poprawiający ich bezpieczeństwo i funkcjonalność przy ul. Rakowieckiej 37a w Warszawie”.

Przy doborze rozwiązań uwzględniono wymagania ustawowe zawarte w Rozporządzeniach Rady Ministrów i zaleceniach służby Agencji Bezpieczeństwa Wewnętrznego, stanowiące podstawowe dokumenty odniesienia w zakresie ochrony informacji niejawnych i bezpieczeństwa teleinformatycznego stosowane

w procesach projektowania, wdrażania i eksploatacji rozwiązań właściwych dla stref ochronnych i pomieszczeń specjalnych w jednostkach organizacyjnych:

1. Ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742).
2. Rozporządzeniu Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. Nr 159, poz. 948).
3. Rozporządzeniu Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. poz. 683);
4. Rozporządzeniu Rady Ministrów z dnia 22 lutego 2017 r. zmieniające rozporządzenie w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. poz. 522).
5. Rozporządzeniu Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. z 2017 r. poz. 1558).
6. Zarządzenia Ministra Sprawiedliwości w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych z dnia 23 stycznia 2014 r. (Dz.Urz.MS z 2014 r. poz.32
7. Wytycznych w sprawie postępowania z informacjami niejawnymi międzynarodowymi – ABW – KWB z dnia 31 grudnia 2010 r..
8. Zarządzenie nr 21 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 19 kwietnia 2016 r. w sprawie wykonywania badań antypodsluchowych przez Agencję Bezpieczeństwa Wewnętrznego.
9. Dokumentach wydanych przez Departament Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego:
 - Zaleceniach dotyczących bezpieczeństwa teleinformatycznego, wersja 2.2, sierpień 2011 r..
 - Szczegółowych zaleceniach dotyczących analizy oraz zarządzania ryzykiem w systemach teleinformatycznych, wersja 2.0, sierpień 2011 r..
 - Zaleceniach Departamentu Bezpieczeństwa Teleinformatycznego ABW dotyczących ochrony elektromagnetycznej systemów teleinformatycznych, wersja 5.0, listopad 2016 r..
 - Zaleceniach konfiguracyjnych dla systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych na wydzielonych stanowiskach z wykorzystaniem systemu operacyjnego Microsoft Windows 10 Professional, wersja 1.0, 4 stycznia 2018 r..
 - Zaleceniach dotyczących opracowywania dokumentu Szczególnych Wymagań Bezpieczeństwa dla systemu teleinformatycznego - wersja 2.1, czerwiec 2012 r..
 - Zaleceniach Departamentu Bezpieczeństwa Teleinformatycznego ABW w zakresie budowy specjalnych stref ochronnych służących ochronie informacji niejawnych, wersja 2.0, listopad 2018 r..

Wdrożone rozwiązania na terenie przedmiotowych pomieszczeń na poziomie czwartego piętra, które będą stanowiły Strefę Ochronną ustanowioną przez Zleceniodawcę w ramach przedsięwzięć organizacyjno-technicznych w zakresie ochrony informacji niejawnych, umożliwią zainstalowanie systemu teleinformatycznego uwzględniając zalecenia określone w dokumentach ustawowych i zaleceniach ABW w zakresie ochrony informacji niejawnych i bezpieczeństwa teleinformatycznego niezbędnego do uzyskania świadectwa akredytacji bezpieczeństwa teleinformatycznego (w trybie art. 48 Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych). Wdrożenie systemu teleinformatycznego, i zastosowane w tym systemie teleinformatycznym środki ochrony elektromagnetycznej (środki zabezpieczenia technicznego sprzętu- systemu) będą uzależnione od klauzuli przetwarzanych informacji niejawnych oraz tzw. Sprzętowej Strefy Ochrony Elektromagnetycznej, która (w przypadku wystąpienia Inwestora z wnioskiem WS-01) zostanie określona przez DBTI ABW i potwierdzona stosownym Certyfikatem Ochrony Elektromagnetycznej.

Szczegółowa konfiguracja systemu teleinformatycznego, przeznaczenie jego poszczególnych elementów, połączenia, wymagane procedury eksploatacyjne oraz klauzule, do jakich będą mogły być przetwarzane dane w systemie teleinformatycznym zostaną przedstawione przez Zamawiającego po wdrożeniu rozwiązania w osobnych n/w opracowaniach:

- „W dokumentacji systemu teleinformatycznego do przetwarzania informacji niejawnych zlokalizowanym w Strefie Ochronnej”,
- „Szczególnych Wymaganiach Bezpieczeństwa Systemu” i „Procedurach Bezpiecznej Eksploatacji Systemu”.

Opracowanie wzorów ww. dokumentów jak również wszelkich zarządzeń leży po stronie Wykonawcy zadania.

Zamawiający po zakończeniu realizacji po spełnieniu wymogów ustawowych może wystąpić do ABW o wydanie opinii dopuszczającej Strefę Ochronną do Użytkowania.

Przeznaczenie i układ funkcjonalny poziom 0 - modernizacja pomieszczeń.

Celem realizacji zadania jest zwiększenie bezpieczeństwa pracy na terenie jednostki organizacyjnej poprzez służowanie korytarza dostępowego na podstawie zmian architektonicznych strefy wejścia do budynku w poziomie parteru. Modernizacja architektoniczna i instalacyjna w poziomie parteru (pomieszczeń recepcji i wejścia głównego) oraz wdrożenie planowanych zabezpieczeń fizycznych i technicznych skutkuje obniżeniem prawdopodobieństwa wystąpienia zdarzeń które mogą powstać w wyniku działań terrorystycznych lub wandalizmu. Planuje się doposażenie strefy wejścia w pomieszczenia ochrony tj. pomieszczenie osób dozorujących oraz pomieszczenie dyspozytorni, a także wprowadzenie kontroli dostępu w miejscach kluczowych pod względem bezpieczeństwa. Nowe przegrody budowlane wykonać zgodnie z przedstawionymi zmianami na rysunku zawartym w dokumentacji technicznej. Nowy układ strefy wejścia głównego zapewni poprawną organizację pracy i zwiększy bezpieczeństwo pracy na terenie jednostki organizacyjnej.

Należy wykonać zmiany architektoniczne związane z funkcją pomieszczeń. Ograniczyć strefę wolnego dostępu (wiatrołapu) z zewnątrz przegrodą budowlaną z bloczków z betonu komórkowego H+H z drzwiami dostępowymi

klasy RC4. Układ pomieszczeń umożliwi pełny ogląd osobom dozorującym z pomieszczenia dyspozytorni na przestrzeń wiatrołapu. Ściany należy wykończyć obustronnie tynkiem jednowarstwowym gipsowym z dwukrotnym malowaniem, z przygotowaniem podłoża i gruntowaniem. Zdemontować niefunkcjonalne drzwi rozsuwane w wiatrołapie. Zamontować bramkę uchylną wyposażoną w szkło antywłamaniowe klasy P6, bramkę dostępową do pomieszczenia z depozytorem oraz skanerem RTG.

Od strony korytarza ograniczyć dostęp oknem blokowanym. Zdemontować istniejącą zabudowę metalową oddzielającą korytarz od klatki schodowej. Wykonać montaż nowej zabudowy przeszklonej szkło P6 z drzwiami rozsuwanymi dostępowymi o szerokości przejścia 200 cm. Drzwi dostępowe rozsuwane doposażone w automatykę z możliwością blokady mechanicznej - ręcznej. Układ blokady mechanicznej - ręcznej zlokalizowany w pomieszczeniu ochrony (pomieszczeniu nr 00/03).

Dla wszystkich nowych otworów drzwiowych i okiennych w ścianach nośnych, wykonać montaż nadproża z belek stalowych.

Relokować tablicę pamiątkową w strefę klatki schodowej oraz doposażyć strefę w wypoczynek z materiałów umożliwiających usytuowanie na drodze ewakuacyjnej.

Instalacja wentylacji mechanicznej.

Na parterze w strefie wejścia, pomieszczenie osób dozorujących oraz pomieszczenie dyspozytorni wyposażać w instalację wentylacyjną nawiewno- wyciągową N/W=60m³/h wykorzystując istniejącą instalację wentylacji mechanicznej w tej strefie.

System bezpieczeństwa i deponowania broni.

Podstawowe założenia.

W celu zapewnienia właściwego poziomu ochrony obiektu oraz skutecznego przeciwdziałania wszelkim zagrożeniom związanym z prawidłowym funkcjonowaniem jednostki organizacyjnej, wdrożone rozwiązania budynkowe uwzględnią elektroniczny system zabezpieczeń technicznych wykonanych w oparciu o poniższe systemy bezpieczeństwa oraz rozwiązania multimedialne:

- autonomiczny system włamania i napadu SSWIN;
- autonomiczny system kontroli dostępu SKD;
- system interkomowy;
- telewizyjny system nadzoru w strefie ochrony peryferyjnej i wewnętrznej;
- system BMS;
- depozytor broni;
- instalacje elektryczne;

Opracowanie techniczne uwzględnia otrzymane od Zamawiającego wytyczne. Uwzględnione zostały wszystkie możliwe do użycia środki techniczne tak, aby wpływ czynnika ludzkiego na bezpieczeństwo pracy ograniczyć do niezbędnego minimum.

Systemy bezpieczeństwa.

Na potrzeby projektowanych i modernizowanych systemów bezpieczeństwa należy wybudować wydzielone, dedykowane okablowanie strukturalne z użyciem kabla F/FTP 4x2xAWG23/1 Kat 6a LSOH oraz kabla U/UTP 4x2xAWG24/1 Kat 5e LSOH z punktem dystrybucyjnym zlokalizowanym w odpowiednio zabezpieczonym pomieszczeniu ochrony.

Nie należy wykorzystywać żadnych elementów (aktywne lub pasywne) sieci komputerowej i telefonicznej na potrzeby transmisji dla systemów bezpieczeństwa. W sieci systemów bezpieczeństwa należy wykorzystać urządzenia aktywne zarządzalne oraz skonfigurować w sposób uniemożliwiający podłączenie do sieci innych elementów niż urządzenia wchodzące w skład systemów bezpieczeństwa.

Newralgiczne systemy bezpieczeństwa SKD-SSWIN należy zasilić z rozdzielnic piętrowej z uwzględnieniem podtrzymania napięcia zasilającego z własnego źródła zasilania (zasilacz buforowy) przez czas 36h. Na terenie parteru wdrożyć system dozoru CCTV. Systemy bezpieczeństwa pomieszczeń strefy parteru zostaną wykonane w stopniu ochrony 3, rozpoznania A wg. normy PN-EN 50131, PN-EN 50132.

Główne elementy systemu bezpieczeństwa Security Expert moduły SP-C, SP-RDM2, SPI-16 należy zamontować w obudowach modułowych systemowych w szafce zamykanej kluczem dostępowym. Zostaną zasilone z w/w rozdzielnic z uwzględnieniem zasilaczy typ PSBEN10A12E PULSAR wyposażonych w akumulatory typ EP12V65 - 12V65Ah celem podtrzymania pracy systemu przez min. 36h przy utracie zasilania podstawowego i gwarantowanego. Nie przewiduje się oddzielnych zasilaczy dla elementów systemu SKD_SSWIN np. zwór/rygli drzwi dostępowych.

W pomieszczeniu ochrony należy zamontować szafkę wiszącą dla modułów systemu SKD_SSWIN oraz szafkę rack dla systemu CCTV, w której jednocześnie zlokalizowana zostanie autonomiczna jednostka UPS zasilająca switch dla systemu depozytora i rejestratora kamer.

Do połączenia urządzeń systemowych SKD/SSWIN/CCTV należy wykorzystać okablowanie F/FTP 4x2xAWG23/1 Kat 6a LSOH oraz 4x2xAWG24/1 Kat 5e LSOH służące do podłączeń czujników wchodzących w skład systemu bezpieczeństwa.

Instalacje systemowe w poziomie i pionie należy prowadzić po wybudowanych trasach w korytach teletechnicznych oraz z wykorzystaniem peszli instalacyjnych RKGL nierozprzestrzeniających płomienia. Instalacje nisko napięciowe 12V/DC zostaną wykonane przy wykorzystaniu okablowania:

- F/FTP 4x2xAWG23/1 Kat 6a LSOH.- połączenia magistralne systemu SKD/SSWIN;
- 4x2xAWG24/1 Kat 5e LSOH – połączenia czujników systemu SKD/SSWIN;
- F/FTP 4x2xAWG23/1 Kat 6a LSOH - połączenia kamer systemu CCTV;
- U/UTP 4x2xAWG24/1 Kat 5e LSOH - podłączenie czytników SX-RD-MB-BT do kontrolera SP-RDM2;
- U/UTP 4x2xAWG24/1 Kat 5e LSOH - podłączenie kontaktronów ISC-PMC-S3S, przycisków wyjścia YPW2D przycisków ewakuacyjnych D-115 i monitoringu
- YNTKSYEWK 2x1mm² – podłączenie zasilania do zwór.

Dla pomieszczeń przewidziano autonomiczne rozwiązanie oparte o system Security Expert, kontrolę dwustronną (moduł SP-RDM2) - wejście i wyjście z pomieszczenia po autoryzacji z wykorzystaniem dedykowanych

kart zbliżeniowych dla czytników SX-RD-MB-BT. Czytniki posiadają funkcję sygnalizacji dźwiękowej w przypadku pozostawienia otwartych drzwi. Przy przejściu kontrolowanym należy zamontować przyciski awaryjnego wyjścia odblokowujące przejście na wypadek ewakuacji oraz zapewniające bezzwłoczną sygnalizację użycia w punkcie ochrony. Przejście objęte systemem kontroli dostępu musi zostać w razie pożaru automatycznie odblokowywane za pośrednictwem modułów systemu sygnalizacji pożaru zgodnie z przyjętym scenariuszem pożarowym.

W charakterze elementów wykonawczych przy drzwiach należy zastosować zwoję elektromagnetyczną rewersyjną z czujnikiem działania hall i kontaktronem.

Wszystkie zdarzenia w systemie muszą być rejestrowane i wizualizowane oraz przesłane do punktów nadzoru z wykorzystaniem platformy integrującej Security Expert.

Za zarządzanie i administrację systemu odpowiedzialny jest administrator strefy. W tym celu administrator wyposażony będzie w stację roboczą. Na etapie realizacji zadania należy zapewnić połączenie z systemem kontroli dostępu za pośrednictwem wydzielonej i dedykowanej sieci dla systemów bezpieczeństwa. Punkt emisji kart dostępu do budynku znajduje się na terenie budynku Zamawiającego. Celem zabezpieczenia pomieszczenia przed utratą poufności i zwiększeniem zabezpieczeń technicznych rozbudować w/w system o moduły SPI-16 pełniące funkcje bezpieczeństwa technicznego – alarmowego. W zależności od wielkości, powierzchni i położenia pomieszczeń podlegających ochronie należy zamontować czujniki zgodnie z postanowieniami dokumentów odniesienia. Do ochrony pomieszczeń została zastosowana taka ilość czujek PIR typu OPTEX CDX-AM, z antymaskingiem i czujników magnetycznych, czytników przejść SX-RD-MB-BT, aby zapewnić pełne zabezpieczenie całej powierzchni i rozliczalność wejść/wyjść. Założenia dotyczące elementów detekcyjnych (w szczególności dobór oraz rozmieszczenie) dla poszczególnych obszarów przedstawiono na rysunku nr A3 (A3-Rzut parteru stan projektowany. Układ architektoniczny – strefa wejścia do budynku).

Wszystkie zdarzenia w systemie należy rejestrować i wizualizować z wykorzystaniem platformy integrującej zamontowanej w jednostce komputerowej zlokalizowanej na terenie ochrony całodobowej.

Na etapie projektu wykonawczego i realizacji zadania dopuszcza się możliwość rozbudowy istniejącego systemu SKD SSWIN.

Rozwiązanie uwzględnia wykorzystywanie jednej karty do przemieszczania się po zespole pomieszczeń, którą dysponuje Użytkownik. Jego zadaniem będzie zaprogramowanie kart celem umożliwienia z korzystania rozwiązań systemu SKD.

Wymagania dotyczące części elektronicznej układu stykowego (chip) blankietu legitymacji służbowej funkcjonariusza i pracownika Służby Więziennej oraz karty kryptograficznej.

Elektroniczny układ stykowy (chip):

- wykonany jest zgodnie ze standardem ISO/IEC 7816 lub równoważnym, w którym zapisywane są certyfikaty oraz klucze kryptograficzne o długości min. 2048 bitów;
- realizuje algorytm RSA;
- funkcjonuje zgodnie z normą ISO/IEC 7816 część 1, 2, 3 lub równoważną;

- posiada, co najmniej 64 kB pamięci zapisywalnej (EEPROM);
- w ramach wewnętrznej pamięci EEPROM przechowuje klucze, certyfikaty i inne obiekty;
- realizuje podpis RSA przy użyciu klucza prywatnego znajdującego się na legitymacji lub karcie z wykorzystaniem algorytmu RSA zgodnie ze specyfikacją PKCS#1 w wersji 1.5;
- posiada bibliotekę dynamiczną DLL dla systemów Microsoft Windows 2012/2016/10/11 z implementacją interfejsu PKCS#11 API, zgodnej ze standardem PKCS#11 v2.01 lub nowszym;
- posiada bibliotekę dynamiczną z implementacją interfejsu PKCS#11 umożliwiającą generowanie nowej pary kluczy RSA przez chip, zapis klucza prywatnego i publicznego, realizację podpisu RSA, deszyfrowanie z użyciem klucza RSA i zapis certyfikatu na legitymację lub kartę, kasowanie obiektów z legitymacji lub karty;
- posiada generator liczb losowych wykorzystywany przez legitymację lub kartę do generowania kluczy na blankiecie legitymacji lub karcie. Generator ten musi być oparty na zjawisku fizycznym;
- umożliwia przechowywanie, co najmniej 15 (piętnastu) kluczy prywatnych o długości min. 2048 bity wraz z ich certyfikatami o typowej wielkości 1 kB;
- umożliwia definiowanie min. 1 kodu PIN oraz związanego z nim 1 kodu PUK na legitymacji lub karcie. Długość kodu PIN oraz PUK wynosi, co najmniej 4 znaki;
- umożliwia zapisywanie dowolnych obiektów danych na legitymacji lub karcie;
- umożliwia zarządzanie dynamicznie przydziałem i zwalnianiem pamięci (wielokrotne usuwanie i zapisywanie ponownie kluczy kryptograficznych i obiektów danych nie powoduje zmniejszenia dostępnej pamięci na te dane);
- posiada przynajmniej jeden z wymienionych certyfikatów bezpieczeństwa dla układu elektronicznego legitymacji lub karty:
 - 1) CommonCriteria EAL4 bądź wyższy poziom lub równoważny,
 - 2) FIPS 140-2 Level3 bądź wyższy poziom lub równoważny;
- współpracuje z Microsoft Windows 2012/2016/10/11 oraz pozwala na uwierzytelnianie w przeglądarce Chrome, Microsoft Edge oraz Mozilla Firefox;
- umożliwia pracę wieloaplikacyjną przy udostępnianiu przez oba interfejsy (PKCS#11 i MS CSP/Minidriver). Klucze i obiekty danych zapisywane za pośrednictwem jednego interfejsu są dostępne dla drugiego interfejsu, jeśli jest to zgodne z jego specyfikacją;
- umożliwia podpisywanie dokumentów utworzonych w OpenOffice (od wersji 3), LibreOffice (od wersji 4) oraz Microsoft Office (od wersji 2003); CHIP-y w naszych legitymacjach są od NXP z oprogramowaniem IDProtect Manager.

System Interkomowy.

Dla potrzeb komunikacji między osobami ochrony a petentem przed wejściem głównym zostanie zamontowany panel komunikacyjny – wideofon HIKVISION wyposażony w wbudowaną kamerę oraz przycisk, umożliwiający nawiązanie łączności z monitorem DS.-KH6320-WTE2-W. System oparty jest na rozwiązaniach cyfrowych z okablowaniem YNTKSYEWK 2x1mm². Zasilanie należy wykonać poprzez zastosowanie zewnętrznego zasilacza 24V/5A DC. Konfiguracja urządzeń odbywa się poprzez intuicyjny interfejs. Wymagana jest dwustronna komunikacja audio-video (full duplex) z redukcją wyświetlenia obrazu. Możliwość komunikacji bezpośredniej (per-to-per) odbywa się za pośrednictwem modułu komunikacyjnego DS.-KAD706. Otwieranie drzwi dostępowych do poszczególnych stref na poziomie parteru będzie realizowane przez funkcjonariusz ochrony. Lokalizacje urządzeń pokazano na rysunku nr A3 (A3-Rzut parteru stan projektowany. Układ architektoniczny – strefa wejścia do budynku).

Telewizyjny system nadzoru.

Telewizyjny system nadzoru w strefie peryferyjnej i wewnętrznej zapewni obserwację przestrzeni zewnętrznej, korytarza dostępowego strefy ochronnej III. Lokalizacja kamer zostanie uzgodniona z Użytkownikiem. System monitoringu wizyjnego zostanie uzupełniony o dodatkowe kamery.

W systemie monitoringu zastosowane zostaną kamery sieciowe wewnętrzne IP 2 Mpx typ IPC-HDW3241T-ZAS-27135 ze zmienną ogniskową (zoom) o rozdzielczości nie mniejszej niż 19200px x 1080px, ze stałą ogniskowym obiektywem, wizyjną detekcją ruchu, pracujące w trybie dzień/noc, z mechanicznym filtrem podczerwieni, poszerzonym zakresem dynamiki i wysoką czułością, cyfrową obróbką sygnału oraz redukcją efektów niepożądanych. Kamery należy połączyć przy pomocy kabla skrętkowego F/FTP 4x2xAWG23/1 Kat 6a LSOH do dedykowanego switch-a/ zlokalizowanego w pomieszczeniu ochrony w strefie ochronnej, w którym umieszczono również lokalny serwer/rejestrator, macierzy dyskowych. System monitoringu musi zapewnić przestrzeń dyskową pozwalającą na odtworzenie zdarzeń systemowych oraz nagrań ze wszystkich kamer, co najmniej z 30 ostatnich dni – zgodnie z wytycznymi zawartymi w dokumentach odniesienia. Podgląd rejestrowanego obrazu jest widoczny dla osób dozoruujących w tym całodobowej obsługi. Lokalna stacja robocza zostanie umieszczona w pomieszczeniu uzgodnionym. W celu zwiększenia efektywności korzystania z systemu przez operatora zaleca się, by telewizyjny system nadzoru integrować z pozostałymi systemami bezpieczeństwa. Lokalizację urządzeń pokazano na rysunku nr A3 (A3-Rzut parteru stan projektowany. Układ architektoniczny – strefa wejścia do budynku).

BMS integracja systemów.

Dla potrzeb monitoringu wprowadza się rozwiązanie Security Expert. Rozwiązanie umożliwia opracowanie skutecznych i nowoczesnych procedur alarmowych i ewakuacyjnych w przypadku sytuacji awaryjnych i stwarzających zagrożenie dla zdrowia i życia ludzi dzięki pełnej i aktualnej informacji o stanie obiektu. Pozwoli także na maksymalne uproszczenie i usprawnienie systemu zarządzania i monitoringu obiektu, kompleksową organizację raportowania i archiwizacji danych dotyczących funkcjonowania całego obiektu, włącznie z przesyłaniem danych i raportów do innych baz danych i systemów informatycznych.

Depozytor.

Na korytarzu dostępowym na poziomie parteru zamontować depozytory broni SAIK GUN S1 na 4 sztuki broni krótkiej i 2 sztuki broni długiej. Minimalne parametry sejfów na broń w klasie S1: obudowa w klasie S1 dla poszczególnych rodzajów broni (4 skrytki na broń krótką + 2 dwie skrytki na broń długą), indywidualne skrytki na poszczególne rodzaje broni, depozytor kluczy w skrytkach do przechowywania i identyfikowania kluczy sejfowych, zwarta obudowa.

Procedura pobierania klucza i zdawania broni:

- osoba chcąc przechować broń na ekranie lcd wybiera rodzaj broni do przechowania wpisuje na ekranie swoje dane oraz kreuje PIN do skrytki,
- pobiera klucz z depozytora → otwiera indywidualny sejf → zdaje broń → zamyka sejf kluczem, zabiera klucz ze sobą na teren strefy lub zostawia go w depozytorze;
- po wyjściu ze strefy podchodzi do depozytora → wpisuje SWÓJ PIN (pin automatycznie wygasa – skrytka jest wolna) → otwiera skrytkę kluczem → wyjmuje broń → zamyka kluczem sejf → klucz umieszcza w skrytce.

Depozytor zasilć napięciem 230V/AC przewodem N2XH-J 3x2,5mm² istniejącej rozdzielnicy. Lokalizację urządzeń pokazano na rysunku nr A2 (A2-Koncepcja rozwiązania –poziom 0. Zwiększenie zabezpieczeń technicznych i fizycznych).

Instalacja gniazd napięcia 230V/AC.

Instalację nowych gniazd wtykowych 230V/AC na terenie pomieszczenia ochrony i pomieszczenia depozytorni należy wykonać z użyciem gniazd natynkowych 1-fazowych podwójnych podzielonych na niezależne obwody oraz przewodem N2XH-J 3x2,5mm². Zgodnie ze standardem budynkowym gniazda w dedykowanym pomieszczeniach montować na wysokości 20cm od podłoża. Na teren przedmiotowych pomieszczeń prowadzić z istniejących tablic korytarzowych kablem N2XH-J 5x6mm² nad sufitem. Na wszystkich obwodach należy umieścić opisy dotyczące numeru oraz rodzaju obwodu. Lokalizację koniecznych do zainstalowania gniazd wtykowych 230V/AC pokazano na rysunku nr A2 (A2-Koncepcja rozwiązania –poziom 0. Zwiększenie zabezpieczeń technicznych i fizycznych).


Instalacja oświetlenia.

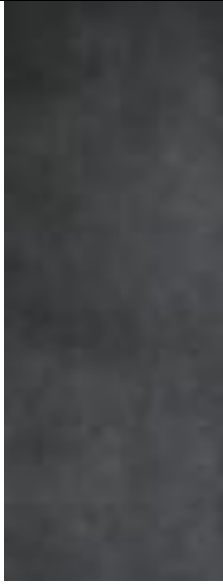


W modernizowanych pomieszczeniach należy zmodernizować istniejącą instalację oświetleniową, zamontować oprawy LED niskoemisyjne, energooszczędne oraz oprawy awaryjne wyposażone w moduł awaryjny zapewniający jej pracę po zaniku napięcia przez okres min. 1 godziny typu 1xLED-AW2. Instalację elektryczną zasilającą poszczególne obwody oświetleniowe należy rozprowadzić z uwzględnieniem podziału topologii ich umiejscowienia. Instalację oświetleniową dla dedykowanych powstałych pomieszczeń należy zasilć z rozdzielnicy wewnętrznej korytarzowej.



Aranżacja wnętrza poziom 0

Zakres ogólny:

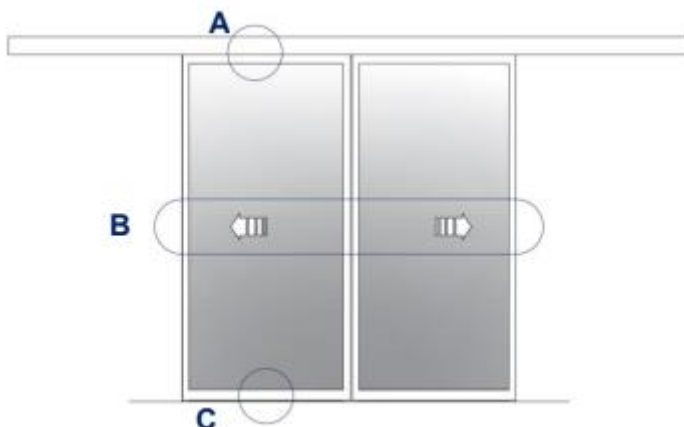
- przetarcie tynków, wykonanie gładzi, malowanie wszystkich ścian i sufitów w zakresie objętym opracowaniem,
- wymiana stolarki drzwiowej w zakresie objętym opracowaniem,
- wykonanie otworów w ścianach działowych oraz nośnych z wykonaniem nadproży prefabrykowanych oraz stalowych,
- wymiana okładzin podłogowych na nowe,
- wykonanie okładzin ścian z tynków dekoracyjnych,
- wymiana sufitów podwieszanych na nowe rastrowe oraz baffle,
- montaż okien podawczych, systemu drzwi przesuwnych,
- dostosowanie systemu oddymiania do warunków po przebudowie pomieszczeń, opcjonalnie w razie potrzeby wykonanie systemu napowietrzania klatki schodowej,
- montaż witryn kuloodpornych,
- przeniesienie tablicy pamiątkowej,
- montaż logo na drzwiach przesuwnych inwestora, zakłada się naklejki – 8 sztuk o powierzchni 1m2, projekt logo przedstawić Inwestorowi do akceptacji na etapie projektu,
- montaż wyposażenia pomieszczeń,

TYNKI DEKORACYJNE	<p>Płyty tynki dekoracyjne w strukturze i fakturze jak na zdjęciu w postaci np. mikrocementu</p> <p>Płyty stosować na okładzinę ścian pom. 0.1, 0.2</p>			
-------------------	---	--	--	--

TYNKI DEKORACYJNE	<p>Płyty tynki dekoracyjne w strukturze i fakturze jak na zdjęciu w postaci np. mikrocementu</p> <p>Płyty stosować na okładzinę ścian 0.4, 0.5 do wysokości spocznika piętra I</p>	
PLYTY GRANITOWE	<p>Płyty granitowe</p> <p>plyt wielkoformatowych z kamienia naturalnego, płyty jasne matowe, stosować płyty o długości większej niż szerokości korytarza</p> <p>np. Imperial White lub np. Colonial White 300/150 gr. 30 mm lub równoważne – płyty biegów i spoczników,</p> <p>np. Absolut Black 300/150 gr. 30 mm lub równoważne – płyty krawędzi stopni,</p>	 <p>Płyta biegów schodowych i spoczników</p>  <p>Płyta krawędzi stopni</p>

SUFITY PODWIESZANE	<p>pomieszczenie 0.2 korytarza</p> <p>wykonanie sufitu baffle metalowe</p> <p>a malowaniem elementów</p> <p>powyżej baffli w kolorze</p> <p>ciemnoszarym lub czarnym,</p> <p>oświetlenie dostosowane do</p> <p>przestrzeni między bafflami lub</p> <p>wpuszczone w baffle.</p>	
SUFITY PODWIESZANE	<p>Sufity podwieszane</p> <p>- komunikacja - sufity</p> <p>rastrowe aluminiowe z</p> <p>malowaniem instalacji i sufitu w</p> <p>kolorze czarnym</p> <ul style="list-style-type: none"> • Siatkę rastra tworzą elementy z blachy aluminiowej o przekroju „U”, o podstawie 10 mm i wysokości 40 mm. • Charakterystyka wyrobu: Rozmiar oczka w osi profili - 60 mm Rozmiar oczka w świetle: - 50 mm . Ze względu na otwarty charakter sufitu wszelkie instalacje ppoż. (sygnalizacyjne i zraszające) mogą być poprowadzone ponad sufitem. • Klasyfikacja ogniowa: wyrób zaliczony do klasy A w zakresie reakcji na ogień, jako materiał niepalny. • Kolor sufitu jasnoszary, 	

WITRYNA P6	<p>Okna aluminiowe klasy P6 o ograniczonej przejrzystości. (spełniają wymagania klasy RC2 wg PN-EN 1627: 2002)</p> <p>Profile lakierowane w kolorze RAL 7035</p> <p>Parametry podajnika:</p> <ul style="list-style-type: none"> – podajnik jednoszufladowy – wymiary komory wewnętrznej: długość ~ 405mm; szerokość ~ 225mm; wysokość ~ 105mm – podajnik wykonany ze stali lakierowanej w kolorze RAL 9006, wyposażony we wkładkę ze stali nierdzewnej
DRZWI PRZESUWNE	<p>Skrzydła malowane w kolorze RAL 7035, przesuwane automatycznie, z czujnikami ruchu, kontrolą dostępu, wymagania zgodnie z dokumentacją rysunkową, do wyboru system drzwi w zależności od wyboru wariantu oddymiania/napowietrzania klatki schodowej,</p> <p>NORMA PN-EN 16005</p> <p>Czujniki zabezpieczające strefy boczne np. GEZE GC 341 lub równoważne</p> <p>Systemowe rozwiązanie kompatybilne z napędem przesuwным np. GEZE ECdrive T2 lub równoważne</p>



Przeznaczenie i układ funkcjonalny poziom 4 – modernizacja pomieszczeń.

Zakres ogólny:

- przetarcie tynków, wykonanie gładzi, malowanie wszystkich ścian i sufitów w zakresie objętym opracowaniem,
- wymiana stolarki drzwiowej w zakresie objętym opracowaniem,
- wykonanie otworów w ścianach działowych oraz nośnych z wykonaniem nadproży prefabrykowanych oraz stalowych,
- wymiana okładzin podłogowych na nowe w miejscu powstałych uszkodzeń – 5 % powierzchni podłóg w

- pomieszczeniach – wykładzina podłogowa,
- dostosowanie systemu oddymiania do warunków po przebudowie pomieszczeń, opcjonalnie w razie potrzeby wykonanie systemu napowietrzania klatki schodowej,
 - montaż logo na drzwiach klatek schodowych na każdym ze skrzydeł,
 - montaż wyposażenia pomieszczeń,
 - montaż krat RC4 z kłódką klasy 5 w otworach zgodnie z dokumentacją rysunkową,
 - montaż konstrukcji stalowej nad stropem pod ustawienie wyposażenia – serwery, sejfy, szafy,
 - murowanie nowych ścian z betonu komórkowego.

Celem realizacji zadania jest modernizacja zespołu pomieszczeń w których będą przetwarzane informacje niejawne na stanowiskach terminalowych SDIP27 level B do klauzuli krajowej „POUFNE” oraz w utworzonej Kancelarii Tajnej na autonomicznym stanowisku SDIP 27 level A „ŚCIŚLE TAJNE”. Nowe przegrody budowlane oraz wzmocnione przegrody budowlane wykonać zgodnie z przedstawionymi zmianami na rysunku technicznym A5 – (A5-Koncepcja rozwiązania –zabezpieczenia fizycznie i techniczne).

Zwiększenie zabezpieczeń technicznych i fizycznych). Podział pomieszczeń zapewni poprawną organizację pracy i funkcjonowanie, sposób i tryb przetwarzania informacji niejawnych zgodnie z *Rozporządzeniem Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. z 2017 r., poz. 1558)*. Należy wykonać zmiany architektoniczne związane z funkcją pomieszczeń. Przegrodę budowlaną na granicy strefy ochronnej III wzmocnić bloczkiem z betonu komórkowego H+H do grubości ściany 25cm. Wykończyć od wewnątrz tynkiem jednowarstwowym gipsowym z dwukrotnym malowaniem, z przygotowaniem podłoża i gruntowaniem. Drzwi dostępne D2 na korytarzu wymienić na drzwi EIS 60 klasy RC4 z dwoma zamkami klasy 7 doposażone w zworę elektromagnetyczną. W skrzydle lewym powyżej drzwi dostępowych D2 klasy RC4, zamontować kratę RC4 celem możliwości przewietrzania korytarza. W prawym skrzydle dokonać zmian architektonicznych celem utworzenia Kancelarii Tajnej, przegrody budowlane wzmocnić bloczkiem z betonu komórkowego H+H do grubości ściany min.18 cm. Wykończyć od wewnątrz tynkiem jednowarstwowym gipsowym z dwukrotnym malowaniem, z przygotowaniem podłoża i gruntowaniem. Podłogę pomieszczeń dedykowanych dla potrzeb serwerowni (pom. nr 4/34) oraz dla potrzeb pomieszczenia sejfów (pom. nr 4/33) wzmocnić konstrukcyjnie hebmami ze względu na jej obecną obciążalność. Zamontować w tych pomieszczeniach podłogę komputerową. Wykonać stopień dla podłogi podniesionej z zachowaniem spocznika. Istniejące świetliki dachowe występujące na korytarzu celem zabezpieczenia dostępu od strony dachu doposażyć w kratę stalową RC4. Kraty RC4 należy również zamontować w oknach pomieszczeń (I i II Strefy Ochronnej). Konstrukcja krat: stała. Kraty muszą być certyfikowane klasy RC4 odporności na włamanie wg PN-EN 1627:2011 oraz Certyfikat Instytutu Mechaniki Precyzyjnej. Konstrukcja kraty w zależności od zastosowania powinna być wykonana z prętów stalowych Ø20 w rozstawie max 150 mm i płaskowników stalowych 6x45 w rozstawie max 400 mm lub prętów stalowych o przekroju kwadratowym 16 x 16 ułożonych warstwowo w kształt kwadratów o boku długości 150 mm, spawanych w ramie z profilu kątownego, profilu ceowego lub profilu zamkniętego. Okna w pomieszczeniu (pom. nr 4/33 i 4/34) zaślepić poprzez oklejenie folią

mrożną zamurować od środka bloczkiem z betonu komórkowego H+H i z licować z istniejącą ścianą murowaną. Na terenie serwerowni i pomieszczeń kancelaryjnych zastosować wykładzinę PCV. Roboty do wykonania zgodnie z normą obronną NO-04-A009:2017. Istniejące drzwi drewniane D1 wymienić na nowe drzwi stalowe z okleiną drewnopodobną, 90x200cm, EI60, samozamykacz, zgodnie z normą obronną NO-04-A009:2017, klamka z szyldem wyposażone w zwoję elektromagnetyczną lub elektrozaczep umożliwiając ich współpracę z systemem bezpieczeństwa SKD Czujnik magnetyczny zamontowany w drzwiach zastosować klasy grade 3. Kolor okleiny drzwiowej do uzgodnienia na etapie realizacji zadania.

Oddymianie klatek schodowych:

Ilości powietrza obliczyć na podstawie kryterium różnicy ciśnienia, przepływu powietrza przez drzwi oraz nadciśnienia 10 Pa z wykonaniem obliczeń. Dla klatki schodowej projektuje się system oparty na czerpni powietrza usytuowanej na dachu budynku. Na każdym z kanałów czerpnych należy zamontować przepustnicę z siłownikiem. Przepustnice w warunkach normalnych w pozycji zamkniętej. Na wypadek uruchomienia systemu przepustnice zostaną otworzone automatycznie (automatyka systemu). Układ automatycznie będzie korzystać z jednej albo drugiej czerpni (jeśli będzie wymagana) w zależności od stopnia zadymienia. Jeśli czujki dymu wykryją dym z jednej strony – przepustnica zostanie zamknięta i układ będzie korzystać z przeciwległej czerpni. Obie czerpnie dla każdego z układów zaprojektować na 100 % wydajności. Nawiew realizowany będzie poprzez wentylatory usytuowane na dachu zgodnie z graficzną częścią opracowania. Wymiary króćców przyłączeniowych do wentylatorów należy dopasować na budowie po dostarczeniu urządzenia. Króćce zróżnicowane dla poszczególnych producentów. Z uwagi na konstrukcję dachu nawiew do klatek schodowych zaprojektować kilkoma kratami nawiewnymi. Takie rozwiązanie pozwoli na minimalizację ingerencji w konstrukcję budynku. Podczas realizacji należy otwory pod kanały nawiewne do klatek dopasować do rzeczywistego rozstawu belek stropowych. Nie wyklucza się konieczności niewielkich przesunięć w stosunku do stanu projektowanego, ponieważ podczas prac projektowych odkrytki istniejących belek wykonywane były wrywkowo.

Kraty nawiewne należy pozostawić jako osiatkowane króćce. Kanały prowadzone na dachu wykonać z blachy ocynkowanej. Spód czerpni montować na wysokości min. 40 cm od powierzchni dachu. Połączenia wentylatorów z systemem kanałów wykonać poprzez złącza elastyczne. System wykonać opcjonalnie w przypadku braku możliwości zapewnienia oddymiania i napowietrzania grawitacyjnego klatki schodowej po wykonanej przebudowie poziomu parteru i wydzieleniu klatki schodowej ppoż.

Prace budowlane i elektroinstalacyjne - zwiększenie tłumienności elektromagnetycznej przegrody budowlanej.

Zgodnie z uzyskaną wytyczną Zamawiającego w pomieszczeniu serwerowni (pom. nr 4/34) należy zwiększyć tłumienność elektromagnetyczną przegrody budowlanej umożliwiając posadowienie na jej terenie jednostki szyfrującej IP KRYPTON K2 Ze względu na swoją (w stosunku do innych podobnych materiałów) skuteczność ekranowania pól statycznych, pól elektrycznych niskich i wysokich częstotliwości, tłumienia impulsowego promieniowania w.cz. w paśmie 1 do 2 GHz do celów zwiększenia tłumienności

elektromagnetycznej przegrody budowlanej dobrano włókninę ekranującą typ Aaronia XDream. Wykonana jest ona obustronnie z włókna miedziano-niklowego na podłożu poliestrowym. W/w włókniną ekranującą wykonać ekranowanie powierzchni ścian, sufitu, podłogi mając na celu uzyskanie w dedykowanym pomieszczeniu zwiększenie poziomu zabezpieczenia miejsca Zakres ekranowania przedstawiono na rysunku nr A5 (A5-Koncepcja rozwiązania –zabezpieczenia fizycznie i techniczne). Zwiększenie zabezpieczeń technicznych i fizycznych). Na równe powierzchnie przegród budowlanych należy klejem „Spray Kon S-200” przykleić elastyczny w/w materiał ekranujący w jednej warstwie na zakładkę 10-15cm i uziemić przy pomocy dedykowanego zestawu uziemiającego (zespołu linek miedzianych) do szyny uziomu „RED”- uziomu bezpieczeństwa. Przed wyłożeniem i wyklejeniem włókniny ekranującej, powierzchnie należy pokryć specjalnym gruntem dedykowanym dla w/w materiału. Zastosowana włóknina ekranująca zwiększy tłumienność przegrody budowlanej w paśmie częstotliwości 10/14kHz-10GHz. Właściwości skuteczności ekranowania zastosowanego materiału wynoszą 99,999%. Poziom tłumienia dla częstotliwości np. 30MHz - 10GHz wynosi >40dB. Powierzchnie budowlane pomieszczenia po wdrożeniu zabezpieczeń akustycznych (opisanych w poprzednim punkcie dokumentacji) i elektromagnetycznych należy wykończyć płytą 2xGK 12,5mm NIDA CİCHA, malowaną na uzgodniony z Użytkownikiem kolor RAL, przykręconą do listew technologicznych. Dziurawienie głębokie materiału ekranującego bez doszczelnienia specjalnymi uszczelkami jest niedopuszczalne. Wszelkie elementy instalacyjne na powierzchni ścian należy instalować za pomocą wkrętów do głębokości max 20mm. Dla potrzeb pomieszczenia objętego ochroną elektromagnetyczną zamontować specjalne drzwi EMC, posiadające właściwości ekranujące określone swoimi parametrami w karcie katalogowej o tłumienności elektromagnetycznej min.60dB wyposażone w uszczelki EMC zapewniając ciągłość powierzchni ekranującej pomieszczenia. System wentylacji i komfortu powietrza pomieszczenia należy wprowadzić na teren serwerowni z zastosowaniem na granicach ekranowanej przegrody budowlanej separatorów plastikowych eliminując emisje przewodzoną ciągów metalowych oraz z wykorzystaniem falowodów wentylacyjnych (zamontowanych na płytach, montażowych) - plastrów miodu o skuteczności ochrony elektromagnetycznej min. 60-100dB, falowodów rurkowych na linia układu klimatyzacji celem wyeliminowania emisji promieniowanej. Wszystkie instalacje elektryczne i teletechniczne występujące na terenie, Strefy Ochronnej II, która zostanie określona przez Zleceniodawcę w ramach przedsięwzięć organizacyjno-technicznych w zakresie ochrony informacji wrażliwych należy wprowadzić przez filtry separacyjne napięciowe 5x16A i sygnałowe 8x1A zamontowane w skrzynce SRF, zamykanej na klucz, plombowanej, zlokalizowanej w pomieszczeniu.

System rozdziału energii dla pomieszczenia (pom. nr 4/34) zorganizować w oparciu o nowo wybudowaną (zgodną z normą PN-EN 61439) rozdzielnicę „R-SN” zasiloną za pomocą kabla N2XH-J 5x6mm² z rozdzielnicą korytarzowej. Doprowadzone z w/w rozdzielnic obwody dla potrzeb zasilenia posadowionych w szafach teleinformatycznych odbiorów należy zabezpieczyć zabezpieczeniami wynikającymi z wykonanego projektu wykonawczego. Doprowadzone z w/w rozdzielnic obwody dla potrzeb zasilenia rozdzielnic wewnętrznej „R-S” należy zabezpieczyć i wprowadzić na teren pomieszczenia przez filtry pasywne separacyjne typ PESF-L201A1-06/PESF-L201A1-10/ PESF-L201A1-16 zamontowane w skrzynce SRF zlokalizowanej w pomieszczeniu obok.

Skrzynkę z filtrami należy poprawnie wykonać i zamontować, celem uniknięcia przenikania elektromagnetycznego (niekontrolowanej emisji ujawniającej). Nowo wybudowaną wewnętrzną rozdzielnicę „R-S” należy zlokalizować na terenie pomieszczenia serwerowni objętego systemem ochrony technicznej (opisanego w dalszej części opracowania). Wszystkie zamontowane wewnątrz rozdzielniczy elementy należy uziemić i połączyć do wspólnej listwy uziemiającej, znajdującej się wewnątrz rozdzielniczy, przewodem miedzianym uziemiającym linką min.Cu10mm. Lokalizację montażu rozdzielnic „R-S”, „R-SN” i skrzynki SRF pokazano na rysunku nr A5 (A5-Koncepcja rozwiązania –zabezpieczenia fizyczne i techniczne. Zwiększenie zabezpieczeń technicznych i fizycznych). Na etapie realizacji zadania zweryfikować ilość opraw oświetleniowych dedykowanych do pomieszczeń (pom. nr 4/34, 4/34.1).

Ochrona elektromagnetyczna.

Ochrona elektromagnetyczna zapewniona zostanie poprzez zespół przedsięwzięć natury technicznej i organizacyjnej (ekranowanie przegrody budowlanej, filtrację obwodów zasilających, separację przestrzenną, prawidłowe uziemienie) zapewniających obniżenie poziomów sygnałów emisji ujawniającej do wartości praktycznie uniemożliwiających prowadzenie infiltracji elektromagnetycznej, prawidłowe wykonanie instalacji elektrycznej i teletechnicznej. Jak również poprzez wyznaczenie strefy ochronnej, w której podejmowane będą działania operacyjne o charakterze specjalnym przeznaczone do wymiany informacji niejawnych/wrażliwych biznesowo.

Ochrona bezpieczeństwa emisji – uziom „RED”.

W celu zabezpieczenia personelu przed porażeniem prądem elektrycznym oraz przed zniszczeniem instalacji elektrycznych i urządzeń aktywnych, w których będą przetwarzane informacje biznesowe oraz przed potencjalną elektromagnetyczną emisją ujawniającą, należy dla pomieszczenia serwerowni (pom. nr 4/3) wykonać uziemienie bezpieczeństwa emisji. Podstawową ochronę instalacji uziemienia bezpieczeństwa emisji należy zapewnić przez prawidłowe wykonanie instalacji uziemiającej o impedancji uziemienia nie wyższej niż 5 Ohm przy częstotliwości 100kHz. Główna szyna uziemiająca uziemienia budynkowego – ochronnego (ST/Zn 25x4) zlokalizowana będzie na terenie jednostki organizacyjnej w pomieszczeniu technicznym, chronionym (pom.nr 1), stąd może być traktowana, jako uziemienie bezpieczeństwa emisji, nie zachodzi konieczność wykonania niezależnego uziomu bezpieczeństwa emisji. Punkt przyłączenia dedykowanego uziomu bezpieczeństwa emisji do szyny (ST/Zn25x4) należy wykonać w skrzynce metalowej zamykanej na klucz i doprowadzić do szyny „RED” zlokalizowanej w skrzynce z filtrami SRF z zastosowaniem czerwonej linki (lub linki żółto-zielonej zakończonej na długości 15cm koszulką termokurczliwą w kolorze czerwonym) 50mm² izolowanej na całej długości w osłonie metalowej (rura stalowa sztywna lub giętka) zachowując ochronę fizyczną dla prowadzonego uziomu bezpieczeństwa emisji. Przyłącze uziomu bezpieczeństwa emisji musi zostać objęte pełną kontrolą z pełną rozliczalnością wejść/wyjść, zalecany monitoring wizyjny zgodnie z wytycznymi dokumentów odniesienia.

Instalacja wentylacji mechanicznej i klimatyzacji

W celu zapewnienia komfortu chłodu do przedmiotowych pomieszczeń (pom. nr 4/15, 4/16, 4/17) zamontować w instalację klimatyzacyjną z jednostkami ściennymi po 1,5-2kW ASYG07KMCE chłodu każde

pomieszczenie. Agregat typu multisplit o mocy chłodniczej 4,5kW AOYG18KBTA3 należy zamontować na dachu bezpośrednio nad tymi pomieszczeniami. Instalacja freonowa doprowadzona będzie poprzez istniejące zamknięte kominki na dachu nad tymi pomieszczeniami. W pomieszczeniu (pom. nr 4/21) na terenie Sali konferencyjnej wykonać instalację klimatyzacyjną z jednostką ścienną. Agregat o mocy chłodniczej 3,5kW AOYG12KMCC firmy Fujitsu należy zamontować na dachu bezpośrednio nad tymi pomieszczeniami. Instalacja freonowa doprowadzona będzie poprzez istniejące zamknięte kominki na dachu nad tymi pomieszczeniami. Identyczną jednostkę zamontować w pomieszczeniu (pom. nr 4/32) jej agregat zostanie posadowiony na dachu. Pomieszczenie serwerowni (pom. nr 4/34) wyposażać w instalację klimatyzacyjną z dwiema jednostkami ściennymi po 3,5kW chłodu typu split z agregatami o mocy chłodniczej 3,5kW AOYG12KMCC firmy Fujitsu pracujące w systemie redundantnym przeznaczonych do pracy całorocznej. Instalację freonową doprowadzić poprzez istniejący zamknięty komin na dachu nad tym pomieszczeniem. Przewody na przejściu przez dach pomieszczenia zabezpieczyć filtrami falowodowymi. Na przewodach z czynnikiem chłodniczym wykonać separację Cu/poliamid/Cu. Pomieszczenie serwerowni (pom. nr 4/34) doposażyć w instalację wentylacyjną nawiewno- wyciągową N/W=60m³/h wykorzystując istniejącą instalację wentylacji mechanicznej w tej strefie. Wszystkie jednostki klimatyzacyjne należy zasilć kablem N2XH-J 3x2,5mm² z rozdzielnic korytarzowej odpowiednio ją doposażając. Kanały wentylacji na granicy przegrody budowlanej stref ochronnych III/II należy doposażyć w kratki stalowe o oczkach 10x10mm. Lokalizacje punktów zasilń jednostek klimatyzacyjnych pokazano na rysunku nr A5 (A5-Koncepcja rozwiązania –zabezpieczenia fizyczne i techniczne).

Instalacja gniazd napięcia 230V/AC, gniazd instalacji teletechnicznych.

Instalację nowych gniazd wtykowych 230V/AC na terenie pomieszczeń (pom. nr 4/32, i pom. nr 4/34) należy wykonać z użyciem gniazd natynkowych 1-fazowych podwójnych podzielonych na niezależne obwody oraz przewodem N2XH-J 3x2,5mm². Zgodnie ze standardem budynkowym gniazda w dedykowanym pomieszczeniach montować na wysokości 20cm od podłoża. Na teren przedmiotowych pomieszczeń do nowych rozdzielnic „T-T” zlokalizowanej w pom. nr.4/32 prowadzić zasilanie z istniejących tablic korytarzowych kablem N2XH-J 5x6mm² nad sufitem. Do rozdzielnic „R-SN” zlokalizowanej w pomieszczeniu nr 4/34 prowadzić zasilanie dwutorowe z istniejących tablic korytarzowych kablem N2XH-J 5x6mm² nad sufitem celem zasilenia serwerów dwu zasilaczowych. Na wszystkich obwodach należy umieścić opisy dotyczące numeru oraz rodzaju obwodu. W pomieszczeniu serwerowni (pom. nr 4/34) w każdej z dwóch szaf rack zamontować jedną jednostkę UPS – model RT-3K, w trzeciej gdzie będą zamontowane serwery dwie jednostki UPS – model RT-3K celem podtrzymania napięciem gwarantowanym sprzętu teleinformatycznego, jednostkę UPS model RT-1K zamontować również w szafce rack w pomieszczeniu (pom. nr 4/34.1) celem podtrzymania zasilania depozytorów skrytkowych w przypadku utraty zasilania podstawowego. Lokalizacje koniecznych do zainstalowania gniazd wtykowych 230V/AC pokazano na rysunku nr A5 (A5-Koncepcja rozwiązania –zabezpieczenia fizyczne i techniczne).

Instalacja oświetlenia.

W modernizowanych pomieszczeniach należy wykonać instalację oświetleniową, zamontować oprawy LED niskoemisyjne, energooszczędne oraz oprawy awaryjne wyposażone w moduł awaryjny zapewniający jej pracę po zaniku napięcia przez okres min. 1 godziny typu 1xLED-AW2. Instalację elektryczną zasilającą poszczególne obwody oświetleniowe należy rozproszyc z uwzględnieniem podziału topologii ich umiejscowienia. Instalację oświetleniową dla dedykowanych powstałych pomieszczeń należy zasilić z rozdzielniczy wewnętrznej korytarzowej.

System teleinformatyczny RED

Na terenie przedmiotowych pomieszczeń należy wdrożyć system teleinformatyczny oparty o terminale o zwiększonym zabezpieczeniu technicznym zgodnym z SDIP-27 dla level B, w których będą przetwarzane informacje niejawne klauzuli krajowej „POUFNE” włącznie. Serwer zarządzający i rozwiązania sieciowe (switchy) klasy CE należy zamontować na terenie serwerowni objętej ochroną elektromagnetyczną. Autonomiczne stanowisko o zwiększonym zabezpieczeniu technicznym zgodnym z SDIP-27 dla level A należy zamontować na terenie Kancelarii Tajnej, na którym będą przetwarzane informacje niejawne o klauzuli krajowej „ŚCIŚLE TAJNE” włącznie. Wdrożone rozwiązania na terenie przedmiotowych pomieszczeń, które będzie stanowiło Strefę Ochronną, ustanowioną przez Zleceniodawcę w ramach przedsięwzięć organizacyjno-technicznych w zakresie ochrony informacji niejawnych, umożliwią zainstalowanie systemu teleinformatycznego uwzględniając zalecenia określone w dokumentach ustawowych i zaleceniach ABW w zakresie ochrony informacji niejawnych i bezpieczeństwa teleinformatycznego. W przypadku wdrożenia systemu, zastosowane w tym systemie teleinformatycznym środki ochrony elektromagnetycznej (środki zabezpieczenia technicznego sprzętu- systemu) będą uzależnione od klauzuli przetwarzanych informacji niejawnych oraz tzw. Sprzętowej Strefy Ochrony Elektromagnetycznej, która może (w przypadku wystąpienia Inwestora z wnioskiem WS-01) zostać określona przez DBTI ABW i potwierdzona stosownym Certyfikatem Ochrony Elektromagnetycznej celem zweryfikowania poprawności doboru rozwiązań systemowych o zwiększonym zabezpieczeniu technicznym. Wymagana min. 24 miesięczna gwarancja producenta.




Konfiguracja sprzętu technicznego systemu teleinformatycznego – stanowisk pracy:

URZĄDZENIE WIELOFUNKCYJNE A4 SDIP-27 LEVEL B: SIL788 - MFP405C (na bazie Xerox VersaLink C405V_DN)		
Funkcje	Kopia, Druk, Skanowanie	
Rodzaj	Laser, kolor	
Prędkość kopiowania/drukowania	Do 35 str./min.	
Maksymalne dopuszczalne obciążenie	Do 85 000 stron miesięcznie	
Porty	USB (D-Sub 9 pin)	
Automatyczny duplex	Tak	
Sieć	100 Mbps F/O ST	
Pamięć drukowania	2 GB	



Podawanie papieru	Taca wielozadaniowa: 150 arkuszy Taca 1: 550 arkuszy Automatyczny odwracający podajnik dokumentów: 50 arkuszy	(zdjęcie poglądowe)
Maksymalny format	A4	
Języki opisu strony	PostScript 3, HP-GL, JPEG, PCL 5e, PCL 6, PDF, TIFF, XPS	
Rozdzielczość	Kopiowanie: 600 x 600 x 8 dpi (ulepszone) Drukowanie: 600 x 600 dpi	
Kontrola wydruku	Czytnik Smart Card	

Zapotrzebowanie 2 sztuki**TERMINAL ZERO CLIENT SDIP-27 LEVEL B: SIL788- TCC (na bazie ClearCube CD7924)**

Procesor	Teradici TERA2321 PCoIP	 
Pamięć	512 MB	
Dysk	Brak	
Interfejsy	<ul style="list-style-type: none"> 2 x DVI 4 x USB (typ A) 1 x USB myszy (typ A) 1 x USB klawiatury (typ A) 2 x audio jack 3.5 mm 1x czytnik kart SmartCard 	
Interfejs sieciowy	Port SFP	
Karta grafiki	Obsługiwana rozdzielczość: <ul style="list-style-type: none"> 2560 x 1600 pojedynczy 1920 x 1200 podwójny 	 (zdjęcia poglądowe)
Wypożyczenie	<ul style="list-style-type: none"> 1x klawiatura USB w układzie QWERTY SIL788 - KL105; 1x mysz dwuprzyciskowa z rolką do przewijania SIL - MO; 1x moduł SFP 1Gbps LC przewody zasilające i sygnałowe niezbędne do prawidłowej pracy zestawu. 	


MONITOR 24": SIL788 - M2410 (na bazie EIZO ColorEdge CS2410)

Przekątna ekranu	24,1"
Matryca	IPS
Kąty widzenia	Poziomo 178°, pionowo 178°
Rozdzielczość	1920 x 1200 (16:10)
Rozmiar piksela	0.270 mm x 0.270 mm
Jasność	300 cd/m²
Czas reakcji	14 ms (gray-to-gray)
Złącze wejściowe	DVI
Wypożyczenie	Przewód zasilający 2m Przewód sygnałowy DVI-DVI 2m


Zapotrzebowanie 20 sztuk

Konfiguracja sprzętu technicznego autonomicznego stanowiska pracy:

STACJA ROBOCZA SDIP-27 LEVEL A: SIL720 - T4 (na bazie HP)	
Procesor	Intel Core i5
RAM	16 GB DDR5 (możliwość rozbudowy do 128 GB)
Dysk twardy	11 x 500 GB SSD w wyjmowanej szufladzie, dwa miejsca na dysk w stacji roboczej
Napęd optyczny	DVD+/-RW
Porty	1 DisplayPort monitor 1 USB (D-Sub 9 pin) klawiatura 1 USB (D-Sub 9 pin) mysz 2 USB (D-Sub 9 pin) 2 F/O ST (1 para) sieć Panel portów USB: 2 x 3.0 typ A zainstalowany w zatoce 5,25" za drzwiczkami obudowy
Grafika	Zintegrowana
Karta dźwiękowa	Zintegrowana
Karta sieciowa	100 Mbps
Klawiatura	Klawiatura USB SIL720 - KL105
Mysz	Mysz USB dwuprzyciskowa z rolką do przewijania SIL - MO + podkładka
System operacyjny	5 x Windows 11 Pro 64 Bit PL + komplet oprogramowania ze sterownikami do systemu operacyjnego Microsoft Windows 11, możliwość downgrade z Windows 11 do Windows 10
Oprogramowanie	5 x Microsoft ESD Office Professional 2021
MONITOR 24": SIL720 - M2410 (na bazie EIZO ColorEdge CS2410)	
Przekątna ekranu	24,1"
Matryca	IPS
Rozdzielczość	1920 x 1200 (16:10)
Rozmiar piksela	0.270 mm x 0.270 mm
Jasność	300 cd/m²
Czas reakcji	14 ms (gray-to-gray)
Złącze wejściowe	DisplayPort



(zdjęcie poglądowe)

DRUKARKA KOLOROWA A4 SDIP-27 LEVEL A: SIL720 - D454 (na bazie HP LaserJet Pro 400 Color M454dn)		
Rodzaj	Laserowa kolorowa	 <p>(zdjęcie poglądowe)</p>
Procesor	1200 MHz	
Pamięć	256 MB NAND Flash + 512 MB DRAM	
Dysk twardy	Brak	
Interfejs	Port USB (D-sub 9 pin)	
Rozdzielczość druku w kolorze i w czerni	600 x 600 dpi (maks. 38400 x 600 dpi)	

Szybkość druku	A4 - do 27 str./min.
Duplex	Tak
Normatywny cykl pracy (miesięcznie, format A4)	Do 50 000 stron
Podawanie papieru	Podajnik 1: uniwersalny na 50 arkuszy Podajnik 2: na 250 arkuszy
Język drukarki	HP PCL 6, HP PCL 5c, emulacja HP Postscript level 3, PDF, URF, PWG Raster
Maksymalny format	A4

Zapotrzebowanie 1 kpl.

Na potrzeby realizacji zadania należy wybudować system okablowania strukturalnego zapewniający niezawodną i wydajną pracę warstwy fizycznej sieci teleinformatycznej z zagwarantowanym zapasem parametrów transmisyjnych. W celu zapewnienia wysokich wymogów parametrów jakościowych i wydajnościowych należy wdrożyć wszystkie komponenty stanowiące system okablowania fabrycznie nowy, pochodzący od jednego producenta lub czołowych producentów zapewniając 25 letnią gwarancję na system okablowania. Instalację wykonać w oparciu o normę ISO 14763-3:2014 z wykorzystaniem kabli wielomodowych OM4 z zakończeniem połączeń na złączach LC i adapterze duplex. Główny punkt dystrybucyjny będzie zlokalizowany w serwerowni w pomieszczeniu (pom. nr 4/34) gdzie zostaną posadowione trzy perforowane szafy rack 42U 800x1000mm. Okablowanie światłowodowe LAN pomiędzy punktami pracy terminalami wykonać przy użyciu kabla OM4 50/125um 4J.

Zakończenie kabli światłowodowych wykonać pigtailami LC/PC w adapterach Duplex zakończonych relacją w puszkach abonenckich natynkowych zlokalizowanych w pomieszczeniach pracy na terenie strefy ochronnej I. Minimalna ilość adapterów LC duplex – 2 sztuki. Powyższe okablowanie wykonać metoda spawania pigtaila do kabli dosyłowych, końce każdej relacji rozszyc zgodnie z sekwencją (włókno 1- czerwone, włókno - 2 zielone). Zalecany montaż zakończeń połączeń światłowodowych strony szaf dystrybucyjny w dedykowanych przełącznicach światłowodowych, na kasetach spawów 3 min 12 włóknowych. Elementy toru kabla połączone w sposób trwały z przełącznicą zapewniające mechaniczne zabezpieczenia światłowodu. Rozszycie kabla wg standardu połączeń oraz przyjętej kolorystyce włókien. Na etapie projektu wykonawczego w Uzgodnieniu z Użytkownikiem rozważyć możliwość wdrożenia rozwiązania z użyciem kabli jednomodowych OS2 9/125um 4J. Dla celów połączeń stanowiska teleinformatycznego Krypton K2 wykonać niezależną odseparowaną sieć światłowodową w realizacji pomieszczenie serwerowni (pom. nr 4/34) a pomieszczenie (pom. nr 4.14.1). Okablowanie łącznikowe między serwerownią piętrową a serwerownią EMC wykonać na bazie kabli OM4 12J.

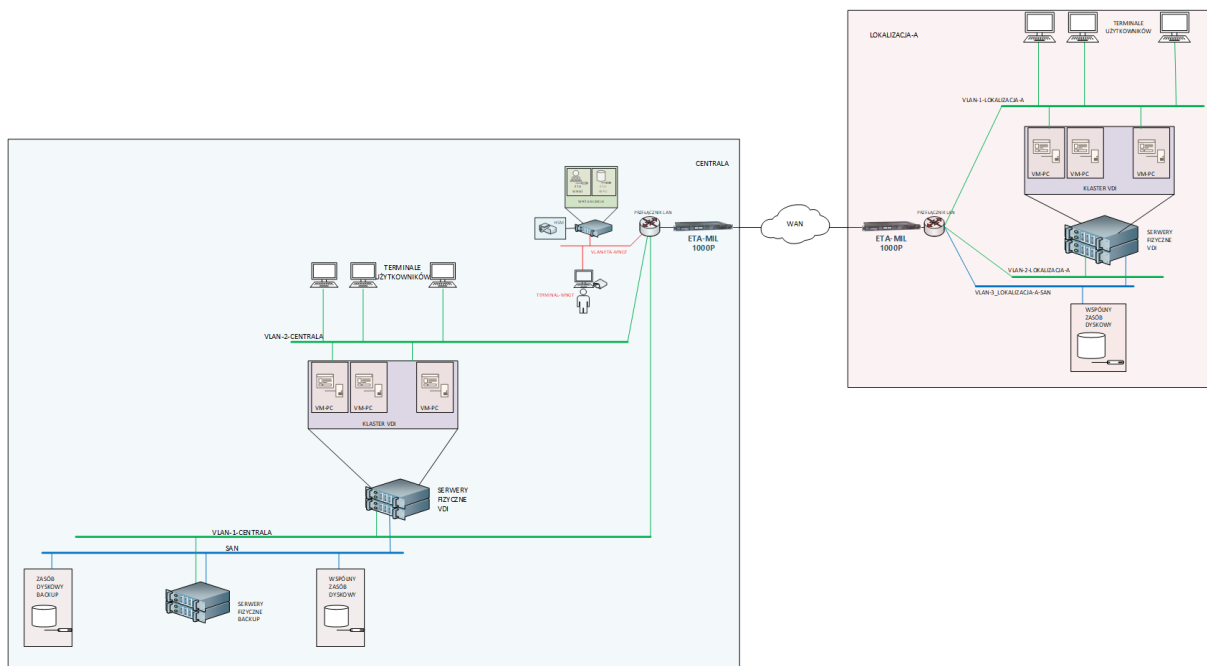
Po wykonaniu instalacji okablowania strukturalnego Wykonawca przeprowadzi odpowiednie testy i pomiary poświadczające, że okablowanie spełnia standardy swojej kategorii, zgodnie z wymogami zawartymi w normach i wymaganiach koniecznych do wystawienia certyfikatu gwarancyjnego przez producenta okablowania. Łącznie z pomiarami należy dostarczyć certyfikat potwierdzający ważną kalibrację przyrządu pomiarowego. Wyniki pomiarów należy udokumentować i przekazać Użytkownikowi wraz dokumentacją powykonawczą i gwarancją. Całe okablowanie światłowodowe ma spełniać wymogi normy ISO 14763:3-2014 po dokonaniu

sprawdzenia tłumienności torów. Wszystkie testy muszą być zakończone wynikiem pozytywny. Do certyfikacji i udzielenia gwarancji należy wykonać pomiary na zgodność z normami ISO 14763:3-2014. W przypadku sieci światłowodowej miernikiem min DSX-2 5000 z przystawkami OLTS. Wymagana jest aktualna kalibracja miernika oraz przystawek światłowodowych OLTS. Lokalizacje koniecznych do zainstalowania gniazd abonenckich pokazano na rysunku nr A5 ((A5-Koncepcja rozwiązania –zabezpieczenia fizyczne i techniczne).

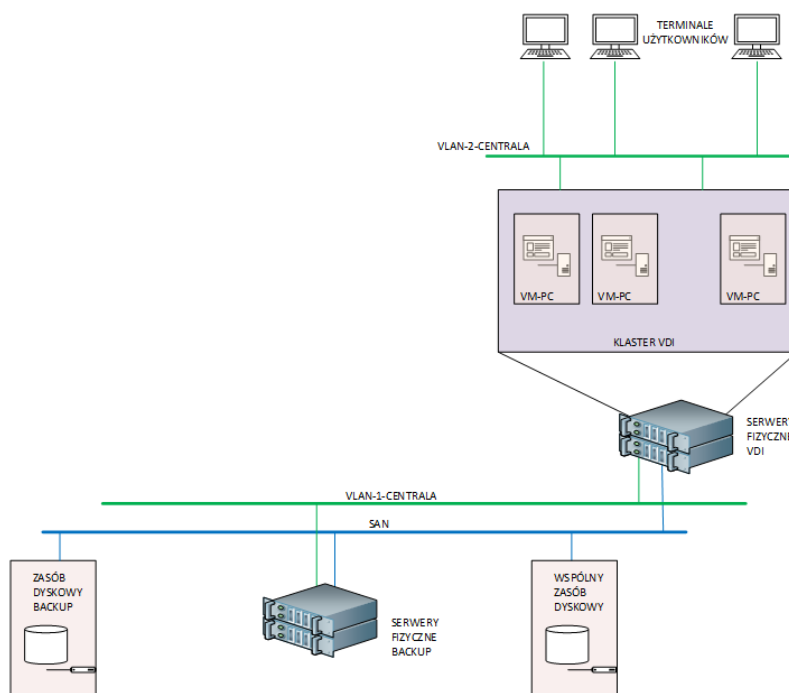
Architektura systemu

Architektura systemu zakłada realizację połączenia sieci z tworzonymi wydziałami zewnętrznymi zgodnie z założeniami przedstawionymi na schemacie poniżej. Elementy systemu powinny przewidywać możliwość rozbudowy usług sieciowych w zakresie funkcjonalności związanych z udostępnianiem usług aplikacyjnych, przetwarzaniem danych, wykonywaniem kopii bezpieczeństwa, integracją oraz narzędzi zarządzania domeną. Połączenia pomiędzy lokalizacjami są nawiązywane za pomocą systemu szyfratorów zapewniającego odpowiedni poziom bezpieczeństwa informacji i pozwalający na uzyskanie świadectwa akredytacji bezpieczeństwa teleinformatycznego (w trybie art. 48 Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych).

Przykładowym rozwiązaniem zapewniającym realizację połączeń pomiędzy centralą IWSW a zamiejscowymi IWSW jest zabezpieczenie przy pomocy szyfratorów ETA-MIL 1000P. W każdej lokalizacji należy zainstalować zostanie jeden szyfrator. Możliwe jest również zainstalowanie dwóch szyfratorów w lokalizacji głównej (środowisko zarządzania) i po jednym szyfratorze w lokalizacji zamiejscowej. Szyfrator powinien zapewnić bezpieczną łączność w rozległych, niezauważalnych sieciach IP (WAN), umożliwiając tworzenie chronionych wirtualnych sieci prywatnych (VPN). Uwierzytelnienie sesji kryptograficznych pomiędzy urządzeniami będzie odbywać się z wykorzystaniem infrastruktury PKI i certyfikatów X.509. Urządzenia szyfrujące powinny być zgodne z normą SDIP-27/A oraz przeznaczone do przetwarzania informacji niejawnych o klauzulach do: "POUFNE" włącznie. Dodatkowo urządzenia szyfrujące powinny posiadać wbudowany firewall i mechanizmy HA oraz możliwość definiowania VLAN-ów i tras statycznych. Ponadto urządzenia szyfrujące muszą być wyposażone w interfejsy światłowodowe SFP. W ramach wskazanego rozwiązania, system PKI składał się będzie z następujących komponentów: Centaur CCK, Centaur PR, Baza danych, serwer FTP, LDAP. W ramach infrastruktury PKI będą generowane klucze kryptograficzne do ochrony poufności i integralności kanałów transmisji danych. Komponenty systemu PKI oraz aplikacja do zarządzania szyfratorami ETA-MIL MGMT zostaną zainstalowane na serwerze usług w środowisku zarządzania. Centaur PR komponent punktu rejestracji zainstalowany zostanie na stacji roboczej operatora systemu. Stacja robocza komponentu szyfratora będzie zlokalizowana na terenie serwerowni i wyposażona w czytnik kart chipowych, aby możliwe było personalizowanie kart kryptograficznych dla urządzeń szyfrujących. Dla podniesienia bezpieczeństwa infrastruktury PKI wykorzystane zostanie urządzenie HSM. W urządzeniu HSM przechowywane będą klucze urzędu infrastruktury PKI. Dopuszcza się zastosowanie innych rozwiązań kryptograficznych, nie gorszych funkcjonalnie niż opisane wyżej, pozwalających na uzyskanie świadectwa akredytacji bezpieczeństwa teleinformatycznego (w trybie art. 48 Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych).



Użytkownicy systemu będą uzyskiwać dostęp poprzez przeglądarkę uruchomioną na terminalu. Terminalem jest urządzenie typu „zero-client” który nie posiada dysku – wszystkie niezbędne zasoby umieszczone będą na serwerze centralnym. Dane użytkowników przechowywane będą na macierzy dyskowej. Za zabezpieczenie danych odpowiadać będzie system kopii zapasowych zlokalizowany w jednostce macierzystej. Zbudowany z serwera nadzorującego zadania backupowe, serwera media agent, repozytorium dyskowego opartego o nośniki NL-SAS dedykowanego do przechowywania danych. Docelowo planowane jest replikacja kopii bezpieczeństwa w lokalizacji wyniesionej.



Serwery dostępne - VDI

Wymaga się dostarczenia min. 2 serwerów o parametrach podanych poniżej w tabeli S2. Wymagana 36- miesięczna gwarancja producenta sprzętu.

Tabela S2.		
SERWERY VDI – sztuk 2		
Lp.	Nazwa elementu,	Wymagania szczegółowe
S2.1	Obudowa	Obudowa typu RACK 19 cali wraz z zestawem do zamontowania w szafie teleinformatycznej 19 cali umożliwiającym wysunięcie obudowy, o wysokości 1U, umożliwiająca instalację minimum 8 dysków HDD lub SSD w formie 2.5-in. SFF 12Gb SAS lub SATA wymiennych od przodu serwera (hot-swap) oraz umożliwiającą instalację redundantnego zasilacza (wszystkie zasilacze wymienne w trybie hot-swap).
S2.2	Płyta główna	Serwerowa płyta główna zapewniająca obsługę: <ul style="list-style-type: none"> – minimum dwóch fizycznych procesorów 64 bitowych, umożliwiającą zastosowanie technologii wirtualizacji, – minimum 32 sloty do obsługi pamięci DDR4 pracującej z częstotliwością co najmniej 4800 MHz, – możliwość wyposażenia serwera w minimum 8TB RAM, – łączna ilość możliwej do zainstalowania pamięci RDIMM oraz pamięci persistent memory powinna wynosić minimum 12TB, – umożliwia instalację minimum dwóch modułów M.2 lub instalację minimum dwóch kart SD z funkcjonalnością duplikacji zapisu (Mirror),
S2.3	Karta graficzna	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.
S2.4	Procesor	Minimum dwa procesory o parametrach nie gorszych niż: <ul style="list-style-type: none"> – liczba rdzeni: 10, częstotliwość taktowania zegara: min. 2.7GHz, – cache L2: min. 26MB, ilość kanałów pamięci: min. 8 – procesor powinien wspierać funkcjonalność dynamicznego i automatycznego zwiększenia wydajności serwera dla aplikacji poprzez zwiększenie częstotliwości taktowania rdzenia, – wyposażony w technologię wirtualizacji,
S2.5	Pamięć operacyjna	Zainstalowane nie mniej niż 512GB RAM taktowane zegarem nie mniejszym niż 4800 MHz. Wspierane zabezpieczenia pamięci RAM: ECC, SDDC, ADDDC
S2.6	Dyski	Minimum 2 szt. dysków dedykowanych dla hypervisora wirtualizacyjnego typu M.2 lub SSD o pojemności min. 800 GB każdy, skonfigurowane w RAID1. Nie dopuszcza się rozwiązania, w którym dyski M.2/SSD zajmują którykolwiek ze slotów PCIe wymienionych w sekcji Dodatkowe sloty I/O.
S2.8	Zasilanie	Co najmniej 2 szt. wysokiej sprawności (certyfikat minimum Titanium) zasilacze prądu zmiennego umożliwiające pracę z sieci o napięciu 230V wraz z kablami umożliwiającymi podłączenie do gniazd elektrycznych typu E oraz kablami umożliwiającymi podłączenie do komputerowych gniazd elektrycznych typu IEC, umożliwiające stabilną i bezprzerwową pracę całej platformy serwerowej w maksymalnej przewidzianej przez producenta konfiguracji przy połowie działających zasilaczy z ogólnej liczby zainstalowanych. Wymiana zasilaczy musi odbywać się bez konieczności wyłączenia urządzenia.
S2.9	Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
S2.10	Interfejsy sieciowe	<ul style="list-style-type: none"> – min. 4 szt. portów Ethernet o przepustowości 1 Gbps typu Base-T w postaci portów zintegrowanych z płytą główną (dopuszcza się rozwiązania w postaci kart rozszerzeń) – min. 1 szt. co najmniej dwuportowa karta FC PCI-E HBA (Host Bust Adapter) z modułami 32Gb FC, umożliwiającymi podłączenie zewnętrznej macierzy/switcha SAN interfejsem FC o przepustowości 32Gb, – min. 1 szt. co najmniej dwuportowa, karta sieciowa 10 Gbps (SFP+) wraz z wkładkami (modułami) SFP+ – jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
S2.11	Inne interfejsy	2 bezpośrednio udostępnione zewnętrzne porty USB 3.0, 1 bezpośrednio udostępniony port VGA.
S2.12	Sloty rozszerzeń	min. 3 sloty PCI-EXPRESS min. generacji 3 w tym min. jedno gniazdo pozwalające na instalację karty pełnej wysokości.

S2.13	Zarządzanie	<p>Serwer wyposażony w zintegrowany z płytą główną, moduł zdalnego zarządzania (konsoli) zapewniający (dla indywidualnego serwera):</p> <ul style="list-style-type: none"> – Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: cpu, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna, – Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, użycie cpu, użycie pamięci oraz komponentów I/O, – Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów, – Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń, – Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3, – Update systemowego firmware, – Monitoring i możliwość ograniczenia poboru prądu, zdalne włączanie/wyłączanie/restart, – Zapis video zdalnych sesji, podmontowanie lokalnych mediów z wykorzystaniem Java client, – Przekierowanie konsoli szeregowej przez IPMI, zrzut ekranu w momencie zawieszenia systemu, – Możliwość przejęcia zdalnego ekranu, – Możliwość zdalnej instalacji systemu operacyjnego, – Alerty Syslog, – Przekierowanie konsoli szeregowej przez SSH, – Wyświetlanie danych aktualnych i historycznych dla użycia energii oraz temperatury serwera, – Możliwość mapowania obrazów ISO z lokalnego dysku operatora, – Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS, – Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę, – wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API, <p>Wymaga się zapewnienia możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z kartą zarządzającą) bez możliwości uzyskania jakiegokolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.</p> <p>Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające:</p> <ul style="list-style-type: none"> – zarządzanie infrastrukturą serwerów i storage bez udziału dedykowanego agenta, – przedstawianie graficznej reprezentacji zarządzanych urządzeń, – możliwość skalowania do minimum 1000 urządzeń, – obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2, – wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych, – udostępnianie szybkiego podglądu stanu środowiska, – udostępnianie podsumowania stanu dla każdego urządzenia, – tworzenie alertów przy zmianie stanu urządzenia, – monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, – konsola zarządzania oparta o HTML 5, – dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, – automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja, – możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania, – tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsolę albo kopiowanie konfiguracji z już zaimplementowanych urządzeń), – dla określonych zdarzeń wraz z przesyłem plików diagnostycznych.
S2.14	Mechanizmy bezpieczeństwa	Zainstalowany czujnik otwarcia obudowy zintegrowany z modulem zarządzania serwerem, hasło włączania, hasło administratora, moduł TPM. Zainstalowany przedni panel zamykany na klucz.
S2.15	Wspierane oprogramowanie	Microsoft Windows Server 2019, 2022, Red Hat Enterprise Linux 7, 8, 9 SUSE Linux Enterprise Server 12 oraz 15, VMware vSphere (ESXi) 6, 7, Ubuntu 18, 20, 22. Serwer musi wspierać oprogramowanie do wirtualizacji będące przedmiotem niniejszego postępowania.
S2.16	Inne	Wysuwane szyny montażowe do szaf typu rack 19 cali wraz z ramieniem do zarządzania kablami Wykonawca zapewnia kable połączeniowe FC oraz LAN umożliwiające przyłączenie serwerów do switchy SAN/LAN. Zainstalowany system operacyjny MS Windows Server 2022 Standard, licencja zgodna z polityką Microsoft.

Macierz dyskowa – produkcyjna.

Jako urządzenie udostępniające przestrzeń dyskową rekomendujemy wysokowydajną macierz dyskową klasy All-Flash, opartą o szybkie dyski SSD NVMe, gwarantujące dużą wydajność i niskie czasy odpowiedzi. Wykorzystanie tej najnowocześniejszej obecnie technologii pozwoli zapewnić wydajną pracę systemu przez wieloletni okres eksploatacji, zapewniając zarówno przestrzeń wystarczającą do obsługi potrzeb systemu, jak i możliwość ewentualnej rozbudowy w razie potrzeby. Przestrzeń dyskową macierzy należy zabudować w oparciu dyski 15TB NVMe pracujące z zabezpieczeniem RAID5. Pojemność systemu dyskowego będzie wynosić 82TiB. Przestrzeń dyskowa zostanie zaprezentowana do serwerów za pomocą redundantnej sieci SAN zbudowanej z dwóch przełączników Fibre Channel, w oparciu o przepustowość pojedynczego linku 32Gbps. Każdy serwer będzie widział zasoby dyskowe dwoma redundantnymi ścieżkami z włączanym mechanizmem warstw wielościeżkowych, pozwalającym na wykrycie awarii pojedynczej ścieżki i transparentnego przełączenia ruchu na ścieżkę aktywną. Wymagana 36- min. miesięczna gwarancja producenta sprzętu.

Tabela M.		
Macierz – 1 sztuka		
Lp.	Nazwa elementu, parametru lub cechy	Wymagania szczegółowe
M.1	Obudowa	<ul style="list-style-type: none"> – do instalacji w standardowej szafie rack 19" dostarczona wraz z szynami montażowymi oraz innymi elementami niezbędnymi do montażu. – musi zawierać układ nadmiarowy dla modułów zasilania i chłodzenia umożliwiający wymianę tych elementów w razie awarii bez konieczności wyłączania macierzy. – powinna posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii macierzy. – zasilanie jednofazowe. – zajętość w szafie serwerowej nie więcej 2U.
M.2	Architektura systemu dyskowego	<ul style="list-style-type: none"> – Oferowane urządzenie musi się składać z pojedynczej macierzy dyskowej. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych połączonych przełącznikami SAN, LAN lub witalizatorem w sieci SAN. – Urządzenie musi się składać z co najmniej dwóch kontrolerów pracujących w trybie symetrycznym active/active wyposażonych łącznie w minimum 24 rdzenie Intel lub AMD. – Konstrukcja macierzy powinna zapewnić sprzętowe rozłożenie operacji I/O pomiędzy kontrolerami macierzy. Operacje I/O muszą być kierowane równomiernie (z tą samą wydajnością) przez porty zewnętrzne dwóch kontrolerów, do których będą podłączone serwery. Kontrolery muszą pracować w trybie wysokiej dostępności, w przypadku awarii jednego kontrolera drugi automatycznie przejmie jego funkcję. – Oferowana macierz musi obsługiwać zarówno dyski flash NVMe lub flash SSD jak i dyski mechaniczne. – Kontrolery dyskowe, obsługujące dyski SAS i dyski mechaniczne powinny wykorzystywać interfejs co najmniej SAS 12Gbps.
M.3	Redundancja	<ul style="list-style-type: none"> – Oferowaną macierz musi cechować brak pojedynczego punktu awarii. Wszystkie krytyczne komponenty muszą być zdublowane. – Uszkodzenie jednego z podzespołów nie może spowodować przerw w pracy urządzenia. Wszystkie komponenty muszą być przystosowane do wymiany podczas pracy macierzy.
M.4	Pamięć cache	<ul style="list-style-type: none"> – Macierz musi być wyposażona w minimum 384 GB pamięci cache per kontroler. – Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM (nie dopuszcza się stosowania dysków SSD lub kart pamięci jako pamięci cache). – Odporność na awarię pamięci cache, wszystkie zapisy do pamięci cache muszą być przechowywane w dwóch kopiach. W przypadku awarii zasilania macierz musi posiadać możliwość automatycznego zrzucenia danych z pamięci cache na dedykowaną przestrzeń dyskową.

M.5	Pojemność użytkowa TiB (base2 1kB=1024B)	<ul style="list-style-type: none"> Macierz dyskowa musi udostępniać minimum 82 TiB przestrzeni użytkowej netto (base2) w konfiguracji RAID 5. Przestrzeń musi być zbudowana w oparciu o wydajne dyski SSD NVMe. Macierz dyskowa wyposażona w 1 globalny dysk zapasowy hot-spare lub rekomendowaną przez producenta nadmiarową przestrzeń dyskową Wymagana przestrzeń dyskowa musi zostać dostarczona bez uwzględnienia mechanizmów redukcji danych takich jak kompresja i de-duplikacja. Musi istnieć możliwość instalacji w macierzy jednocześnie dysków flash, jak i dysków mechanicznych (bez wykorzystania funkcjonalności wirtualizacji zewnętrznych macierzy). Macierz musi mieć możliwość rozbudowy do 240 wewnętrznych dysków SAS. Nie dopuszcza się stosowania dodatkowych zewnętrznych kontrolerów macierzy dyskowych w celu rozbudowy oferowanej macierzy.
M.6	Interfejsy	<ul style="list-style-type: none"> Macierz musi posiadać 8 interfejsów FC 32 Gbps SFP+. Macierz musi mieć możliwość rozbudowy o interfejsy iSCSI 10Gb/s. Macierz musi mieć możliwość rozbudowy o interfejsy FC o prędkościach 16, 32 Gbps. Macierz musi posiadać dedykowane 2 porty do zarządzania przez sieć Ethernet 1 Gbps.
M.7	Półki dyskowe	<ul style="list-style-type: none"> Macierz musi mieć możliwość instalacji w półkach dyskowych dysków typu NL-SAS, SAS, SSD. Półki dyskowe muszą umożliwiać wymianę uszkodzonych dysków twardych „na gorąco”.
M.8	Obsługiwane dyski	<ul style="list-style-type: none"> Macierz musi obsługiwać co najmniej dyski 2,5" oraz 3,5". Oferowany model macierzy musi wspierać co najmniej obsługę następujących typów dysków: a) NVMe SSD - 1.9TB, 3.8TB, 7.6TB, 15TB, 30TB. b) SSD - 1.9TB, 3.8TB, 7.6TB, 15TB, 30TB. c) SAS - 2.4TB d) NL-SAS - 6TB, 10TB, 14TB
M.9	Optymalizacja danych	<ul style="list-style-type: none"> Macierz musi posiadać mechanizmy redukcji danych przechowywanych na nośnikach Flash (NVMe SSD, SSD SAS) w oparciu o kompresję i deduplikację. Macierz musi posiadać funkcję optymalizacji wykorzystania dysków NVMe, SSD, SAS, NLSAS poprzez automatyczną migrację fragmentów woluminów na szybsze lub wolniejsze dyski w zależności od obciążenia tzw. tiering. Funkcja ta musi działać na 2 i 3 warstwach dyskowych. Zamawiający wymaga dostarczenia licencji na tę funkcję. Macierz musi posiadać funkcję migracji całych woluminów logicznych w obrębie dysków wewnętrznych macierzy jak i dysków zwirtualizowanych zainstalowanych w innych macierzach. Funkcja musi być realizowana bez zatrzymania aplikacji i musi być w pełni transparentna dla działających aplikacji na migrowanym woluminie. Zamawiający wymaga dostarczenia licencji na tę funkcję.
M.10	Poziomy RAID	<ul style="list-style-type: none"> Macierz musi obsługiwać następujące poziomy zabezpieczeń RAID-10, RAID-5, RAID-6 (lub równoważny, gwarantujący zabezpieczenie przez awarią dwóch dysków w grupie).
M.11	Monitoring	<ul style="list-style-type: none"> Macierz musi obsługiwać priorytety ruchu I/O tzw. Quality of Service. Zamawiający wymaga dostarczenia licencji na tę funkcję. Wymagane jest monitorowanie i raportowanie wydajności Macierzy, obejmujące również środowiska wirtualizacyjne (co najmniej Vmware). Wymagane jest zbieranie co najmniej następujących danych: a) wielkość przestrzeni dyskowej macierzy: całościowa, wolna, wykorzystana, b) czas dostępu do danych na wolumenach logicznych, c) wykorzystanie interfejsów do wykonywania kopii pomiędzy macierzami, d) czas odpowiedzi interfejsów do wykonywania kopii pomiędzy macierzami, e) wykorzystanie pamięci Cache, f) wykorzystanie dysków SSD lub NVMe, g) przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, woluminów logicznych, dysków oraz kontrolerów. Zbieranie danych wymienionych w punkcie a) do g) powyżej - co 15 minut lub w czasie krótszym niż 15 minut. Czas przechowywania danych wymienionych w punkcie a) do g) nie krócej niż 30 dni, przy czym po 7 dniach dane mogą zostać zagregowane. Możliwość eksportowania danych wymienionych w punkcie a) do g) w formacie tekstowym, csv, xls lub innym umożliwiającym ich odczyt przy użyciu programu Microsoft Excel. Maszyn wirtualnych: a) korelacja maszyn wirtualnych z wolumenami logicznymi macierzy, b) wydajność i czas odpowiedzi maszyn wirtualnych.
M.12	Thin provisioning	<ul style="list-style-type: none"> Macierz musi posiadać funkcję udostępniania zasobów dyskowych do hostów w trybie tzw. ThinProvisioning. Zamawiający wymaga dostarczenia licencji na tę funkcję. Macierz musi umożliwiać utworzenie wolumenu logicznego o rozmiarze co najmniej 256TB.

M.13	Zarządzanie przestrzenią dyskową	<ul style="list-style-type: none"> – Macierz musi umożliwiać zwiększenie pojemności woluminów logicznych w trybie bezprzerwowym. Zamawiający wymaga dostarczenia licencji na tę funkcję. – Macierz musi umożliwiać administratorowi funkcję wyboru wskazanych konkretnych pojedynczych fizycznych dysków do grup raid.
M.14	Zarządzanie macierzą	<ul style="list-style-type: none"> – Macierz musi posiadać interfejs graficzny oraz interfejs linii poleceń, umożliwiający tworzenie i obsługę skryptów. – Macierz powinna posiadać oprogramowanie do zarządzania, pozwalające na co najmniej: <ol style="list-style-type: none"> a) Tworzenie i nazywanie wolumenów logicznych LUN, b) Mapowanie wolumenów logicznych do serwerów wraz z możliwością konfigurowania zoningu w sieci SAN (wsparcie dla przełączników Cisco oraz Brocade), c) Monitorowanie wykorzystywanej przestrzeni, efektywnej i surowej (RAW) macierzy. – Zamawiający wymaga dostarczenia licencji na te funkcje.
M.15	Wewnętrzne kopie danych	<ul style="list-style-type: none"> – Macierz musi posiadać funkcję tworzenia wewnętrznych kopii danych opartych o: <ol style="list-style-type: none"> a) Klonowanie z ang. Clone. Możliwość wykonania kopii na inny rodzaj dysków i inny typ zabezpieczenia RAID, b) Migawkę z ang. Snapshot. – Zamawiający wymaga dostarczenia licencji na te funkcje.
M.16	Zewnętrzne kopie danych	<ul style="list-style-type: none"> – Macierz musi posiadać funkcje replikacji danych do drugiej macierzy tego samego typu w trybie synchronicznym i asynchronicznym. Możliwość uruchomienia obu trybów replikacji tj. replikacja synchroniczna i asynchroniczna w tym samym czasie. Musi istnieć wsparcie do definiowania grup konsystencji (z ang. Consistency Group) dla uruchomionych zadań replikowanych woluminów. – Zamawiający nie wymaga dostarczenia licencji na te funkcje.
M.17	Systemy operacyjne	<ul style="list-style-type: none"> – Macierz musi posiadać możliwość podłączenia wielu serwerów w trybie wysokiej dostępności, co najmniej dwoma ścieżkami. – Macierz musi wspierać LUN Mapping, LUN Masking. – Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, VMware, Linux, Solaris. – Macierz musi być certyfikowana w zakresie VMware Metro Storage Cluster.
M.18	Multipathing	<ul style="list-style-type: none"> – Macierz musi zostać dostarczona wraz z oprogramowaniem producenta do zapewnienia wielościeżkowości tzw. multipathing. Oprogramowanie musi wspierać min. Następujące systemy operacyjne: Windows, Linux, VMware. – Dostarczona licencja musi umożliwiać podłączenie dowolnej ilości serwerów do oferowanej macierzy dyskowej.
M.19	Kasowanie danych	<ul style="list-style-type: none"> – Macierz musi zostać dostarczona z oprogramowaniem do bezpiecznego usuwania danych z woluminów dyskowych. Musi istnieć możliwość wielokrotnego nadpisania danych. – Zamawiający wymaga dostarczenia licencji na tę funkcjonalność.
M.20	Wirtualizacja macierzy dyskowych	<ul style="list-style-type: none"> – Zaoferowane urządzenie musi posiadać wbudowany silnik wirtualizacyjny działający w trybie wysokiej dostępności. Nie dopuszcza się stosowania zewnętrznych wirtualizatorów. – Macierz musi pozwalać na wirtualizację zasobów dyskowych znajdujących się na innych macierzach dyskowych różnych producentów za pomocą protokołu FC, w szczególności producentów takich jak: NetApp, HP, IBM, Fujitsu, HDS, EMC. – Nie jest wymagane dostarczenie licencji.

Przełączniki SAN.

Dedykowana sieć dostępu do zasobów dyskowych będzie zbudowana w oparciu o dwa przełączniki, każdy wyposażony w 16 portów FC o przepustowości 32Gbps. Każdy z przełączników ma możliwość rozbudowy do 24 portów FC 32Gbps. Wymagana 36- min. miesięczna gwarancja producenta sprzętu

Tabela P1.		
Przełączniki SAN – 2 sztuki		
Lp.	Nazwa elementu, parametru lub cechy	Wymagania szczegółowe (pojedynczy przełącznik)
P1.1	Obudowa	<ul style="list-style-type: none"> Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19" oraz zapewniać techniczną możliwość montażu w szafie 19". Wraz z przełącznikiem należy dostarczyć odpowiedni zestaw montażowy do szafy 19". Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 24 aktywne porty 32Gbps to 77W. Maksymalna ilość ciepła wydzielanego przez przełącznik FC wyposażony w 24 aktywne porty 32Gbps to 215 BTU na godzinę.
P1.2	Architektura	<ul style="list-style-type: none"> Przełącznik FC musi być wykonany w technologii FC minimum 32 Gbs i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, 4 Gbs w zależności od rodzaju zastosowanych wkładek SFP. Przełącznik FC musi realizować sprzętową obsługę zoniingu (przez tzw. układ ASIC) na podstawie portów i adresów WWN. Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware'u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC. Rodzaj obsługiwanych portów, co najmniej: E, D oraz F. Dostarczony przełącznik FC musi być wyposażony w 16 aktywnych portów FC obsadzonych 16 wkładkami SFP+ 32Gbs SWL. Przełącznik FC musi zapewniać obsługę protokołu NVMe over FC. Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
P1.3	Parametry wydajnościowe	<ul style="list-style-type: none"> Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubskrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika wyposażonej we wkładki 32Gbs mogą pracować równocześnie z pełną prędkością 32Gb/s. Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji (24 porty) wyposażonej we wkładki 32Gbs musi wynosić minimum 768 Gb/s end-to-end. Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 900ns.
P1.4	Obsługa połączeń między przełącznikami	<ul style="list-style-type: none"> Przełącznik FC musi posiadać możliwość obsługi mechanizmu agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu ISL Trunk o przepustowości minimum 256 Gb/s half duplex (dla wkładek 32Gbs) dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek. Urządzenie musi posiadać możliwość uruchomienia powyższej funkcjonalności w przyszłości, nie jest wymagana dostawa licencji. Przełącznik FC musi obsługiwać mechanizm balansowania ruchu, pomiędzy co najmniej 16 różnymi połączeniami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o 3 parametry nagłówka ramki FC: DID, SID i OXID. Przełącznik FC musi posiadać możliwość jednoczesnej obsługi mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID. Urządzenie musi posiadać możliwość uruchomienia powyższej funkcjonalności w przyszłości, nie jest wymagana dostawa licencji. Przełącznik FC musi posiadać możliwość przydzielenia, co najmniej 1700 tzw. buffer credits do wybranego portu FC przełącznika. Urządzenie musi posiadać możliwość uruchomienia powyższej funkcjonalności w przyszłości, nie jest wymagana dostawa licencji.

P1.5	Bezpieczeństwo	<ul style="list-style-type: none"> – Przelącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa: <ul style="list-style-type: none"> • mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przelączników FC do uczestnictwa w sieci fabric • uwierzytelnianie (autentykacja) przelączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP • uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP • szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2. • definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control) • definiowanie kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+ • szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS • obsługa SNMP v1 oraz v3 • IP Filter dla portu administracyjnego przelącznika • wgrywanie nowych wersji firmware przelącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP • wykonywanie kopii bezpieczeństwa konfiguracji przelącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP
P1.6	Narzędzia diagnostyczne	<ul style="list-style-type: none"> – Przelącznik FC musi być dostarczony z następującymi narzędziami diagnostycznymi i mechanizmami obsługi ruchu FC: <ul style="list-style-type: none"> • logowanie zdarzeń poprzez mechanizm „syslog”, • ciągle monitorowanie parametrów pracy przelącznika, portów, wkładek SFP i sieci fabric z automatycznym powiadamianiem administratora, wyłączeniem pracy portu lub przesunięciem przepływów tzw. slow drain na niski priorytet w przypadku przekroczenia zdefiniowanych wartości granicznych. Powiadamianie administrator musi być możliwe za pomocą wysyłania wiadomości e-mail, pułapki SNMP lub komunikatu w logu. Urządzenie musi posiadać możliwość uruchomienia powyższej funkcjonalności w przyszłości, nie jest wymagana dostawa licencji. • port diagnostyczny tzw. D_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przelącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przelącznikami, testowe obciążenie połączenia pełną przepustowością 16Gbps/32Gbps oraz pomiar opóźnień i odległości między przelącznikami z dokładnością co najmniej do 5m dla wkładek SFP 16Gbps lub 32Gbps. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przelącznika i całej sieci fabric. • FCping • FC traceroute • kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przelącznika • sprzętowe monitorowanie przepływów danych dla automatycznie wykrywanych par urządzeń komunikujących się przez dany port przelącznika. Dla każdego monitorowanego przepływu muszą być gromadzone statystyki dotyczące, co najmniej liczby wysłanych i odebranych ramek, przepustowości, liczby zapisów i odczytów SCSI. Urządzenie musi posiadać możliwość uruchomienia powyższej funkcjonalności w przyszłości, nie jest wymagana dostawa licencji. • sprzętowy generator ruchu umożliwiający symulowanie komunikacji w wielodomenowych sieciach SAN bez konieczności angażowania fizycznych urządzeń takich jak serwery lub macierze dyskowe. Urządzenie musi posiadać możliwość uruchomienia powyższej funkcjonalności w przyszłości, nie jest wymagana dostawa licencji. • mechanizm umożliwiający kopiowanie pierwszych 64 bajtów ramek dla wybranych przepływów danych do pamięci lokalnej przelącznika w celu dalszej analizy. Urządzenie musi posiadać możliwość uruchomienia powyższej funkcjonalności w przyszłości, nie jest wymagana dostawa licencji. • mechanizm umożliwiający sprzętowe identyfikowanie ramek FC oznaczonych parametrem VM ID oraz integrację tego mechanizmu z systemami monitorowania przepływów danych w szczególności w zakresie przepustowości, liczby zapisów i odczytów na sekundę oraz opóźnień operacji zapisu i odczytu. Urządzenie musi posiadać możliwość uruchomienia powyższej funkcjonalności w przyszłości, nie jest wymagana dostawa licencji. • Przelącznik musi obsługiwać wysyłanie komunikatów FPIN typu: Link Integrity Notification, Delivery Notification, Peer Congestion Notification, Congestion Notification. Urządzenie musi posiadać możliwość uruchomienia powyższej funkcjonalności w przyszłości, nie jest wymagana dostawa licencji.
P1.7	Zarządzanie	<ul style="list-style-type: none"> – Przelącznik FC musi mieć możliwość konfiguracji przez: <ul style="list-style-type: none"> • polecenia tekstowe w interfejsie znakowym konsoli terminala • przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie. – Przelącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC. – Przelącznik FC musi zapewniać obsługę interfejsu zarządzającego REST API.

P1.8	Inne	<ul style="list-style-type: none"> – Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu. – Przełącznik FC musi realizować kategoryzację ruchu na podstawie wartości parametru CS_CTL w nagłówku ramki FC oraz odpowiednie przydzielenie ramki do kategorii o wysokim, średnim lub niskim priorytecie.
------	------	--

Przełącznik LAN – CORE

Wymaga się, aby sieć działała na sprzęcie nie gorszym niż wyspecyfikowany poniżej (w tabeli specyfikacja pojedynczego przełącznika). Wymagana 36- min. miesięczna gwarancja producenta sprzętu.

Przełączniki LAN PROD – 2 szt.

Lp.	Symbol	Opis	Ilość
1	N9K-C93180YC-EX	Nexus 9300 with 48p 10/25G SFP+ and 6p 100G QSFP28	1
2	NXOS-10.1.2	Nexus 9500, 9300, 3000 Base NX-OS Software Rel 10.1.2	1
3	N3K-C3064-ACC-KIT	Nexus 3K/9K Fixed Accessory Kit	1
4	NXA-FAN-30CFM-F	Nexus 2K/3K/9K Single Fan, port side exhaust airflow	4
5	NXA-PAC-650W-PE	Nexus NEBs AC 650W PSU - Port Side Exhaust	2
6	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	2
7	SFP-10G-SR	10GBASE-SR SFP Module	10
8	N93-LIC-PAK	N9300 License PAK Expansion	1
9	N93-LAN1K9	LAN Enterprise License for Nexus 9300 Platform	1

Przełącznik LAN – ACCESS

Wymaga się, aby sieć działała na sprzęcie nie gorszym niż wyspecyfikowany poniżej. Wymagana 36- min. miesięczna gwarancja producenta sprzętu.

Przełączniki LAN Access – 1 szt.

Lp.	Symbol	Opis	Ilość
1	N9K-C93180YC-FX	Nexus 9300 with 48p 1/10/25G, 6p 40/100G, MACsec	1
2	MODE-NXOS	Mode selection between ACI and NXOS	1
3	NXK-AF-PE	Dummy PID for Airflow Selection Port-side Exhaust	1
4	NXOS-9.3.3	Nexus 9500, 9300, 3000 Base NX-OS Software Rel 9.3.3	1
5	C1-SUBS-OPTOUT	OPT OUT FOR "Default" DCN Subscription Selection	1
6	NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	1
7	NXA-PAC-500W-PE	Nexus NEBs AC 500W PSU - Port Side Exhaust	2
8	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	2
9	NXA-FAN-30CFM-F	Nexus Fan, 30CFM, port side exhaust airflow	4
10	GLC-SX-MMD	1000BASE-SX SFP MODULE	32

Wspólne wymagania minimalne dla przełączników LAN:

1. Przełącznik musi zapewniać:
 - a. minimum 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP/SFP+ bezpośrednio w obudowie przełącznika lub na karcie liniowej,
 - b. minimum 6 portów definiowanych za pomocą wkładek QSFP, bezpośrednio w obudowie przełącznika lub na karcie liniowej, przy czym każdy z tych portów QSFP powinien mieć możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps.
2. Parametry wydajnościowe:
 - a. Wymagana jest prędkość przełączania „wirespeed” dla każdego portu przełącznika,
 - b. Obsługiwana łączna przepływność (pasmo) min. 3 Tbps,
 - c. Obsługiwana łączna przepustowość pakietowa przełącznika min. 1,000 mpps,
 - d. Opóźnienie przełączania pakietów nie większe niż 2 μ s.
3. Przełącznik musi spełniać następujące wymagania dla warstwy L2:
 - a. Trunking IEEE 802.1Q VLAN;
 - b. Wsparcie dla 4094 sieci VLAN;
 - c. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN
 - d. Wsparcie sprzętowe dla minimum 250 tysięcy adresów MAC
 - e. IEEE 802.1w Rapid Spanning Tree (RST)
 - f. IEEE 802.1s Multiple Spanning Tree (MST)
 - g. Wsparcie sprzętowe dla tunelowania QinQ
 - h. Spanning Tree Guard lub odpowiadający;
 - i. Internet Group Management Protocol (IGMP) Versions 2, 3;
 - j. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach (MCEC, vPC lub odpowiadający mechanizm),
 - k. Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 32 interfejsów fizycznych w wiązkę;
 - l. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
4. Przełącznik musi zapewniać możliwość rozszerzenia funkcjonalności o wsparcie warstwy L3
 - a. Sprzętowe przełączanie pakietów w warstwie L3,
 - b. Routing w oparciu o trasy statyczne,
 - c. Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6.
 - d. Policy Based Routing (PBR) dla IPv4,
 - e. VRRP v3,
 - f. Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol),
 - g. Wsparcie sprzętowe dla minimum 768 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP,
 - h. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode I tryb SSM (Source Specific Multicast),
 - i. Wsparcie dla IGMPv3 oraz MSDP,

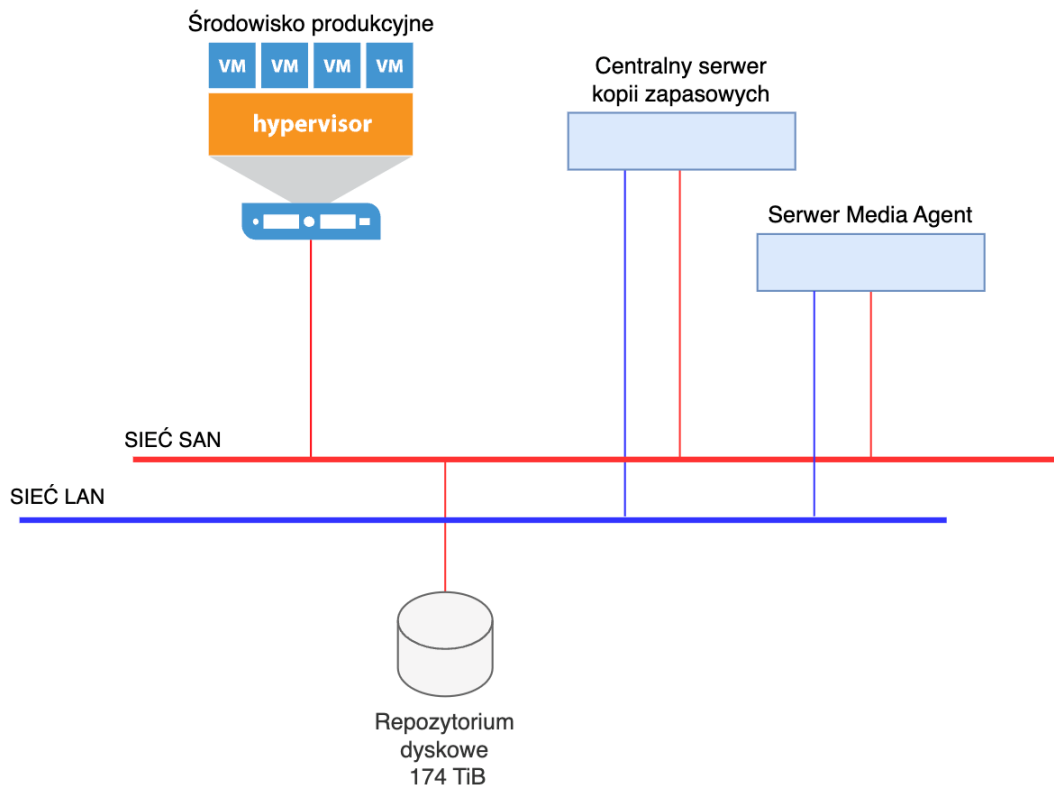
- j. Wsparcie dla minimum 32, 000 tras multicastowych,
 - k. Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking),
 - l. Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP),
 - m. Minimum 1000 wejściowych oraz 1000 wyjściowych wpisów dla ACL - access control list.
5. Przełącznik musi zapewniać możliwość rozszerzenia funkcjonalności o następujące mechanizmy związane z funkcjonalnością VXLAN:
- a. Obsługa co najmniej 256 sprzętowych VTEP (VXLAN Tunnel Endpoint).
 - b. Sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway).
 - c. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności, PIM Anycast RP.
 - d. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast).
 - e. Implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol).
 - f. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługa danego SVI na wszystkich VTEP w domenie VXLAN).
6. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
- a. Layer 2 IEEE 802.1p (CoS);
 - b. Klasyfikacja QoS w oparciu o listy (ACL (Access control list) w warstwach 2, 3, 4;
 - c. Kolejowanie na wyjściu w oparciu o CoS 802.1p;
 - d. Bezwzględne (strict-priority) kolejowanie na wyjściu;
 - e. Kolejowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm odpowiadający;
 - f. Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych;
 - g. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych;
 - h. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb.
7. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
- a. Wejściowe ACL (standardowe oraz rozszerzone);
 - b. Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
 - c. Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6,
 - d. Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
 - e. ACL oparte o VLAN-y (VACL);
 - f. ACL oparte o porty (PACL);
 - g. DHCP Snooping;
 - h. ARP Inspection;
 - i. IP Source Guard;
 - j. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast,

- k. multicast, broadcast.
8. Wymagania dotyczące zarządzania i zabezpieczenia przełącznika:
- a. Port zarządzający 100/1000 Mbps;
 - b. Port konsoli CLI;
 - c. Zarządzanie In-band;
 - d. SSHv2;
 - e. Authentication, authorization, and accounting (AAA);
 - f. RADIUS;
 - g. TACACS+
 - h. Syslog;
 - i. SNMP v1, v2, v3;
 - j. RMON (przynajmniej grupy Events, Alarms);
 - k. Openflow 1.3;
 - l. sFlow;
 - m. IEEE 802.1ab LLDP;
 - n. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback);
 - o. Role-Based Access Control RBAC;
 - p. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing);
 - q. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu. (mirror);
 - r. Network Time Protocol (NTP);
 - s. Precision Time Protocol IEEE 1588;
 - t. Diagnostyka procesu BOOT;
 - u. Ping;
 - v. Traceroute.
9. Wymagania dotyczące narzędzi programowania i zarządzania przełącznikiem:
- a. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API.
 - b. Wbudowana powłoka bash do zarządzania systemem Linux przełącznika.
 - c. Wsparcie dla kontenera LXC (Linux Container) wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika. Kontener musi mieć możliwość wykorzystywania portów fizycznych przełącznika.
 - d. Interfejs programistyczny REST API wraz z upublicznionym SDK.
 - e. Możliwość zainstalowania klienta Chef.
 - f. Możliwość zainstalowania agenta Puppet.
 - g. Wsparcie dla NETCONF i zarządzania poprzez XML.

10. Oferowane przełączniki muszą być wyposażone w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów (port side exhaust).
11. Oferowane przełączniki muszą być wyposażone w moduły SFP/SFP+ pochodzące od tego samego producenta co switch celem uniknięcia problemów z serwisowaniem urządzeń.
12. Obudowa o rozmiarach maksymalnie 1RU (rack unit), musi być przeznaczona do montażu w szafie typu RACK 19”.
13. Wymagana jest min.36 miesięczna gwarancja producenta. W obrębie gwarancji zawarte musi być:
14. Dostęp do aktualnych wersji oprogramowania oraz dokumentacji producenta.
15. Sposób obsługi zgłoszeń gwarancyjnych w trybie 24x7.
16. Wymiana sprzętu następnego dnia roboczego po identyfikacji usterki.

Architektura rozwiązania – system kopii zapasowych

System będzie wykonywał regularne kopie zapasowe zarówno maszyn wirtualnych jak i baz danych, tak aby zapewnić szybkie i pełne odtworzenie kopii zapasowej w razie awarii wymagającej takich działań. System kopii zapasowych zbudowany zostanie na dedykowanym rozwiązaniu sprzętowym, na który będą się składać serwery systemu kopii zapasowych i repozytorium dyskowe.



Oprogramowanie systemu kopii zapasowych

Kluczowym elementem proponowanego rozwiązania jest dostarczenie i wdrożenie systemu kopii zapasowych dla zabezpieczenia wdrożonego środowiska. Powyższy system kopii zapasowych i odtwarzania należy oprzeć na oprogramowaniu lidera systemów do zabezpieczenia danych klasy enterprise. Takim rozwiązaniem adresujemy szerokie spektrum systemów wirtualnych, fizycznych, aplikacji oraz backup danych ze stacji roboczych. Rozwiązanie musi udostępniać wszystkie powyższe funkcjonalności wraz z globalną deduplikacją blokową na bazie własnego oprogramowania niezależnie od platformy sprzętowej, z której korzysta Klient i na jakim sprzęcie jest zaimplementowany system. Dzięki temu agnostycznemu pod kątem hardware'u podejściu, koszty implementacji, utrzymania czy rozbudowy środowiska są na niższym i przewidywalnym stałym poziomie. Takie podejście daje Klientom oprócz zaawansowanych funkcjonalności znaczne ograniczenie kosztów utrzymania systemu, uproszczenie architektury oraz dużo lepszą elastyczność. Zaleca się zastosowanie centralnej architektury bazującej na jednej domenie backupowej. Głównym urządzeniem będzie serwer backupowy odpowiadający za zarządzanie całym środowiskiem. Do składowania kopii backupowych z systemów dedykowany zostanie drugi serwer, do którego podłączone zostaną repozytoria składowania danych. Do składowania kopii zapasowych będzie przeznaczony repozytorium dyskowe.

Oprogramowanie systemu kopii zapasowych – 1 kpl.

Wymogi podstawowe

1. Rozwiązanie musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient), taka architektura pozwoli na elastyczną skalowalność rozwiązania bez względu na dynamikę przyrostu danych.
2. Oprogramowanie nie może preferować platformy sprzętowej, nie może być profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych. Niedopuszczalne jest, aby funkcjonalności związane z zabezpieczaniem danych były w jakikolwiek sposób związane czy zależne od konkretnego typu czy producenta urządzenia.
3. Jeśli system korzysta z bazy danych to wszelkie potrzebne licencje muszą być dostarczone i stanowić całość oferty, z tym, iż licencje dla silnika bazodanowego muszą pozwalać na zainstalowanie go: na serwerze fizyczny (minimum 2xCPU po 12 core), klastrze active-passive czy serwerze wirtualnym w środowisku Vmware i Hyper-V.
4. Licencje muszą pozwalać na stworzenie dla serwera zarządzającego rozwiązania wysokodostępного z częstotliwością replikacji bazy katalogowej nie dłuższym niż 15 minut (RPO nie większe niż 15 min dla uruchomienia zapasowego serwera zarządzającego). Jeśli do stworzenia takowego rozwiązania potrzebne są licencje replikacyjne, klastrowe, współdzielona przestrzeń dyskowa to muszą zostać zaoferowane. Licencje muszą pozwalać na skonfigurowanie serwerów zarządzających oraz ich replikację dla co najmniej trzech lokalizacji, gdzie pierwsza jest lokalizacja produkcyjną, druga i trzecia są typu standby dla serwera zarządzającego.

5. Jako opcja musi istnieć możliwość zainstalowania serwera zarządzającego na systemie operacyjnym Linux z zachowaniem możliwości replikacji bazy katalogowej i tworzeniem serwerów typu standby.
6. Proces przełączenia musi umożliwiać:
 - Przełączenie manualne inicjalizowane przez administratora
 - Przełączenie automatyczne w przypadku wykrycia awarii
7. Przełączenie serwera zarządzającego musi odbywać się w pełni automatycznie poprzez administratora, który decyduje, kiedy ma ono nastąpić, przełączanie serwera zarządzającego musi być możliwe pomiędzy różnymi typami infrastruktury:
 - serwer fizyczny -> serwer fizyczny
 - serwer fizyczny -> serwer wirtualny (onpremis)
 - serwer fizyczny -> serwer wirtualny (AWS, Azure, Google)
 - serwer wirtualny (onpremis) -> serwer fizyczny
 - serwer wirtualny (onpremis) -> serwer wirtualny (onpremis)
 - serwer wirtualny (onpremis) -> serwer wirtualny (AWS, Azure, Google)
8. Rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji.
9. Oprogramowanie musi umożliwiać zdalne instalowanie i odinstalowywanie klienta systemu z centralnego serwera dla systemów Windows, Linux i Unix – musi być to możliwe z jednego serwera pełniącego rolę cache dla wszystkich binarii klienckich
10. System musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów.
11. System musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania
12. Dla dowolnego transferu danych z klienta musi istnieć możliwość definiowania/ograniczania pasma dla transferu danych – funkcjonalność ta musi być dostępna także przy włączonej deduplikacji na kliencie
13. System musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja, backup laptopów) z jednej konsoli administracyjnej oraz także z konsoli webowej
14. Agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji z środowisk typu DMZ
15. Automatyczne tunelowanie komunikacji TCP/IP pomiędzy agentami systemu – jeśli agent systemu wykryje ograniczenia w komunikacji, wtenczas automatycznie zestawia połączenie tunelowe wykorzystujące tylko jeden port TCP/IP
16. System musi umożliwiać konfigurację, którymi kartami sieciowymi ma przebiegać komunikacja i transfer danych, wybór interface musi odbywać się co najmniej poprzez nazwę domeny, subnet, zakres IP
17. Komunikacja agentów systemu z serwerami musi odbywać się poprzez SSL – konfiguracja tego typu transferu nie może powodować konieczności instalowania dodatkowego oprogramowania

18. System musi umożliwić przechowywanie jedynie unikalnych bloków danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych. Deduplikacja musi być realizowana poprzez oprogramowanie systemu na dowolnym sprzęcie czy to w warstwie serwera systemu czy klienta. Pojedynczy serwer systemu musi umożliwiać przechowywanie danych po deduplikacji minimum do 500 TB (rozbudowa do tej wielkości może nastąpić tylko poprzez dodanie dodatkowej przestrzeni do składowania danych poprzez dodanie dysków, półki dyskowej a nie przez wymianę urządzenia).
19. Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i Macintosh
20. Logiczna Globalna deduplikacja – system musi oferować deduplikację globalną co oznacza, iż niezależnie z jakich klientów dane będą deduplikowane (serwery fizyczne, hosty wirtualne, bazy i aplikacje) – deduplikacja musi opierać się na jednej logicznej centralnej bazie deduplikacyjnej
21. Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera systemu. Niedopuszczalne jest łączenie systemu z dodatkowym oprogramowaniem czy sprzętem (appliance) dla uzyskania funkcjonalności deduplikacji danych.
22. Deduplikacja blokowa musi obejmować dane nie tylko backupowane ale i archiwizowane, przy czym wielkość bloku nie może być większa niż 128KB.
23. System musi zapewniać wspólny stopień deduplikacji (jedna baza deduplikacyjna) dla danych czy to z backupu czy archiwizacji.
24. System musi umożliwiać wykonywanie kopii w post procesie do drugiej lokalizacji przesyłając jedynie unikalne bloki danych (dla dowolnych danych: czy to z procesu backupu czy archiwizacji). A więc replikacja danych do innej lokalizacji musi być wykonywana na danych po deduplikacji i funkcjonalność ta musi być realizowana i zarządzana z poziomu systemu.
25. Proces przesyłania danych (replikacji) na inny serwer systemu celem tworzenia dodatkowej kopii danych nie może być zależny od warstwy sprzętowej, a więc dowolny producent serwera, dowolny producent macierzy/półki dyskowej
26. System musi pozwalać na instalację bazy deduplikacyjnej w układzie wysokiej dostępności (minimum na dwóch serwerach) w taki sposób, aby awaria pojedynczego serwera nie powodowała utraty możliwości backupu z deduplikacją i odtwarzania wcześniejszych kopii danych
27. System musi pozwalać na odtwarzanie zdeduplikowanych danych nawet w momencie, gdy baza deduplikacyjna jest niedostępna. Proces odtwarzania (nawadniania) zdeduplikowanych danych nie korzysta z bazy deduplikacyjnej.
28. Na jednym serwerze systemu (na jednej instancji systemu operacyjnego) może być zainstalowane minimum dwie bazy deduplikacyjne pozwalające zwiększyć skalowalność systemu.

29. System musi zapewniać dostęp zintegrowany z usługą katalogową, minimum to Active Directory, a więc tak zwany „single sign on” – pojedyncze logowanie: użytkownik po zalogowaniu do domeny AD, nie potrzebuje wykonywać następnego logowania, aby zarządzać systemem poprzez konsolę administracyjną
30. System musi być odporny na tzw. „atak na wzorec czasu”: to znaczy, iż przy radykalnej zmianie czasu na serwerze zarządzającym o co najmniej 1 godzinę do tyłu lub o 4 godziny do przodu względem danego czasu na serwerze – System musi automatycznie zatrzymać swoje jakiegokolwiek działania aby zabezpieczyć dane przed wykasowaniem (ekspiracją).
31. System musi zapewniać elastyczne delegowanie uprawnień oraz audytowanie działań użytkowników. Z tym, że delegowanie uprawnień musi pozwalać na przydział uprawnień per serwer czy grupa serwerów, przydział uprawnień musi pozwalać na definiowanie uprawnień dla grup użytkowników z domeny AD.
32. System musi pozwalać na zarządzanie z poprzez „cmd” z tym, że uruchomienie jakiegokolwiek komendy/polecenia musi zostać poprzedzone koniecznością zalogowania (autentyfikacji) do systemu, funkcjonalność musi dotyczyć dowolnej platformy (minimum Windows/Linux) i nie może polegać na konieczności instalowania czy konfigurowania dodatkowych komponentów np. SSH.
33. Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach
34. System musi posiadać funkcjonalność blokowania danych do odczytu dla administratora, to znaczy, że administrator systemu nawet mając pełne uprawnienia nie może odtworzyć danych, jeśli nie jest ich właścicielem, funkcjonalność ta musi być dostępna nie tylko dla danych z laptopów/desktopów, ale i dla serwerów (także dla danych plikowych i bazodanowych)
35. System musi pozwalać na skonfigurowanie mechanizmu podwójnej autentyfikacji administratora – do uruchomienia konsoli administracyjnej systemu potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod wysyłany do administratora np. poprzez mail
36. Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu.
37. Możliwość szyfrowania musi pozwalać na elastyczny wybór miejsca szyfrowania: szyfrowanie danych na kliencie, szyfrowanie danych na serwerze backupowym i szyfrowanie tylko transmisji pomiędzy klientem backupowym a serwerem
38. System musi pozwalać na ustawianie haseł dostępu do nośników tzw: media password
39. System musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrującym zgodnymi z KMIP – minimum dla:
 - Fortanix Data Security Manager
 - HashiCorp Vault
 - IBM Security Key Lifecycle Manager (SKLM)
 - Safenet
 - StorMagic SvKMS
 - Thales CipherTrust Manager
 - Vormetric

- Amazon Web Services (AWS) key management service
 - Microsoft Azure Key Vault
40. System musi umożliwiać składowanie kopii bazy katalogowej w chmurze producenta oprogramowania, funkcjonalność ta musi być w cenie produktu i pozwalać na automatyczne składowanie kopii bazy
41. System musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (Ransomware), minimum to:
- Zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane
 - Monitorowanie nietypowych aktywności na serwerach za pomocą np. metody: Honeypot
 - Monitorowanie nietypowych aktywności na serwerach plikowych i desktopach, monitorowanie musi odbywać się nie rzadziej, niż co 5 minut i każdy niestandardowy wynik jest automatycznie wysyłany w postaci alertu lub notyfikacji
 - Monitorowanie różnych typów plików i weryfikowanie czy typ pliku jest zgodny i czytelny z nagłówkiem tego pliku (detekcja uszkodzeń plików czy ich zaszyfrowania)
 - Air Gap (izolowanie i segmentowanie składowanych kopii backupowych) – musi polegać na wbudowanym automatycznym mechanizmie wyłączania komunikacji pomiędzy pozostałymi komponentami systemu backupowego. Tak więc komunikacja z wybranym segmentem środowiska backupowego odbywa się tylko w określonym przedziale czasowym dla potrzeb replikacji kopii backupowych, natomiast przez pozostały czas żadne procesy systemu backupowego nie mają możliwości komunikacji z tym środowiskiem.
 - Możliwość definiowania serwerów komunikacyjnych (tzw. bram/gateway) przez które wykonywana jest komunikacja pomiędzy modułami systemu backupowego, w szczególności pomiędzy serwerem zarządzającym a serwerem medii czy serwerem z dowolnym agentem backupowym
 - Możliwość definiowania kierunku inicjalizowania komunikacji sieciowej pomiędzy komponentami systemu backupowego
 - Możliwość zablokowania zmiany retencji (czas przechowywania kopii backupowych) na krótszą dla kopii backupowych składowanych na dowolnych typach nośników.
42. System musi posiadać rozbudowany system powiadamiania o zdarzeniach poprzez email.
43. System musi posiadać zaawansowane mechanizmy exportu i analizy logów poprzez:
- Syslog serwer
 - Splunk (dedykowany plug-in do Splunk dla analizy danych)
44. Automatyczne monitorowanie stanu systemu poprzez wiadomości SMS na urządzeniach mobilnych i telefonach
45. System musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to:

- Raport zmian/wzrostu środowiska systemu
 - Raport wykorzystania licencji
 - Raport wykonanych zadań backupowych
 - Raporty obciążenia serwerów backupowych – minimum monitorowanie użycia CPU i pamięci RAM
46. System musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail
47. System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV
48. System musi pozwalać na definiowanie alertów per zadanie backupowe lub zadanie odtwarzania danych przy spełnieniu minimum kryterii:
- Czas zadania dłuższy niż zadany
 - Ilość danych większa niż
 - Ilość danych mniejsza niż
 - Ilość nie zbackupowanych plików większa niż
 - Ilość nie zbackupowanych plików większa niż ...%
 - Wielkość backupowanych danych większa niż ...
49. Notyfikacje alertów muszą być wysyłane minimum poprzez mail.
50. Raport spełnienia wymogów SLA dla parametrów:
- Ilości dodatkowych kopii backupowych
 - RTO
 - RPO
51. System musi zapewniać funkcjonalność wznowiania zadań backupowych.
52. System musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanych – inline copy (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywania danych.
53. System musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami – tzw. multistreaming. Polega ona na tym, iż agent systemu równolegle czyta różne obszary danych i bez pośredniczenia dysków automatycznie wysyła je do serwera, który zapisuje te dane na dyski. Funkcjonalność ta musi być dostępna dla dowolnych typów danych: backup plikowy, bazodanowy
54. Funkcjonalność multistreamingu musi być dostępna dla deduplikacji bez względu czy następuje na kliencie czy na serwerze systemu
55. Rozwiązanie musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego.
56. System musi oferować funkcjonalność backupu blokowego, polegającego na tym, iż agent buduje własną bazę zmian bloków danych, przez co backup przyrostowy nie wymaga odczytu całych plików tylko

zmienionych bloków wielokrotnie przyspieszając backup. Funkcjonalność ta musi być dostępna dla backupu danych plikowych.

57. System musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji.
58. System ma realizować procesy backupu oraz odzyskiwania danych, procesy te muszą być uruchamiane ręcznie i poprzez wbudowany kalendarz, możliwość definiowania zadań poprzez wbudowany w system kalendarz musi być możliwa nie tylko dla zadań backupowych, ale także dla zadań odtwarzania danych a więc restore
59. System musi dla backupu środowiska AWS oferować:
 - Bezagentowy backup całych maszyn wirtualnych i ich odtwarzanie wraz z odtwarzaniem pojedynczych plików
 - Możliwość zapisu backupu maszyn wirtualnych na dowolnym nośniku backupowym.
 - Możliwość odtworzenia pojedynczego dysku wirtualnej maszyny i podłączenie go do innej maszyny wirtualnej EC2
 - Możliwość wykonywania migawek (snapshotów) wirtualnych maszyn i automatyczne zarządzanie ich retencją
 - Możliwość wykonywania jednorazowego konsystentnego backupu maszyn wirtualnych EC2, na których pracują systemy Microsoft Exchange, Microsoft Sharepoint, Microsoft SQL Server, MySQL, Oracle lub Active Directory?
 - Backup i odtwarzanie danych z baz danych RDS: MS SQL, MySQL, PostgreSQL oraz Oracle (eksport danych na storage backupowy)
 - Możliwość wykonywania snapshotów baz danych AWS RDS: Aurora, MariaDB, Microsoft SQL Server, MySQL, PostgreSQL.
 - Backup oraz odtwarzanie danych składowanych w usłudze S3, EFS oraz FSx.
 - Możliwość zapisu danych zdedyplikowanych bezpośrednio w usłudze S3, bez konieczności używania dodatkowego cache'u oraz rozwiązań typu appliance
 - Możliwość automatycznego włączania oraz wyłączania maszyn wirtualnych EC2, na których zainstalowano oprogramowanie serwera backupowego
 - Możliwość konwersji maszyn wirtualnych Microsoft Hyper-V, Vmware oraz Azure do maszyn wirtualnych EC2
 - Możliwość konwersji maszyn wirtualnych EC2 do maszyn typu Vmware oraz Azure
 - Możliwość wykonywania backupu usługi AWS DynamoDB
 - Możliwość backupu środowiska VMWare Cloud on AWS
 - Możliwość automatycznego wyłączania i włączania serwerów backupowych
 - Możliwość automatycznej replikacji maszyn wirtualnych Vmware do AWS EC2
 - Możliwość wykorzystania EBS Direct Read API w czasie backupu maszyn wirtualnych EC2

- Możliwość integracji z AWS KMS w celu zarządzania kluczami szyfrującymi
- Możliwość backupu maszyn wirtualnych EC2 z innego konta Amazon (Cross-account backup)
- Możliwość migracji zdeduplikowanych danych do chmury AWS za pomocą urządzenia Snowball
- Możliwość wykonywania konsystentnych snapshotów dysków wirtualnych podłączonych do maszyn wirtualnych Azure VM, na których składowane są dane systemów Oracle, SAP HANA, Microsoft SQL Server, DB2, MongoDB, MySQL, PostgreSQL oraz pliki na systemach Windows oraz Linux

60. System musi dla backupu środowiska Azure oferować:

- Bezagentowy backup całych maszyn wirtualnych Azure VM i ich odtwarzanie wraz z odtwarzaniem pojedynczych plików.
- Możliwość zapisu backupu maszyn wirtualnych na dowolnym nośniku backupowym.
- Możliwość odtworzenia pojedynczego dysku wirtualnej maszyny i podłączenie go do innej maszyny wirtualnej w Azure VM
- Możliwość wykonywania migawek (snapshotów) wirtualnych maszyn i automatyczne zarządzanie ich retencją
- Możliwość wykonywania jednorazowego konsystentnego backupu maszyn wirtualnych Azure VM, na których pracują systemy Microsoft Exchange, Microsoft Sharepoint, Microsoft SQL Server, MySQL, Oracle lub Active Directory?
- Backup i odtwarzanie danych z baz danych (PaaS): MS SQL, MySQL, PostgreSQL (eksport danych na storage backupowy)
- Backup oraz odtwarzanie danych składowanych w Azure Blob oraz Azure File Shares oraz Azure Data Lake Storage Gen2
- Możliwość zapisu danych zdeduplikowanych bezpośrednio na Azure Blob Storage, bez konieczności używania dodatkowego cache'u oraz rozwiązań typu appliance
- Możliwość automatycznego włączania oraz wyłączania maszyn wirtualnych Azure, na których zainstalowano oprogramowanie serwera backupowego
- Możliwość wykonywania konsystentnych snapshotów dysków wirtualnych podłączonych do maszyn wirtualnych Azure VM, na których składowane są dane systemów Oracle, SAP for Oracle, SAP HANA, Microsoft SQL Server, DB2 oraz pliki na systemach Windows oraz Linux
- Możliwość migracji zdeduplikowanych danych do chmury Azure za pomocą Azure Data Box
- Możliwość automatycznego wyłączania i włączania serwerów backupowych
- Możliwość integracji z Azure Key Vault w celu zarządzania kluczami szyfrującymi
- Możliwość automatycznej replikacji maszyn wirtualnych Hyper-V i Vmware do Azure
- Możliwość automatycznej replikacji maszyn wirtualnych Azure pomiędzy regionami
- Możliwość backupu bazy danych Cosmos DB (Core SQL API)

- Możliwość konwersji backupu systemu operacyjnego Windows wraz z danymi do maszyny wirtualnej Azure
 - Możliwość backupu Azure DevOps and GitHub
61. System musi dla backupu środowiska GCP oferować
- Bezagentowy backup całych maszyn wirtualnych i ich odtwarzanie wraz z odtwarzaniem pojedynczych plików
 - Możliwość zapisu backupu maszyn wirtualnych na dowolnym nośniku backupowym.
 - Możliwość wykonywania migawek (snapshotów) wirtualnych maszyn i automatyczne zarządzanie ich retencją
 - Backup i odtwarzanie danych z baz danych Cloud SQL: MySQL oraz PostgreSQL (eksport danych na dowolny storage backupowy)
 - Backup oraz odtwarzanie danych składowanych w usłudze GCP Cloud Storage
 - Możliwość zapisu danych zdeduplikowanych bezpośrednio w usłudze GCP Cloud Storage, bez konieczności używania dodatkowego cache'u oraz rozwiązań typu appliance
62. System musi posiadać (jako opcja) zintegrowane w systemie mechanizmy indeksowania pełnokontekstowego i wyszukiwania danych. Indeksowaniu powinny podlegać dane zbackupowane i zarchiwizowane już znajdujące się w systemie.
63. System musi realizować funkcjonalność weryfikacji wykonanych kopii.
64. System powinien umożliwiać wykorzystanie funkcjonalności Bare Metal Restore dla odtwarzania systemu po awarii, wsparcie musi być dostępne dla systemów:
- Windows
 - Linux: Debian/Oracle Linux/RHEL/CentOs/SuSe/Ubuntu
65. System musi umożliwiać integrację z mechanizmami kopii migawkowych czołowych producentów pamięci masowych minimum: HDS, Dell, HP, NetApp, EMC, IBM, Pure Storage, Nimble Storage, Tintri, Kaminario, z tym że takowy backup sterowany przez system a wykonywany przez daną macierz dyskową musi być dostępny nie tylko dla zasobów plikowych ale i aplikacji.
66. Dla producentów: NetApp, EMC i HDS system musi umożliwiać nie tylko integrację z mechanizmami tworzenia kopii migawkowych (tzw. Snapshot) ale musi integrować się także z mechanizmami replikacyjnymi, a więc sterować replikami wykonywanymi przez macierze
67. System powinien umożliwiać (jako opcja) obsługę urządzeń składowania danych w chmurze, minimum: Azure, Amazon, Google Cloud, jeśli do włączenia tej funkcjonalności potrzebne są jakieś dodatkowe komponenty to muszą być zaoferowane
68. System musi umożliwiać odtwarzanie danych plikowych pomiędzy systemami operacyjnymi np. odtwarzanie danych plikowych Linux na systemie Windows
69. System musi pozwalać na odtwarzanie tylko samych uprawnień do plików
70. System musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL)

71. System (jako opcja) powinien umożliwiać analizę logów z systemów zewnętrznych, na bazie zdefiniowanych kryteriów powinien generować alarmy lub akcje. Minimalne wsparcie to: Windows Event Log.
72. Możliwość (jako opcja) odtwarzania backupów plikowych poprzez udostępnienia CIFS lub NFS. A więc dostęp do zbackupowanych danych widocznych jako udostępnione przez sieć zasoby CIFS/NFS
73. System musi posiadać wbudowany mechanizm tworzenia kopii otwartych plików na platformie Windows i Linux
74. System musi wspierać wykonanie kopii na systemach klasy Windows, Linux i Unix
75. System musi posiadać szerokie wsparcie dla środowisk Linux, minimum: RHEL, SuSe, Debian, Fedora, Gentoo, Mandriva, Oracle Linux, Red Flag Linux, Scientific Linux, Ubuntu, Slackware
76. System musi posiadać szerokie wsparcie dla środowisk Unix, minimum: AIX, FreeBSD, HP-UX, Solaris
77. System musi umożliwiać uruchamianie skryptów przed i po backupie, z tym iż musi posiadać mechanizm definiowania konta użytkownika na którym te skrypty byłyby uruchamiane. Mechanizm ten musi być centralnie zarządzany poprzez konsolę administracyjną. Niedopuszczalna jest konieczność np. zmiany konta serwisowego dla danego agenta – konta serwisowe muszą być centralnie definiowane i zarządzane.
78. System musi wspierać backup całych maszyn wirtualnych/kontenerów dla czołowych rozwiązań wirtualizacyjnych, kontenerowych i chmurowych:
 - Alibaba Cloud
 - Amazon
 - Citrix Xen
 - Google Cloud Platform
 - Huawei FusionCompute
 - Microsoft Azure
 - Microsoft Azure Stack Hub
 - Microsoft Azure Stack HCI
 - Microsoft Hyper-V
 - Kubernetes
 - Nutanix Acropolis Hypervisor (AHV)
 - OpenStack
 - Oracle Cloud Classic
 - Oracle Cloud Infrastructure
 - Oracle VM
 - Red Hat Virtualization
 - vCloud Director
 - VMware

To znaczy musi posiadać dedykowany komponent do backupu minimum całej maszyny wirtualnej/kontenera/aplikacji/wolumenu bez konieczności instalowania agenta wewnątrz np. maszyny z możliwością granularnego odtwarzania pojedynczych plików. Dla maszyn wirtualnych musi być możliwość zainstalowania agenta plikowego i bazodanowego dla zabezpieczenia zasobów z wewnątrz maszyny wirtualnej – funkcjonalność ta musi być zawarta dla wszystkich wymaganych wirtualizatorów i być w cenie rozwiązania.

79. System musi wspierać wersje środowisk VMware 4.1, 5.0.x, 5.1.x, 5.5, 5.5.1, 5.5.2, 5.5.3, 6.0, 6.0.1, 6.5, 6.7, 7.0, 7.0.3 poprzez integrację z vStorage API
80. Dla backupu i odtwarzania środowisk wirtualnych opartych o VMware musi być możliwość wyboru różnych transportów: SAN, Hot-add, NBD, SSL, NAS - gdzie transport NAS pozwala na bezpośredni odczyt i zapis danych maszyny wirtualnej z urządzenia NAS
81. System musi wspierać środowisko Hyper-V dla:
- Microsoft Windows Server 2008 R2 SP1
 - Microsoft Windows Server 2012
 - Microsoft Hyper-V Server 2012
 - Microsoft Windows Server 2012 R2
 - Microsoft Hyper-V Server 2012 R2
 - Microsoft Windows Server 2016 (z Core Edition)
 - Microsoft Hyper-V Server 2016 (z Core Edition)
 - Microsoft Windows Server, version 1709 (z Core Edition)
 - Microsoft Hyper-V Server, version 1709 (z Core Edition)
 - Microsoft Windows Server 2019 (z Core Edition)
 - Microsoft Hyper-V Server 2019 (z Core Edition)
 - Microsoft Windows Server 2022 (z Core Edition)
 - Microsoft Hyper-V Server 2022 (z Core Edition)
82. System musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych.
83. System musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej minimum dla VMware i Hyper-V.
84. System musi umożliwiać konwertowanie maszyn wirtualnych pomiędzy wirtualizatorami, minimum:
- VMware do: Hyper-V, Azure, Amazon, Google Cloud Platform, Openstack, Oracle Cloud Infrastructure
 - Hyper-V do: Azure, Amazon, VMware
 - Amazon do: Azure, VMware
 - Azure do: Amazon, Hyper-V, VMware
85. System musi wspierać mechanizm CBT (change block tracking) minimum dla VMware i Hyper-V

86. System musi umożliwiać konwersję zbackupowanego serwera Windows i Linux do maszyny wirtualnej w środowisku:
- Hyper-V
 - Vmware
87. Możliwość (jako opcja) synchronizacji maszyn wirtualnych Vmware do środowiska Amazon, Azure
88. System musi umożliwiać wykonanie kopii na gorąco bazy danych MySQL, Postgress, Oracle, Informix na dowolnej platformie systemu operacyjnego (Windows/Linux/Unix) poprzez dedykowanego agenta bazodanowego, transfer danych musi odbywać się bez pośredniczenia dysków, a więc transfer danych z agenta bazodanowego bezpośrednio do serwera backupowego celem zapisu na dany nośnik.
89. System musi umożliwiać wykonanie kopii na gorąco bazy danych MS SQL, Oracle, MySQL, Postgress, DB2, Informix konfiguracja agenta nie może powodować konieczności tworzenia skryptów uruchamianych po stronie klienta niezależnie czy jest to serwer fizyczny czy wirtualny. Brak skryptów musi dotyczyć dowolnych typów backupów: backup automatyczny uruchamiany poprzez harmonogram, backup manualny.
90. Odtwarzanie danych z backupu bazodanowego (MS SQL, Oracle, MySQL, Postgress, DB2, Informix) musi odbywać się poprzez konsolę administracyjną bez konieczności konfigurowania skryptów
91. Dla silników bazodanowych MS SQL, Oracle i SAP HANA musi istnieć mechanizm backupu logów transakcyjnych z częstotliwością co 1 minuta nawet w przypadku, gdy serwer zarządzający systemem backupowym jest niedostępny
92. Konfiguracja agentów backupowych dla: MS SQL, Oracle, mySQL musi odbywać się poprzez interface graficzny, jakkolwiek modyfikacja zasobów do backupu (np. dodanie nowej bazy) nie może powodować konieczności modyfikacji skryptów czy to dla backupów planowanych czy wykonywanych na żądanie
93. System musi umożliwiać wykonanie kopii na gorąco Active Directory a następnie odzyskania pojedynczych obiektów AD wraz z hasłami użytkowników
94. System musi umożliwiać odtwarzanie backupu wykonywanego online dedykowanym agentem, do pliku celem późniejszego odtwarzania bez udziału systemu. Funkcjonalność ta musi być dostępna minimum dla MS SQL, Oracle i Exchange
95. System musi umożliwiać wykonanie kopii na gorąco aplikacji MS Exchange a następnie odzyskania pojedynczych wiadomości. Dedykowany agent do backupu Exchange musi wspierać backup środowiska Exchange DAG poprzez nazwę DAG nawet w konfiguracji bez adresu IP
96. System musi umożliwiać odtwarzanie pojedynczych tabel dla minimum: Oracle, DB2, PostgreSQL, MySQL, Informix, MS SQL
97. Dla minimum mySQL i PostgreSQL musi istnieć mechanizm backupu z wykorzystaniem mechanizmu backupu blokowego
98. Automatyczny backup logów transakcyjnych dla baz danych w oparciu o procent wolnego miejsca na systemie plikowym, minimum dla: Oracle, SQL, Notes, SAP/Oracle

99. Dla MS SQL możliwość skonfigurowania rozszerzenia pozwalającego backupować i odtwarzać bazy bezpośrednio z konsoli Management Studio
100. Wsparcie dla backupu online dla minimum MS SQL Server 2005/2008/2008 R2/2012/2014/2016/2017/2019 na platformie Windows
101. Dedykowany agent bazodanowy dla backupu MS SQL (2017/2019) na platformie Linux: Ubuntu, SuSe, RHEL
102. Możliwość (jako opcja) archiwizacji danych z baz Oracle do plików XML
103. Odtwarzanie baz SAP opartej na silniku Oracle do pliku, a więc odtwarzanie backupu online na dysk (tzw. application free restore)
104. Dedykowani agenci (jako opcja) do backupu systemów Big Data: Hadoop, Greenplum, GPFS, Splunk
105. Możliwość integracji kopii migawkowych dla backupu konsystentnego aplikacji i baz danych minimum: Vmware, Hyper-V, MS SQL, Exchange, MySQL, Oracle – zarządzanie kopiami migawkowymi musi odbywać się z konsoli administracyjnej systemu backupowego a integracja zarządzania nie może odbywać się na bazie skryptów
106. Możliwość backupu i odtwarzania, (jako opcja) dedykowanym agentem dokumentów i maili dla Office 365:
- SharePoint Online
 - Exchange Online
 - OneDrive
 - Teams
107. Możliwość, (jako opcja) pełnokontekstowego indeksowania i wyszukiwania treści z danych backupowanych (dokumenty i maile) z O365
108. System musi zapewniać (jako opcja) backup laptopów i desktopów – funkcjonalność ta musi być w pełni zintegrowana z systemem (ta sama konsola, to samo repozytorium danych, ta sama deduplikacja) o funkcjonalnościach:
- Portal samoobsługowy musi być dostępny poprzez dowolną przeglądarkę sieci Internet minimum: Edge, Chrome, Opera, Mozilla, Safari
 - System musi umożliwiać backup laptopów czy desktopów z systemami Windows, Linux i Macintosh
 - Dostęp do danych zbackupowanych z laptopów czy desktopów musi być możliwy z urządzeń mobilnych poprzez dedykowanego klienta minimum dla IOS i Android
 - Dla backupu laptopów i desktopów system backupowy musi oferować dedykowanego agenta, który pozwala skonfigurować zadanie backupowe tak by było wykonane w przedziale czasowym bez podawania konkretnej daty czy czasu jego uruchomienia, agent nie może tworzyć kopii danych na lokalnych zasobach stacji/laptopa.
 - System musi zapewniać współdzielenie plików pochodzących z backupu laptopów i desktopów z użytkownikami z domeny AD oraz z użytkownikami spoza domeny.

- System musi oferować możliwość synchronizacji wybranego katalogu/foldera z stacji roboczej celem automatycznego backupu danych w nim zapisanych (backup ciągły)
- Każdy użytkownik desktopa czy laptopa musi posiadać możliwość zarządzania własnymi danymi, minimalna oczekiwana funkcjonalność to:
 - ✓ Odtwarzanie własnych danych
 - ✓ Uruchomienie backupu
 - ✓ Wstrzymanie backupu
 - ✓ Możliwość zdefiniowania innego okna backupowego
 - ✓ Możliwość monitorowania postępu działania zadania
 - ✓ Możliwość przeglądania danych z stacji roboczej czy laptopa poprzez dedykowanego klienta dla urządzeń mobilnych, a więc użytkownik posiadając jedynie urządzenie mobilne może nie tylko odczytywać dane z backupowej kopii ale także przeglądać dane na stacji roboczej nawet w momencie gdy jest poza siedzibą firmy – korzysta jedynie z dostępu do internetu (do przeglądania danych nie jest potrzebne żadne dodatkowe połączenie VPN)
- Wirtualny dysk - System musi oferować funkcjonalności jak:
 - ✓ możliwość synchronizacji wybranego katalogu/foldera z stacji roboczej celem automatycznego backupu danych w nim zapisanych (backup ciągły)
 - ✓ możliwość przesłania katalogów i plików ręcznie
 - ✓ możliwość udostępniania zawartości innym użytkownikom także zewnętrznym
 - ✓ zarządzanie poprzez przeglądarkę i dedykowaną aplikację na urządzeniach minimum iOS i Android
- Zabezpieczenie przed kradzieżą, system musi posiadać możliwość zdalnego zaszyfrowania danych w przypadku kradzieży laptopa, to znaczy, iż w przypadku utraty urządzenia administrator lub użytkownik włącza opcję szyfrującą i jeśli urządzenie pojawi się w sieci wtenczas automatycznie dane zostaną zaszyfrowane
- Możliwość archiwizowania danych plikowych na stacji roboczej: jeśli dane pliki spełniają kryteria archiwizacyjne to dany plik zostaje skasowany albo zamieniony na skrót (stub)

109. Rozwiązanie musi pozwalać na archiwizację danych z możliwością pozostawiania znaczników (stub) na zasobach produkcyjnych (dla zasobów plikowych Windows/Linux/Unix) serwerów fizycznych, archiwizacja musi korzystać z tej samej architektury systemu co backup i korzystać z tego samego repozytorium danych.

110. System musi posiadać funkcjonalności archiwizacyjne (archiwizacja plikowa) takie jak:

- Oprogramowanie musi wspierać archiwizację zgodnych z wyznaczonymi kryteriami danych z systemów produkcyjnych na inne tańsze pamięci masowe. Mechanizm ten pozwoli na zmniejszenie ilości danych na systemach produkcyjnych.
- Oprogramowanie musi obsługiwać strategię wielowarstwowego aktywnego archiwum. Na przykład, umożliwiać przenoszenie zarchiwizowanych plików pomiędzy różnorodnymi urządzeniami pamięci

masowej, w sposób zautomatyzowany przez politykę do wykonania krótko-, średnio- i długoterminowe okresów retencji, przy zachowaniu przejrzystego jedno- krokowego odzyskiwania dla użytkowników końcowych.

- Oprogramowanie musi być zintegrowane z modułem do tworzenie kopii zapasowych w celu redukcji czasu okien backupowych przy zabezpieczaniu dużej ilości danych.
 - Oprogramowanie musi umożliwiać deduplikację danych archiwizowanych na poziomie bloków w celu redukcji ilości przestrzeni na dyskach fizycznych. Oprogramowanie musi umożliwiać globalną deduplikację dla archiwizacji i kopii zapasowych w celu minimalizowania zużycia pamięci masowej.
 - Oprogramowanie musi zapewniać przezroczysty dostęp użytkowników do danych archiwalnych poprzez mechanizm skrótów
111. System musi (jako opcja) umożliwiać rozbudowę o archiwizację poczty (minimum Exchange), archiwizacja poczty musi umożliwiać archiwizowanie maili z skrzynek pocztowych oraz archiwizowanie ruchu pocztowego (journaling lub SMTP journaling)
112. Oprogramowanie musi umożliwiać (jako opcja) pełnokontekstowo indeksować maile wraz z załącznikami oraz posiadać centralną konsolę do wyszukiwania danych i monitorowania zgodności z przepisami/normami bezpieczeństwa (compliance).
113. System musi umożliwiać (jako opcja) pełnokontekstowe indeksowania treści danych dla wybranych typów plików, także z backupu stacji roboczych, indeksacja musi odbywać się dla danych znajdujących się już w systemie.
114. System musi umożliwiać (jako opcja) przeprowadzanie wielu wyszukiwań (eDiscovery) i zbierać wszystkie wyniki w jednej lokalizacji.
115. System musi oferować mechanizm składowania kopii backupowych (retencja danych) oparty o czas i cykle. Oznacza to iż kopia backupowa jest przechowywana w repozytorium przez określony czas (np. tydzień, miesiąc, rok) a jej automatyczne skasowanie jest wykonane jeśli spełniony jest jednocześnie warunek ilości cykli a więc ilość backupów typu pełnego lub backupów syntetycznych znajdujących się w systemie
116. Musi istnieć dedykowany agent do backupu online aplikacji MongoDB
117. System musi oferować integrację z mechanizmami deduplikacyjnymi urządzeń typu appliance minimalne wsparcie to Catalyst i urządzenie StoreOnce. Integracja z StoreOnce musi być dostępna nie tylko dla Windows, ale także dla Unix i Linux.
118. System (jako opcja) musi oferować rozbudowę o funkcjonalność przeszukiwania i analizy zasobów plikowych dla maszyn wirtualnych (minimum Vmware) całość działań związanych musi odbywać się na kopiach backupowych maszyn wirtualnych a nie na środowisku produkcyjnym
119. System (jako opcja) musi posiadać zaawansowaną funkcjonalność analizy zasobów plikowych minimum o funkcjonalnościach:
- Detekcja powtarzających się zasobów
 - Raportowanie praw dostępu do plików

- Raportowanie i analiza dostępu do zasobów i ich modyfikacji
 - Możliwość kasowania plików z zasobów produkcyjnych
120. System (jako opcja) musi pozwalać na wyszukiwanie danych wrażliwych (np. numery PESEL) i pozwalać osobie uprawnionej nie tylko na raportowanie takich zdarzeń, ale także umożliwiać kasowanie plików nie tylko z systemów produkcyjnych, ale i z kopii backupowej
121. Musi istnieć możliwość zarządzania systemem poprzez Windows PowerShell
122. Agent do spójnego backupu bazy HBASE – backup pełny i przyrostowy
123. Agent do backupu systemów plikowych: Lustre, GlusterFS
124. Wsparcie (jako opcja) dla replikacji maszyn wirtualnych Vmware z wykorzystaniem VAAI (VSphere APIs for I/O)
125. Monitorowanie i alertowanie klientów systemu którzy są trybie offline, a więc komunikacja z nimi przez system backupowy nie jest możliwa
126. Możliwość backupu baz Oracle bez instalacji oprogramowania backupowego natomiast dane zbackupowane muszą być składowane i zarządzane przez system backupowy
127. System musi posiadać integrację z ServiceNow o funkcjonalnościach:
- Dedykowany plugin do ServiceNow
 - Możliwość zgłaszania zdarzeń backupowych i odtworzeniowych bezpośrednio z konsoli ServiceNow
128. Możliwość (jako opcja) rozbudowy środowiska o moduł VTL dla backupu danych po sieci SAN i LAN na dowolnym sprzęcie typu x86
129. Możliwość włączenia backupu pojedynczego pliku wieloma strumieniami
130. Możliwość zwiększenia bezpieczeństwa systemu poprzez integrację z CyberArk
131. Musi istnieć możliwość wskazania klucza szyfrującego (Bring Your Own Key – BYOK), który będzie wykorzystywany do szyfrowania kopii backupowych
132. Dedykowane moduły do integracji z Terraform
133. Możliwość anonimizacji danych wrażliwych (data masking) minimum dla logów systemu wysyłanych np. do wsparcia
134. Podstawowe komponenty systemu jak: serwer zarządzający, serwery składujące i deduplikujące dane muszą wspierać system operacyjny Linux, a więc musi istnieć możliwość bezpośredniego zainstalowania na systemie Linux tych komponentów bez jakiegokolwiek warstwy wirtualizacyjnej

Wymogi dla licencjonowania

1. Niedopuszczalne jest, aby licencjonowanie było zależne od ilości składowanych danych (kopii backupowych) na dowolnych nośnikach (np. dysk, taśma VTL...) czy to z deduplikacją czy bez.
2. Niedopuszczalne jest, aby licencjonowanie było zależne od ilości komponentów środowiska backupowego, które będą wykorzystywane w procesie backupu czy odtwarzania danych.

3. Niedopuszczalne jest, aby licencjonowanie zależne było od ilości serwerów fizycznych czy ich mocy (ilości procesorów) niezależnie czy dane są z nich backupowane bezpośrednio czy tworzą platformę wirtualizacyjną, która jest backupowana.
4. Zaoferowane licencje nie mogą ograniczać wielkości przestrzeni do składowania danych czy replik ich do innych lokalizacji. Jakakolwiek rozbudowa przestrzeni dyskowej czy to w siedzibie podstawowej czy innej nie może wymagać zakupu jakichkolwiek licencji dla systemu.
5. Oferowana licencja oraz architektura systemu muszą pozwalać na backup danych na:
 - nielimitowana ilość napędów fizycznych;
 - nielimitowaną przestrzeń w rozwiązaniach chmurowych (minimum: AWS, Azure, Google).
6. W przypadku wielu lokalizacji licencja musi pozwalać na nielimitowaną replikację danych po deduplikacji pomiędzy lokalizacjami.
7. Zaoferowane licencje na system muszą zapewnić backup danych dla całego środowiska.

Centralny serwer kopii zapasowych.

Tabela S3.		
SERWERY CENTRALNY BACKUP – 1 szt		
Lp.	Nazwa elementu, parametru lub cechy	Wymagania szczegółowe
S3.1	Obudowa	Obudowa typu RACK 19 cali wraz z zestawem do zamontowania w szafie teleinformatycznej 19 cali umożliwiającym wysunięcie obudowy, o wysokości 1U, umożliwiającą instalację minimum 8 dysków HDD lub SSD w formie 2.5-in. SFF 12Gb SAS lub SATA wymiennych od przodu serwera (hot-swap) oraz umożliwiającą instalację redundantnego zasilacza (wszystkie zasilacze wymienne w trybie hot-swap).
S3.2	Płyta główna	Serwerowa płyta główna zapewniająca obsługę: <ul style="list-style-type: none"> – minimum dwóch fizycznych procesorów 64 bitowych, umożliwiającą zastosowanie technologii wirtualizacji, – minimum 32 sloty do obsługi pamięci DDR4 pracującej z częstotliwością co najmniej 4800 MHz, – możliwość wyposażenia serwera w minimum 8TB RAM, – łączna ilość możliwej do zainstalowania pamięci RDIMM oraz pamięci persistent memory powinna wynosić minimum 12TB, – umożliwia instalację minimum dwóch modułów M.2 lub instalację minimum dwóch kart SD z funkcjonalnością duplikacji zapisu (Mirror),
S3.3	Karta graficzna	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.
S3.4	Procesor	Minimum dwa procesory o parametrach nie gorszych niż: <ul style="list-style-type: none"> – liczba rdzeni: 8 – częstotliwość taktowania zegara: min. 2.9GHz, – cache L2: min. 22MB – ilość kanałów pamięci: min. 8 – procesor powinien wspierać funkcjonalność dynamicznego i automatycznego zwiększenia wydajności serwera dla aplikacji poprzez zwiększenie częstotliwości taktowania rdzenia, – wyposażony w technologię wirtualizacji,
S3.5	Pamięć operacyjna	Zainstalowane nie mniej niż 32 GB RAM taktowane zegarem nie mniejszym niż 4800 MHz. Wspierane zabezpieczenia pamięci RAM: ECC, SDDC, ADDDC
S3.6	Dyski	Zainstalowane minimum 2 szt. dysków SSD o pojemności min. 400 GB każdy, parametr DWDP – min 4. Złożone w grupę RAID1.

S3.7	Kontroler macierzy	Zainstalowany kontroler dyskowy wyposażony w minimum 8GB pamięci cache, nie zajmujący żadnego ze slotów PCIe wymienionych w punkcie Dodatkowe sloty I/O. Kontroler powinien obsługiwać jednocześnie dyski SAS/SATA oraz dyski NVMe. Pamięć cache kontrolera powinna być chroniona przed utratą danych w przypadku awarii zasilania poprzez kopię danych na pamięć typu flash. Nie akceptuje się rozwiązań wykorzystujących tzw. podtrzymanie zasilania cache za pomocą układu baterii. Kontroler powinien obsługiwać następujące grupy RAID: 0,1,10,5,50,6,60. Wymaga się, aby kontroler posiadał funkcjonalność kontynuowania procesu odbudowy macierzy RAID przerwanej na skutek awarii zasilania. Zmiana pojemności zdefiniowanych dysków wirtualnych powinna odbywać się online. Wymaga się także możliwości zmiany typu RAID grupy dyskowej w trybie online.
S3.8	Zasilanie	Co najmniej 2 szt. wysokiej sprawności (certyfikat minimum Titanium) zasilacze prądu zmiennego umożliwiające pracę z sieci o napięciu 230V wraz z kablami umożliwiającymi podłączenie do gniazd elektrycznych typu E oraz kablami umożliwiającymi podłączenie do komputerowych gniazd elektrycznych typu IEC, umożliwiające stabilną i bezprzerwową pracę całej platformy serwerowej w maksymalnej przewidzianej przez producenta konfiguracji przy połowie działających zasilaczy z ogólnej liczby zainstalowanych. Wymiana zasilaczy musi odbywać się bez konieczności wyłączenia urządzenia.
S3.9	Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
S3.10	Interfejsy sieciowe	<ul style="list-style-type: none"> – min. 4 szt. portów Ethernet o przepustowości 1 Gbps typu Base-T w postaci portów zintegrowanych z płytą główną (dopuszcza się rozwiązania w postaci kart rozszerzeń) – jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
S3.11	Inne interfejsy	2 bezpośrednio udostępnione zewnętrzne porty USB 3.0, 1 bezpośrednio udostępniony port VGA.
S3.12	Sloty rozszerzeń	min. 3 sloty PCI-EXPRESS min. generacji 3 w tym min. jedno gniazdo pozwalające na instalację karty pełnej wysokości.
S3.13	Mechanizmy bezpieczeństwa	Zainstalowany czujnik otwarcia obudowy zintegrowany z modulem zarządzania serwerem, hasło włączania, hasło administratora, moduł TPM. Zainstalowany przedni panel zamykany na klucz.
S3.14	Wspierane oprogramowanie	Microsoft Windows Server 2019, 2022, Red Hat Enterprise Linux 7, 8, 9 SUSE Linux Enterprise Server 12 oraz 15, VMware vSphere (ESXi) 6, 7, Ubuntu 18, 20, 22.
S3.15	Inne	Wysuwane szyny montażowe do szaf typu rack 19 cali wraz z ramieniem do zarządzania kablami
S3.16	Zarządzanie	<p>Serwer wyposażony w zintegrowany z płytą główną, moduł zdalnego zarządzania (konsoli) zapewniający (dla indywidualnego serwera):</p> <ul style="list-style-type: none"> – Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: cpu, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna, – Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, użycie cpu, użycie pamięci oraz komponentów I/O, – Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów, – Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń, – Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3, – Update systemowego firmware, – Monitoring i możliwość ograniczenia poboru prądu, – Zdalne włączanie/wyłączanie/restart, – Zapis video zdalnych sesji, – Podmontowanie lokalnych mediów z wykorzystaniem Java client, – Przekierowanie konsoli szeregowej przez IPMI, – Zrzut ekranu w momencie zawieszenia systemu, – Możliwość przejścia zdalnego ekranu, – Możliwość zdalnej instalacji systemu operacyjnego, – Alerty Syslog, – Przekierowanie konsoli szeregowej przez SSH, – Wyświetlanie danych aktualnych i historycznych dla użycia energii oraz temperatury serwera, – Możliwość mapowania obrazów ISO z lokalnego dysku operatora, – Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS, – Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę, – wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API,

S3.16	Zarządzanie	<p>Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające:</p> <ul style="list-style-type: none"> – zarządzanie infrastrukturą serwerów i storage bez udziału dedykowanego agenta, – przedstawianie graficznej reprezentacji zarządzanych urządzeń, – możliwość skalowania do minimum 1000 urządzeń, – obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2, – wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych, – udostępnianie szybkiego podglądu stanu środowiska, – udostępnianie podsumowania stanu dla każdego urządzenia, – tworzenie alertów przy zmianie stanu urządzenia, – monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, – konsola zarządzania oparta o HTML 5, – dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, – automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja, – możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania, – definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń, – definiowanie roli użytkowników oprogramowania, – obsługa REST API oraz Windows PowerShell, – obsługa SNMP, SYSLOG, Email Forwarding,
-------	-------------	--

Serwer kopii zapasowych – media agent.

Tabela S4.		
SERWERY MEDIA-AGENT – 1 szt		
Lp.	Nazwa elementu, parametru lub cechy	Wymagania szczegółowe
S4.1	Obudowa	Obudowa typu RACK 19 cali wraz z zestawem do zamontowania w szafie teleinformatycznej 19 cali umożliwiającym wysunięcie obudowy, o wysokości 1U, umożliwiającą instalację minimum 8 dysków HDD lub SSD w formie 2.5-in. SFF 12Gb SAS lub SATA wymiennych od przodu serwera (hot-swap) oraz umożliwiającą instalację redundantnego zasilacza (wszystkie zasilacze wymienne w trybie hot-swap).
S4.2	Płyta główna	Serwerowa płyta główna zapewniająca obsługę: <ul style="list-style-type: none"> – minimum dwóch fizycznych procesorów 64 bitowych, umożliwiającą zastosowanie technologii wirtualizacji, – minimum 32 sloty do obsługi pamięci DDR4 pracującej z częstotliwością co najmniej 4800 MHz, – możliwość wyposażenia serwera w minimum 8TB RAM, – łączna ilość możliwej do zainstalowania pamięci RDIMM oraz pamięci persistent memory powinna wynosić minimum 12TB, – umożliwia instalację minimum dwóch modułów M.2 lub instalację minimum dwóch kart SD z funkcjonalnością duplikacji zapisu (Mirror),
S4.3	Karta graficzna	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.
S4.4	Procesor	Minimum dwa procesory o parametrach nie gorszych niż: <ul style="list-style-type: none"> – liczba rdzeni: 8 – częstotliwość taktowania zegara: min. 2.9GHz, – cache L2: min. 22MB – ilość kanałów pamięci: min. 8 – procesor powinien wspierać funkcjonalność dynamicznego i automatycznego zwiększenia wydajności serwera dla aplikacji poprzez zwiększenie częstotliwości taktowania rdzenia, – wyposażony w technologię wirtualizacji,
S4.5	Pamięć operacyjna	Zainstalowane nie mniej niż 128 GB RAM taktowane zegarem nie mniejszym niż 3200 MHz. Wspierane zabezpieczenia pamięci RAM: ECC, SDDC, ADDDC

S4.6	Dyski	Zainstalowane dyski: - minimum 2 szt. dysków SSD o pojemności min. 400 GB każdy, parametr DWDP – min 4, złożone w grupę RAID1, - minimum 2 szt. Dysków SSD o pojemności min 1.9TB każdy, parametr DWPD – min 4, złożone w grupę RAID1, - minimum 2 szt. Dysków SSD o pojemności min 1.9TB każdy, parametr DWPD – min 4, złożone w grupę RAID1,
S4.7	Kontroler macierzy	Zainstalowany kontroler dyskowy wyposażony w minimum 8GB pamięci cache, nie zajmujący żadnego ze slotów PCIe wymienionych w punkcie Dodatkowe sloty I/O. Kontroler powinien obsługiwać jednocześnie dyski SAS/SATA oraz dyski NVMe. Pamięć cache kontrolera powinna być chroniona przed utratą danych w przypadku awarii zasilania poprzez kopię danych na pamięć typu flash. Nie akceptuje się rozwiązań wykorzystujących tzw. podtrzymanie zasilania cache za pomocą układu baterii. Kontroler powinien obsługiwać następujące grupy RAID: 0,1,10,5,50,6,60 . Wymaga się, aby kontroler posiadał funkcjonalność kontynuowania procesu odbudowy macierzy RAID przerwanego na skutek awarii zasilania. Zmiana pojemności zdefiniowanych dysków wirtualnych powinna odbywać się online. Wymaga się także możliwości zmiany typu RAID grupy dyskowej w trybie online.
S4.8	Zasilanie	Co najmniej 2 szt. wysokiej sprawności (certyfikat minimum Titanium) zasilacze prądu zmiennego umożliwiające pracę z sieci o napięciu 230V wraz z kablami umożliwiającymi podłączenie do gniazd elektrycznych typu E oraz kablami umożliwiającymi podłączenie do komputerowych gniazd elektrycznych typu IEC, umożliwiające stabilną i bezprzerwową pracę całej platformy serwerowej w maksymalnej przewidzianej przez producenta konfiguracji przy połowie działających zasilaczy z ogólnej liczby zainstalowanych. Wymiana zasilaczy musi odbywać się bez konieczności wyłączenia urządzenia.
S4.9	Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
S4.10	Interfejsy sieciowe	<ul style="list-style-type: none"> – min. 4 szt. portów Ethernet o przepustowości 1 Gbps typu Base-T w postaci portów zintegrowanych z płytą główną (dopuszcza się rozwiązania w postaci kart rozszerzeń), – min. 1 szt. co najmniej dwuportowa karta FC PCI-E HBA (Host Bust Adapter) z modułami 32Gb FC, umożliwiającymi podłączenie zewnętrznej macierzy/switcha SAN interfejsem FC o przepustowości 32Gb, – min. 1 szt. co najmniej dwuportowa, karta sieciowa 10 Gbps (SFP+) wraz z wkładkami (modułami) SFP+ – jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
S4.11	Inne interfejsy	2 bezpośrednio udostępnione zewnętrzne porty USB 3.0, 1 bezpośrednio udostępniony port VGA.
S4.12	Sloty rozszerzeń	min. 3 sloty PCI-EXPRESS min. generacji 3 w tym min. jedno gniazdo pozwalające na instalację karty pełnej wysokości.
S4.13	Zarządzanie	Serwer wyposażony w zintegrowany z płytą główną, moduł zdalnego zarządzania (konsoli) zapewniający (dla indywidualnego serwera): <ul style="list-style-type: none"> – Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: cpu, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna, – Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, użycie cpu, użycie pamięci oraz komponentów I/O, – Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów, – Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń, – Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3, – Update systemowego firmware, – Monitoring i możliwość ograniczenia poboru prądu, – Zdalne włączanie/wyłączanie/restart, – Zapis video zdalnych sesji, – Podmontowanie lokalnych mediów z wykorzystaniem Java client, – Przekierowanie konsoli szeregowej przez IPMI, – Zrzut ekranu w momencie zawieszenia systemu, – Możliwość przejęcia zdalnego ekranu, – Możliwość zdalnej instalacji systemu operacyjnego, – Alerty Syslog,

S4.13	Zarządzanie	<ul style="list-style-type: none"> – Przekierowanie konsoli szeregowej przez SSH, – Wyświetlanie danych aktualnych i historycznych dla użycia energii oraz temperatury serwera, – Możliwość mapowania obrazów ISO z lokalnego dysku operatora, – Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS, – Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę, – wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API, <p>Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające:</p> <ul style="list-style-type: none"> – zarządzanie infrastrukturą serwerów i storage bez udziału dedykowanego agenta, – przedstawianie graficznej reprezentacji zarządzanych urządzeń, – możliwość skalowania do minimum 1000 urządzeń, – obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2, – wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych, – udostępnianie szybkiego podglądu stanu środowiska, – udostępnianie podsumowania stanu dla każdego urządzenia, – tworzenie alertów przy zmianie stanu urządzenia, – monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, – konsola zarządzania oparta o HTML 5, – dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, – automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja, – możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania, – definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń, – definiowanie roli użytkowników oprogramowania, – obsługa REST API oraz Windows PowerShell, – obsługa SNMP, SYSLOG, Email Forwarding,
S4.14	Mechanizmy bezpieczeństwa	Zainstalowany czujnik otwarcia obudowy zintegrowany z modulem zarządzania serwerem, hasło włączania, hasło administratora, moduł TPM. Zainstalowany przedni panel zamykany na klucz.
S4.15	Wspierane oprogramowanie	Microsoft Windows Server 2019, 2022, Red Hat Enterprise Linux 7, 8, 9 SUSE Linux Enterprise Server 12 oraz 15, VMware vSphere (ESXi) 6, 7, Ubuntu 18, 20, 22. Serwer musi wspierać oprogramowanie do wirtualizacji będące przedmiotem niniejszego postępowania.
S4.16	Inne	Wysuwane szyny montażowe do szaf typu rack 19 cali wraz z ramieniem do zarządzania kablami Wykonawca zapewnia kable połączeniowe FC oraz LAN umożliwiające przyłączenie serwerów do switchy SAN/LAN. Zainstalowany system operacyjny MS Windows Server 2022 Standard, licencja zgodna z polityką Microsoft.

Repozytorium dyskowe kopii zapasowych.

W celu sporządzania kopii zapasowych danych rekomendujemy rozwiązanie oparte o dedykowaną macierz dyskową, która stanowić będzie zasób, na który trafiać będą zabezpieczone dane. Zastosowana macierz dyskowa klasy hybrydowej, zostanie wyposażona w dyski 14TB NL-SAS. Przestrzeń dyskowa macierzy zostanie zbudowana w oparciu jedną pulę dyskową z zabezpieczeniem RAID6. Pula dyskowa będzie miała pojemność 174TiB. Dedykowana przestrzeń dyskowa zostanie zaprezentowana do serwera kopii zapasowych za pomocą redundantnych ścieżek, o przepustowości pojedynczego linku 32Gbps. Proponowane repozytorium dyskowe posiada prosty sposób skalowania poprzez rozbudowę o dodatkowe nośniki danych zainstalowane w półkach dyskowych.

Tabela M2.		
Macierz – 1 sztuka		
Lp.	Nazwa elementu, parametru lub cechy	Wymagania szczegółowe
M2.1	Obudowa	<ul style="list-style-type: none"> – do instalacji w standardowej szafie rack 19" dostarczona wraz z szynami montażowymi oraz innymi elementami niezbędnymi do montażu. – musi zawierać układ nadmiarowy dla modułów zasilania i chłodzenia umożliwiający wymianę tych elementów w razie awarii bez konieczności wyłączania macierzy. – powinna posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii macierzy. – zasilanie jednofazowe. – zajętość w szafie serwerowej nie więcej 5U.
M2.2	Architektura systemu dyskowego	<ul style="list-style-type: none"> – Oferowane urządzenie musi się składać z pojedynczej macierzy dyskowej. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych połączonych przełącznikami SAN, LAN lub witalizatorem w sieci SAN. – Urządzenie musi się składać z co najmniej dwóch kontrolerów pracujących w trybie symetrycznym active/active – Konstrukcja macierzy powinna zapewnić sprzętowe rozłożenie operacji I/O pomiędzy kontrolerami macierzy. Operacje I/O muszą być kierowane równomiernie (z tą samą wydajnością) przez porty zewnętrzne dwóch kontrolerów, do których będą podłączone serwery. Kontrolery muszą pracować w trybie wysokiej dostępności, w przypadku awarii jednego kontrolera drugi automatycznie przejmie jego funkcję. – Kontrolery dyskowe, obsługujące dyski SAS i dyski mechaniczne powinny wykorzystywać interfejs co najmniej SAS 12Gbps. – Oferowana architektura musi pozwalać na realizację wszystkich prac serwisowych w trybie bezprzerwowym.
M2.3	Redundancja	<ul style="list-style-type: none"> – Oferowaną macierz musi cechować brak pojedynczego punktu awarii. Wszystkie krytyczne komponenty muszą być zdublowane. – Uszkodzenie jednego z podzespołów nie może spowodować przerw w pracy urządzenia. Wszystkie komponenty muszą być przystosowane do wymiany podczas pracy macierzy.
M2.4	Pamięć cache	<ul style="list-style-type: none"> – Macierz musi być wyposażona w minimum 64 GB pamięci cache per kontroler. – Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM (nie dopuszcza się stosowania dysków SSD lub kart pamięci jako pamięci cache). – Odporność na awarię pamięci cache, wszystkie zapisy do pamięci cache muszą być przechowywane w dwóch kopiach. W przypadku awarii zasilania macierz musi posiadać możliwość automatycznego zrzucenia danych z pamięci cache na dedykowaną przestrzeń dyskową.
M2.5	Pojemność użytkowa TiB (base2 1kB=1024B)	<ul style="list-style-type: none"> – Macierz dyskowa musi udostępniać minimum 174 TiB przestrzeni użytkowej netto (base2) w konfiguracji RAID 6. Przestrzeń musi być zbudowana w oparciu o wydajne dyski NL-SAS. – Macierz dyskowa wyposażona w 1 globalny dysk zapasowy hot-spare lub rekomendowaną przez producenta nadmiarową przestrzeń dyskową. – Musi istnieć możliwość instalacji w macierzy jednocześnie dysków flash, jak i dysków mechanicznych (bez wykorzystania funkcjonalności wirtualizacji zewnętrznych macierzy). – Macierz musi mieć możliwość rozbudowy do 180 wewnętrznych dysków SAS. – Nie dopuszcza się stosowania dodatkowych zewnętrznych kontrolerów macierzy dyskowych w celu rozbudowy oferowanej macierzy.
M2.6	Interfejsy	<ul style="list-style-type: none"> – Macierz musi posiadać 4 interfejsy FC 32 Gbps SFP+ z możliwością rozbudowy do 8 poprzez dokupienie wyłącznie wkładek SFP 32Gbps SFP+. – Macierz musi mieć możliwość rozbudowy o interfejsy iSCSI 10Gb/s. – Macierz musi mieć możliwość rozbudowy o interfejsy FC o prędkościach 16, 32 Gbps. – Macierz musi posiadać dedykowane 2 porty do zarządzania przez sieć Ethernet 1 Gbps.
M2.7	Półki dyskowe	<ul style="list-style-type: none"> – Macierz musi mieć możliwość instalacji w półkach dyskowych dysków typu NL-SAS, SAS, SSD. – Półki dyskowe muszą umożliwiać wymianę uszkodzonych dysków twardych „na gorąco”.
M2.8	Obsługiwane dyski	<ul style="list-style-type: none"> – Macierz musi obsługiwać co najmniej dyski 2,5" oraz 3,5". Oferowany model macierzy musi wspierać co najmniej obsługę następujących typów dysków: <ul style="list-style-type: none"> a) SSD – 1.9TB, 3.8TB, 7.6TB, 15TB. b) SAS – 1.2TB, 2.4TB c) NL-SAS – 6TB, 10TB, 14TB

M2.9	Optymalizacja danych	<ul style="list-style-type: none"> Macierz musi posiadać funkcję optymalizacji wykorzystania dysków SSD, SAS, NLSAS poprzez automatyczną migrację fragmentów woluminów na szybsze lub wolniejsze dyski w zależności od obciążenia tzw. tiering. Funkcja ta musi działać na 2 i 3 warstwach dyskowych. <p>Zamawiający wymaga dostarczenia licencji na tę funkcję.</p> <ul style="list-style-type: none"> Macierz musi posiadać funkcję migracji całych woluminów logicznych w obrębie dysków wewnętrznych macierzy jak i dysków zwirtualizowanych zainstalowanych w innych macierzach. Funkcja musi być realizowana bez zatrzymania aplikacji i musi być w pełni transparentna dla działających aplikacji na migrowanym woluminie. Zamawiający wymaga dostarczenia licencji na tę funkcję.
M2.10	Poziomy RAID	<ul style="list-style-type: none"> Macierz musi obsługiwać następujące poziomy zabezpieczeń RAID-10, RAID-5, RAID-6 (lub równoważny, gwarantujący zabezpieczenie przez awarią dwóch dysków w grupie).
M2.11	Monitoring	<ul style="list-style-type: none"> Macierz musi obsługiwać priorytety ruchu I/O tzw. Quality of Service. Zamawiający wymaga dostarczenia licencji na tę funkcję. Wymagane jest monitorowanie i raportowanie wydajności Macierzy, obejmujące również środowiska wirtualizacyjne (co najmniej Vmware). Wymagane jest zbieranie co najmniej następujących danych: <ul style="list-style-type: none"> a) wielkość przestrzeni dyskowej macierzy: całościowa, wolna, wykorzystana, b) czas dostępu do danych na wolumenach logicznych, c) wykorzystanie interfejsów do wykonywania kopii pomiędzy macierzami, d) czas odpowiedzi interfejsów do wykonywania kopii pomiędzy macierzami, e) wykorzystanie pamięci Cache, f) wykorzystanie dysków SSD lub NVMe, g) przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, woluminów logicznych, dysków oraz kontrolerów. Zbieranie danych wymienionych w punkcie a) do g) powyżej - co 15 minut lub w czasie krótszym niż 15 minut. Czas przechowywania danych wymienionych w punkcie a) do g) nie krócej niż 30 dni, przy czym po 7 dniach dane mogą zostać zagregowane. Możliwość eksportowania danych wymienionych w punkcie a) do g) w formacie tekstowym, csv, xls lub innym umożliwiającym ich odczyt przy użyciu programu Microsoft Excel. Maszyn wirtualnych: <ul style="list-style-type: none"> a) korelacja maszyn wirtualnych z wolumenami logicznymi macierzy, b) wydajność i czas odpowiedzi maszyn wirtualnych.
M2.12	Thin provisioning	<ul style="list-style-type: none"> Macierz musi posiadać funkcję udostępniania zasobów dyskowych do hostów w trybie tzw. ThinProvisioning. Zamawiający wymaga dostarczenia licencji na tę funkcję. Macierz musi umożliwiać utworzenie wolumenu logicznego o rozmiarze co najmniej 256TB.
M2.13	Zarządzanie przestrzenią dyskową	<ul style="list-style-type: none"> Macierz musi umożliwiać zwiększenie pojemności woluminów logicznych w trybie bezprzerwowym. Zamawiający wymaga dostarczenia licencji na tę funkcję. Macierz musi umożliwiać administratorowi funkcję wyboru wskazanych konkretnych pojedynczych fizycznych dysków do grup RAID.
M2.14	Zarządzanie macierzą	<ul style="list-style-type: none"> Macierz musi posiadać interfejs graficzny oraz interfejs linii poleceń, umożliwiający tworzenie i obsługę skryptów. Macierz powinna posiadać oprogramowanie do zarządzania, pozwalające na co najmniej: <ul style="list-style-type: none"> a) Tworzenie i nazywanie woluminów logicznych LUN, b) Mapowanie woluminów logicznych do serwerów wraz z możliwością konfigurowania zoniingu w sieci SAN (wsparcie dla przełączników Cisco oraz Brocade), c) Monitorowanie wykorzystywanej przestrzeni, efektywnej i surowej (RAW) macierzy. Zamawiający wymaga dostarczenia licencji na te funkcje.
M2.15	Wewnętrzne kopie danych	<ul style="list-style-type: none"> Macierz musi posiadać funkcję tworzenia wewnętrznych kopii danych opartych o: <ul style="list-style-type: none"> a) Klonowanie z ang. Clone. Możliwość wykonania kopii na inny rodzaj dysków i inny typ zabezpieczenia RAID, b) Migawkę z ang. Snapshot. Zamawiający wymaga dostarczenia licencji na te funkcje.
M2.16	Zewnętrzne kopie danych	<ul style="list-style-type: none"> Macierz musi posiadać funkcje replikacji danych do drugiej macierzy tego samego typu w trybie synchronicznym i asynchronicznym. Możliwość uruchomienia obu trybów replikacji tj. replikacja synchroniczna i asynchroniczna w tym samym czasie. Musi istnieć wsparcie do definiowania grup konsystencji (z ang. Consistency Group) dla uruchomionych zadań replikowanych woluminów. Zamawiający nie wymaga dostarczenia licencji na te funkcje.

M2.17	Systemy operacyjne	<ul style="list-style-type: none"> – Macierz musi posiadać możliwość podłączenia wielu serwerów w trybie wysokiej dostępności, co najmniej dwoma ścieżkami. – Macierz musi wspierać LUN Mapping, LUN Masking. – Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, VMware, Linux, Solaris. – Macierz musi być certyfikowana w zakresie VMware Metro Storage Cluster.
M2.18	Multipathing	<ul style="list-style-type: none"> – Macierz musi zostać dostarczona wraz z oprogramowaniem producenta do zapewnienia wielościeżkowości tzw. multipathing. Oprogramowanie musi wspierać min. Następujące systemy operacyjne: Windows, Linux, VMware. – Dostarczona licencja musi umożliwiać podłączenie dowolnej ilości serwerów do oferowanej macierzy dyskowej.
M2.19	Kasowanie danych	<ul style="list-style-type: none"> – Macierz musi zostać dostarczona z oprogramowaniem do bezpiecznego usuwania danych z woluminów dyskowych. Musi istnieć możliwość wielokrotnego nadpisania danych. – Zamawiający wymaga dostarczenia licencji na tę funkcjonalność.
M2.20	Wirtualizacja macierzy dyskowych	<ul style="list-style-type: none"> – Zaoferowane urządzenie musi posiadać wbudowany silnik wirtualizacyjny działający w trybie wysokiej dostępności. Nie dopuszcza się stosowania zewnętrznych wirtualizatorów. – Macierz musi pozwalać na wirtualizację zasobów dyskowych znajdujących się na innych macierzach dyskowych różnych producentów za pomocą protokołu FC, w szczególności producentów takich jak: NetApp, HP, IBM, Fujitsu, HDS, EMC. – Nie jest wymagane dostarczenie licencji.

Oprogramowanie

Systemy operacyjne

Zastosowany system operacyjny musi być wspierany przez producenta dostarczonych serwerów. Systemy operacyjne muszą pracować w architekturze 64 bitowej. Wymaga się dostarczenia wszystkich niezbędnych licencji dla systemów operacyjnych. Dla systemów operacyjnych z rodziny linux zamawiający wymaga zapewnienia wykupienia wsparcia producenta na okres minimum 36 miesięcy podany w warunkach świadczenia usługi utrzymaniowej. Wszystkie poziomy wsparcia muszą być świadczone bezpośrednio przez producenta oprogramowania na rzecz Zamawiającego.

Wirtualizacja

Dla budowanego systemu wymaga się zastosowania rozwiązania opartego o wirtualizację. Zamawiający wymaga zapewnienia wsparcia dla systemu backup (oprogramowanie i sprzęt) na okres 36 miesięcy. Wsparcie producenta dla dostarczonych licencji musi być świadczone bezpośrednio na rzecz Zamawiającego na okres minimum 36 miesięcy.

Sposób świadczenia usługi wsparcia	24 godziny na dobę/7 dni w tygodniu/365 dni w roku
Możliwość pobierania aktualizacji	TAK
Możliwość podniesienia wersji oprogramowania	TAK
Zgłaszanie problemów za pomocą	telefonu i serwisu internetowego
Wsparcie zdalne	TAK
Dostęp do portalu internetowego bazy wiedzy i forum producenta	TAK
Czasy reakcji na zgłoszenia serwisowe w godzinach określonych w czasie świadczenia usługi	Priorytet 1 (krytyczny) - 30 minut od zgłoszenia

Wymaga się, aby oprogramowanie do wirtualizacji spełniało poniższe wymagania:

- oprogramowanie do wirtualizacji musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego,
- w oprogramowaniu warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego,
- oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne tego serwera wyposażone w 768 logicznych wątków, 24TB pamięci fizycznej RAM tego serwera oraz 16 procesorów fizycznych tego serwera,
- oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z ilością od 1 do 768 procesorów wirtualnych,
- oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 24 TB pamięci operacyjnej RAM,
- oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do 10 wirtualnych kart sieciowych dla każdej z nich. Dodatkowo, oprogramowanie musi posiadać możliwość utworzenia maszyny wirtualnej bez przydzielonej wirtualnej karty sieciowej,
- oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowo, 3 porty równoległe i 20 urządzeń USB
- oprogramowanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, SLES 12, SLES 11, SLES 10, SLES 9, RHEL 8, RHEL 7, RHEL 6, RHEL 5, RHEL 4, RHEL 3, RHEL Atomic 7, Solaris 11, Solaris 10, Debian, CentOS, FreeBSD, Asianux, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X, Photon OS, eCommStation 1/2/2.1, Oracle Linux , CoreOS, NeoKylin, Amazon Linux 2,
- W celu osiągnięcia maksymalnego współczynnika konsolidacji, zaoferowane oprogramowanie musi umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są posadowione
- Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych
- oprogramowanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP mode w Microsoft Windows 7 a także instalacji wszystkich funkcjonalności w tym Microsoft Hyper-V pakietu Microsoft Windows Server 2012 na maszynie wirtualnej
- oprogramowanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji bez ingerencji w systemy operacyjne maszyn wirtualnych (bezagentowość)

- oprogramowanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta „root”
- oprogramowanie do wirtualizacji musi zapewnić możliwość powielania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi
- oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
- Konsola zarządzająca zaoferowanego oprogramowania musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, minimalnie z: Microsoft Active Directory i Open LDAP oraz umożliwiać federacyjne zarządzanie tożsamością w oparciu o Microsoft Active Directory Federation Services (ADFS).
- oprogramowanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej
- oprogramowanie musi posiadać funkcjonalność tworzenia wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta (hypervisora wirtualizacyjnego) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji minimum 4000 portów
- Pojedynczy wirtualny przełącznik w zaoferowanym oprogramowaniu, w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej, musi posiadać możliwość przyłączania do niego minimum dwóch fizycznych kart sieciowych
- Wirtualne przełączniki w zaoferowane oprogramowaniu muszą posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN)
- oprogramowanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi
- oprogramowanie musi umożliwiać wykorzystanie technologii przepustowości sieci komputerowych do 200GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi
- oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
- oprogramowanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych
- oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów

- fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania. Replikacja musi gwarantować współczynnik RPO (ang. Recovery Point Objective) na poziomie minimum 5 minut
- oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
 - oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług na przenoszonych maszynach wirtualnych. Wymaga się wsparcia natywnego szyfrowania ruchu sieciowego dla maszyn wirtualnych podczas ich przenoszenia między serwerami fizycznymi
 - oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, oraz w środowisku z więcej niż pojedynczym wirtualizatorem, musi umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z wirtualizatorów na kolejnym, działającym w tym samym klastrze wirtualizatorze (funkcjonalność HA) (ang. high availability)
 - oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter w środowisku z minimalnie dwoma wirtualizatorami oraz w przypadku potrzeby wgrania aktualizacji do warstwy wirtualizacji, musi posiadać możliwość w przypadku wywołania startu aktualizacji, automatycznego przeniesienia bezprzerwowego działających maszyn wirtualnych do innego wirtualizatora nie objętego aktualizacją, przed rozpoczęciem samej aktualizacji
 - oprogramowanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym wirtualizatorem oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci
 - oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, w środowisku z minimum dwoma wirtualizatorami, musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii wirtualizatora, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną
 - oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB
 - oprogramowanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej
 - Producent zaoferowanego oprogramowania do wirtualizacji musi wspierać rozwiązania do automatyzacji procesów oraz wirtualizacji sieci (SDN, ang. software defined network).
 - oprogramowanie musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader

- oprogramowanie musi wspierać TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest zaoferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, poprzez weryfikację podpisu cyfrowego, że hypervisor uruchomił się w niezmienionej formie
- Wirtualizator w zaoferowanym oprogramowaniu musi mieć możliwość włączenia funkcji “Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Microsoft Windows 10 oraz Microsoft Windows Server 2016.
- oprogramowanie musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych
- oprogramowanie musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym Microsoft Windows 10 oraz Microsoft Windows 2016. Zamawiający wymaga aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 10 lub Microsoft Windows 2016 wirtualny TPM widziany był jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM musi być przechowywana w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana.
- oprogramowanie musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Zamawiający wymaga aby w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, funkcjonalność szybkiego uruchamiania powodowała eliminację czasochłonnej fazy inicjalizacji serwera fizycznego
- oprogramowanie musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej. Dodatkowo centralna konsola zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej wirtualizatora. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach. Taka funkcjonalność powinna być dostępna dla minimum dwóch producentów serwerów obecnych na rynku
- oprogramowanie musi posiadać wsparcie dla natywnych dysków 4K
- oprogramowanie musi wspierać protokół precyzyjnej synchronizacji czasu PTP (ang. Precision Time Protocol)
- Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych w ramach klastra serwerów w celu utwardzenia/hardening (maksymalnego zwiększenia bezpieczeństwa dostępu) systemu wirtualizacji.

- Zaoferowane oprogramowanie musi mieć funkcjonalność migracji w trybie rzeczywistym dysków działających maszyn wirtualnych z jednego podsystemu dyskowego do innego bez konieczności przerywania pracy maszyny wirtualnej, której dysk jest migrowany
- Licencjonowanie zaoferowanego oprogramowania lub zapewnienie udzielenia licencji na zaoferowane oprogramowanie spełniające wymagania Standardowe musi posiadać możliwość swobodnego przeniesienia praw do użytkowania na dowolny podmiot wymieniony w umowie ramowej i dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny.
- oprogramowanie musi posiadać certyfikację dla pakietu NVIDIA AI Enterprise, natywnego dla chmury zbioru zoptymalizowanych aplikacji AI i frameworków przeznaczonych dla kompleksowego rozwiązania AI;
- oprogramowanie musi umożliwiać włączenie najnowszej generacji procesorów graficznych NVIDIA do swojego środowiska wirtualnego i skorzystanie z takich funkcji jak Multi-Instance GPU (MIG), pozwalające na współdzielenie cykli GPU przez wielu użytkowników.
- oprogramowanie umożliwia uruchamianie poufnych kontenerów w serwerach opartych na procesorach EPYC™ firmy AMD.
- oprogramowanie zapewnia podstawowe funkcje serwera zarządzania kluczami (KMS), które upraszcza włączenie szyfrowania i zaawansowanych funkcji bezpieczeństwa.
- oprogramowanie obejmuje walidację FIPS, a także zaktualizowane przewodniki audytów.

Oprogramowanie dostępne – VDI.

Wymaga się aby oprogramowanie do realizacji bezpiecznego dostępu do systemu, spełniało poniższe wymagania:

- oprogramowanie musi być licencjonowane na zasadach: ilość licencji zapewnia jednoczesną pracę dowolnych użytkowników;
- oprogramowanie musi umożliwiać instalację i użytkowanie niezbędnej ilości hostów wirtualizacyjnych (ang. hypervisor) wymaganych do uruchomienia wirtualnych maszyn (stacji roboczych użytkowników);
- Serwer/host wirtualizacyjny (ang. hypervisor), na którym będą posadowione maszyny wirtualne użytkowników, musi pochodzić od tego samego producenta co zaoferowane oprogramowanie do wirtualizacji stacji roboczych i aplikacji wraz z oprogramowaniem do zarządzania i monitorowania stacji roboczych;
- oprogramowanie do wirtualizacji stacji roboczych musi wspierać Microsoft Windows 10, Microsoft Windows Server 2012R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Ubuntu 18.04, CentOS 8.0, RHEL 8.0 jako systemy operacyjne zainstalowane na wirtualnych stacjach roboczych;
- oprogramowanie do wirtualizacji stacji roboczych musi wspierać dostęp do wirtualnych stacji roboczych przez aplikację kliencką, która można zainstalować na minimum: Microsoft Windows 8.1 (32 lub 64 bit), Microsoft Windows 10, MacOS X, Android, iOS, ChromeOS. Dostęp do stacji roboczych musi być zapewniony przez urządzenia klasy terminal typu Zero Client lub Thin Client. Dla pozostałych systemów

- operacyjnych, do maszyny wirtualnej, musi być możliwy dostęp bezpośrednio przez przeglądarkę internetową obsługującą HTML5;
- W oprogramowaniu serwer/serwery zarządzające infrastrukturą wirtualnych stacji roboczych muszą być instalowane na maszynach fizycznych lub wirtualnych z systemami operacyjnymi: Microsoft Windows Server 2012 R2 lub nowsze. W/w systemy dopuszczalne są w wersji Standard lub Enterprise;
 - W oprogramowaniu konfiguracja i zarządzanie dostępem do sesji i aplikacji terminalowych musi być realizowana z poziomu tej samej pojedynczej konsoli zarządzającej dostępnej w przeglądarce;
 - oprogramowanie do wirtualizacji stacji roboczych musi posiadać możliwość instalacji więcej niż jednej instancji serwera zarządzającego połączeniami, tak aby w przypadku awarii takiego serwera zapewnić możliwość nawiązania nowej sesji przez inny serwer zarządzający;
 - W oprogramowaniu dostęp do centralnej konsoli zarządzającej musi być możliwy przy wykorzystaniu przeglądarek, minimum: Internet Explorer, Chrome lub Firefox;
 - oprogramowanie musi posiadać funkcjonalność integracji centralnej konsoli do zarządzania z usługami katalogowymi Microsoft Active Directory;
 - W zaoferowanym oprogramowaniu centralna konsola do zarządzania musi posiadać możliwość przydzielania i konfiguracji uprawnień do poszczególnych wirtualnych stacji roboczych lub grup wirtualnych stacji roboczych;
 - W oprogramowaniu centralna konsola do zarządzania musi posiadać możliwość integracji z tokenami RSA (Remote Secure Access) celem zapewnienia możliwości uwierzytelniania dwuskładnikowego dla logowania do wirtualnych stacji roboczych;
 - oprogramowanie do wirtualizacji stacji roboczych musi zapewniać możliwość szybkiego dynamicznego tworzenia grup wielu nowych wirtualnych stacji roboczych oraz tworzenia grup wirtualnych stacji w skład których wchodzi fizyczne stacje już posiadane przez Zamawiającego.
 - oprogramowanie do wirtualizacji stacji roboczych musi zapewniać możliwość tworzenia grup wirtualnych stacji roboczych, w których:
 - przypisanie użytkownika do wirtualnej stacji roboczej następuje automatycznie, na stałe, po pierwszym zalogowaniu i wówczas wszystkie dane użytkownika pozostają zapisane na dysku maszyny wirtualnej pomimo jego wylogowania;
 - przypisanie użytkownika do wirtualnej stacji roboczej następuje przy każdym kolejnym logowaniu i wówczas użytkownik za każdym razem otrzymuje nowo wykreowaną wirtualną stację roboczą.
 - oprogramowanie do wirtualizacji stacji roboczych musi zapewniać mechanizm pozwalający na podłączenie do wirtualnej stacji roboczej urządzeń typu dysk usb, pendrive, tablet producenta Wacom poprzez włączenie w/w urządzeń do portu USB urządzenia fizycznego (np. zero client) na którym dostępna jest i działająca poprawnie aplikacja klienta do podłączenia do maszyny wirtualnej;
 - oprogramowanie do wirtualizacji stacji roboczych musi zapewniać możliwość wirtualizacji wybranych aplikacji (zwirtualizowana aplikacja musi mieć postać pojedynczego pliku wykonywalnego

- z rozszerzeniem „exe” lub „msi”) z możliwością uzależnienia uruchomienia tej aplikacji na wirtualnych maszynach od członkostwa użytkownika w Microsoft Active Directory;
- oprogramowanie musi zapewniać możliwość uruchamiania aplikacji niezgodnych z daną wersją systemu operacyjnego – np. możliwość uruchomienia aplikacji działającej natywnie tylko w systemie Microsoft Windows 7 – na systemie Microsoft Windows 10;
 - oprogramowanie do wirtualizacji stacji roboczych musi zapewniać mechanizm umożliwiający wydruk danych wytworzonych w wirtualnej stacji roboczej na drukarkach lokalnych lub sieciowych podłączonych do urządzenia fizycznego na którym zainstalowana jest aplikacja klienta dostępowego do wirtualnej stacji roboczej;
 - W oprogramowaniu, warstwa wirtualizacji posadowionej bezpośrednio na sprzęcie serwerowym (ang. hypervisor), musi posiadać możliwość alokacji dla wirtualnych stacji roboczych większej ilości pamięci RAM niż fizycznie zainstalowanej w serwerze w celu osiągnięcia maksymalnego możliwego stopnia konsolidacji. Wspomniana powyżej warstwa wirtualizacji musi być dostarczona jako oprogramowanie wraz z przedmiotowym oprogramowaniem do wirtualizacji stacji roboczych;
 - Oprogramowanie do wirtualizacji musi zapewnić obsługę aplikacji 3D wewnątrz wirtualnych stacji roboczych wykorzystujących API OpenGL lub DirectX bez obciążania procesorów fizycznych w serwerach fizycznych, na których posadowione są maszyny wirtualne;
 - oprogramowanie do wirtualizacji stacji roboczych musi zapewnić możliwość skonfigurowania wirtualnych stacji roboczych posiadających 255 lub więcej GB pamięci RAM;
 - oprogramowanie musi być dostarczone wraz z opisanymi oznaczeniami producenta umożliwiającymi ich identyfikację na stronie przedmiotowego producenta lub w narzędziu udostępnianym przez producenta zaoferowanego oprogramowania.

System bezpieczeństwa i deponowania kluczy i materiałów niejawnych.

Podstawowe założenia.

W celu zapewnienia właściwego poziomu ochrony obiektu oraz skutecznego przeciwdziałania wszelkim zagrożeniom związanym z prawidłowym funkcjonowaniem jednostki organizacyjnej, wdrożone rozwiązania budynkowe uwzględnią elektroniczny system zabezpieczeń technicznych wykonanych w oparciu o poniższe systemy bezpieczeństwa oraz rozwiązania multimedialne:

- autonomiczny system włamania i napadu SSWIN;
- autonomiczny system kontroli dostępu SKD;
- telewizyjny system nadzoru w strefie ochrony peryferyjnej i wewnętrznej, system interkomowy;
- system BMS;
- depozytory elektroniczne;
- sejfy do przechowywania informacji niejawnych,
- instalacje elektryczne;

Opracowanie techniczne uwzględnia otrzymane od Zamawiającego wytyczne. Uwzględnione zostały wszystkie możliwe do użycia środki techniczne tak, aby wpływ czynnika ludzkiego na bezpieczeństwo pracy zespołu Kancelarii Tajnej ograniczyć do niezbędnego minimum.

Systemy bezpieczeństwa.

Na potrzeby projektowanych i modernizowanych systemów bezpieczeństwa należy wybudować wydzielone, dedykowane okablowanie strukturalne z użyciem kabla F/FTP 4x2xAWG23/1 Kat 6a LSOH oraz kabla U/UTP 4x2xAWG24/1 Kat 5e LSOH z punktem dystrybucyjnym zlokalizowanym w odpowiednio zabezpieczonym pomieszczeniu (pom. nr 4/34.1). Nie należy wykorzystywać żadnych elementów (aktywne lub pasywne) sieci komputerowej i telefonicznej na potrzeby transmisji dla systemów bezpieczeństwa. W sieci systemów bezpieczeństwa należy wykorzystać urządzenia aktywne zarządzalne oraz skonfigurować w sposób uniemożliwiający podłączenie do sieci innych elementów niż urządzenia wchodzące w skład systemów bezpieczeństwa.

Newralgiczne systemy bezpieczeństwa SKD-SSWIN należy zasilić z rozdzielnic „R-SN”, z uwzględnieniem podtrzymania napięcia zasilającego z własnego źródła zasilania (zasilacz buforowy) przez czas 36h. Istniejący na terenie poziomu czwartego system dozoru CCTV należy jedynie doposażyć w dodatkowe kamery. Systemy bezpieczeństwa pomieszczeń strefy OIN zostaną wykonane w stopniu ochrony 3, rozpoznania A wg. normy PN-EN 50131, PN-EN 50132.

Główne elementy systemu bezpieczeństwa Security Expert moduły SP-C, SP-RDM2, SPI-16 należy zamontować w obudowach modułowych systemowych w szafce zamykanej kluczem dostępowym. Zostaną zasilone z w/w rozdzielnic z uwzględnieniem zasilaczy typ PSBEN10A12E PULSAR wyposażonych w akumulatory typ EP12V65 - 12V65Ah celem podtrzymania pracy systemu przez min. 36h przy utracie zasilania podstawowego i gwarantowanego. Nie przewiduje się oddzielnych zasilaczy dla elementów systemu SKD_SSWIN np. zwór/rygli. W pom. nr 4/34.1 zamontowana zostanie szafka wisząca dla modułów systemu SKD_SSWIN oraz szafka rack, w której zlokalizowana zostanie autonomiczna jednostka UPS zasilająca switch dla systemu depozytorów. Do połączenia urządzeń systemowych SKD/SSWIN/CCTV należy wykorzystać okablowanie F/FTP 4x2xAWG23/1 Kat 6a LSOH oraz 4x2xAWG24/1 Kat 5e LSOH służące do podłączeń czujników wchodzących w skład systemu bezpieczeństwa. Instalacje systemowe w poziomie i pionie należy prowadzić po wybudowanych trasach w korytach teletechnicznych oraz z wykorzystaniem peszli instalacyjnych RKGL nierozprzestrzeniających płomienia. Instalacje nisko napięciowe 12V/DC zostaną wykonane przy wykorzystaniu okablowania:

- F/FTP 4x2xAWG23/1 Kat 6a LSOH.- połączenia magistralne systemu SKD/SSWIN;
- 4x2xAWG24/1 Kat 5e LSOH – połączenia czujników systemu SKD/SSWIN;
- F/FTP 4x2xAWG23/1 Kat 6a LSOH - połączenia kamer systemu CCTV;
- U/UTP 4x2xAWG24/1 Kat 5e LSOH - podłączenie czytników SX-RD-MB-BT do kontrolera SP-RDM2;
- U/UTP 4x2xAWG24/1 Kat 5e LSOH - podłączenie kontaktronów ISC-PMC-S3S, przycisków wyjścia YPW2D przycisków ewakuacyjnych D-115 i monitoringu
- YNTKSYEWK 2x1mm² – podłączenie zasilania do zwór.

Dla pomieszczeń przewidziano autonomiczne rozwiązanie oparte o system Security Expert, kontrolę dwustronną (moduł SP-RDM2) - wejście i wyjście z pomieszczenia po autoryzacji z wykorzystaniem dedykowanych kart zbliżeniowych dla czytników SX-RD-MB-BT. Czytniki posiadają funkcję sygnalizacji dźwiękowej w przypadku pozostawienia otwartych drzwi. Przy przejściu kontrolowanym należy zamontować przyciski awaryjnego wyjścia odblokowujące przejście na wypadek ewakuacji oraz zapewniające bezzwłoczną sygnalizację użycia w punkcie ochrony. Przejście objęte systemem kontroli dostępu musi zostać w razie pożaru automatycznie odblokowywane za pośrednictwem modułów systemu sygnalizacji pożaru zgodnie z przyjętym scenariuszem pożarowym. W charakterze elementów wykonawczych przy drzwiach należy zastosować zwoję elektromagnetyczną rewersyjną z czujnikiem działania hall i kontaktronem. Wszystkie zdarzenia w systemie muszą być rejestrowane i wizualizowane oraz przesłane do punktów nadzoru z wykorzystaniem platformy integrującej Security Expert. Za zarządzanie i administrację systemu odpowiedzialny jest administrator strefy. W tym celu administrator wyposażony będzie w stację roboczą. Na etapie realizacji zadania należy zapewnić połączenie z systemem kontroli dostępu za pośrednictwem wydzielonej i dedykowanej sieci dla systemów bezpieczeństwa. Punkt emisji kart dostępu do budynku znajduje się na terenie budynku Zamawiającego.

Celem zabezpieczenia pomieszczenia przed utratą poufności rozbudować w/w system o moduły SPI-16 pełniące funkcje bezpieczeństwa technicznego – alarmowego. W zależności od wielkości, powierzchni i położenia pomieszczeń podlegających ochronie należy zamontować detektory zgodnie z postanowieniami dokumentów odniesienia. Do ochrony pomieszczeń została zastosowana taka ilość czujek sejsmicznych VD-500, PIR typu OPTEX CDX-AM, z antymaskingiem i czujników magnetycznych, czytników przejść SX-RD-MB-BT, aby zapewnić pełne zabezpieczenie całej powierzchni i rozliczalność wejść/wyjść. Założenia dotyczące elementów detekcyjnych (w szczególności dobór oraz rozmieszczenie) dla poszczególnych obszarów przedstawiono na rysunku nr A5 (A5-Koncepcja rozwiązania –zabezpieczenia fizyczne i techniczne). Włączanie/wyłączenie Systemu SSWIN odbywa się centralnie z poziomu dedykowanej klawiatury numerycznej. Na etapie wykonania projektu uzgodnić możliwość dodatkowo rozbudowania tylko korytarza dostępowego i BSK celem zwiększenia funkcjonalności pracy. Lokalizacje klawiatur pokazano na ww. rysunku Wszystkie zdarzenia w systemie należy rejestrować i wizualizować z wykorzystaniem platformy integrującej zamontowanej w jednostce komputerowej zlokalizowanej na terenie OIN.

Rozwiązanie uwzględnia wykorzystywanie jednej karty do przemieszczania się po zespole pomieszczeń, którą dysponuje Użytkownik. Jego zadaniem będzie zaprogramowanie kart celem umożliwienia korzystania z rozwiązań systemu SKD.

Wymagania dotyczące części elektronicznej układu stykowego (chip) blankietu legitymacji służbowej funkcjonariusza i pracownika Służby Więziennej oraz karty kryptograficznej.

Elektroniczny układ stykowy (chip):

- wykonany jest zgodnie ze standardem ISO/IEC 7816 lub równoważnym, w którym zapisywane są certyfikaty oraz klucze kryptograficzne o długości min. 2048 bitów;

- realizuje algorytm RSA;
- funkcjonuje zgodnie z normą ISO/IEC 7816 część 1, 2, 3 lub równoważną;
- posiada co najmniej 64 kB pamięci zapisywalnej (EEPROM);
- w ramach wewnętrznej pamięci EEPROM przechowuje klucze, certyfikaty i inne obiekty;
- realizuje podpis RSA przy użyciu klucza prywatnego znajdującego się na legitymacji lub karcie z wykorzystaniem algorytmu RSA zgodnie ze specyfikacją PKCS#1 w wersji 1.5;
- posiada bibliotekę dynamiczną DLL dla systemów Microsoft Windows 2012/2016/10/11 z implementacją interfejsu PKCS#11 API, zgodnej ze standardem PKCS#11 v2.01 lub nowszym;
- posiada bibliotekę dynamiczną z implementacją interfejsu PKCS#11 umożliwiającą generowanie nowej pary kluczy RSA przez chip, zapis klucza prywatnego i publicznego, realizację podpisu RSA, deszyfrowanie z użyciem klucza RSA i zapis certyfikatu na legitymację lub kartę, kasowanie obiektów z legitymacji lub karty;
- posiada generator liczb losowych wykorzystywany przez legitymację lub kartę do generowania kluczy na blankiecie legitymacji lub karcie. Generator ten musi być oparty na zjawisku fizycznym;
- umożliwia przechowywanie co najmniej 15 (piętnastu) kluczy prywatnych o długości min. 2048 bity wraz z ich certyfikatami o typowej wielkości 1 kB;
- umożliwia definiowanie min. 1 kodu PIN oraz związanego z nim 1 kodu PUK na legitymacji lub karcie. Długość kodu PIN oraz PUK wynosi co najmniej 4 znaki;
- umożliwia zapisywanie dowolnych obiektów danych na legitymacji lub karcie;
- umożliwia zarządzanie dynamicznie przydziałem i zwalnianiem pamięci (wielokrotne usuwanie i zapisywanie ponownie kluczy kryptograficznych i obiektów danych nie powoduje zmniejszenia dostępnej pamięci na te dane);
- posiada przynajmniej jeden z wymienionych certyfikatów bezpieczeństwa dla układu elektronicznego legitymacji lub karty:
 - 1) CommonCriteria EAL4 bądź wyższy poziom lub równoważny,
 - 2) FIPS 140-2 Level3 bądź wyższy poziom lub równoważny;
- współpracuje z Microsoft Windows 2012/2016/10/11 oraz pozwala na uwierzytelnianie w przeglądarce Chrome, Microsoft Edge oraz Mozilla Firefox;
- umożliwia pracę wieloaplikacyjną przy udostępnianiu przez oba interfejsy (PKCS#11 i MS CSP/Minidriver). Klucze i obiekty danych zapisywane za pośrednictwem jednego interfejsu są dostępne dla drugiego interfejsu, jeśli jest to zgodne z jego specyfikacją;
- umożliwia podpisywanie dokumentów utworzonych w OpenOffice (od wersji 3), LibreOffice (od wersji 4) oraz Microsoft Office (od wersji 2003); CHIP-y w naszych legitymacjach są od NXP z oprogramowaniem IDProtect Manager.

System Interkomowy.

Dla potrzeb komunikacji między pomieszczeniami (pom. 4/31.1) oraz (pom. 4/16) przed wejściem głównym zostanie zamontowany panel komunikacyjny – wideofon HIKVISION wyposażony w wbudowaną kamerę oraz przycisk, umożliwiający nawiązanie łączności z monitorem DS.-KH6320-WTE2-W. Wewnątrz korytarza dostępowego zostaną również zamontowane stacje komunikacyjne. System oparty jest na rozwiązaniach cyfrowych z okablowaniem YNTKSYEWK 2x1mm². Zasilanie należy wykonać poprzez zastosowanie zewnętrznego zasilacza 24V/5A DC. Konfiguracja urządzeń odbywa się poprzez intuicyjny interfejs. Wymagana jest dwustronna komunikacja audio-video (full duplex) z redukcją wyświetlenia obrazu. Możliwość komunikacji bezpośredniej (per-to-per) odbywa się za pośrednictwem modułu komunikacyjnego DS.-KAD706 Lokalizacje urządzeń pokazano na rysunku nr A5 (A5-Koncepcja rozwiązania –zabezpieczenia fizyczne i techniczne).

Telewizyjny system nadzoru.

Istniejący telewizyjny system nadzoru w strefie peryferyjnej i wewnętrznej zapewni obserwację przestrzeni zewnętrznej, korytarza dostępowego strefy ochronnej III. Lokalizacja kamer zostanie uzgodniono z Użytkownikiem System monitoringu wizyjnego zostanie uzupełniony o dodatkowe kamery

W systemie monitoringu zastosowane zostaną kamery sieciowe wewnętrzne IP 2 Mpx typ IPC-HDW3241T-ZAS-27135 ze zmienną ogniskową (zoom) o rozdzielczości nie mniejszej niż 19200px x 1080px, ze stało ogniskowym obiektywem, wizyjną detekcją ruchu, pracujące w trybie dzień/noc, z mechanicznym filtrem podczerwieni, poszerzonym zakresem dynamiki i wysoką czułością, cyfrową obróbką sygnału oraz redukcją efektów niepożądanych. Kamery należy połączyć przy pomocy kabla skrętkowego F/FTP 4x2xAWG23/1 Kat 6a LSOH do dedykowanego switch-a zlokalizowanego w PD w strefie ochronnej, w którym umieszczono również lokalny serwer/rejestrator, macierzy dyskowych.

System monitoringu musi zapewnić przestrzeń dyskową pozwalającą na odtworzenie zdarzeń systemowych oraz nagrań ze wszystkich kamer, z co najmniej 30 ostatnich dni – zgodnie z wytycznymi zawartymi w dokumentach odniesienia. Podgląd rejestrowanego obrazu jest widoczny dla osób dozoruujących w tym całodobowej obsłudze. Lokalna stacja robocza zostanie umieszczona w pomieszczeniu uzgodnionym. W celu zwiększenia efektywności korzystania z systemu przez operatora zaleca się, by telewizyjny system nadzoru integrować z pozostałymi systemami bezpieczeństwa. Lokalizację urządzeń pokazano na rysunku nr A5 (A5-Koncepcja rozwiązania –zabezpieczenia fizyczne i techniczne).

BMS integracja systemów.

Dla potrzeb monitoringu wprowadza się rozwiązanie Security Expert. Rozwiązanie umożliwia opracowanie skutecznych i nowoczesnych procedur alarmowych i ewakuacyjnych w przypadku sytuacji awaryjnych i stwarzających zagrożenie dla zdrowia i życia ludzi dzięki pełnej i aktualnej informacji o stanie obiektu. Pozwoli także na maksymalne uproszczenie i usprawnienie systemu zarządzania i monitoringu obiektu, kompleksową organizację raportowania i archiwizacji danych dotyczących funkcjonowania całego obiektu, włącznie z przesyłaniem danych i raportów do innych baz danych i systemów informatycznych.

Depozytory.

Na korytarzu dostępowym na poziomie czwartego piętra zamontować depozytory kluczy. Na terenie strefy ochronnej III zamontować depozytor skrytek SAIK BOXINBOX 35* + 10 skrytek na telefony, na terenie strefy ochronnej II w lewym skrzydle zamontować depozytor skrytek SAIK BOXINBOX 30. Natomiast na terenie strefy ochronnej II w prawym skrzydle zamontować depozytor SAIK BOXINBOX 35.

Parametry techniczne jednostek: stalowa obudowa z automatycznie uchylanymi i blokowanymi indywidualnymi drzwiczkami, komplet pudełek Rfi D do skrytek z możliwością referowania i plombowania, komplet breloków do kluczy (odporne na uderzenia, bezpieczne nie radiowe, technologia rozpoznawania: stykowa Dallas), całkowicie stalowe, nie linkowe kłódki do mocowania kluczy na brelokach (z numerami seryjnymi), możliwość przechowywania telefonów komórkowych w skrytkach zamykanych na kluczyk (rozw. Mechaniczne), panel sterowniczy z 7" ekranem, dotykowym, odporny na przenoszenie wirusa (certyfikat), czytnik kart zbliżeniowych: MIFARE lub UNIQUE lub instalacja przesłanego czytnika, kolor obudowy z palety RAL 7037 lub inny uzgodniony z Użytkownikiem na etapie realizacji zadania, zasilanie awaryjne: min.36 h (z automatycznym testowaniem akumulatora), automatyczna syrena alarmowa, komunikaty głosowe (wersja do wyboru dla każdego pracownika osobno: pol, eng, fra, deu, ukr, rus, arabic), wyjścia podłączeniowe do innych systemów (KD, ppoż), oprogramowanie instalowane na Windows oraz WEB (do wyboru na każdym etapie użytkowania). Depozytory zasilic napięciem 230V/AC przewodem N2XH-J 3x2,5mm² z nowobudowanej rozdzielnicy „R-SN” Lokalizację urządzeń pokazano na rysunku nr A5 (A5-Koncepcja rozwiązania –zabezpieczenia fizyczne i techniczne).

Sejfy do przechowywania materiałów niejawnych.

Zgodnie z wymaganiami Użytkownika na terenie zespołu pomieszczeń w strefie ochronnej II należy dostarczyć i zamontować 20 sztuk sejfów typ ML 45/S1 – K w klasie S1 (klasa A Zarządzenie MS) odporności na włamanie zgodnie z normą PN-EN 14450:2018-02. Wymiary zewnętrzne sejfu (450 x 400 x 460 mm, wys. x szer. x gł.). Wymiary wewnętrzne sejfu (444 x 384 x 345 mm, wys. x szer. x gł.) Waga 47 kg, Kolor RAL 7035, Zamykany atestowanym zamkiem: kluczowym klasy A. Wyposażony w jedną półkę z możliwością regulacji zawieszenia. Sejf przytwierdzić do podłoża za pomocą kotwy chemicznej. Dla potrzeb nowo utworzonej Kancelarii Tajnej należy dostarczyć i zamontować dwie sztuki szaf klasy MS1/C 185 –SK w klasie S2 (klasa C Zarządzenie MS) odporności na włamanie zgodnie z normą PN-EN 14450:2018-02. Wymiary zewnętrzne szafy (1850 x 700 x 500) mm, wys. x szer. x gł.). Wymiary wewnętrzne szafy (1750 x 600 x 375)mm, wys. x szer. x gł.). Waga 210 kg, Kolor RAL 7035, Zamykane atestowanym zamkiem: kluczowym klasy K1S2. Wyposażone w trzy półki z możliwością regulacji zawieszenia. Sejfy przytwierdzić do podłoża za pomocą kotwy chemicznej.

Dopuszcza się dostarczenie sejfów o zbliżonych parametrach z zastrzeżeniem wypełnienia wszystkich wymogów określonych w Zarządzeniu Ministra Sprawiedliwości w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych z dnia 23 stycznia 2014 r. przewidzianych dla odpowiednich klauzuli przetwarzania informacji.

System sygnalizacji pożaru.

Dla potrzeb zespołu pomieszczeń w wyniku wprowadzonych zmian architektonicznych należy uwzględnić relokowanie części czujników i dołożenie czujników pożarowych. Dodatkowe czujniki dymu w zespołu pomieszczeń należy wpiąć w istniejące w pętlę systemu p.poż. Celem eliminacji emisji przewodzonej i promieniowanej należy dla dedykowanego pomieszczenia nr 4/34 – pomieszczenia serwerowni zastosować rozwiązanie z montażem czujników dymu wpiętego w pętlę, zabezpieczonego rozwiązaniem EMC – bez konieczności montażu podcentrali systemu p.poż. Lokalizację urządzeń pokazano na rysunku nr A5 (A5-Koncepcja rozwiązania – zabezpieczenia fizyczne i techniczne).

Ochrona przeciwporażeniowa.

Instalację odbiorczą należy wykonać w istniejącym układzie w oparciu o istniejącą rozdzielnicę korytarzową i nowo wybudowane rozdzielnice „T-T”, „R-SN” i „R-S”. Podstawową ochronę przeciwporażeniową (przed dotykem bezpośrednim) stanowi izolacja robocza przewodów i kabli oraz osłony zewnętrzne urządzeń. Do każdego gniazda wtykowego i urządzenia elektrycznego doprowadzony zostanie osobny przewód neutralny N i osobny przewód ochronny PE. Przewody ochronne prowadzone będą w izolacji koloru zielono-żółtego i zostaną podłączone do szyn ochronnych PE w poszczególnych rozdzielnicach zasilających. Ochrona przeciwporażeniowa jest zrealizowana następująco: ochrona podstawowa – izolowanie części czynnych, ochrona dodatkowa – samoczynne wyłączenie zasilania poprzez zastosowanie wyłączników nadprądowych oraz wyłączników różnicowoprądowych, przewody PE mają izolację koloru żółto-zielonego, zaś neutralne N koloru niebieskiego. Z przewodem PE podłączono: bolce ochronne gniazd wtykowych, zacisk PE rozdzielnic „T1” i „T2”. Instalację należy wykonać zgodnie z PN-IEC 6003-4-41 i SEP-E-001. Ochrona przez zastosowanie szybkiego wyłączania realizowana będzie przez urządzenia ochronne przetężeniowe – wyłączniki z wyzwalaczami nadprądowymi oraz rozłączniki bezpiecznikowe. Ochronę uzupełniającą stanowią aparaty różnicowoprądowe o znamionowym prądzie różnicowym nie większym niż 30mA.

Oznaczenia.

Na etapie realizacji inwestycji uzgodnić na roboczo z Zamawiającym, sposób oznaczeń wykonanej instalacji, tak żeby zachować jednolity sposób oznaczeń na terenie całego obiektu. Wszystkie gniazda i przewody oznaczono w sposób trwały jednoznacznie je identyfikujący.

Serwisowalność urządzeń, badania i pomiary.

Czynności serwisowe wykonywać zgodnie z zaleceniami producentów sprzętu. Postępować zgodnie z określonymi wymaganiami Użytkownika obiektu. Po wykonaniu realizacji zadania przeprowadzić testy i pomiary tłumienności elektromagnetycznej przegrody budowlanej.

Przygotowanie przez Wykonawcę wzoru dokumentów niezbędnych do uzyskania akredytacji systemów teleinformatycznych.

Dla wdrażanego systemu teleinformatycznego – autonomicznego stanowiska komputerowego do przetwarzania informacji niejawnych o klauzuli do Tajne/Ścisłe Tajne włącznie w zespole pomieszczeń Kancelarii Tajnej Inspektoratu Wewnętrznego Służby Więziennej:

- 1) Opracowanie, wymaganych w obszarze ochrony informacji niejawnych i bezpieczeństwa teleinformatycznego, wewnętrznych dokumentów prawnych Inspektoratu Wewnętrznego Służby Więziennej: (zarządzeń, decyzji).
- 2) Przygotowanie wniosku WS-01 wraz z załącznikami w celu uzyskania dla pomieszczenia, w którym zainstalowany będzie system teleinformatyczny do przetwarzania informacji niejawnych o klauzuli do Tajne/Ścisłe Tajne włącznie, Certyfikatu Ochrony Elektromagnetycznej DBTI ABW potwierdzającego Sprzętową Strefę Ochrony Elektromagnetycznej dla tego pomieszczenia.
- 3) Wykonanie dokumentacji niezbędnej do akredytacji bezpieczeństwa systemu teleinformatycznego do przetwarzania informacji niejawnych o klauzuli do Tajne/Ścisłe Tajne włącznie w zespole pomieszczeń Kancelarii Tajnej Inspektoratu Wewnętrznego Służby Więziennej w Warszawie:
 - dokument: *Szacowanie ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym* – zgodny z wymaganiami określonymi w:
 - Rozporządzeniu Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U nr 159, poz. 948);
 - dokumencie Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego: Szczegółowe zalecenia dotyczące analizy oraz zarządzania ryzykiem w systemach teleinformatycznych, wersja 2.0, sierpień 2011 r.
 - dokument: *Szczególne Wymagania Bezpieczeństwa dla systemu teleinformatycznego do przetwarzania informacji niejawnych o klauzuli do Tajne/Ścisłe Tajne włącznie* - zgodny z wymaganiami dokumentów ustawowych i dokumentu DBTI ABW: Zalecenia dotyczące opracowywania dokumentu *Szczególnych Wymagań Bezpieczeństwa dla systemu teleinformatycznego* – w wersji 2.1 z czerwca 2012 r.;
 - dokument: *Konfiguracja systemu operacyjnego MS Windows 10 w systemie teleinformatycznym do przetwarzania informacji niejawnych o klauzuli do Tajne/Ścisłe Tajne włącznie* – zgodny z zaleceniami DBTI ABW;
 - dokument: *Procedury Bezpiecznej Eksploatacji dla systemu teleinformatycznego do przetwarzania informacji niejawnych o klauzuli do Tajne/Ścisłe Tajne włącznie* – zgodny z wymaganiami dokumentów ustawowych i zaleceniami DBTI ABW;

- Plan testów bezpieczeństwa systemu teleinformatycznego do przetwarzania informacji niejawnych o klauzuli do Tajne/Ścisłe Tajne włącznie;
 - Raport z testów bezpieczeństwa systemu teleinformatycznego do przetwarzania informacji niejawnych o klauzuli do Tajne/Ścisłe Tajne włącznie;
 - dokumenty/formularze Administratora Systemu i Inspektora Bezpieczeństwa Teleinformatycznego określone w dokumentach normatywnych oraz w Szczególnych Wymaganiach Bezpieczeństwa i Procedurach Bezpiecznej Eksploatacji.
- 4) Opracowanie danych uzupełniających do Planu Ochrony Informacji Niejawnych w Inspektoracie Wewnętrznym Służby Więziennej w Warszawie, związanych z przetwarzaniem informacji niejawnych w ww. systemie teleinformatycznym.
 - 5) Opracowanie danych uzupełniających do Instrukcji określającej sposób i tryb przetwarzania informacji niejawnych o klauzuli Zastrzeżone w Inspektoracie Wewnętrznym Służby Więziennej w Warszawie, związanych z przetwarzaniem informacji niejawnych w ww. systemie teleinformatycznym.
 - 6) Opracowanie danych uzupełniających do Instrukcji określającej sposób i tryb przetwarzania informacji niejawnych o klauzuli Poufne w Inspektoracie Wewnętrznym Służby Więziennej w Warszawie, związanych z przetwarzaniem informacji niejawnych w ww. systemie teleinformatycznym.
 - 7) Przygotowanie wniosku WA-01 wraz z załącznikami w sprawie akredytacji bezpieczeństwa systemu teleinformatycznego do przetwarzania informacji niejawnych o klauzuli do Tajne/Ścisłe Tajne włącznie.

Dla wdrażanego systemu teleinformatycznego – lokalnej sieci komputerowej (LAN) do przetwarzania informacji niejawnych o klauzuli do Poufne włącznie w siedzibie Inspektoratu Wewnętrznego Służby Więziennej w Warszawie:

- 1) Opracowanie, wymaganych w obszarze ochrony informacji niejawnych i bezpieczeństwa teleinformatycznego, wewnętrznych dokumentów prawnych Inspektoratu Wewnętrznego Służby Więziennej (zarządzeń, decyzji).
- 2) Przygotowanie wniosku WS-01 wraz z załącznikami w celu uzyskania dla pomieszczeń, w których zlokalizowane będą elementy lokalnej sieci komputerowej (LAN) do przetwarzania informacji niejawnych o klauzuli do Poufne włącznie, Certyfikatu Ochrony Elektromagnetycznej DBTI ABW potwierdzającego Sprzętową Strefę Ochrony Elektromagnetycznej dla tych pomieszczeń.
- 3) Wykonanie dokumentacji niezbędnej do akredytacji bezpieczeństwa systemu teleinformatycznego - lokalnej sieci komputerowej (LAN) do przetwarzania informacji niejawnych o klauzuli do Poufne włącznie w siedzibie Inspektoratu Wewnętrznego Służby Więziennej w Warszawie:
 - dokument: Szacowanie ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w lokalnej sieci komputerowej (LAN) do przetwarzania informacji niejawnych o klauzuli do Poufne włącznie – zgodny z wymaganiami określonymi w:

- Rozporządzeniu Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U nr 159, poz. 948);
 - dokumencie Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego: Szczegółowe zalecenia dotyczące analizy oraz zarządzania ryzykiem w systemach teleinformatycznych, wersja 2.0, sierpień 2011 r.;
 - dokument: Szczególne Wymagania Bezpieczeństwa dla systemu teleinformatycznego - lokalnej sieci komputerowej (LAN) do przetwarzania informacji niejawnych o klauzuli do Poufne włącznie - zgodny z wymaganiami dokumentów ustawowych i dokumentu DBTI ABW: Zalecenia dotyczące opracowywania dokumentu Szczególnych Wymagań Bezpieczeństwa dla systemu teleinformatycznego – w wersji 2.1 z czerwca 2012 r.;
 - dokument: Konfiguracja systemu operacyjnego w systemie teleinformatycznym - lokalnej sieci komputerowej (LAN) do przetwarzania informacji niejawnych o klauzuli do Poufne włącznie – zgodny z zaleceniami DBTI ABW;
 - dokument: Procedury Bezpiecznej Eksploatacji dla systemu teleinformatycznego - lokalnej sieci komputerowej (LAN) do przetwarzania informacji niejawnych o klauzuli do Poufne włącznie – zgodny z wymaganiami dokumentów ustawowych i zaleceniami DBTI ABW;
 - dokumenty/formularze Administratora Systemu i Inspektora Bezpieczeństwa Teleinformatycznego określone w dokumentach normatywnych oraz w Szczególnych Wymagań Bezpieczeństwa i Procedurach Bezpiecznej Eksploatacji.
- 4) Opracowanie danych uzupełniających do Planu Ochrony Informacji Niejawnych Inspektoratu Wewnętrznego Służby Więziennej w Warszawie, związanych z przetwarzaniem informacji niejawnych w lokalnej sieci komputerowej (LAN) do przetwarzania informacji niejawnych o klauzuli do Poufne włącznie.
- 5) Opracowanie danych uzupełniających do Instrukcji określającej sposób i tryb przetwarzania informacji niejawnych o klauzuli Zastrzeżone w Inspektoracie Wewnętrznym Służby Więziennej w Warszawie, związanych z przetwarzaniem informacji niejawnych w lokalnej sieci komputerowej (LAN) do przetwarzania informacji niejawnych o klauzuli do Poufne włącznie.
- 6) Opracowanie danych uzupełniających do Instrukcji określającej sposób i tryb przetwarzania informacji niejawnych o klauzuli Poufne w Inspektoracie Wewnętrznym Służby Więziennej w Warszawie, związanych z przetwarzaniem informacji niejawnych w lokalnej sieci komputerowej (LAN) do przetwarzania informacji niejawnych o klauzuli do Poufne włącznie.
- 7) Przygotowanie wniosku WA-01 wraz z załącznikami w sprawie akredytacji bezpieczeństwa teleinformatycznego systemu teleinformatycznego - lokalnej sieci komputerowej (LAN) do przetwarzania informacji niejawnych o klauzuli do Poufne włącznie.

SPIS RYSUNKÓW

Nr rys. 1. RZUT PARTERU STAN ISTNIEJĄCY – UKŁAD ARCHITEKTONICZNY STREFY WEJŚCIA DO BUDYNKU.

Nr rys. 2. RZUT PIĘTRA „+4” STAN ISTNIEJĄCY – UKŁAD ARCHITEKTONICZNY POMIESZCZEŃ PIĘTRA „+4”

Nr rys. 3. RZUT PARTERU STAN PROJEKTOWANY – UKŁAD ARCHITEKTONICZNY STREFY WEJŚCIA DO BUDYNKU.

Nr rys. 4. RZUT PIĘTRA „+4” STAN PROJEKTOWANY – UKŁAD ARCHITEKTONICZNY POMIESZCZEŃ PIĘTRA „+4”.

Nr rys. 5 RZUT PIĘTRA „+4” STAN PROJEKTOWANY – ZWIĘKSZENIE ZABEZPIECZEŃ TECHNICZNYCH I FIZYCZNYCH.

Wykonano w 4 egz.

Egz. 1-2 wersja papierowa, 2 egz. płyta CD-ROM - adresat

Wyk: Radosław Lenart, Arkadiusz Wild