KONCEPCJA TECHNICZNA

Przebudowy i rozbudowy systemów bezpieczeństwa technicznego wspierającego Ochronę.

w Muzeum Sztuki i Techniki Japońskiej Manggha w Krakowie

Kraków, lipiec 2026

Spis zawartości opracowania:

1. PRZEDMIOT OPRACOWANIA

Przedmiotem opracowania jest koncepcja przebudowy i rozbudowy systemu bezpieczeństwa wraz z niezbędnymi pracami instalacyjnymi i budowlanymi w budynkach Muzeum Sztuki i Techniki Japońskiej Manggha w Krakowie.

2. ZAŁOŻENIA KONCEPCYJNE

Założenia do niniejszego opracowania stanowią:

- Umowa i uzgodnienia z Inwestorem,
- Opinia NIM (nr DOZP.434.7.2025) z dn. 10.12.2025r.
- Projekty istniejących instalacji,
- Wizja lokalna w obiekcie,
- Rozmowy z przedstawicielami Użytkownika,
- Obowiązujące normy i przepisy.

3. ZAKRES OPRACOWANIA

W zakresie opracowania znajdują się następujące systemy:

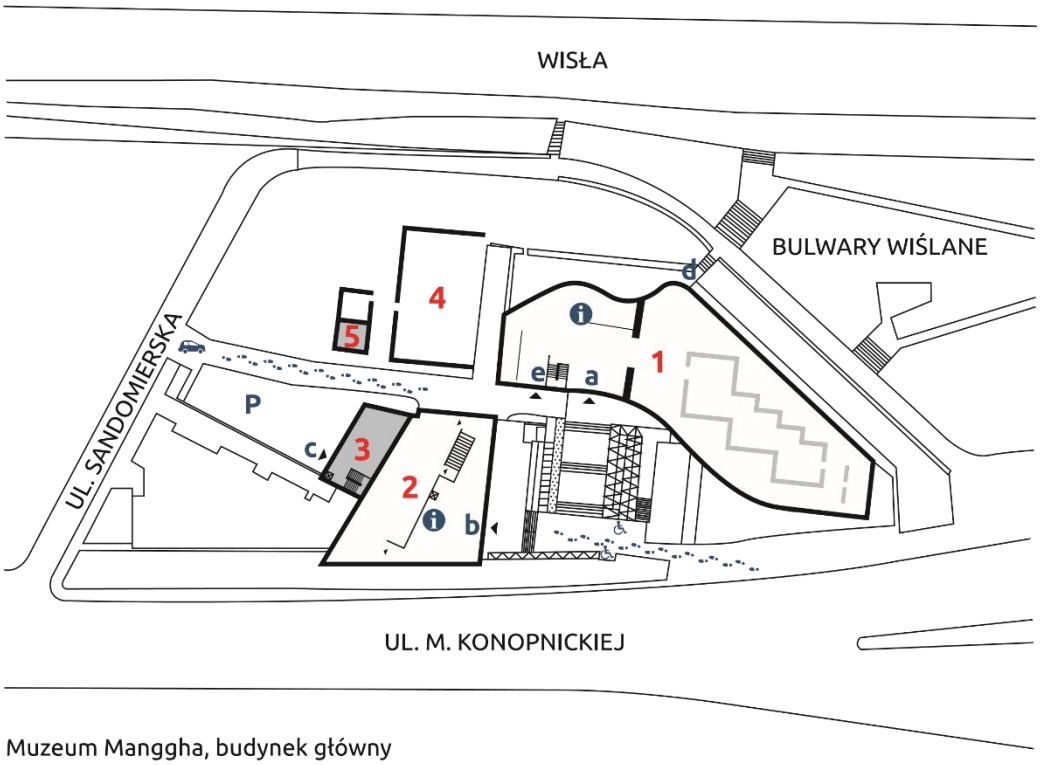
- Kontroli dostępu (SKD),
- Sygnalizacji włamania i napadu (SSWiN),
- Telewizji dozorowej (CCTV),
- Systemy, instalacje, roboty pomocnicze i uzupełniające.

4. OGÓLNA CHARAKTERYSTYKA OBIEKTU

Muzeum zostało powołane do życia i otwarte w 1994 roku jako Centrum Sztuki i Techniki Japońskiej Manggha. Przez pierwszych dziesięć lat istnienia stanowiło oddział Muzeum Narodowego w Krakowie, W roku 2005, usamodzielnione decyzją Ministra Kultury, otrzymało status państwowej instytucji kultury, a od roku 2007 działa jako placówka muzealna.

Obecnie obiekty wchodzące w skład kompleksu Manggha zajmują obszar pomiędzy ulicami Marii Konopnickiej, Sandomierską oraz Bulwarami Wiślanymi - szczegóły pokazane na rys.1.

Rys. 1 szkic rozmieszczenia obiektów.



1 – Muzeum Manggha, budynek główny
(wewnątrz: Café Manggha, Mangghashop, kasa)
2 – Galeria Europa – Daleki Wschód
3 – Szkoła Języka Japońskiego (I poziom) / Biblioteka (II poziom)
4 – Ogród japoński
5 – Pawilon herbaciany

a – wejście główne do Muzeum Manggha
b – wejście do Galerii Europa – Daleki Wschód
c – wejście do Szkoły Języka Japońskiego / Biblioteki
d – wejście przez Bulwary wiślane
e – wejście do lobby (poziom -1 Muzeum Manggha)
P – parking

schody podjazd winda recepcja - punkt informacyjny

podjazd brukowany bez poręczy

Źródło: manggha.pl

5. STAN ISTNIEJĄCY

Obecnie na terenie Manggha zidentyfikowano następujące systemy bezpieczeństwa obiektowego:

- telewizja dozorowa (CCTV),
- system kontroli dostępu (SKD),
- system sygnalizacji włamania i napadu (SSWiN),
- System sygnalizacji pożarowej (SSP),
- System detekcji wycieków (SDW).
- Inne (instalacja domofonowa, zdalne otwieranie bram itp.)

Z dalszych prac i analiz wyłączone zostały: System Sygnalizacji Pożarowej (SSP) oraz System Detekcji Wycieków (SDW). W opinii Użytkownika system SSP jest sprawy, natomiast system detekcji wycieków będzie przedmiotem osobnych działań.

Eksploatowane systemy uruchomione zostały w 2006 roku. Przebudowywane w latach 2010-2013 (m.in. po powodzi i częściowym zalaniu) oraz rozbudowane w 2015-2016 roku przy okazji budowy Galerii Europa – Daleki Wschód (GE-DW). Po tym okresie poddawane były jedynie bieżącym naprawom i konserwacjom.

W budynku Szkoły Języka Japońskiego i Biblioteki zainstalowany jest niezależny i autonomiczny system sygnalizacji włamania z przekazywaniem informacji o alarmie do Centrum Nadzoru Manggha (nie podlega modernizacji).

6. KONCEPCJA ZMIAN

6.1. ZAŁOŻENIA OGÓLNE

Celem podjętych działań jest zapewnienie niezawodnego, spójnego i nowoczesnego systemu bezpieczeństwa dla całego obiektu. Biorąc pod uwagę aktualny stan systemów zakłada się całkowitą wymianę systemów SDK, SSWiN oraz CCTV. Nowe rozwiązania powinny być nowoczesne i gwarantować długi okres użytkowania. Bazując na ustaleniach (rozdział 5), koncepcja zakład odtworzenie obecnych zdolności oraz ich poprawę. Poprawa obejmie usuwanie stref martwych (CCTV i SSWiN) oraz rozbudowę SKD o dodatkowe przejścia.

Ze względu na ograniczone środki część prac może zostać wykonana w późniejszym okresie. Obecnie realizowane systemy będą musiały być przygotowane pod przyszłe rozbudowy.

Wykaz prac i dostaw:

a) wymianę istniejących systemów z zachowaniem stanu ilościowego kamer, czujków, przejść i innych elementów pomocniczych,
b) rozbudowę systemów o dodatkowe kamery, czujki i przejścia oraz dodatkowe funkcjonalności w celu wyeliminować stref pozbawionych nadzoru,
c) uniezależnienie działania systemów od warunków pogodowych i oświetleniowych oraz poprawę nadzoru w strefach przebywania gości i zwiedzających,
d) rozbudowa systemu SKD o możliwości awizacyjne i odczyt kodów QR w wytypowanych przejściach.
e) zintegrowanie SKD i CCTV oraz wydzielenie SSWiN jak systemu całkowicie niezależnego.
f) przebudowa i modernizację obecnych centrów nadzoru p.115 (Manggha) oraz p.205 (GE-DW).
g) zapewnienie prawidłowej ochrony dla pomieszczeń magazynu broni i tajnej kancelarii (SKD i SSWiN w stopniu GRADE 3)
h) dostawę wyposażenia dla centrum nadzoru i pracowników ochrony,
i) aranżację fragmentu garażu dla posadowienia szaf głównych systemów monitoringu, zabezpieczenia i kontroli,
j) wykonanie niezbędnych zmian i rozbudowa instalacji elektrycznej w zakresie zasilania realizowanych systemów bezpieczeństwa,
k) dostawa i uruchomienie centralnego UPS-a,
l) budowa szlabanu od strony ul. Sandomierskiej,

m) dostawa profesjonalnego rozwiązania firewall,
n) Instalacja videodomofonowa w wybranych punktach,
o) wykonanie projektu wykonawczego dla ofertowanych prac.

Wykonawca musi uwzględniać wpływ prowadzonych robót na działanie Muzeum. Prace nie mogą kolidować z bieżącą działalnością wystawienniczą i imprezami towarzyszącymi. Rozpoczęcie prac musi zostać poprzedzone przygotowaniem i zatwierdzeniem szczegółowego harmonogramu.

Prace muszą uwzględnić nieprzerwane działanie systemów bezpieczeństwa.

6.2. BEZPIECZEŃSTWO TELEINFORMATYCZNE I CYBERBEZPIECZEŃSTWO

6.2.1. Wspólne wytyczne sieciowe dla SKD, SSWiN i CCTV i pozostałych.

Wykonawca powinien zapewnić, aby wszystkie systemy bezpieczeństwa technicznego były wdrożone z uwzględnieniem następujących zasad:

a) systemy SKD, SSWiN i CCTV powinny być odseparowane logicznie i fizycznie od sieci biurowej Muzeum,
b) zaleca się stosowanie osobnych VLAN-ów lub wydzielonych segmentów dla:
    a. kamer CCTV,
    b. rejestratorów/NVR/VMS,
    c. kontrolerów SKD,
    d. central SSWiN,
    e. stanowisk operatorskich,
    f. stanowisk administracyjnych,
    g. serwerów zarządzających i systemów archiwizacji,
c) komunikacja między segmentami powinna być ograniczona do niezbędnych usług i portów,
d) ruch między segmentami powinien być kontrolowany przez zaporę ogniową (firewall), listy kontroli dostępu (ACL) lub inne mechanizmy kontroli dostępu umożliwiające definiowanie i egzekwowanie polityk dostępowych pomiędzy poszczególnymi segmentami sieci,
e) urządzenia systemów bezpieczeństwa nie mogą być bezpośrednio dostępne z Internetu,
f) zakazuje się stosowania przekierowań portów do kamer, rejestratorów, central alarmowych, kontrolerów SKD i paneli administracyjnych,
g) nie przewiduje się możliwości stałego zdalnego dostępu serwisowego
h) zdalny dostęp serwisowy może być realizowany wyłącznie przy zastosowani łącznie poniższych wytycznych:
    a. za zgodą i wiedzą Zamawiającego (Użytkownika)
    b. przez VPN opartych o standard IPSec lub SSL VPN,
    c. z użyciem uwierzytelniania wieloskładnikowego MFA,
    d. z możliwością przypisywania uprawnień dostępowych do określonych grup użytkowników,
    e. z pełnym logowaniem sesji,

    f. tylko na czas prowadzenia prac.

i) należy wyłączyć nieużywane usługi i protokoły, jeżeli nie są wymagane i zatwierdzone przez Zamawiającego, w szczególności:
    a. Telnet,
    b. FTP,
    c. HTTP bez TLS,
    d. UPnP,
    e. SNMPv1/v2,
    f. funkcje P2P/cloud access;
j) komunikacja administracyjna powinna odbywać się wyłącznie przez szyfrowane protokoły, np. HTTPS, SSH, SNMPv3,
k) wszystkie urządzenia powinny korzystać z wiarygodnego źródła czasu, najlepiej wewnętrznego serwera NTP,
l) wykonawca powinien przekazać Zamawiającemu wykaz:
    a. adresów IP,
    b. portów,
    c. usług,
    d. reguł komunikacji,
    e. kont technicznych,
    f. zależności między systemami
m) przed odbiorem należy potwierdzić brak ekspozycji urządzeń i paneli administracyjnych do Internetu.

6.2.2. System Kontroli Dostępu — SKD

Zalecenia dotyczące cyberbezpieczeństwa:

a) System SKD powinien umożliwiać zarządzanie użytkownikami na podstawie imiennych kont, bez konieczności korzystania ze współdzielonych kont administracyjnych.
b) System powinien obsługiwać role i poziomy uprawnień, co najmniej:
    a. administrator,
    b. operator,
    c. serwis,
    d. audytor lub użytkownik tylko do odczytu.
c) Nadawanie, zmiana i odbieranie uprawnień dostępu powinny być rejestrowane w logach systemowych.
d) System powinien umożliwiać szybkie blokowanie:
    a. utraconych kart,
    b. nieaktywnych identyfikatorów,
    c. kont byłych pracowników,
    d. kont serwisowych po zakończeniu prac.
e) Zaleca się stosowanie identyfikatorów i czytników zapewniających odpowiedni poziom bezpieczeństwa kryptograficznego.
f) Nie zaleca się wdrażania systemów opartych wyłącznie na nieszyfrowanej komunikacji czytnik–kontroler, np. klasycznym Wiegand, jeżeli nie zastosowano dodatkowych zabezpieczeń.
g) Preferowane są rozwiązania obsługujące bezpieczną komunikację między czytnikiem a kontrolerem, np. OSDP Secure Channel lub mechanizm równoważny.
h) Kontrolery SKD powinny przechowywać konfigurację i uprawnienia w sposób zabezpieczony przed nieuprawnionym odczytem lub modyfikacją.
i) System powinien rejestrować co najmniej:
    a. użycie identyfikatora,
    b. próbę dostępu nieuprawnionego,
    c. otwarcie drzwi,
    d. wymuszenie otwarcia,

e. zbyt długie otwarcie drzwi,
f. sabotaż urządzeń,
g. zmianę konfiguracji,
h. nadanie lub odebranie uprawnień,
i. działania administratorów,
j. eksport raportów.

j) System powinien umożliwiać cykliczny przegląd uprawnień użytkowników.

k) Wykonawca powinien przewidzieć procedurę obsługi:
a. nowych użytkowników,
b. użytkowników odchodzących,
c. zagubionych kart,
d. kart tymczasowych,
e. gości,
f. firm zewnętrznych.

l) Dostęp serwisowy do systemu SKD powinien być domyślnie wyłączony i aktywowany wyłącznie na czas prac zaakceptowanych przez Zamawiającego.

m) Wszystkie domyślne hasła, kody instalatora i konta fabryczne muszą zostać zmienione przed odbiorem systemu.

n) Wykonawca powinien przekazać Zamawiającemu pełne prawa administracyjne do systemu SKD.

o) System powinien umożliwiać wykonanie kopii zapasowej:
a. konfiguracji kontrolerów,
b. bazy użytkowników,
c. harmonogramów,
d. stref dostępu,
e. uprawnień,
f. logów lub raportów zdarzeń.

p) Należy zapewnić możliwość odtworzenia konfiguracji systemu SKD po awarii kontrolera, serwera lub stacji zarządzającej.

q) Tryb działania przejść w sytuacjach awaryjnych powinien być jednoznacznie opisany, w szczególności:

a. awaria zasilania,
b. awaria komunikacji,
c. ewakuacja,
d. alarm pożarowy,
e. awaria kontrolera.

r) Rozwiązanie powinno umożliwiać integrację z innymi systemami wyłącznie przez udokumentowane i kontrolowane interfejsy.

s) Eksport danych z systemu SKD powinien być dostępny wyłącznie dla upoważnionych osób.

t) Historia zdarzeń SKD powinna być chroniona przed modyfikacją przez użytkowników nieposiadających odpowiednich uprawnień.

6.2.3. System Sygnalizacji Włamania i Napadu — SSWiN

Zalecenia dotyczące cyberbezpieczeństwa:

a) Wszystkie centrale, manipulatory, ekspandery, moduły komunikacyjne i aplikacje zarządzające powinny być skonfigurowane bez domyślnych haseł i kodów instalatora.
b) Kody administratora, instalatora, serwisowe i użytkowników powinny być unikalne i przekazane Zamawiającemu w sposób poufny.
c) System powinien umożliwiać rozdzielenie uprawnień co najmniej na:
    a. użytkownika,
    b. administratora,
    c. instalatora,
    d. serwis,
    e. operatora monitoringu.
d) Dostęp instalatora lub serwisu powinien być możliwy wyłącznie za wiedzą i zgodą Zamawiającego.
e) Zaleca się, aby dostęp serwisowy był czasowo ograniczony i możliwy do wyłączenia przez Zamawiającego.
f) System powinien rejestrować co najmniej:
    a. uzbrojenie systemu,
    b. rozbrojenie systemu,
    c. alarmy,
    d. alarmy napadowe,
    e. sabotaże,
    f. awarie,
    g. brak zasilania,
    h. brak komunikacji,
    i. zmiany konfiguracji,
    j. wejście w tryb serwisowy,
    k. zdalne połączenia serwisowe,
    l. działania administratorów i instalatorów.
g) Transmisja alarmów do stacji monitorowania lub centrum ochrony powinna być zabezpieczona przed przechwyceniem, podszyciem się i nieuprawnioną modyfikacją.

h) Jeżeli system korzysta z transmisji GSM/LTE, należy zapewnić odpowiedni poziom bezpieczeństwa kanału komunikacyjnego.
i) Moduły komunikacyjne nie powinny udostępniać paneli administracyjnych bezpośrednio do Internetu.
j) System powinien umożliwiać wykrywanie i sygnalizowanie:
    a. sabotażu obudowy,
    b. sabotażu linii dozorowych,
    c. utraty komunikacji,
    d. zaniku zasilania,
    e. awarii akumulatora,
    f. próby nieautoryzowanego dostępu.
k) Wykonawca powinien opisać sposób reakcji systemu na awarie komunikacji, zasilania i urządzeń peryferyjnych.
l) System powinien umożliwiać wykonanie kopii zapasowej konfiguracji centrali oraz urządzeń powiązanych.
m) Wykonawca powinien przekazać Zamawiającemu:
    a. pełną konfigurację systemu,
    b. listę użytkowników i poziomów uprawnień,
    c. wykaz kodów administracyjnych i serwisowych,
    d. procedurę zmiany kodów,
    e. procedurę odtworzenia systemu po awarii.
    f. Po zakończeniu wdrożenia konta tymczasowe i kody używane podczas instalacji muszą zostać usunięte albo zmienione.
n) System powinien umożliwiać okresową zmianę kodów użytkowników i kodów serwisowych.
o) W przypadku integracji SSWiN z SKD, CCTV, systemem ppoż. lub BMS, integracja powinna być udokumentowana i ograniczona do niezbędnego zakresu.
p) Integracja nie może umożliwiać niekontrolowanego przejęcia sterowania nad systemem alarmowym z poziomu innego systemu.
q) Wykonawca powinien zapewnić procedurę testowania poprawności działania systemu po aktualizacjach lub zmianach konfiguracji.

6.2.4. System Telewizji Dozorowej — CCTV

Zalecenia dotyczące cyberbezpieczeństwa:

a) Wszystkie kamery, rejestratory, serwery VMS, stacje operatorskie i aplikacje zarządzające muszą być skonfigurowane bez domyślnych haseł.

b) System CCTV powinien umożliwiać stosowanie imiennych kont użytkowników.

c) System powinien obsługiwać role i poziomy uprawnień, co najmniej:

   a. operator podglądu bieżącego,

   b. operator odtwarzania nagrań,

   c. użytkownik eksportujący nagrania,

   d. administrator,

   e. serwis,

   f. audytor lub użytkownik tylko do odczytu.

d) Dostęp do nagrań archiwalnych powinien być ograniczony wyłącznie do upoważnionych osób.

e) Eksport nagrań powinien być rejestrowany w logach i możliwy wyłącznie dla osób posiadających odpowiednie uprawnienia.

f) System powinien umożliwiać zachowanie integralności eksportowanego materiału, np. przez:

   a. sumy kontrolne,

   b. podpis cyfrowy,

   c. znak wodny,

   d. dedykowany odtwarzacz z weryfikacją integralności,

   e. inny równoważny mechanizm.

g) System powinien rejestrować co najmniej:

   a. logowania i nieudane próby logowania,

   b. dostęp do podglądu na żywo,

   c. odtwarzanie nagrań,

   d. eksport nagrań,

   e. usunięcie lub nadpisanie nagrań,

   f. zmianę konfiguracji kamer,

   g. zmianę konfiguracji rejestratora lub VMS,

h. utratę sygnału z kamery,
i. awarie dysków,
j. awarie usług,
k. działania administratorów,
l. zdalne sesje serwisowe.

h) Kamery powinny umożliwiać:
a. aktualizację firmware,
b. zmianę kont i haseł,
c. wyłączenie nieużywanych usług,
d. konfigurację kont z różnymi poziomami dostępu,
e. szyfrowany dostęp administracyjny,
f. rejestrowanie zdarzeń administracyjnych.

i) Rejestrator lub system VMS powinien umożliwiać:
a. centralne zarządzanie kontami,
b. centralne zarządzanie uprawnieniami,
c. monitorowanie stanu kamer,
d. monitorowanie stanu dysków,
e. alarmowanie o utracie obrazu,
f. alarmowanie o awarii zapisu,
g. archiwizację konfiguracji.

j) Retencja nagrań powinna być zgodna z polityką Zamawiającego i zasadą minimalizacji danych.

k) System powinien umożliwiać automatyczne usuwanie lub nadpisywanie nagrań po zakończeniu okresu retencji.

l) Należy zapewnić możliwość zabezpieczenia nagrań incydentalnych przed automatycznym nadpisaniem na czas prowadzenia czynności wyjaśniających.

m) System powinien umożliwiać stosowanie masek prywatności w miejscach, gdzie pole widzenia kamery może obejmować obszary niewymagające monitorowania.

n) Kamery powinny być skonfigurowane tak, aby ograniczać zakres obserwacji do obszarów niezbędnych z punktu widzenia bezpieczeństwa muzeum, osób i zbiorów.

o) System powinien umożliwiać wykonanie kopii zapasowej:

a. konfiguracji kamer,
b. konfiguracji VMS/NVR,
c. kont użytkowników,
d. ról i uprawnień,
e. ustawień retencji,
f. harmonogramów nagrywania,
g. map i układów widoków operatorskich.

p) Wykonawca powinien zapewnić procedurę odtworzenia systemu CCTV po awarii:
   a. kamery,
   b. rejestratora,
   c. serwera VMS,
   d. stacji operatorskiej,
   e. macierzy lub dysków.

q) Stacje operatorskie CCTV powinny być zabezpieczone przed nieautoryzowanym użyciem, w szczególności przez:
   a. indywidualne konta,
   b. ograniczenie możliwości instalowania oprogramowania,
   c. ograniczenie dostępu do systemu operacyjnego,
   d. brak pracy na koncie administracyjnym.

r) Wykonawca powinien przekazać Zamawiającemu pełne prawa administracyjne do systemu CCTV.

s) Po zakończeniu wdrożenia należy usunąć lub zablokować wszystkie konta tymczasowe, instalacyjne i testowe.

6.2.5. Wymagania odbiorowe wspólne dla systemów SKD, SSWiN i CCTV

Przed odbiorem końcowym wykonawca powinien przedstawić Zamawiającemu:

a) dokumentację powykonawczą każdego system
b) wykaz urządzeń, wersji firmware i oprogramowania,
c) wykaz kont administracyjnych, serwisowych i operatorskich,
d) potwierdzenie zmiany haseł domyślnych,
e) potwierdzenie usunięcia kont tymczasowych,
f) wykaz aktywnych usług i portów,
g) procedurę backupu i odtwarzania,
h) procedurę aktualizacji,
i) procedurę obsługi kont i uprawnień,
j) procedurę zdalnego dostępu serwisowego,
k) procedurę reagowania na incydenty,
l) wyniki testów działania logów,
m) wyniki testu odtworzenia konfiguracji,
n) potwierdzenie braku bezpośredniego dostępu urządzeń z Internetu,
o) protokół szkolenia administratorów i operatorów.

6.2.6. Wymagania dodatkowe dla stacji roboczych

Stacje robocze powinny mieć zablokowane porty USB dla szeregowych użytkowników, dostęp jedynie z dedykowanego konta, które to konto będzie mieć dostęp jedynie do przenoszonych danych, bez pełnego dostępu do zasobów.

Stacje robocze muszą mieć trwale wyłączoną możliwość komunikacji WiFi, Bluetooth i innych z urządzeniami mającymi dostęp do Internetu.

6.3. WYMAGANIA DO PRAC PROJEKTOWYCH – ZAKRES I FORMA

6.3.1. Przedmiot opracowania. Projekt Wykonawczy (PW)

Wykonawca przygotuje i przedstawi do zatwierdzenia kompletną dokumentację projektową **Projekt Wykonawczy** (PW). Projekt będzie obejmował instalacje niskoprądowe, instalacje elektryczne i prace wykończeniowe (modernizacyjne). Dokumentacja musi zawierać rozwiązania techniczne, obliczenia, schematy, rysunki wykonawcze, zestawienia materiałowe oraz wszelkie opracowania niezbędne do realizacji inwestycji.

a) Zakres merytoryczny dokumentacji. Dokumentacja projektowa powinna obejmować:
    a. inwentaryzację stanu istniejącego,
    b. analizę i ocenę otoczenia i możliwych zagrożeń,
    c. analizę uwag Użytkownika (punkt 6.3.3 niniejszego opracowania),
    d. analizę uwarunkowań technicznych i eksploatacyjnych, a w tym harmonogram prac uwzględniający konieczność utrzymania funkcjonalności przebudowywanych systemów przez cały czas realizacji,
    e. dobór urządzeń i materiałów,
    f. opracowanie tras kablowych i lokalizacji urządzeń,
    g. wytyczne branżowe dla instalacji powiązanych (jeżeli wystąpią),
    h. specyfikacje techniczne wykonania i odbioru robót,
    i. zestawienia materiałowe (ilościowe).
b) Wymagania projektowe. Projekt należy wykonać zgodnie z:
    a. obowiązującymi przepisami prawa,
    b. warunkami technicznymi dla budynków i budowli,
    c. aktualnymi normami PN i PN-EN,
    d. wymaganiami Zamawiającego,
    e. zasadami wiedzy technicznej i dobrymi praktykami inżynierskimi.
c) Zawartość. Dokumentacja powinna zawierać co najmniej:
    a. analizę i ocenę ryzyk,
    b. założenia projektowe,
    c. opis techniczny,
    d. obliczenia techniczne,
    e. schematy ideowe i funkcjonalne,

f. rzuty z rozmieszczeniem urządzeń i przebiegiem tras instalacyjnych (niezależnie dla każdego z systemów),
g. zestawienia materiałów i urządzeń z jednoznacznym wskazaniem producenta, typu i ilości,
h. wytyczne wykonawcze w tym rysunki warsztatowe wskazujące sposoby montażu poszczególnych elementów (kamery, czujki PIR, czujki magnetyczne, przejścia kontroli dostępu,
i. harmonogram realizacyjny,
j. informacje dotyczące uruchomienia, testów i odbiorów.

d) Koordynacja międzybranżowa

Projektant zobowiązany jest do uwzględnienia wymagań wynikających z architektury obiektu, jego funkcji i przeznaczenia oraz konstrukcji, i instalacji znajdujących się w obiekcie.

e) Gwarancja i wsparcie

Projektowane rozwiązania powinny umożliwiać objęcie urządzeń gwarancją wykonawcy oraz zapewniać możliwość świadczenia usług serwisowych przez co najmniej 5 lat.

f) Nadzory autorskie

Do zakończenia prac oraz przez okres jednego roku od podpisania protokołu odbioru końcowego Projektant będzie zobowiązany świadczyć usługę nadzoru autorskiego.

g) Wymagania poligraficzne i edycyjne

Zaakceptowaną przez Zamawiającego Dokumentację należy przekazać w wersji papierowej (2 egz.) oraz w wersji elektronicznej (pendrive) 2 kpl. w formatach:

część edytowalna: DOC, XLS i DWG, część nie edytowalna: PDF

6.3.2. Wytyczne wykonawcze do ujęcia i rozwinięcia w PW

a) Wszystkie kable i przewody będą prowadzone i układane w następujący sposób:
    a. podtynkowo w bruzdach podlegających zaprawieniu,
    b. natynkowo / naściennie w uchwytach,
    c. natynkowo / naściennie w rurach osłonowych karbowanych,
    d. natynkowo / naściennie w rurkach lub kanałach PCV,
    e. w metalowych korytach kablowych (nie zaleca się wykorzystywania istniejących tras),
    f. w listwach przypodłogowych,
    g. przy przejściach przez ściany i stropy w przepustach.
b) Wszystkie przejścia przez strefy pożarowe uszczelnić do klasy przegrody.
c) Przewody należy prowadzić pełnymi odcinakami bez wykonywania zbędnych połączeń. Jeżeli zastosowana technologia wymaga połączenia przewodów poza urządzeniami należy wykonać je w przeznaczonych do tego celu puszkach lub zasobnikach. Nie dopuszcza się połączeń skręcanych lub lutowanych. Połączenia wykonać przy pomocy złączek uwzględniających średnicę lub przekrój łączonych żył.
d) Wszystkie kable powinny być oznaczone numerycznie, w sposób trwały, tak od strony gniazda lub urządzenia końcowego, jak i od strony szafy, rozdzielni czy puszek montażowych. Dobór systemu oznaczania oraz jednolity sposób „numeracji" należy jednoznacznie pokazać w PW i nanieść na rzutach i schematach w DPW.
e) Dodatkowe wytyczne dotyczące estetycznego prowadzenia okablowania i montażu urządzeń:
    a. w części wystawowej budynku wykorzystać do przeprowadzenia okablowania miejsc wcześniej naruszonych (np. przez wcześniejsze zdemontowane struktury), ograniczenie przebić i podkuć
    b. projektować przebieg różnych typów instalacji obok siebie, we wspólnych szachtach, korytach lub kanałach, o ile nie ma w tym zakresie przeciwwskazań technicznych,
    c. przewody i urządzenia mocować punktowo w fugach muru,
    d. unikać tworzenia nowych bruzd instalacyjnych, przeprowadzać przewody w fugach pomiędzy cegłami lub kamieniami w obrębie murów nietynkowanych i tynkowanych,

e. ukrywać instalację pod tynkami, w przestrzeniach stropowych lub nad sufitami podwieszanymi,
f. lokalizować czujniki i urządzenia powyżej linii wzroku zwiedzającego, z wykorzystaniem naturalnych osłon (np. gzymsów, belek, attyk, uskoków, nisz, atrap architektonicznych itp.),
g. dobierać kolor i wielkości (rozmiar) projektowanych czujników i urządzeń do wielkości pomieszczeń oraz planowanych zamiarów wystawienniczych,
h. unikać sąsiedztwa czujników i urządzeń z eksponatami,
i. uzgodnić ilość i lokalizację gniazd dodatkowych np. w listwach przypodłogowych, posadzkach, sufitach i nad sufitami, umożliwiających podłączenie w przyszłości dodatkowych lub zamiennych punktów monitoringu,
j. stosować „maskownice" do urządzeń upodobniających je do finalnego wystroju wnętrza,
k. w sytuacji przeprowadzenia przewodów w pomieszczeniach bez tynków, należy zastosować standaryzowane osłony (np. z tworzyw sztucznych lub metalowych) dobranych z Użytkownikiem, mocowanych punktowo w fugach,
l. należy wykorzystać rozwiązania kolorystyczne odwracające uwagę zwiedzających od instalacji (skorzystanie z własności widzenia):
   − intensywność oświetlenia skoncentrowana na istocie muzealnej,
   − pogłębienie mroku otwartej przestrzeni „technicznej" poprzez dobór kolorów z palety szarości i czerni ponad strefami wyróżnionymi światłem,
   − podwieszenie ażurowych detali maskujących - imitujących sufit lub istniejące konstrukcje wsporcze.

6.3.3. Problemy zgłaszane przez użytkowników i audytorów do ujęcia i rozwinięcia w PW

a) częste problemy z naprawą, rozbudową i konserwacją zamkniętego systemu jakim jest istniejące rozwiązanie,
b) awarie systemów po niekontrolowanych, krótkotrwałych wyłączeniach zasilania (awarie i prace rekonfiguracyjne TAURON),
c) problemy z uszkadzaniem i zamalowywaniem elementów SSWiN w trakcie prac remontowych (malowanie) i rearanżacyjnych na powierzchniach wystawienniczych (kilka razy rocznie),
d) przysłanianie i utrata widoczności (SSWiN, CCTV) na powierzchniach magazynowych i garażowych,
e) przysłanianie i utrata widoczności (SSWiN, CCTV) w efekcie prac rearanżacyjnych na powierzchniach wystawienniczych,
f) niska jakość obrazu z kamer, często brak możliwości identyfikacji twarzy,
g) bardzo słaba jakość obrazu CCTV w porze nocnej,
h) strefy nie objęte monitoringiem na Galeriach (stale i czasowo po rearanżacjach)
i) kamery zewnętrzne są „oślepiane" przez słońce,
j) znaczna ilość drobnych awarii poszczególnych elementów CCTV, SSWiN, SKD – rejestratory, czujniki, czytniki, kontaktrony, kamery, zasilacze (w tym akumulatory), zwory magnetyczne, elektrorygle,
k) pojedyncze problemy z okablowaniem,
l) luki w obrazie CCTV od strony bulwarów wiślanych
m) bardzo słaba widoczność terenów wzdłuż ogrodzenia nocą.
n) przypadkowe rozłączenia w szafie rack CCTV,
o) zwarcia w instalacji SSWiN/SKD wywołane wilgocią,
p) słabe wsparcie systemów monitoringu w obszarze ciągu samochodowo-pieszego od ulicy Sandomierskiej, na parkingu, wejściu do Szkoły, Pawilonu herbaciarni i wjazdach do garaży,
q) brak skutecznego nadzorowania gości biorących udział w imprezach zamkniętych (głownie w obszarze ogrodu oraz Sali widowiskowej),
r) pozostawianie otwartych przejść objętych kontrolą dostępu.
s) Brak zabezpieczenia sieci teleinformatycznej biurowej przez profesjonalne rozwiązanie typu *firewall*.

6.3.4. Dokumentacja powykonawcza, Projekt Powykonawczy (DPW)

a) Przedmiot opracowania

Przedmiotem opracowania będzie wykonanie kompletnej Dokumentacji powykonawczej **Projekt Powykonawczy** (DPW) całości zrealizowanych prac ze szczególnym naciskiem na łatwość i użyteczność zastosowania DPW w okresie eksploatacji, obejmującej opis zastosowanych rozwiązań technicznych, obliczenia potwierdzające prawidłowość doboru, schematy, rysunki wykonawcze, zestawienia materiałowe, instrukcje obsługi i serwisowania oraz wszelkie opracowania niezbędne w okresie eksploatacji.

b) Zakres i sposób wykonania dokumentacji

Dokumentacja powykonawcza powinna obejmować:

- pełną inwentaryzację stanu istniejącego w chwili zgłoszenia prac do odbioru,
- opis zastosowanych rozwiązań z uwzględnieniem realizowanych funkcji,
- szczegółowy wykaz ilościowy zastosowanych urządzeń i materiałów,
- schematy ideowe systemów z naniesieniem wszelkich oznaczeń identyfikujących,
- schematy połączeń dla poszczególnych szaf, rozdzielnic, central, kontrolerów, urządzeń magistralowych i puszek,
- widoki elewacji dla poszczególnych szaf, rozdzielnic, central, kontrolerów, urządzeń magistralowych i puszek,
- rzuty z naniesieniem szczegółowego przebiegu tras kablowych (w tym rzędne),
- rzuty z naniesieniem szczegółowego posadowienia poszczególnych elementów (dla każdego systemu odrębnie),
- listę kablową obejmującą co najmniej typ przewodu, jego przebieg i oznaczenie,
- karty katalogowe w języku polskim lub karty w języku oryginalnym wraz z załączonym tłumaczeniem; jeżeli karta obejmuje wiele urządzeń należy wyraźnie zaznaczyć, które z nich są zainstalowane,
- pełną instrukcję obsługi,
- skrócone instrukcje obsługi dla poszczególnych urządzeń + egzemplarze zalaminowane,
- instrukcję konserwacji i serwisowania,
- wykaz czynności serwisowych niezbędnych do utrzymania gwarancji wraz z tabelą harmonogramową,
- program szkolenia obsług,

- załączniki w postaci nośników elektronicznych z kopiami zainstalowanych wersji oprogramowania, szczegółami „customizacyjnymi" i backup-ami umożliwiającymi odtworzenie systemu (szczegółowe wytyczne w punkcie 6.2)

Rysunki w dokumentacji powykonawczej muszą być czytelne. Przebiegi i elementy instalacji powinny wyraźnie odcinać się od obrysów pomieszczeń i nie być w żaden sposób przysłaniane. Przebiegi powinny odzwierciedlać dokładny układ trasy, a elementy należy umieszczać na rysunkach zgodnie z rzeczywistym miejscem montażu.

Istotne fragmenty rysować w powiększeniu umożliwiającym prawidłowe rozpoznanie.

Dokumentację powykonawczą należy przekazać w wersji papierowej (3 egz.) w segregatorach koloru żółtego oraz w wersji elektronicznej (pendrive) 2 kpl. w formatach:

część edytowalna: DOC, XLS i DWG.; nie edytowalna: PDF.

Dodatkowo do wersji elektronicznej należy dołączyć pełny skan dokumentacji papierowej w formacie: PDF.

6.3.5. Szkolenie obsługi

Po zakończeniu prac należy uzgodnić z Zamawiającym cykl szkoleń w zakresie obsługi i serwisu zainstalowanych systemów i urządzeń.

Program szkolenia powinien przewidzieć część wykładową oraz ćwiczenia z obsługi (podstawowe działania administracyjne, zachowanie w przypadkach konkretnych alarmów itp.)

Należy przewidzieć 4 tury szkolenia podstawowego (dla każdej zmiany oddzielnie) oraz szkolenie dla kadry zarządzającej. W pojedynczym szkoleniu uczestniczyć będzie nie więcej niż 4 osoby.

Przed szkoleniem należy przekazać pełne i skrócone instrukcje obsługi.

6.4. WYMAGANIA DLA URZĄDZEŃ

Należy stosować urządzenia i materiały:

- fabrycznie nowe,
- pochodzące z legalnego kanału dystrybucji,
- posiadające otwartą architekturę i integrujące się poprzez otwarte protokoły komunikacyjne,
- posiadające wymagane certyfikaty, deklaracje zgodności i dopuszczenia,
- zapewniające dostępność części zamiennych i wsparcia technicznego przez okres eksploatacji,
- spełniające wymagania wskazane w rozdziale 6.2 Bezpieczeństwo teleinformatyczne i cyberbezpieczeństwa.

Rozwiązania powinny bazować na urządzeniach renomowanych producentów o ugruntowanej pozycji rynkowej.

Zamawiający nie dopuszcza rozwiązań:

- o architekturze zamkniętej,
- o ograniczonym dostępie dystrybucyjnym ,
- z rynku „home” i „smart home”.

Zastosowane urządzenia powinny zapewniać rozwiązanie obecnych problemów eksploatacyjnych, a w szczególności:

- niezawodność działania,
- bezpieczeństwo użytkowników,
- możliwość dalszej rozbudowy,
- łatwość eksploatacji i serwisowania,
- kompatybilność z istniejącą infrastrukturą obiektu,
- optymalizację kosztów eksploatacyjnych.

6.5. SYSTEM MONITORINGU WIZYJNEGO (CCTV)

Stan obecny telewizji dozorowej:

System składa się z 62 kamer analogowych różnych producentów. Rozdzielczość waha się od 420 do 960 TVL. Obraz zapisywany jest na pięciu rejestratorach (1 x analogowy TruVision TVR 4216; 3 x hybrydowy TruVision TVR15H; 1 x hybrydowy HikVision). Transmisja wizji odbywa się po kablu koncentrycznym RG 59 (Manggha) lub po skrętce UTP z zastosowaniem konwerterów pasywnych (głównie kamery z GE-DW). Minimalny 30-dniowy czas archiwizacji nagrań jest zachowany.

Obraz z kamer jest wyświetlany na 12 monitorach (różna wielkość, stan techniczny i rozdzielczość) zlokalizowanych w centrum ochrony (p.115 Manggha). Do pracy z systemem służy stacja robocza oraz klawiatura sterująca. Obraz z kamer obszaru GE-DW (30 kamer) może być również wyświetlany w pomieszczeniu technicznym tego obszaru (p.205).

Należy wymienić wszystkie obecnie istniejące kamery systemu CCTV.

Należy rozbudować system o dodatkowe kamery oraz dodatkowe punkty (gniazda) zgodnie z poniższymi tabelami.

Na etapie projektowania uzgodnić z Zamawiającym szczegółowo punkty umiejscowienia (braku przesłaniania) oraz dobrać parametry obiektywów dla wszystkich kamer.

Na etapie montażu uzgodnić z Zamawiającym ustawienie wszystkich kamer (kierunek, zakres obrazu, głębia).

Wykaz dodatkowych kamer (likwidacja stref martwych)

Lp.	lokalizacja	rodzaj kamery
1	Korytarz biurowy od przejścia do wejścia	wewnętrzna
2	Korytarz od strony 115 w kierunku garaż, 108 i 109	wewnętrzna
3	Korytarz od strony 109 w kierunku 205	wewnętrzna
4	Korytarz od strony 205 w kierunku 201/202/203	wewnętrzna
5	Szatnia dolna (koło Lobby), w kierunku toalet i 106	wewnętrzna
6	Korytarz przy magazynach zbiorów	wewnętrzna
7	Sala wielofunkcyjna od nagłośnienia strona prawa	wewnętrzna
8	Sala wielofunkcyjna od reżyserki w stronę sceny	wewnętrzna
9	Lobby z narożnika płn.-wsch. w kierunku ogrodu	wewnętrzna
10	Widok tarasu od strony ogrodu	zewnętrzna
11	Elewacja pod tarasem z zach. na wschód	bispektralna*
12	Pod mostkiem wzdłuż elewacja na zach.	bispektralna*

13	Elewacja od ronda Grunwaldzkiego w stronę mostka	bispektralna*
14	Elewacja od mostka w stronę ronda Grunwaldzkiego	bispektralna*
15	Szatnia przed Galerią od wewnątrz w stronę holu	wewnętrzna
16	Galeria zewnętrzna ściana od strony Wisły	wewnętrzna
17	Galeria zewnętrzna, wyjście ewakuacyjne w stronę ronda	wewnętrzna
18	Galeria zewnętrzna, wzdłuż ściany południowej	wewnętrzna
19	Galeria wewnętrzna, kamera dodatkowa	wewnętrzna
20	Galeria wewnętrzna, kamera dodatkowa	wewnętrzna
21	Galeria wewnętrzna, kamera dodatkowa	wewnętrzna
22	Klatka schodowa z restauracji widok na drzwi 107	wewnętrzna
23	Restauracja, widok w stronę schodów do Sali wielofunkcyjnej	wewnętrzna
24	Sklepik, widok z nad kasy w stronę sklepu i okien	wewnętrzna
25	Szatnia GE-DW (parter) z wewnątrz na windę i toaletę	wewnętrzna
26	Hol wejściowy GE-DW, widok na kasę od ściany tylnej	wewnętrzna
27	Parter GE-DW Korytarz w stronę Galerii	wewnętrzna
28	Parter GE-DW klatka za pomieszczeniem ochrony	wewnętrzna
29	2 p. GE-DW, pomieszczenie z wyjściem na dach	wewnętrzna
30	Brama wjazdowa od ul. Sandomierskiej w kierunku szkoła, parking	zewnętrzna
31	Z narożnika szkoły w stronę bramy od ul. Sandomierskiej	zewnętrzna
32	Z narożnika szkoły w stronę pawilonu herbacianego	zewnętrzna
33	W szkole, parter widok na wejście (od wewnątrz)	wewnętrzna
34	W szkole, pierwsze piętro widok wejść do sali	wewnętrzna
35	W szkole, drugie piętro widok wejść do biblioteki	wewnętrzna
36	Kamera rezerwowa	wewnętrzna
37	Kamera rezerwowa	wewnętrzna
38	Kamera rezerwowa	wewnętrzna
39	Kamera rezerwowa	wewnętrzna
40	Kamery rezerwowa	bispektralna*

* Zamawiający dopuszcza dostawę dwóch niezależnych kamer (termicznej i optycznej)

Wykaz dodatkowych gniazd dla kamer wewnętrznych (likwidacja potencjalnych martwych stref dla Galerii)

lokalizacja	**rodzaj kamery**	**ilość**	**uwagi**
Galeria Manggha (część zewnętrzna)	wewnętrzna	1	Przy wejściu
Galeria Manggha (część wewnętrzna)	wewnętrzna	5	na ściankach od góry
Galeria GE-DW dolna	wewnętrzna	4	listwa dodatkowa
Galeria GE-DW górna	wewnętrzna	4	listwa dodatkowa

Kamery kopułkowe zewnętrzne/wewnętrzne z doświetlaczami wraz z uchwytami i systemem montażu.

Kamery tubowe zewnętrzne/wewnętrzne z doświetlaczami, obowiązkowymi obudowami, uchwytami i systemem montażu.

Kamery zewnętrzne termowizyjne lub kamery dualne wraz z uchwytami i systemem montażu.

Nie przewiduje się stosowania kamer typu Rybie oko (FishEye). Komunikacja bazująca na rozwiązaniach sieciowych (IP)

Urządzenia muszą spełniać odpowiednie standardy ONVIF (S, T, G)

System skalowalny w sposób liniowy i przewidywalny finansowo

Integracja co najmniej z systemem SKD i videodomofonami, możliwość dalszej integracji z SSP i SSWiN.

System musi posiadać możliwości analityczne i automatycznie reagować na występujące zdarzenia alarmowe.

Stanowisko nadzoru główne (p.115 Manggha): 6 x monitor główny + stacja robocza z dwoma monitorami, prosta możliwość przełączania i konfiguracji widoku z kamer

Stanowisko nadzoru pomocnicze w GE-DW: 2 x monitor główny, stacja robocza z dwoma monitorami.

Na czas wykonywania prac stanowisko pomocnicze tymczasowa konfiguracja: 4 x monitor główny, stacja robocza z dwoma monitorami (docelowo dwa monitory główne do przeniesienia na stanowisko nadzoru).

Wszystkie elementy (cały system) musi mieć podtrzymanie zasilania (dedykowane UPS-y) na 4 godziny nieprzerwanej pracy.

Wymagania dla poszczególnych elementów systemu.

Kamery:

Parametr	Wymagania minimalne
Budowa	Kamera kopułowa z doświetlaczem, uchwytem ściennym i/lub sufitowym
Rozdzielczość	6 MP
Przetwornik	1/1,8”
Obiektyw	2,8mm
Czułość (oświetlenie)	Praca w kolorze dzień/noc
Kompresja	co najmniej H.264 i H.265
Inteligentna analiza obrazów	co najmniej klasyfikacja człowiek/pojazd, wtargnięcie w obszar oraz obustronne przekroczenie linii (we/wy)
Zapis lokalny	karta pamięci
Wejście alarmowe	tak
Wyjście alarmowe	tak
Wejście audio	Tak, liniowe lub wbudowany mikrofon
Obudowa	IP67, IK10
Warunki pracy	-30 do +55 st. C, wilgotność do 95% bez kondensacji
Doświetlenie	IR + światło białe na co najmniej 36m
Zasilanie	PoE
Gwarancja producenta	5 lat lub doubezpieczenie gwarancji do 5 lat

Parametr	Wymagania minimalne
Budowa	Kamera tubowa doświetlaczem
Rozdzielczość	6 MP
Przetwornik	1/1,8”
Obiektyw	2,8mm
Czułość (oświetlenie)	Praca w kolorze dzień/noc
Kompresja	co najmniej H.264 i H.265
Inteligentna analiza obrazów	co najmniej klasyfikacja człowiek/pojazd, wtargnięcie w obszar oraz obustronne przekroczenie linii (we/wy)
Zapis lokalny	karta pamięci
Wejście alarmowe	tak
Wyjście alarmowe	tak
Wejście audio	Tak, liniowe lub wbudowany mikrofon
Obudowa	IP67, IK10
Doświetlenie	IR + światło białe na co najmniej 30m
Zasilanie	PoE
Gwarancja producenta	5 lat lub doubezpieczenie gwarancji do 5 lat

Parametr	Wymagania minimalne
Budowa	Kamera bispektralna, tubowa, zewnętrzna z uchwytem ściennym
Moduł termowizyjny	
Rozdzielczość:	256x192 pixeli
Pole widzenia:	50 st. X 35 st. +/- 5 st.
Czułość termiczna:	50 mK
Moduł optyczny	
Rozdzielczość	4 MP
Przetwornik	CMOS o rozmiarze od 1/2,8” do 1/1,2”
Obiektyw	Z przedziału 2,8 - 4,3 mm
Czułość (oświetlenie)	Praca w kolorze dzień/noc
Kompresja	co najmniej H.264 i H.265
Strumienie	Dwa strumienie obrazu termowizyjnego i dwa strumienie obrazu optycznego
Inteligentna analiza obrazów	Klasyfikacja człowiek/pojazd, Wtargnięcie w obszar Wyświetlanie częściowego obrazu z kanału termowizyjnego na pełnym podglądzie z kanału optycznego lub równoległe wyświetlanie obrazu na jednym z monitorów dwóch oknach obok siebie Predefiniowane tryby (White Hot, Black Hot)
Zapis lokalny	karta pamięci
Wejście alarmowe	tak
Wyjście alarmowe	tak
Wejście audio	Tak, liniowe lub wbudowany mikrofon
Obudowa	IP67, IK10
Warunki pracy	-30 do +60 st. C, wilgotność do 95% bez kondensacji
Doświetlenie	IR + światło białe na co najmniej 30m
Zasilanie	PoE
Gwarancja producenta	5 lat lub doubezpieczenie gwarancji do 5 lat

* Zamawiający dopuszcza zainstalowanie dwóch niezależnych kamer (termicznej i optycznej), tak aby spełnić wszystkie powyższe wymagania

Parametr	Wymagania minimalne
Budowa	Kamera szybkoobrotowa z doświetlaczem (dzień/noc) metalowa, wraz z systemem montażowym
Rozdzielczość	4 MP
Przetwornik	1/1,8”
Powiększenie optyczne	x25
Dzień/noc	ICR (mechaniczny)
Kompresja	co najmniej H.264 i H.265
Inteligentna analiza obrazów	
Zapis lokalny	Tak
Wejście alarmowe	4
Wyjście alarmowe	2
Wejście audio	Tak, lub wbudowany mikrofon
Obudowa	IP67, IK10
Warunki pracy	Temperatura robocza od -40°C do +70°C, wilgotność do 95% (wymagana wbudowana grzałka)
Doświetlenie IR zasięg	200m
Zasilanie	PoE
Gwarancja producenta	5 lat lub doubezpieczenie gwarancji do 5 lat

Serwer:

Parametr	Wymagania minimalne
Obudowa	RACK max. 3U, szyny montażowe
Zasilanie	Dwa zasilacze redundantne
Procesor	Min: Xeon Silver 4410Y (INTEL) lub EPYC 9124 (AMD)
Pamięć RAM	32GB DDR5 ECC REG z możliwością rozbudowy (nie wymiany!) do 64GB
Dysk serwera	2x 480GB SSD NVMe PCIe do pracy ciągłej
Oprogramowanie	System: Windows Server Standard 2025 z licencjami na zastosowaną ilość rdzeni
Gwarancja producenta	Minimum 36 mies. door-to-door

Stacja kliencka:

Parametr	Wymagania minimalne
Procesor	Min. Intel Corei5/i7 lub AMD Ryzen 7
Pamięć RAM	Min 32GB DDR5 (2x16), taktowanie min. 4,8GHz
Dysk	SSD min. 1TB M.2 PCIe NVMe
Oprogramowanie	Windows 11 Pro
Karta graficzna	Dedykowana min. 8GB RAM
Obudowa, zasilacz	Desktop, min. 650W, certyfikowany (min. 80 Plus Gold)
Gwarancja	Minimum 36 mies. On-Site

Monitor główny (do Video Wall)

Parametr	**Wymagania minimalne**
Wielkość i rodzaj ekranu	48” do 50” +/-0.5”, matryca IPS z podświetlaniem LED, Full HD (1920 × 1080)
Jasność	500 cd/m2
Poziom kontrastowości statycznej	1200:1
Nieprzerwana praca	24/7
Wejścia wideo	1x HDMI
sterowanie	TAK – np. RS232 IN/OUT
Monitor do ściany wizyjnej CCTV	TAK, ramka nie więcej niż 4mm
Montaż i obudowa	VESA, obudowa metalowa
Gwarancja producenta	5 lat lub doubezpieczenie gwarancji do 5 lat

Monitor stacji roboczej

Parametr	**Wymagania minimalne**
Typ i rozmiar ekranu	27” do pracy ciągłej
Rozdzielczość	Full HD (1920 × 1080)
Czas reakcji	15 ms
Złącza wideo	1x HDMI 1.4
Monitor o wąskiej ramce	3mm (góra, lewa, prawa)
Gwarancja producenta	5 lat lub doubezpieczenie gwarancji do 5 lat

Dekodery należy dobrać tak jakościowo i ilościowo aby można było jednocześnie wyświetlić obrazy ze 96 kamer na stanowisku nadzoru oraz 64 kamer na stanowisku pomocniczym (wybór kamer dowolny). Nie dopuszcza się rozwiązań opartych o komputery wyposażone w karty graficzne

Dekoder

Parametr	**Wymagania minimalne**
Rodzaj	dedykowane rozwiązanie sprzętowe
Wydajność	dekodowanie do 36 kanałów przy rozdzielczości 1080p
Ilość wyświetlanych obrazów na wyjście	od 1 do 25
Funkcje ściany wideo (TV Wall)	Wsparcie dla zaawansowanego zarządzania oknami: funkcja łączenia ekranów, dynamicznego nakładania i przesuwania okien (warstwowość obrazu), swobodnego skalowania (roaming pomiędzy monitorami całej ściany) oraz zapisywania i szybkiego wywoływania co najmniej 64 predefiniowanych scen (układów kamer).

Interfejsy wyjściowe	4x HDMI.
Wsparcie dla kamer termowizyjnych	Tak
Wsparcie audio	Tak
Analityka metadanych	Urządzenie musi wspierać bezpośrednie dekodowanie i wizualizację zaawansowanych metadanych z kamer IP bez pośrednictwa stacji PC, w tym: renderowanie dynamicznych map cieplnych (Heat Maps) oraz generowanie wykresów statystyk zliczania osób bezpośrednio na wyjściach HDMI
Dekodowanie zapisanych plików wideo	Tak
Obsługa sterowania wieloma ekranami za pomocą komputera PC lub klawiatury	Tak
Minimalna ilość portów	4 x 1Gbps Eth (RJ45, optyczne lub kombinacja)
Gwarancja producenta	5 lat lub doubezpieczenie gwarancji do 5 lat

Przewiduje się zastosowanie rejestratorów IP 16 i/lub 32 kanałowych

Parametr	**Wymagania minimalne 16 kanałowy**	**Wymagania minimalne 32 kanałowy**
Liczba kanałów IP obsługiwanych jednocześnie	16	32
Pasmo wejściowe / wyjściowe	160Mb/s / 160Mb/s	320Mb/s / 400Mb/s
Rozdzielczość nagrywanych kamer	12MP	
Wspierane formaty kompresji	H.265 / H.264 / MJPEG	
obsługa HDD	4 x 12TB SATA	8 x 12TB SATA
wyjście video	1x HDMI (4K) 1x VGA (1080p)	2x HDMI (4K) 1x VGA (1080p)
obudowa	Rack 2U, uchwyty lub szyny	
Sieć	2 x Gbps Eth	2 x Gbps Eth (dual IP)
Złącza dodatkowe	1x RS-232, 1x RS-485, 2 x USB (w tym min. jeden w standardzie 3.0)	
Analityka, wsparcie AI	Pełna obsługa i rejestracja zaawansowanych funkcji AI realizowanych przez kamery IP, takich jak: ochrona obwodowa (klasyfikacja człowiek/pojazd), detekcja i rozpoznawanie twarzy, rozpoznawanie tablic rejestracyjnych (LPR) oraz metadane	
Kompatybilność	ONVIF (T + G)	
Gwarancja	5 lat lub doubezpieczenie gwarancji do 5 lat	

W przypadku pełnej kompatybilności z proponowanym rozwiązaniem można wykorzystać istniejący rejestrator hybrydowy HikVision (warunek: objęcie gwarancją Wykonawcy na pełny okres)

Kolorystykę elementów dobrać i uzgodnić z zamawiającym na etapie PW

Oprogramowanie VMS

System VMS ma umożliwiać zarządzać w trybie ciągłym (24/7/365).

Parametry i funkcjonalności:

a) Pojedynczy serwer obsługujący do 500 kanałów wideo w wersji IP
b) Wszystkie urządzenia systemu komunikują się za pomocą protokołu TCP/IP
c) Automatyczne wylogowanie w momencie braku aktywności
d) Wykorzystanie kreatora systemu w zakresie konfiguracji podłączonych urządzeń
e) Nadawanie uprawnień oraz możliwość tworzenia sub-administratorów
f) Tworzenie użytkowników o określonych uprawnieniach w systemie
g) Obsługa protokołu ONVIF profil S, T + G
h) Zarządzanie urządzeniami i ich konfiguracja
i) Zarządzanie nagrywaniem
    - Ciągłe nagrywanie, nagrywanie uruchamiane zdarzeniem lub poleceniem.
    - Zgrywanie plików wideo przechowywanych na jednym nośniku do wybranej lokalizacji
    - Ustawianie planu nagrywania: Szablon czasowy na cały dzień, szablon według zdarzeń na cały dzień i szablon użytkownika
    - Pomocnicza przestrzeń dyskowa (konfigurowanie, zarządzanie)
j) Zarządzanie zdarzeniami i alarmami. Zdarzeniami mogą być:
    - Zdarzenia w kamerach: ruch, utrata obrazu wideo, przekroczenie linii itd.
    - Zdarzenia w kamerach: alarm przekroczonej temperatury powiązany z wiadomością email
    - Zdarzenia z serwera VCA: detekcja ruchu, przekroczenie linii, detekcja pozostawienia obiektu, detekcja przebywania w strefie, detekcja sabotażu oraz zmiany sceny, pobieranie statusu temperatury, pobieranie informacji o maskowaniu
    - Zdarzenia z wejść alarmowych urządzeń
    - Zdarzenia dotyczące użytkowników: zalogowanie lub wylogowanie użytkownika

- Zdarzenia definiowane przez użytkownika
- Zdarzenia szablonowe

k) Zarządzanie akcjami wywołanymi przez zdarzenia np. nagrywanie, tworzenie etykiet, przechwytywanie obrazu, łączenie z wyjściami alarmowymi oraz wywoływanie zdarzeń definiowanych przez użytkownika

l) Zarządzanie dowodami, możliwość zabezpieczania i blokowania nagrań wideo oraz zrzutów ekranu przed nadpisaniem, kategoryzacja zdarzeń archiwalnych, dodawanie opisów tekstowych do incydentów oraz możliwość eksportu powiązanych materiałów do zewnętrznych plików.

m) Możliwość tworzenia bramek logicznych sterujących regułami VCA

n) Modyfikowanie i tworzenie zdarzenia w celu stworzenia zdarzenia, którego nie ma na przekazanej liście zdarzeń,

o) Wywoływanie zdarzeń, jako alarmów i ustawianie działań związanych z alarmami, w tym wywołanie odpowiednich kamer, map, układów, wyskakujących okienek.

p) Wywołanie ostrzeżeń dźwiękowych i zdarzeń definiowanych przez użytkownika.

q) Ustawianie harmonogramu dla alarmów i zdarzeń, co najmniej: szablon całodniowy, na dzień roboczy, na weekend i szablon użytkownika

r) Ustawianie priorytetu alarmów: wysoki, średni, niski i użytkownika

s) Ustawianie kategorii alarmu: prawdziwy, fałszywy, do potwierdzenia i do zweryfikowania

t) Zarządzanie mapami:

- dodawanie do map interaktywnych elementów pokazujących stany kamer, we/wy alarmowych, punktów dostępowych oraz ikony zintegrowanych urządzeń firm trzecich
- dodawanie etykiet tekstowych
- dodawanie stref

u) Zarządzanie rolami i użytkownikami w tym ustawienie minimalnej siły hasła, ustawianie maksymalnego czasokresu obowiązywania hasła, blokowanie klienta po okresie nieaktywności.

v) Zarządzanie konfiguracją i konserwacja systemu:

- ustawienia Microsoft Active Directory (protokół LDAP)
- możliwość ustawienia statycznego adresu IP do dostępu WAN
- ustawianie okresu dla przechowywania danych zarejestrowanych w systemie
- predefiniowanie szablonów harmonogramu, w tym harmonogramu nagrywania, harmonogramu uzbrajania, harmonogramu dostępu,
- predefiniowanie reguł dla raportów,

- tworzenie raportów dotyczących aktywności użytkownika (wszystkie czynności związane z systemem), odebranych przez niego alarmów
- generowanie raportów na temat stanu i kondycji systemu
- ustawianie niepowtarzalnych ID dla kamer w systemie
- tworzenie kopii zapasowej i przywracanie bazy danych

Powyższy opis ma charakter poglądowy, poszczególne funkcjonalności mogą być realizowane w inny sposób.

6.6. SYSTEM KONTROLI DOSTĘPU (SKD)

W budynku Muzeum Manggha funkcjonuje ok. 30 przejść kontroli dostępu (w tym 8 dwustronnych). Drzwi wyposażone są w zwory elektromagnetyczne (6 przejść), pozostałe w elektrorygle.
W budynku Galeria Europa – Daleki Wschód funkcjonuje ok. 15 przejść kontroli dostępu (w tym 1 dwustronne). Drzwi wyposażone są w zwory elektromagnetyczne.

W obiekcie występują przejścia jednostronnie (wejścia do pomieszczeń) oraz dwustronne (ciągi komunikacyjne). Przejście kontrolowane jednostronnie oznacza, iż od strony przestrzeni kontrolowanej znajdować się będzie czytnik kart zbliżeniowych, natomiast od wewnątrz pomieszczenia przycisk wyjścia i przycisk ewakuacyjny. Przejście kontrolowane dwustronnie oznacza, iż z obu stron zastosowany będzie czytnik kart zbliżeniowych oraz przycisk ewakuacyjny w kierunku ewakuacji.

System kontroli dostępu (SKD) ma pracować w oparciu o architekturę klient-serwer. Serwer umożliwia konfigurację, zarządzanie i zapis informacji z rozproszonych w systemie kontrolerów przejść. Kontrolery powinny komunikować się z serwerem poprzez sieć IP. Każdy kontroler dostępu ma być urządzeniem w pełni autonomicznym. W przypadku braku komunikacji z serwerem, kontroler ma umożliwiać dostęp do chronionych pomieszczeń i przejść uprawnionym użytkownikom oraz zapisywać zdarzenia we wbudowanej pamięci. Działanie kontrolera ma być niezależne od dostępności i jakości komunikacji z serwerem. Po przywróceniu połączenia z serwerem wszystkie zdarzenia zapisane w kontrolerze mają zostać pobrane przez serwer i zapisane w bazie danych systemu.
System powinien umożliwiać zarządzenia trasami obchodów pracowników ochrony i generowanie raportów okresowych.
Zasilanie SKD ma spełnić wymóg 4 godzinnego podtrzymania w przypadku zaniku napięcia.

Dodatkowe przejścia
Należy zmodernizować wszystkie istniejące przejścia Systemu Kontroli Dostępu oraz rozbudować system o kolejne przejścia wyposażone w zwory elektromagnetyczne

Lp.	Lokalizacja	Rodzaj przejścia,
1	Drzwi w korytarzu C4 Manggha	Dwustronne
2	Drzwi A9 Manggha	Jednostronne

3	016 Manggha	Jednostronne + czytnik QR
4	204 Manggha	Jednostronne
5	Drzwi z biur na klatkę schodową (piętro 1) GE-DW	Jednostronne
6	012 Magazyn Manggha	Jednostronne
7	Pokój socjalny (koło Galerii) Manggha	Jednostronne
8	Magazyn wewnątrz Galeria Manggha	Jednostronne
9	Wejście do pomieszczenia technicznego	Jednostronne

Modernizacja ma polegać na wymianie wszystkich elementów SKD – również zasilaczy i okablowania. Wymienić należy wszystkie przyciski wyjścia i przyciski ewakuacyjne.
Wymianie nie podlega wyposażenie drzwi (zwory magnetyczne lub elektrorygle oraz kontaktrony) jeżeli jest sprawne. W przypadku niesprawności/uszkodzenia podlegają również wymianie.
Przejścia do pomieszczeń magazynu broni i tajnej kancelarii wykonać w stopniu 3 (Grade 3).
Zweryfikować poprawność pracy SKD we współpracy z SSP w przypadku alarmu pożarowego (zwolnienie przejść SKD).
Po zakończeniu prac system musi mieć możliwość dalszej rozbudowy do co najmniej 120 przejść.
Dla uporządkowania ruchu osobowego w okolicach sali wielofunkcyjnej planuje się wyposażenie części SKD w dodatkowe czytniki kodu QR i PIN oraz funkcję (usługę) awizacji.
Zamawiający dopuszcza w tych lokalizacjach czytniki uniwersalne (karta/kod QR/PIN)
Wykaz przejść/wjazdów z dodatkowymi czytnikami kodu QR:

a) 016 (Manggha)
b) 107 (Manggha)
c) 116 (Manggha)
d) 200 (Manggha)
e) Szlaban od ul. Sandomierskiej

Parametry i funkcjonalności moduł awizacji:

a) eksportować informacje o rejestracji gości oraz zapisy dotyczące dostępu,
b) generować kod QR umożliwiający dostęp do dozwolonych obszarów,
c) dostosowywać grupy gości,
d) wyświetlać łączną liczbę gości.

Kontroler i moduły rozszerzające (parametry dla każdego przejścia)

Parametr	Wymagania minimalne
Pojemność użytkowników	10 000
Pojemność kart	20 000
Pojemność zdarzeń	500 000
Interfejs sieciowy	1000Mbps Eth
Wejścia/wyjścia alarmowe	2 + 2
Wejście kontaktron	1
Wejście przycisku wyjścia	1
Wejście sabotażowe	1
Obsługa czytników Wiegand	2
Obsługa czytników niestandardowych (RS-485)	2
Anti-passback (APB)	Tak, w obrębie każdego z budynków.
Warunki pracy	-10 do +50 st. C; wilg. 90% bez kondensacji
Gwarancja	5 lat

Czytnik

Parametr	Wymagania minimalne
Obsługiwane protokoły	OSDP, RS-485
Obsługa standardu	Obsługuje DESfire
Sygnalizacja dźwiękowa	tak
Montaż	natynkowy
Gwarancja	5 lat

Czytnik uniwersalny

Parametr	Wymagania minimalne
Obsługiwane protokoły	OSDP, RS-485
Obsługa standardu	Obsługuje DESfire
Alternatywne metody uwierzytelniania	kod QR, kod PIN *
Sygnalizacja dźwiękowa	tak
Montaż	natynkowy
Gwarancja	5 lat

* Zamawiający dopuszcza zastosowanie na jednym przejściu dwóch czytników realizujących łącznie trzy metody dostępu (karta/kod QR/PIN)

Zwora elektromagnetyczna

Parametr	Wymagania minimalne
montaż	nawierzchniowy
konstrukcja	Przeciwsabotażowa (brak elementów montażowych od strony chronionej)
Siła trzymania	2500N
Gwarancja	5 lat

Przycisk ewakuacyjny w kolorze zielonym, aktywacja przycisku nie powinna wymagać zbicia szybki (przykładowy: GBC RES)

Przycisk wyjścia – biały z elementem luminescencyjnym na przełączniku (przykładowy: BT-2DN lub wersja natynkowa: BT-2DSN).

Kolorystykę elementów SKD dobrać i uzgodnić z zamawiającym na etapie PW

6.7. SYSTEM SYGNALIZACJI WŁAMANIA i NAPADU (SSWiN)

Należy wymienić wszystkie istniejące elementy systemu SSWiN.

W budynku Muzeum Manggha zainstalowanych jest obecnie około 70 czujek różnego typu, około 15 czujek magnetycznych (kontaktron), kilka klawiatur i sygnalizatorów.

W budynku Galeria Europa – Daleki Wschód zainstalowanych jest około 60 czujek różnego typu (dualnych, PIR i zbicia szyby), około 15 czujek magnetycznych (kontaktron) i 2 klawiatury i sygnalizator.

Wymagania ogólne

Główna część systemu SSWiN (zarówno centrala, jak i wszystkie ekspandery czy moduły rozszerzeń) musi bezwzględnie spełniać wymogi normy EN 50131-1 na poziomie Stopnia 3 (Grade 3). System musi posiadać architekturę modułową, umożliwiającą podział na minimum 32 niezależne strefy. Wszelka transmisja danych na magistralach komunikacyjnych łączących centralę z manipulatorami i ekspanderami musi być w pełni szyfrowana.

Lokalizacja poszczególnych central i modułów przygotować na etapie PW, ilość dobrać tak w każdej lokalizacji było minimum 10% wolnych wejść dozorowych (nie mniej niż jedno). W modułach obsługujących sale wystawowe ilość wolnych wejść ma być 20% (nie mniej niż 2 na lokalizację).

Organizacja oznakowania, adresowania, opisywania elementów systemu ma precyzyjne określać miejsca, z którego otrzymujemy alarm włamaniowy, napad, awarie oraz lokalizacje każdego elementu.

Zakłada się całkowite odseparowanie i pełną niezależność SSWiN od pozostałych systemów bezpieczeństwa.

Pomieszczenia magazynu broni i tajnej kancelarii zabezpieczyć w stopniu 3 (Grade 3).

Czujki ścienne mają być zamontowane na uchwytach dystansowych.

W trakcie prac projektowych może wyniknąć konieczność zastosowania czujek nietypowych (kurtynowa, z czujnikiem zmierzchu itp.)

Nie wymaga się aby elementy peryferyjne SSWiN były od tego samego producenta.

Dostarczyć min. 3 szt. pilotów do zdalnej konfiguracji czujek (lub narzędzia alternatywne).

Zasilanie rezerwowe SSWiN ma zapewnić w przypadku zaniku zasilania sieciowego podtrzymanie pracy przez 24h oraz dodatkowo 30 min pracy w stanie alarmu.

Centrala SSWiN oraz moduły rozszerzeń

Parametr	Wymagania minimalne
Stopień ochrony	Grade III
Obsługa linii	3EOL, z programowaniem wartości rezystorów
Zasilacz	Wbudowany, z diagnostyką
Możliwość rozbudowy	do 256 wejść (64 wyjść)
Możliwość programowania z urządzeń zewnętrznych	Tak, USB lub eth
Pamięć nieulotna	co najmniej 24 000 zdarzeń

Czujka pasywna podczerwieni (PIR)

Parametr	Wymagania minimalne
Stopień ochrony	Grade III
Antymasking	tak, aktywny
Cyfrowa kompensacja temperatury	tak
Zdalna konfiguracja	tak (pilot)
Uchwyt montażowy	tak, umożliwiający montaż z dystansem od ścian

Czujka dualna (PIR+MV) ścienna

Parametr	Wymagania
Stopień ochrony	Grade III
Antymasking	tak, aktywny
Cyfrowa kompensacja temperatury	tak
Zdalna konfiguracja	Tak (pilot)
Warunki pracy	Również w obszarach nieogrzewanych, zabrudzonych, przemysłowych
Uchwyt montażowy	tak

Czujka dualna (PIR+MV) dookólna

Parametr	Wymagania
Stopień ochrony	Grade III
Antymasking	tak, aktywny
Cyfrowa kompensacja temperatury	tak
Zdalna konfiguracja	Tak (pilot)
Warunki pracy	Również w obszarach nieogrzewanych, zabrudzonych, przemysłowych

Czujka zbicia szyby

Parametr	Wymagania minimalne
Analiza	Dwutorowa (niska i wysoka częstotliwość)

Sygnalizator akustyczno-optyczny zewnętrzny lub wewnętrzny

Parametr	Wymagania minimalne
Stopień ochrony	Grade III

Przycisk napadowy

Parametr	Wymagania minimalne
Stopień ochrony	Grade III
Mechanizm blokady w stanie alarmu	tak

Klawiatura

Parametr	Wymagania minimalne
Stopień ochrony	Grade III
Wyświetlacz	Co najmniej 2 linie
Klawiatura	Przyciski fizyczne lub sensoryczne
Klapka zabezpieczająca	W wybranych lokalizacjach

Rozmieszczenie dodatkowych czujek oraz kolorystykę dobrać i uzgodnić z Zamawiającym na etapie PW.

6.8. INSTALACJE, PRACE i SYSTEMY POMOCNICZE

6.8.1. Wydzielona sieć LAN

Sieć dla systemów bezpieczeństwa musi zostać zrealizowana w architekturze gwiazdy dwupoziomowej. Warstwa Dostępowa (zakończona w szafkach (PD), Warstwa Dystrybucyjna w szafach GPD (Pomieszczenie Techniczne). Połączenie między PD a GPD musi być realizowane za pomocą dedykowanych magistral światłowodowych.

Separacja ruchu. Przełączniki muszą obsługiwać pełną separację logiczną ruchu poszczególnych systemów bezpieczeństwa oraz zarządzania za pomocą np. sieci wirtualnych.

6.8.1.1. Część pasywna

Dla obsługi systemów bezpieczeństwa należy zaprojektować i wykonać nową, odseparowaną od innych usług sieć LAN.

Wydzielona sieć LAN ma być zgodna z normami i dyrektywami: ISO 11801, EN 50173-1: 2011, EN 50173-2: 2008/ A1: 2011, EN 50174-1: 2010/A1: 2011, PN-EN 50310:2016, TIA/EIA-568-B.2, PN/E 08106/EN 60529, PN-EN-60297-3-100, PN-EN 60529:2003, EIA-310-B i dyrektywami 73/23/EWG oraz 93/68/AWG.

W przypadku sprzeczności zapisów obowiązuje norma przywołana wcześniej.

Zakres sieci LAN obejmuje:

- Dostawę komponentów infrastruktury pasywnej kategorii 6A ISO (nieekranowanej) wchodzących w skład systemów okablowania strukturalnego klasy EA: kable, panele krosowe, panele i elementy porządkujące, gniazda abonenckie, oraz kable krosowe.
- Dostawę komponentów infrastruktury pasywnej światłowodowej jednomodowej (zgodnej z normą ITU-T G.652.D lub G.657.A) wchodzących w skład systemów okablowania strukturalnego klasy OS2: kable światłowodowe, przełącznice światłowodowe (panele krosowe), panele i elementy porządkujące, gniazda i puszki abonenckie, a także kable krosowe (patchcordy) oraz pigtaile światłowodowe.
- posadowienie w budynku Manggha co najmniej dwóch szaf głównych (pomieszczenie techniczne),
- w obu budynkach zakłada się zlokalizowanie niezbędnej liczby szaf pośredniczących (preferowane szafki rack wiszące od 18 do 24U), umiejscowienie do ustalenia z Zamawiającym.

Wymagania dla szafek RACK 19” (stojące/wiszące)

- Wysokość montażowa: od 18U do 24U
- Poziom szczelności: min IP21
- Konstrukcja – rama skręcana lub spawana
- Nośność statyczna szafy stojącej 300kg, wiszącej 60 kg
- Głębokość 600mm lub 800mm (w zależności od proponowanego osprzętu)

Wymagania dla szaf przemysłowych RACK 19”

- Poziom szczelności: min. IP54;
- Minimalna grubość blach – 1 mm dla blach stalowych, 2 mm dla blach aluminiowych;
- Konstrukcja ramowa;
- Antykorozyjne wykończenie elementów wewnętrznych;
- Min. dwa komplety 19” profili montażowych 42U;
- Zamek min. 3-punktowy;
- Cokół z możliwością wyprowadzenia kabli z tyłu oraz z boków;
- Możliwość przełożenia drzwi prawo-lewo;
- Możliwość łączenia szaf w szereg;
- Wymagany kąt otwarcia drzwi min. 270°;
- Głębokość zgodna z przyjętymi urządzeniami, z uwzględnieniem zapasu na wtyki i okablowanie;
- Wszystkie elementy szafy muszą tworzyć ciągłość elektryczną;
- Szafa musi posiadać możliwość integracji z systemami klimatyzacji.

Wymagania techniczne i parametry transmisyjne kabla U/UTP kat. 6A

- Klasa okablowania E_A
- Kategoria 6A
- Kabel w pełni nieekranowany (U/UTP)
- Konstrukcja rdzenia: 4 skręcone pary żył miedzianych, odseparowane od siebie wewnętrznym separatorem krzyżowym (krzyżakiem) lub specjalnym oplotem izolacyjnym,

- Średnica żyły minimum 23 AWG (wsparcie PoE), kabel w pełni miedziany (niedopuszczalne jest stosowanie żył miedziowanych typu CCA/CCS)
- Pełna charakterystyka pracy w paśmie minimum do 500 MHz. Dopuszcza się oferowanie kabli o rozszerzonej charakterystyce pracy potwierdzonej przez producenta w karcie katalogowej (do 550, 600 lub 650 MHz)
- Zapewnienie pełnej obsługi aplikacji 10GBASE-T (Ethernet 10 Gb/s) na maksymalnym dystansie stałego łącza do 100 metrów.
- Klasa reakcji na ogień zgodnie z rozporządzeniem CPR: $B2_{CA}$
- Parametry transmisyjne kabla muszą być potwierdzone certyfikatem niezależnego laboratorium badawczego (np. GHMT, 3P, ETL, DELTA)

Wymagania techniczne dla modułu RJ45 Keystone kat. 6A (U/UTP)

- Moduł musi w pełni spełniać wymagania wydajnościowe dla toru transmisyjnego kategorii 6A oraz klasy E_A
- Moduł musi posiadać certyfikat niezależnego laboratorium badawczego (np. GHMT, 3P, ETL, DELTA)
- Moduł w pełni nieekranowany (U/UTP), wykonany z tworzywa sztucznego o wysokiej odporności mechanicznej i właściwościach samogasnących,
- Technologia zarabiania bez narzędziowa – montaż kabla na module musi odbywać się bez użycia dedykowanych narzędzi uderzeniowych

Wymagania techniczne i parametry transmisyjne kabla OS2 24J

- Klasa OS2
- Włókno jednomodowe typu G.652 lub G.657.A1/A2
- Kabel o konstrukcji uniwersalnej (wewnętrzno-zewnętrznej), całkowicie dielektryczny, odporny na promieniowanie UV oraz wyposażony w zabezpieczenie przeciwwilgociowe. Rdzeń kabla musi być otoczony elementami wzmacniającymi, zapewniającymi podstawową ochronę przed gryzoniami oraz odpowiednią wytrzymałość na rozciąganie podczas zaciągania.
- Pełna charakterystyka pracy w pasmach transmisyjnych dla fal o długości 1310 nm oraz 1550 nm. Maksymalne tłumienność jednostkowa nie może przekraczać 0,4 dB/km dla fali 1310 nm oraz 0,25 dB/km dla fali 1550 nm.
- Zapewnienie pełnej obsługi aplikacji 10GBASE-LR / ER (Ethernet 10 Gb/s), 40GBASE-LR4 (40 Gb/s) oraz 100GBASE-LR4 (100 Gb/s)

- Klasa reakcji na ogień zgodnie z rozporządzeniem CPR: $B2_{CA}$

Kable światłowodowe należy zakończyć w przełącznicach złączami LC duplex zgodnymi z:

- Normy transmisyjne: ISO/IEC 11801 oraz PN-EN 50173-1.
- Normy konstrukcyjne: IEC 61754-20 oraz TIA/EIA-604-10 (FOCIS-10)

Należy zakończyć wszystkie włókna z obu stron kabli.

Stosować skrzynki zapasu kabla (min. 20mb) na wejściu i wyjściu z budynków oraz w Pomieszczeniu Technicznym.

Wszystkie elementy toru transmisyjnego (kabel, panele krosowe, gniazda RJ45) muszą pochodzić od jednego producenta i wchodzić w skład jednego systemu strukturalnego objętego jednolitą, długoterminową gwarancją systemową producenta (minimum 25 lat). Niedopuszczalne jest stosowanie rozwiązań komponentowych od różnych dostawców.

Wymagania techniczne dla gniazd (obudów) modułu RJ45:

- Materiał: tworzywo sztuczne (ABS, poliwęglan) odporne na uderzenia, zarysowania oraz promieniowanie UV. Tworzywo musi spełniać wymogi samogaśnięcia.
- Moduły w obudowie gniazda muszą być zorientowane pod kątem (skośnie, od 30° do 45° w dół).
- Obudowy gniazd muszą być w pełni kompatybilne ze standardem montażowym Keystone i umożliwiać montaż minimum dwóch nieekranowanych modułów RJ45 kat. 6A bez użycia adapterów innych producentów
- Konstrukcja gniazda podtynkowego po montażu modułów Keystone musi pozostawiać w standardowej puszce instalacyjnej (Ø 60 mm) przestrzeń gwarantującą zachowanie minimalnego promienia gięcia dla nieekranowanego kabla kat. 6A
- Każdy otwór na moduł RJ45 w obudowie gniazda musi być wyposażony w automatyczną przesłonę przeciwpyłową na sprężynie (otwierającą się przy wsuwaniu wtyku i zamykającą po jego wyjęciu).
- Obudowa gniazda na płycie czołowej musi posiadać zintegrowane, przezroczyste okienko opisowe (z wymienną wkładką) umożliwiające jednoznaczne i trwałe oznakowanie.

Kolorystykę elementów sieci LAN i sieci elektrycznej dobrać i uzgodnić z zamawiającym na etapie PW

6.8.1.2. Cześć aktywna

Zaprojektować i zastosować przełączniki dostępowe z zapasem w zakresie:

- Przepustowości - 25%
- Mocy elektrycznej (PoE) – 20%

Dostosować moc pojedynczego portu do największego planowanego odbiornika.

Dobrać ilość przełączników z 10% zapasem ilości portów w stosunku do ilości zakończeń w danym PD.

Przełącznik (switch) PoE, minimum 16 x 100Mbps Eth + 1 x 1Gbps OPTO + 1 x 1Gbps Eth, rack.

W przypadku zastosowania przełączników 24-portowych sumaryczna ilość portów dla urządzeń końcowych nie może być mniejsza niż 216.

Przełącznik agregacyjny pracujący w na warstwie 3 (Layer 3 – Network) dobrać tak, aby posiadał zapas przepustowości min. 25%.

Każdy z przełączników dostępowych powinien być połączony bezpośrednio z przełącznikiem agregacyjnym bezpośrednim linkiem 1Gbps OPTO.

Połączenia 1Gbps i 10 Gbps dopuszczalne pod warunkiem, że urządzenia znajdują się w tej samej szafie

W przełączniku agregacyjnym powinien pozostać zapas co najmniej 2 portów 1 Gbps OPTO oraz 2 portów 10Gbps OPTO.

W przypadku przełącznika agregacyjnego dopuszcza się zastosowanie stosu przełączników zamiast pojedynczego pod warunkiem:

- przełączniki agregacyjne/rdzeniowe będą pracowały w architekturze stosu sprzętowego (Hardware Stacking).
- Połączenie urządzeń w stos nastąpi za pomocą dedykowanych, fabrycznych portów magistralowych (Stacking Ports) o przepustowości minimum 20 Gbps na jedno urządzenie (zalecane 40 Gbps lub więcej)
- Architektura stosu musi być zrealizowana w topologii pierścienia (Ring) w celu zapewnienia pełnej redundancji połączeń magistralowych. W przypadku uszkodzenia jednego z kabli stakujących lub awarii pojedynczego przełącznika, pozostałe urządzenia w stosie muszą kontynuować pracę bez utraty pakietów danych i bez konieczności restartu systemu.

6.8.1.3. Zmiany w instalacji elektrycznej, zasilanie

Zmiany w instalacji elektrycznej będą obejmowały przeprojektowanie i przebudowę całość zasilania dla poszczególnych rozproszonych elementów systemów bezpieczeństwa w tym istniejące rozdzielnie w pomieszczeniach nadzoru obu budynków.

Należy przestrzegać wskazanych czasów podtrzymania w wypadku zaniku zasilania sieciowego.

Każda z szaf i szafek LAN ma być wyposażona w UPS (UPS-y).

Czas podtrzymania szaf w przypadku zaniku zasilania sieciowego: 4 godziny pracy w warunkach pełnego obciążenia (uwzględnić pracę oświetlaczy).

Szczegóły należy uzgodnić z Zamawiającym i uwzględnić w PW na etapie projektowania.

6.8.2. Modernizacja i doposażenie Pomieszczenia nadzoru

Wytyczne do prac modernizacyjnych pomieszczenia wartowni:

1. Przed rozpoczęciem prac należy:

- zdemontować i przekazać do Zamawiającego system nagłośnienia, zabezpieczyć do przedłużenia kable systemu nagłośnienia,
- przenieść centralę systemu detekcji zalania,
- zabezpieczyć systemy, które po remoncie nadal mają być nadal eksploatowane,
- zdemontować zbędne elementy sieci zasilającej, LAN, okablowanie nieczynnych systemów.

2. Malowanie ścian pomieszczenia wartowni;
3. Wymiana kasetonów sufitowych;
4. Wymiana podłogi na płyty winylowe;
5. Wymiana: blatu roboczego z płyty meblowej w kształcie litery L (zaokrąglony do 30%) o wymiarach 410x610cm o szerokości 60 cm wysokość 75cm, kolor jasno szary;
6. Wymiana:15 szt.: szafki pod blatowe otwierane zamykane na klucz o wymiarach: 30cm(szer.)x52cm(gł.)x75cm(wys.), kolor jasno szary;
7. Wymiana: 4 szt.: szafki pod blatowe szufladowe (4 szuflady) zamykane na klucz o wymiarach 40cm(szer.)x52cm(gł.)x75cm(wys.) kolor jasno szary;
8. Montaż 2 szt. szafka wisząca metalowa malowana proszkowo na klucze z 200 zawieszkami, szafka zamykana na zamek mechaniczny o podwyższonej klasie bezpieczeństwa, materiał: stalowa malowana proszkowo, kolor szary;

9. 2 szt. fotele przeznaczone do intensywnej eksploatacji w systemie 24 godziny na dobę, 7 dni w tygodniu (365/7/24), dedykowane do stanowisk wartowniczych, monitoringu, ochrony, dyspozytorni lub centrów nadzoru;

- Nośność fotela: minimum 150 kg.
- gwarancja producenta minimum 36 miesięcy, obejmująca użytkowanie w systemie wielozmianowym 365/7/24
- Stabilna podstawa pięcioramienna wykonana z metalu lub innego materiału o porównywalnej wytrzymałości.
- Mechanizm synchroniczny lub równoważny, umożliwiający regulację kąta nachylenia oparcia i siedziska oraz blokadę w kilku pozycjach.
- Regulacja wysokości siedziska za pomocą podnośnika gazowego przystosowanego do pracy o zwiększonej intensywności.
- Ergonomicznie wyprofilowane oparcie zapewniające odpowiednie podparcie odcinka lędźwiowego kręgosłupa.
- Regulowane podłokietniki (minimum regulacja wysokości), wykonane z trwałych materiałów odpornych na uszkodzenia.
- Siedzisko i oparcie wykonane z materiałów o wysokiej odporności na ścieranie i rozdarcia, przeznaczonych do użytkowania wielozmianowego.
- Fotel powinien spełniać wymagania ergonomiczne określone w obowiązujących normach dotyczących wyposażenia stanowisk pracy oraz posiadać deklarację zgodności lub równoważny dokument producenta.

10. Stół kwadratowy o wymiarach min. 75x75cm wysokość 80cm z płyty meblowej
11. 2 szt. krzesła tapicerowane
12. 2 szt. Półka przeznaczona do montażu ściennego z płyty meblowej laminowanej, metalu lub materiału o równoważnej trwałości i odporności na użytkowanie o wymiarach: 150cm głębokość nie większa niż 20 cm (półka wąska).
13. 1 półka ścienna o wymiarach około 60 cm szerokości oraz 40 cm głębokości, wykonana z trwałych materiałów zapewniających nośność minimum 20 kg. Konstrukcja powinna umożliwiać stabilny i bezpieczny montaż do ściany wraz z kompletem elementów mocujących.
14. Płyty ścienne zabezpieczające powierzchnię ścian przed uszkodzeniami mechanicznymi powodowanymi przez użytkowanie foteli biurowych oraz elementów wyposażenia ruchomego o wymiarach

15. Siedzisko tapicerowane z oparciem, o wymiarach nie mniejszych niż 200 cm długości i 60 cm głębokości, przeznaczone do intensywnego użytkowania. Wyposażone w otwierane siedziska z funkcją schowka, Konstrukcja stabilna, a tapicerka wykonana z materiału odpornego na ścieranie i łatwego w utrzymaniu czystości.
16. 15 szt. Szafki ubraniowe 2-drzwiowe 2Kx1D (2 kolumny x 1 drzwiczki w kolumnie)
17. - wymiary całkowite: 180x60x49cm (WxSxG) przeznaczone dla każdego pracownika osobno, wykonane z trwałej stali, wyposażone w indywidualnie zamykane komory do bezpiecznego przechowywania odzieży i rzeczy osobistych.
18. 1 szt. Szafa metalowa na dokumenty, dwudrzwiowa o wymiarach 180x80x40cm, 3 półki, malowana proszkowo w kolorze szarym zamykana na klucz.
19. 1 szt. Szafa metalowa, dwudrzwiowa o wymiarach nie mniejszych niż 180x80x50cm, 3 półki, malowana proszkowo w kolorze szarym zamykana na klucz.
20. Zestaw 6 szt. profesjonalnych radiotelefonów przenośnych cyfrowo-analogowych przeznaczonych do ochrony obiektów, zapewniających niezawodną łączność głosową w trybie pracy grupowej. Urządzenia o podwyższonej odporności mechanicznej i środowiskowej (min. IP i standardy równoważne MIL-STD), przystosowane do pracy ciągłej, z akumulatorami o zwiększonej pojemności. W zestawie 4 ładowarki biurkowe sieciowe umożliwiające jednoczesne ładowanie urządzeń.
21. Zestaw 2 szt. profesjonalnych latarek ręcznych o wysokiej mocy światła, przeznaczonych do pracy wartowniczej i ochrony obiektów, wykonanych z trwałej obudowy o podwyższonej odporności (min. IP), przystosowanych do intensywnej eksploatacji. W zestawie ładowarki oraz akumulatory o dużej pojemności zapewniające długi czas pracy.

6.8.3. Pomieszczenie techniczne

Zadaniem Wykonawcy będzie wydzielenie fragmentu garażu na potrzeby pomieszczenia technicznego (PT), w którym będą zlokalizowane szafy teleinformatyczne CCTV oraz centrale i serwery systemów bezpieczeństwa.

Zamawiający wymaga szaf o podwyższonych parametrach klimatycznych i mechanicznych (szafy przemysłowe) umieszczonych za odpowiednimi przegrodami uniemożliwiającymi dostęp i przypadkowe uszkodzenie. Wymagane objęcie obszaru nadzorem systemów bezpieczeństwa, zapewnienie oświetlenia i dostęp do zasilania 230V (gniazda serwisowe).

Należy przewidzieć/rozważyć klimatyzację szaf lub wydzielonego pomieszczenia

6.9. SYSTEMY I URZĄDZENIA DODATKOWE

6.9.1. System liczenia osób

Dla potrzeby zapewnienia bezpieczeństwa (monitoringu ilości osób odwiedzających) planuje się wprowadzić system zliczania osób w oparciu o rozbudowę systemy CCTV o stosowną funkcjonalność lub dostawę i wdrożenie niezależnego systemu.

Miejsca zliczania:

a) Wyjście główne Muzeum Manggha
b) Wejście zewnętrzne do Galerii z Holu (Manggha)
c) Wejście do Galerii wewnętrznej (Manggha)
d) Kładka od stron Bulwarów wiślanych
e) Wejście głownie do Galerii Europa – Daleki Wschód
f) Galeria I (GE-DW)
g) Galeria II we.1 (GE-DW)
h) Galeria II we.2 (GE-DW)

Kamera stałopozycyjna stereoskopowa z dwoma obiektywami do zliczania osób wraz z uchwytem sufitowym lub ściennym powinna być przeznaczona do pracy w systemie dozoru wizyjnego jako specjalizowana sieciowa kamera dual-lens do zliczania osób, przeznaczona do montażu nad wejściami, wyjściami i przejściami komunikacyjnymi. Urządzenie powinno realizować precyzyjne liczenie ruchu osobowego w obu kierunkach, filtrowanie obiektów według wysokości oraz raportowanie statystyczne do systemu nadrzędnego, przy zachowaniu funkcji standardowej kamery IP.

Parametr	Wymagania minimalne
Budowa	dedykowana obudowa dwuobiektywowa
Przetwornik	Progressice scan CMOS 1/2,7” lub 1/2.8”
Czułość (oświetlenie)	Praca w kolorze dzień/noc
Kompresja	co najmniej H.264 i H.265
Analiza i funkcje dedykowane	zliczanie osób w obu kierunkach ruchu filtrowania obiektów według wysokości detekcja ruchu, sabotaż wideo, utrata połączenia, przesyłanie statystyk w czasie rzeczywistym oraz cyklicznie.
Zapis lokalny	karta pamięci
Wejście alarmowe	tak
Wyjście alarmowe	tak

Obudowa	IP67
Warunki pracy	-30 do +60 st. C, wilgotność do 95% bez kondensacji
Doświetlenie	IR do 5m
Zasilanie	PoE
Gwarancja producenta	5 lat lub doubezpieczenie gwarancji do 5 lat

Wymagania w zakresie oprogramowanie do systemu zliczania osób:

- Konfiguracji kierunku wejścia i wyjścia dla zasobów w grupie zliczania osób.
- Ustawiania czasu regularnego czyszczenia wszystkich danych dotyczących zliczania osób.
- Włączania funkcji maksymalnej pojemności i skonfiguruj maksymalną liczbę osób, które mogą wejść.
- Konfiguracji alarmu przekroczenia progu liczby osób oraz prealarm przekroczenia progu liczby osób dla wybranej grupy zliczania osób.
- Przeprowadzenie monitorowanie w czasie rzeczywistym wybranych grup zliczania osób. Wyświetlania „na żywo” podglądu wielu zliczanych grup.
- Wyświetlania liczby osób pozostałych w grupie zliczania osób oraz liczbę osób, które mogą wejść.
- Ręcznej korekty poszczególnych grup
- Wyświetlania wyników analizy według kamer lub grup zliczania.
- Tworzenia rankingu grup zasobów i kamer według liczby osób wchodzących i wychodzących.
- Ustawiania kierunku jako „Wejście”, „Wyjście” lub „Wejście i wyjście” na potrzeby analizy statystycznej.
- Wyświetlania liczby osób, które weszły, osób, które przeszły obok, oraz wskaźnika odwiedzin.
- Przeglądania następujących typów raportów: raport dzienny, raport tygodniowy, raport miesięczny, raport roczny oraz raport dla niestandardowego przedziału czasowego.
- Wyświetlania porównania statystyk również w niestandardowych okresach,
- Wyświetlania szczytowej liczby osób według różnych kryteriów.
- Eksportowania raportu.

6.9.2. System videodomofonowy

Dla poprawy bezpiecznej komunikacji należy zastosować system videodomofonowy w następujących lokalizacjach:

a) wjazd do garażu Manggha (wraz z otwieraniem drzwi obok bramy)
b) wjazd do garażu GE-DW strona lewa
c) wjazd do garażu GE-DW strona lewa
d) brama wjazdowa od ulicy Sandomierskiej
e) słupek przy szlabanie od ulicy Sandomierskiej (wraz z otwieraniem szlabanu)
f) furtka od ulicy Konopnickiej
g) drzwi A9

Zakłada się integracje systemu videodomofonowego z systemem CCTV.
Minimalny zakres integracji to wywołanie na ekran bieżący kamery pokazującej aktywowany domofon.
Stacje monitorowe (odbiorcze) po jednej w pomieszczeniach ochrony w obu budynkach.
System ma umożliwiać otwieranie przejść skojarzonych z videodomofonami.
Wymagania:

Moduł główny stacji bramowej

- kamera min. 2 MP typu Fisheye z oświetlaczem,
- mikrofon i głośnik,
- 2 przekaźniki do sterowania zamkami,
- 2 wejścia alarmowe
- Ramka maskująca do montażu podtynkowego

Stacja wewnętrzna

- ekranem dotykowym min. 7” (1024×600),
- mikrofon, głośnik
- Co najmniej 8 wejść, slot SD lub microSD
- Możliwość montażu podtynkowego i natynkowego.

Zasilanie z przełącznika PoE zgodnie ze standardem IEEE 802.3af. W przypadku odcinków powyżej 100 m możliwość trybu Extend.

6.9.3. Szlaban wjazdowy

Dla uporządkowania ruchu samochodowego od strony ulicy Sandomierskiej przewiduje się umiejscowienie szlabanu wjazdowo- wyjazdowego.

Podstawowe zasady:

a) Pierwszeństwo mają pojazdy wyjeżdzające (stosowne oznakowanie i sygnalizacja świetlna – światło czerwone/zielone)

b) Wjazd na podstawie

- Numeru rejestracyjnego (kamera odczytująca rejestrację na wysokości min. 1,5m od podłoża)
- Czytnika SKD (karta i/lub kod QR)
- Decyzją ochrony (na wywołanie ze stacji videodomofonowej)

c) Wyjazd bez ograniczeń (kamera i pętla indukcyjna)

Dobór kamer odczytujących numery rejestracyjne na etapie PW

Wytyczne:

Obudowa w kolorze szarym

Zasilanie 230V AC

System wyłamania ramienia na wypadek staranowania

System wysprzęglenia mechanicznego zabezpieczony kluczem

Długość robocza ramienia min 5,0 mb

Ramię wyposażone w pasy LED (kolor czerwony)

Żywotność min. 3mln cykli

Czas otwarcia do 6 sek.

sygnalizacja świetlna – światło czerwone/zielone

Możliwość podłączenia pętli indukcyjnej

Wykonanie fundamentu i pętli indukcyjnej z rozebraniem i odtworzeniem istniejącej kostki granitowej.

6.9.4. Dodatkowa kamera przy Pawilonie herbacianym

W obszarze dziedzińca Pawilonu herbacianego należy zainstalować kamerę zewnętrzną. Zaprojektować i doprowadzić stosowne okablowanie. Obowiązują wszystkie warunki zgodnie z rozdziałem 6.5.

6.9.5. Firewall

Należy dostarczyć urządzenie o wyspecyfikowanych poniżej parametrach.

Architektura urządzenia, obudowa, interfejsy

1) Urządzenie musi stanowić dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań typu serwerowego bazującego na ogólnodostępnych podzespołach PC ogólnego przeznaczenia.
2) Urządzenie musi pełnić rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall).
3) Urządzenie musi być wyposażone w 8 portów miedzianych Gigabit Ethernet oraz minimum 2 porty 10Gigabit Ethernet definiowane przy pomocy wkładek/twinax.
4) Urządzenie musi obsługiwać interfejsy VLAN (802.1Q) na interfejsach fizycznych.
5) Urządzenie musi być wyposażone w dedykowany port konsoli/port USB co najmniej 3.0 oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band.
6) Urządzenie musi być wyposażone w dodatkowy port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu uaktualnienia oprogramowania urządzenia,
7) Urządzenie musi mieć możliwość montażu w szafie rack 19” oraz posiadać w zestawie dołączone niezbędne elementy montażowe. Jeśli urządzenie nie jest przystosowane do montażu w szafie rack, należy dostarczyć dedykowany uchwyt od producenta sprzętu.
8) Wysokość urządzenia typu rack nie może przekraczać rozmiaru 1U.

Parametry wydajnościowe

9) Urządzenie musi zapewniać przepustowość nie mniejszą niż 8 Gb/s dla funkcji NGFW obejmujących kontrolę aplikacji oraz 8 Gb/s dla funkcji NGFW obejmujących kontrolę aplikacji i IPS. Parametry muszą być potwierdzone w dokumentacji producenta.
10) Maksymalna liczba sesji (z kontrolą aplikacji) nie może być mniejsza niż 290 000 z możliwością zestawiania co najmniej 50 000 nowych połączeń na sekundę.
11) Urządzenie musi zapewniać wsparcie dla VPN IPSec na poziomie co najmniej 9 Gb/s.

Funkcjonalność urządzenia

12) Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
13) Urządzenie musi mieć możliwość uruchomienia w trybie firewalla L3, jak i w trybie transparentnym.
14) Urządzenie musi obsługiwać routing statyczny i dynamiczny (RIP, OSPF, BGP).

15) Urządzenie musi posiadać możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory.
16) Urządzenie musi obsługiwać funkcjonalność Network Address Translation (NAT oraz PAT).
17) Urządzenie musi zapewniać mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby.
18) Urządzenie musi zapewniać funkcjonalności NGFW obejmujące identyfikację i kontrolę aplikacji, IPS, filtrowanie URL, ochronę przed złośliwym oprogramowaniem oraz integrację z usługami reputacyjnymi.
19) System musi umożliwiać definiowanie polityk bezpieczeństwa z wykorzystaniem tożsamości użytkownika, informacji o urządzeniu końcowym, aplikacji, kategorii URL oraz informacji o zagrożeniach i reputacji.
20) System musi posiadać otwarte API dla współpracy z systemami zewnętrznymi w tym co najmniej z systemami SIEM (Security Information and Event Management).
21) Urządzenie musi umożliwiać konfiguracją IPsec IKEv2 oraz SSL VPN Remote Access z możliwością uwierzytelniania w serwerze RADIUS/LDAP/AD. W ramach połączenia VPN System musi umożliwić stworzenie, kilku różnych grup dostępowych do sieci. System musi posiadać możliwość definiowania powitalnego banneru dla połączenia VPN RA oraz możliwości tunelowania całego ruchu jak i również tzw. „split tunelingu" (funkcja ta musi mieć możliwość konfiguracji per grupa VPN RA).
22) Moduł wykrywania aplikacji (AVC) musi zapewniać:
    a) Możliwość identyfikacji i kontroli aplikacji sieciowych z wykorzystaniem aktualizowanej przez producenta bazy sygnatur aplikacji.
    b) możliwość tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług,
    c) wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji,
    d) Możliwość definiowania własnych sygnatur lub reguł identyfikacji aplikacji i wykorzystania ich w politykach bezpieczeństwa.
23) Moduł IPS (Intrusion Prevention System) musi zapewniać:
    a) możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez moduł),
    b) możliwość pracy w trybie pasywnym (IDS),

c) możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym:
   i. złośliwe oprogramowanie,
   ii. skanowanie sieci,
   iii. ataki na usługę VoIP,
   iv. próby przepełnienia bufora,
   v. ataki na aplikacje P2P,
   vi. zagrożenia dnia zerowego, itp.
d) możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna),
e) wiele sposobów wykrywania zagrożeń w tym:
   i. sygnatury ataków opartych na exploitach,
   ii. reguły oparte na zagrożeniach,
   iii. mechanizm wykrywania anomalii w protokołach,
   iv. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego,
f) możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakresu protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu,
g) mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives),
h) możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń,
i) wiele możliwości reakcji na zdarzenia w tym takie, jak:
   i. tylko monitorowanie,
   ii. blokowanie ruchu zawierającego zagrożenia,
   iii. zastąpienie zawartości pakietów,
   iv. zapisywanie pakietów,
j) możliwość detekcji ataków i zagrożeń opartych na protokole IPv6,
k) możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o:
   i. systemach operacyjnych,
   ii. serwisach,
   iii. otwartych portach, aplikacjach,

iv. zagrożeniach,

l) możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych,

m) możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.,

n) możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji,

o) możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego,

p) mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne,

q) możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie,

r) System IPS musi wykorzystywać aktualizowane sygnatury zagrożeń dostarczane przez producenta oraz umożliwiać tworzenie własnych reguł detekcji.

s) możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS,

t) Rozwiązanie musi umożliwiać identyfikację hostów potencjalnie skompromitowanych na podstawie analizy ruchu, zdarzeń bezpieczeństwa lub informacji reputacyjnych.

u) Rozwiązanie powinno wspierać administratora w optymalizacji polityk bezpieczeństwa poprzez rekomendacje lub mechanizmy automatyzacji.

24) Moduł filtracji URL musi zapewniać:

a) kategoryzację stron – w co najmniej 70 kategoriach,

b) bazę URL o wielkości nie mniejszej niż 250 mln URL,

25) Urządzenie musi zapewniać możliwość wykrywania i śledzenia transferu co najmniej następujących kategorii plików w ruchu sieciowym:

a) pliki systemowe,

b) pliki graficzne,

c) pliki PDF,

d) pliki wykonywalne,

e) pliki multimedialne,

f) pliki pakietu Office,

g) pliki skompresowane.

26) Urządzenie musi posiadać możliwość monitorowania jak i kontrolowania transferu plików w co najmniej następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download.

27) Rozwiązanie musi zapewniać ochronę przed złośliwym oprogramowaniem wykorzystując co najmniej dwa mechanizmy spośród: analiza sygnaturowa, analiza reputacyjna, analiza behawioralna, sandbox lokalny lub chmurowy, analiza statyczna plików.

28) Urządzenie musi zapewniać możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach:

a) pliki wolne od złośliwego kodu,

b) pliki zawierające złośliwy kod,

c) pliki podejrzane,

d) pliki o własnej, zdefiniowanej przez użytkownika kategorii.

29) Podsystem wykrywania oprogramowania złośliwego musi zawierać narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna).

Pozostałe wymagania

30) Urządzenie musi być objęte **co najmniej 36-miesięcznym** serwisem świadczonym bezpośrednio przez producenta w reżimie 8x5xNBD uprawniającym do:

a) wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia,

b) wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia,

c) aktualizacji oprogramowania urządzenia,

d) dostępu do aktualizacji sygnatur IPS, mechanizmów filtrowania webowego i aktualizacji filtrów antymalware'owych.

31) W zakres dostawy wchodzą także licencje dla połączeń VPN zdalnego dostępu:

a) co najmniej **25 szt. licencji** pozwalających na autoryzację komputerów/telefonów

b) wsparcie na licencję również powinno być świadczone w okresie **co najmniej 36 miesięcy**.

System zarządzania oraz składowania logów dla firewall

1. Wraz z urządzeniem zostanie dostarczona dedykowana platforma zarządzająca, mogąca mieć formę oprogramowania dla maszyny wirtualnej i spełniającą następujące wymagania:

a) umożliwia agregację wszystkich zdarzeń IDS/IPS oraz centralne monitorowanie i analizę działającą w czasie rzeczywistym
b) jest dostępna przez interfejs WEB, bez potrzeby instalacji dodatkowego oprogramowania klienckiego
c) zapewnia interfejs, który może zostać dostosowany do wymagań użytkownika, w szczególności administrator posiada możliwość definiowania widoków (dashboard), które spełniają jego indywidualne kryteria
d) ma możliwość konfigurowania limitu powtórzeń danego zdarzenia w określonym czasie zanim zostanie wygenerowany alarm
e) ma możliwość automatycznej konfiguracji pobierania zestawów sygnatur na najnowsze zagrożenia i podatności. Ma możliwość informowania o zmianach w pakietach z nowymi sygnaturami/regułami
f) zapewnia zarządzanie oparte o role, gdzie każdy z użytkowników systemu może mieć różne widoki interfejsu oraz różne możliwości konfiguracyjne w zależności od roli, do której został przypisany
g) zapewnia funkcjonalność typu harmonogram zadań umożliwiającą automatyczne uruchamianie rutynowych czynności administracyjnych takich jak kopie zapasowe, uaktualnienia, tworzenie raportów, stosowanie polityk bezpieczeństwa oraz automatyczne dostrajanie polityki IPS
h) zapewnia grupowanie urządzeń i polityk w celu ułatwienia zarządzania konfiguracją
i) ma możliwość przechowywania atrybutów hostów definiowanych przez użytkownika takich jak jego krytyczność tak, aby ułatwić czynności monitorowania sieci
j) daje możliwość znaczącej redukcji nakładów operacyjnych oraz przyśpieszenie reakcji na zagrożenia poprzez automatyczną prioretyzację alarmów w oparciu o korelację zagrożeń ze skutecznością ataku na docelowego hosta
k) ma możliwość dynamicznego dostrajania systemu IDS/IPS przy zachowaniu minimalnej interwencji administratora
l) zapewnia możliwość automatycznego uaktualniania reguł publikowanych przez producenta, automatyczną dystrybucję i stosowanie reguł na urządzeniach IPS
m) ma możliwość wykonywania i odtwarzania kopi zapasowych zarówno urządzeń bezpieczeństwa, jak i platformy zarządzającej
n) zapewnia funkcjonalność pozwalającą na zarządzanie cyklem życia incydentu, od początkowego powiadomienia, poprzez odpowiedzi, aż do rozwiązania

o) zapewnia możliwość wglądu w reguły, które wygenerowały dany incydent oraz powiązanego z nim pakietu

p) zapewnia możliwość synchronizowania czasu pomiędzy wszystkimi komponentami przez protokół NTP

q) zapewnia możliwość logowania wszystkich czynności wykonywanych przez administratora zarówno lokalnie jak i na zdalnym serwerze

r) zapewnia szerokie możliwości generowania raportów włączając w to raporty predefiniowane oraz możliwość kompletnego dostosowania raportów do wymagań użytkownika

s) zapewnia informowanie o zagrożeniach poprzez

a. wysłanie e-maila,

b. wysłanie trap SNMP,

c. przesłanie informacji do serwera Syslog,

d. uruchomienie skryptu użytkownika

e. wysłanie informacji do jednego lub kilku rozwiązań typu SIEM poprzez zaszyfrowane połączenie

t) posiada zaawansowany system przeszukiwania logów pozwalający na przeprowadzanie analizy

a. aktualnego stanu danego urządzenia,

b. podglądu historii dostępnych zasobów,

c. możliwość eliminacji powtarzających się alarmów (tzw. Black Listing)

u) ma możliwość ustanawiania i wymuszania polityki zgodności jak i alarmowania w przypadku jej naruszeń w czasie rzeczywistym

v) ma możliwość przypisywania następujących parametrów w polityce kontroli dostępu dla danych interfejsów, podsieci, vlanów i użytkowników:

a. dozwolone porty i protokoły

b. dozwolone aplikacje według różnych kategorii

c. dozwolone kategorie stron internetowych (URL filtering)

d. dedykowaną politykę wykrywania zagrożeń IPS dla każdej z reguł zapory ogniowej

e. sposób traktowania wyspecyfikowanego ruchu w danej regule: przepuszczanie bez analizy, analiza, blokowanie ciche, blokowanie z resetowaniem sesji, blokowanie interaktywne

w) w ramach funkcji kategoryzacji zapytań HTTP (URL filtering) rozwiązanie ma możliwość interaktywnego blokowania z resetowaniem zapytań. W ramach tej funkcji jest zapewniona

możliwość zdefiniowania własnej strony internetowej ostrzegającej o naruszeniu polityki kontroli dostępu i zrzuceniu zablokowanej próby połączenia
x) pozwala na łatwą nawigację pomiędzy obiektami. Pozwala podejrzeć, w którym innym obiekcie jest on zagnieżdżony lub w której polityce jest użyty
y) posiada narzędzie do monitorowania połączeń, które zostały sklasyfikowane do odpowiedniej reguły („hit count"). Narzędzie pozwala na monitorowanie jak dużo połączeń zachodzi dla konkretnych reguł w określonej jednostce czasu oraz pozwala na szybkie wyszukanie reguł niepotrzebnych, do których przez zadany okres nie trafił żaden ruch.
z) pozwala na wysłanie na sensor tylko wybranych elementów modyfikowanej konfiguracji
aa) określa przewidywany czas implementacji polityki na sensor przed implementacją
bb) pozwala przed rekonfiguracją na przegląd implementowanych zmian w porównaniu do aktualnych ustawień urządzenia zarządzanego
2. Zamawiający dopuszcza dostarczenie systemu zarządzania i raportowania producenta oferowanego rozwiązania lub rozwiązania równoważnego, pod warunkiem spełnienia wszystkich wymaganych funkcji zarządzania, monitorowania, raportowania i składowania logów określonych w OPZ. Dopuszcza się realizację wymaganych funkcji przez jeden lub więcej komponentów programowych producenta.

6.9.6. UPS

Dostawa, podłączenie i uruchomienie urządzenia UPS podtrzymującego zasilanie części budynku Manggha (obwody TOA1 i TY – do weryfikacji na etapie PW).
Podstawowe parametry i wymagania:

- wykonanie projektu (PW) podtrzymania zasilania dla części muzealnej i konferencyjnej bez systemów wentylacji.
- dostawa zasilacza UPS 40kVA/40kW, 3faz
- zestaw akumulatorów na 12-15min minut autonomicznej pracy przy obciążeniu 40kW, akumulatory umieszczone na stelażu bateryjnym wyposażonym w rozłącznik bezpiecznikowy;
- zabudowa tablicy bezpiecznikowej/sekcji dla rezerwowanych obwodów.
- wykonanie pomiarów jakości energii elektrycznej po montażu.
- wykonanie pomiarów i prób powykonawczych,
- Warunki pracy: -5 do +50 st. C

7. UWAGI KOŃCOWE

Etap realizacji (Wykonawca)

- Niniejsza koncepcja nie stanowi Projektu, zagadnienia w niej pominięte nie stanowią podstawy do ich wykluczenia.
- Na etapie przetargu zgłosić i wyjaśnić z Zamawiającym wszelkie wątpliwości i ewentualne optymalizacje.
- Na etapie Projektowania (PW) przedstawić rozwiązania wariantowe.
- Całość prac należy przeprowadzić zgodnie zobowiązującymi normami i przepisami, w tym przepisami p-poż i BHP.
- Należy uzgodnić z Zamawiającym Projekt Wykonawczy (PW), harmonogram i kolejność prac oraz sposób i terminy wpięcia urządzeń do zasilania.
- Należy uzgodnić integrację z systemem sygnalizacji pożaru (SSP).

Etap eksploatacji (Użytkownik)

- Przeprowadzić weryfikację elementów infrastruktury współpracującej z systemami bezpieczeństwa i przywrócić je do właściwego stanu technicznego (drzwi, okna, fragmenty murów i elewacji, kable zasilające i wspólne trasy kablowe)
- Należy dopilnować szkoleń pracowników z nowopowstałych systemów łącznie w weryfikacją stopnia opanowania i biegłości posługiwania się.
- Zaleca się codzienną kontrolę działania systemów
- W przypadku zmian wystroju (re-aranżacji), przestrzeni wystawienniczej należy zweryfikować prawidłowość ustawienia i montażu elementów projektowanych systemów w tym kamer CCTV, czujek ruchu, itp.
- Zapewnić stałą obsługę konserwacyjną i przeglądy systemów.
- Użytkować system zgodnie z zaleceniami producenta ujętymi w instrukcji użytkowania i wskazówkami przekazanymi podczas szkolenia po zainstalowaniu systemu.
- Zgłaszać i usuwać wszelkie zauważone usterki.
- Należy prowadzić Rejestr Obsługi Systemów.