

Przedsięwzięcie pt. "Rewitalizacja kompleksu przy Narutowicza 60 w Łodzi, z przeznaczeniem na Centrum Inicjatyw Prozdrowotnych i Społecznych" dofinansowany z Europejskiego Funduszu Rozwoju Regionalnego w ramach programu regionalnego Fundusze Europejskie dla Łódzkiego 2021-2027".

Umowa nr FELD.05.02-IZ.00-0023/25 -00 zawarta w dn. 21.11.2025 r.

Oznaczenie sprawy: ZP/13/2026

Załącznik nr 2.9 do SWZ

BEZPIECZEŃSTWO OBIEKTU

1. WSTĘP

1.1. Cel dokumentu

Niniejszy dokument określa wytyczne w zakresie wyposażenia obiektu muzealnego w systemy bezpieczeństwa mające na celu:

- ochronę zwiedzających i pracowników obiektu,
- ochronę eksponatów i zbiorów muzealnych,
- ochronę infrastruktury i mienia obiektu,
- zapewnienie kontroli dostępu do pomieszczeń,
- monitorowanie i rejestrowanie zdarzeń bezpieczeństwa.

Zakłada się prowadzenie ruchu zwiedzających w trybie ekspozycji stałych i czasowych, zajęć edukacyjnych oraz wydarzeń specjalnych (warsztaty, spotkania, wernisaże), z okresowym zwiększeniem natężenia ruchu w godzinach szczytu i w trakcie imprez.

Wytyczne zawarte w niniejszym dokumencie stanowią wymagania minimalne dla bezpieczeństwa obiektu i powinny być uwzględnione w projektach wyposażenia muzeum, zgodnie z obowiązującymi przepisami prawa dotyczącymi ochrony bezpieczeństwa. Dokument jest kompatybilny ze „Standardami w zakresie wyposażenia IT i TLT w budynkach UM w Łodzi” i należy go stosować łącznie z tymi Standardami, które stanowią odrębny załącznik określający szczegółowe wymagania techniczne systemów bezpieczeństwa.

1.2. Zakres zastosowania

Niniejsze wytyczne dotyczą wszystkich pomieszczeń muzeum, w tym:

- pomieszczeń ekspozycyjnych,
- warsztatów edukacyjnych,
- pomieszczeń magazynowych i przechowalnie zbiorów,
- pomieszczeń biurowych i administracyjnych,
- ciągów komunikacyjnych (korytarze, schody, wyjścia ewakuacyjne),
- pomieszczeń technicznych i serwerowni,
- stref wejścia do obiektu.

2. OGÓLNE ZASADY BEZPIECZEŃSTWA

2.1. Wielowarstwowe podejście do bezpieczeństwa

System bezpieczeństwa obiektu muzealnego powinien opierać się na wielowarstwowym modelu ochrony obejmującym:

- Ochronę fizyczną (bariera/y, zamki, systemy metryki dostępu),
- Zabezpieczenia techniczne (systemy alarmowe, telewizja dozorowa, czujniki),
- Zasoby ludzkie (pracownicy ochrony, personel muzeum),
- Procedury operacyjne (protokoły alarmowe, plan ewakuacji, przeszkolenie).

2.2. Integracja systemów

Wszystkie systemy bezpieczeństwa powinny być zintegrowane w jedną spójną architekturę z możliwością:

- Centralnego monitorowania i sterowania,
- Raportowania i archiwizacji zdarzeń,
- Współpracy z Centrum Bezpieczeństwa (stanowiskiem dozoru),
- Automatycznego wyzwalania procedur alarmowych.

2.3. Normy i regulacje

Projektowanie i instalacja systemów bezpieczeństwa powinna być zgodna z:

- Ustawą o ochronie bezpieczeństwa osób i mienia,
- Ustawą o ochronie przeciwpożarowej,
- Polskimi Normami (PN) dotyczącymi systemów alarmowych,
- Wytycznymi Uniwersytetu Medycznego w Łodzi w zakresie systemów IT i teletechnicznych,
- Standardami międzynarodowymi (EN, ISO) w zakresie bezpieczeństwa fizycznego.

3. SYSTEM TELEWIZJI DOZOROWEJ (CCTV)

3.1. Standard systemu

System powinien być zainstalowany zgodnie ze Standardami IT Uniwersytetu Medycznego w Łodzi, Sekcja 2.1 – System telewizji dozorowej.

System IP z kamerami o minimalnej liczbie Mpix nie mniejszej niż 8 Mpix. Rejestrator cyfrowy umożliwiający zapis strumienia wideo ze wszystkich podłączonych kamer z najwyższą możliwą rozdzielczością oraz liczbą klatek nie mniejszą niż 12 kl/sek. dla jednej kamery i czasie rejestracji nie mniejszym niż 30 dni w zapisie ciągłym.

3.2. Rozmieszczenie kamer

Kamery telewizji dozorowej powinny być zainstalowane w następujących lokalizacjach:

Obowiązkowe:

- Każde pomieszczenie ekspozycyjne (pokoje wystawiennicze),
- Każdy warsztat edukacyjny,
- Główne wejście do obiektu,
- Wejście boczne (ulica Narutowicza),
- Korytarze i ciągi komunikacyjne,
- Wejście do stanowiska ochrony (stróżówka),
- Pomieszczenia magazynowe i przechowalnie zbiorów.

- Pomieszczenie IT
- Podejścia do wejść (przed i za bramą wejściową),
- Strefy postoju samochodów (parking),
- Zewnętrzne części obiektu (fasada, wyjścia ewakuacyjne)
- Teren zewnętrzny w tym parkingi i teren parku kieszonkowego.

3.3. Parametry techniczne kamer

- **Typ:**
 - Wewnętrzne: kopułkowe (dome) lub kulowe (turret) z funkcją noktowizji (IR),
 - Zewnętrzne: bullet z funkcją noktowizji IR, wandaloodporne
- **Wszystkie kamery z możliwością zdalnej regulacji powiększenia i ostrości: Kamera zmiennogoniskowa motozoom z regulowanym kątem widzenia**
- **Kąt widzenia:** Dobierany w zależności od lokalizacji, minimum 110°,
- **Oświetlenie minimalne:** Minimum 0,1 lux w nocy (z IR),
- **Matryca:** Czujnik CMOS, rozmiar co najmniej 1/1.8"

3.4. Okablowanie i infrastruktura

Infrastruktura sieciowa powinna być realizowana zgodnie ze Standardami IT Uniwersytetu Medycznego w Łodzi, Sekcja 2.1 – System telewizji dozorowej.

3.5. Stanowisko dozоровe

Stanowisko ochrony na parterze w stróżówce powinno być wyposażone w:

- Komputer stacjonarny o wysokiej wydajności,
- Główny monitor (minimum 50") – stały podgląd wszystkich kamer,
- Monitor pomocniczy (minimum 27") – automatyczna zmiana na kamerę z wykrytą anomalią,
- Oprogramowanie do zarządzania systemem CCTV,
- Urządzenie drukujące do dokumentacji,
- Niezawodne zasilanie (UPS).

3.6. Funkcjonalność zaawansowana

System powinien wspierać:

- Wykrywanie ruchu (motion detection),
- Alerting przy przekroczeniu stref wrażliwych,
- Automatyczne nagrywanie przy alarmie,
- Eksport nagrań w formatach standardowych,
- Audyt zdarzeń (logi dostępu do nagrań).

4. SYSTEM SYGNALIZACJI WŁAMANIA I NAPADU

4.1. Standard systemu

System powinien być zainstalowany zgodnie ze Standardami IT Uniwersytetu Medycznego w Łodzi oraz możliwość integracji z istniejącym na UMED systemem poprzez ETHM (SATEL), Sekcja 2.1 – System

sygnalizacji włamania i napadu. Określenie stopnia zabezpieczenia, dobór detektorów i ich lokalizacja powinien być poprzedzony projektową analizą ryzyka i zagrożeń.

4.2. Alarmy w systemie

System powinien obejmować dwa niezależne kanały alarmowe:

Alarm Napadowy Cichy (Silent Alarm)

- Sygnalizacja bez dźwięku w obiekcie,
- Powiadomienie bezpośrednio do Centrum Bezpieczeństwa i pracownika ochrony (aplikacja mobilna, SMS, email),
- Zastosowanie w przypadkach dyskretnego powiadomienia o zagrożeniu,
- Minimalizacja paniki zwiedzających.

Alarm Napadowy (Panic Alarm)

- Dźwiękowe i optyczne sygnały alarmowe zarówno wewnątrz jak i na zewnątrz obiektu,
- Przyspieszenie interwencji ochrony,
- Przycisk aktywacyjny w stanowisku ochrony i dostępny dla personelu muzeum,
- Przesłanie automatycznego powiadomienia do responsywnych służb.

4.3. Czujniki

- **Czujniki ruchu dualne (PIR+MV) z funkcją antymaskingu:** W każdym pomieszczeniu na parterze (wejścia, korytarze, magazyny),
- **Czujniki magnetyczne (kontakty):** Na oknach i drzwiach objętych ochroną,
- **Czujniki tłuczonego szkła:** W pomieszczeniach z witrynami eksponatów,
- **Radiowe przyciski napadowe:** Dla personelu muzeum i pracownika ochrony

4.4. Manipulator systemu alarmowego

- **Lokalizacja:** Pomieszczenie ochrony (stróżówka na parterze),
- **Typ:** Klawiatura kodowa z wyświetlaczem LCD, lub panel dotykowy obsługi systemu,
- **Dostęp:** Ograniczony do personelu ochrony i kierownika obiektu,
- **Funkcje:** Uzbijanie, rozbrajanie, przejście w tryb częściowy (nocy), potwierdzanie alarmów.

4.5. Monitoring zewnętrzny

- **Nadajnik dwutorowy sygnałów alarmowych centrali:** podłączony do zew. stacji monitorowania,

4.6. Procedury alarmu

Każde uruchomienie alarmu powinno być zarejestrowane z:

- Datą i godziną zdarzenia,
- Typem alarmu (cichy, napadowy),
- Lokalizacją (pomieszczenie, czujnik),
- Potwierdzeniem przez pracownika ochrony,

5. SYSTEM KONTROLI DOSTĘPU

5.1. Standard systemu

W obiektach Zamawiającego stosowany jest system kontroli dostępu SALTO, w związku z czym Zamawiający wymaga zastosowania systemu kontroli dostępu w pełni kompatybilnego z aktualnie posiadanymi rozwiązaniami SALTO oraz uwzględnienie możliwości zarządzania wszystkimi obiektami z poziomu jednego, nadrzędnego systemu.

System powinien być zainstalowany zgodnie ze Standardami IT Uniwersytetu Medycznego w Łodzi, Sekcja 2.1 – System kontroli dostępu. Wymogi uwzględniające charakter obiektu:

5.2. Punkty dostępu

Zamawiający wymaga, aby wszystkie wejścia, o których mowa poniżej, były zabezpieczone w systemie SALTO.

Wejścia główne i wtórne:

- **Wejście główne** (na parterze, przy stróżówce): Bramka ze szklanymi drzwiami pod tą samą kontrolą (zależnie od spójności z koncepcją wewnątrz), z ręczną bramką boczną umożliwiającą przejazd wózka inwalidzkiego,
- **Wejście boczne** (ulica Narutowicza, zamknięte z ulicy): Drzwi z kontrolą dostępu (czytnik + elektrozaczep lub zwora),
- Inne wejścia w uzgodnieniu z zarządcą.

Pomieszczenia chronione:

- Magazyny zbiorów (SALTO - czytnik),
- Pracownie i warsztaty (SALTO - czytnik),
- Pomieszczenia administracyjne (SALTO - czytnik),
- Archiwum i katalogownia (SALTO - czytnik).

5.3. Okucia elektromagnetyczne

Każde pomieszczenie z kontrolą dostępu powinno być wyposażone w:

1. Każde przejście objęte systemem kontroli dostępu należy wyposażyć w odpowiedni zespół okuć elektromagnetycznych, dobrany do funkcji i kierunku otwierania drzwi:
 - elektrozaczep na drzwiach otwieranych na zewnątrz lub w innych bezpiecznych kierunkach,
 - zworę elektromagnetyczną na ciężkich drzwiach do magazynów oraz w przypadkach, gdy wymagane jest zwiększone dociskanie skrzydła.

2. Wszystkie przejścia objęte systemem kontroli dostępu muszą być sterowane przez kontrolery pracujące w trybie on-line, zintegrowane z centralnym systemem KD. Kontroler może obsługiwać do dwóch przejść jedno- lub dwustronnych, zgodnie z projektem wykonawczym i rozmieszczeniem szafek teletechnicznych.
3. Dopuszcza się stosowanie kontrolerów przejść instalowanych poza bezpośrednim sąsiedztwem drzwi (np. w szafach teletechnicznych lub pomieszczeniach technicznych), pod warunkiem zapewnienia:
 - ciągłości zasilania i komunikacji z systemem nadrzędnym,
 - właściwego oznaczenia, które przejścia są obsługiwane przez dany kontroler,
 - możliwości serwisu i wymiany urządzeń bez ingerencji w konstrukcję drzwi i okuć.
4. Dobór rodzaju okucia (elektrozaczep, zwora, dodatkowe elementy mechaniczne) oraz liczby kontrolerów na kondygnację należy określić na etapie projektu wykonawczego systemu KD, z uwzględnieniem wymagań ochrony przeciwpożarowej, ewakuacji oraz zaleceń producenta systemu SALTO i obowiązujących „Standardów w zakresie wyposażenia IT i TLT w budynkach UM”

5.4. Modele dostępu

Każdy użytkownik (pracownik, gość) powinien mieć przypisane uprawnienia dostępu do:

- Stref (pomieszczenia, obszary),
- Czasów (godziny pracy, specjalne okna czasowe),
- Typu akcji (wejście, wyjście, przejście do magazynu).

Strefy dostępu:

- **PUBLIC:** Pomieszczenia ekspozycyjne (dostęp dla wszystkich),
- **STAFF:** Warsztaty i pomieszczenia edukacyjne (pracownicy muzeum),
- **SECURE:** Magazyny i archiwa (autoryzowani pracownicy),
- **ADMIN:** Pomieszczenia administracyjne (kierownictwo i pracownicy biura).

5.5. Rejestracja dostępu

- **Online:** Każdy przejazd poprzez bramkę i czytnik jest rejestrowany w bazie SALTO,
- **Audyt:** Możliwość przeglądu dzienników dostępu (kto, kiedy, gdzie),
- **Alerty:** Automatyczne powiadomienie o nieautoryzowanych próbach dostępu,
- **Raportowanie:** Cotygodniowe raporty na temat aktywności dostępu.

6. SYSTEM SYGNALIZACJI POŻARU

System sygnalizacji pożaru (SSP) powinien zostać wykonany na podstawie projektu SSP zgodnie z obowiązującymi przepisami i normami, po uzgodnieniu i akceptacji przez rzeczoznawcę ds. zabezpieczeń p.poż. oraz konserwatorem obiektu.

7. OCHRONA FIZYCZNA I DZIAŁANIA OCHRONY

7.1. Zasoby ludzkie

Stanowisko ochrony na parterze (Stróżówka):

- Jeden pracownik ochrony w stanowisku stacjonarnym,
- Monitorowanie bramki, kamer i systemów bezpieczeństwa,
- Rejestrowanie przyjazdów i wyjazdów,
- Obsługa ataków bezpieczeństwa.

Ochrona ruchoma na obiekcie:

- Drugi pracownik ochrony w roli ruchomej (patrolowanie),
- Regularne obchody po obiekcie (minimum co 2 godziny),
- Sprawdzanie pomieszczeń magazynowych i archiwum,
- Interwencja w przypadku alarmu.

7.2. Wyposażenie ochrony

- Urządzenia radiowe (Talkie-walkie) do komunikacji,
- Latarki LED profesjonalne,
- Identyfikatory pracowników,
- Dokumentacja zdarzeń (dziennik ochrony).

7.3. Procedury operacyjne

Otwieranie obiektu:

- Wyłączenie stref systemu alarmowego,
- Sprawdzenie strefy za pomocą CCTV,
- Otwarcie wejścia głównego (bramka),
- Weryfikacja pomieszczeń ekspozycyjnych.

Zamykanie obiektu:

- Kontrola wszystkich pomieszczeń,
- Sprawdzenie zamknięcia okien i drzwi,
- Aktywacja stref systemu alarmowego,
- Zamknięcie wejścia głównego (bramka).

Procedury alarmowe:

- Zarejestrowanie typu alarmu,
- Podgląd na CCTV z kamery przypisanej do alarmu,
- Podjęcie działań (interwencja, ewakuacja, powiadomienie służb),
- Dokumentacja zdarzenia.

8. INFRASTRUKTURA SIECIOWA I ZASILANIE

8.1. Okablowanie strukturalne

Infrastruktura IT powinna być realizowana zgodnie ze Standardami IT Uniwersytetu Medycznego w Łodzi, Sekcja 2.1 – Okablowanie strukturalne.

8.2. Zasilanie systemów bezpieczeństwa

- **UPS (Uninterruptible Power Supply):** System zasilania awaryjnego dla serwerów i rejestratorów,
- **Baterie zapasowe:** Dla bezprzewodowych czujników i kontrolerów (minimum 2 lata pracy),

- **Agregat prądowórczy:** Dla pełnej operacyjności obiektu w przypadku długotrwałej przerwy w dostawie prądu.

8.3. Redundancja i niezawodność

- **Dual WAN:** Dwie niezależne łącza internetowe dla systemu SALTO,
- **Backup serwera:** Automatyczne kopie zapasowe baz danych systemu dostępu,
- **Monitoring systemów:** Automatyczne alerty na wypadek awarii komponentów kluczowych.

9. PROCEDURY RAPORTOWANIA I AUDYTU

9.1. Dziennik ochrony

Pracownik ochrony powinien prowadzić dziennik zawierający:

- Godziny pracy (rozpoczęcie, koniec dyżuru),
- Liczby odwiedzających,
- Zdarzenia niezwykle (alarmy, problemy techniczne),
- Notatki dotyczące bezpieczeństwa.

9.2. Raporty systemów

- **Raport CCTV:** Cotygodniowe zestawienie wybranych nagrań i zdarzeń,
- **Raport dostępu:** Dzienny dziennik nowych użytkowników, zmian uprawnień,
- **Raport alarmowy:** Wszystkie zdarzenia alarmowe z logami i akcjami,
- **Raport techniczny:** Stan systemów, awarie, serwis.

9.3. Archiwizacja danych

- **Nagrania CCTV:** Minimum 30 dni online, starsze przechowywane na nośnikach offline,
- **Dzienniki dostępu:** Minimum 12 miesięcy,
- **Logi alarmów:** Minimum 12 miesięcy,
- **Dystrybucja:** Kopie bezpieczeństwa przechowywane w bezpiecznej lokalizacji.

10. SZKOLENIE I DOKUMENTACJA

10.1. Szkolenie personelu

- Pracownicy ochrony: Szkolenie z obsługi systemów CCTV, alarmowego i dostępu,
- Personel muzeum: Procedury alarmowe, wpływ na bezpieczeństwo osobiste,
- Kierownictwo: Zarządzanie dostępem, raportowanie incydentów.

10.2. Dokumentacja techniczna

- Schematy blokowe systemów,
- Procedury obsługi i awaryjne,
- Instrukcje dla użytkowników (pracownicy, goście),
- Plany ewakuacji i wyjść awaryjnych,
- Kontakty do serwisów technicznych i służb ratunkowych.

10.3. Audyty bezpieczeństwa

- **Przeglądy kwartalne:** Ocena funkcjonalności systemów,

- **Testy procedur:** Przeszkolenia ewakuacyjne, ćwiczenia alarmowe,
- **Przeglądy roczne:** Pełny audytu bezpieczeństwa przez specjalistę externe.

11. ZGODNOŚĆ Z WYMOGAMI PRAWNYMI

Niniejszy dokument oraz wdrażane systemy bezpieczeństwa muszą być zgodne z:

- **Ustawa o ochronie bezpieczeństwa osób i mienia z 1997 r.** – wymogi dotyczące ochrony fizycznej i systemów alarmowych,
- **Ustawa o ochronie przeciwpożarowej z 1991 r.** – wymagania przeciwpożarowe,
- **RODO (Rozporządzenie o Ochronie Danych Osobowych)** – ochrona danych z CCTV i rejestrów dostępu,
- **Przepisy BHP** – bezpieczeństwo pracowników i odwiedzających,
- **Polskie Normy (PN-EN)** – normy dotyczące systemów alarmowych i monitoringu,
- **Standardy IT Uniwersytetu Medycznego w Łodzi** – wymogi techniczne dla systemów teletechnicznych.