

ZINTEGROWANY SYSTEM BEZPIECZEŃSTWA MUW

INWENTARYZACJA

Wykonawca dokona szczegółowej inwentaryzacji systemów będących obecnie w obiekcie celem włączenia ich do projektowanego Zintegrowanego Systemu Bezpieczeństwa (ZSB).

PROJEKT

- 1) Projektant opracuje projekt ZSB MUW, który realizować będzie funkcje:
 - Systemu Kontroli Dostępu (SKD);
 - Systemu Depozytorów Kluczy;
 - Systemu CCTV – rozbudowa i integracja istniejącego systemu (IP CCTV);
 - Systemu monitoringu stanu zamknięcia/otwarcia drzwi zewnętrznych;
 - System patrolowania
 - Systemu sygnalizacji włamania i napadu (SSWiN) w wybranych lokalizacjach obiektu – rozbudowa, integracja bądź wymiana istniejących systemów lokalnych;
- 2) Zaprojektowany ZSB będzie współpracował z istniejącym systemem sygnalizacji alarmu pożaru SAP (w tym z systemem wizualizacji).
- 3) Dodatkowo w ramach projektu ZSB należy przewidzieć możliwość jego rozbudowy o system rejestracji czasu pracy pracowników MUW, system parkingowy, jak również możliwość rozbudowy systemu CCTV czy systemu kontroli dostępu;
- 4) W przypadku braku możliwości integracji obecnie funkcjonujących systemów (nie dotyczy systemu SAP wraz z wizualizacją), projektant zaprojektuje systemy zamiennie;
- 5) Projektant opracuje dokumentację budowlaną wykonawczą zamienną / uzupełniającą do dokumentacji przekazanej przez Zamawiającego;
- 6) Projektant przedstawi projekt systemu do akceptacji Zamawiającego

Wymagania w zakresie możliwości Systemu i aplikacji obsługującej System

- 1) Aplikacja na bazie której Wykonawca zaprojektuje ZSB ma cechować się otwartą architekturą tj. podatnością na rozszerzenia, możliwością rozbudowy systemu zarówno pod względem sprzętowym, jak i oprogramowania;
- 2) Aplikacja musi obligatoryjnie wykorzystywać interfejs w języku polskim;
- 3) Aplikacja musi wykorzystywać sprawdzone rozwiązania dla obiektów dużych i rozproszonych;
- 4) Aplikacja ma zapewniać integrację i nadzór w czasie rzeczywistym informacji o stanie bezpieczeństwa obiektów, ich analizę i wspomaganie w podejmowaniu decyzji, w zależności od rodzaju wykrytych zagrożeń;
- 5) Aplikacja ma zapewniać centralne zarządzanie każdym z podłączonych do niego urządzeń np. konfigurowanie parametrów pracy, modyfikację uprawnień dostępu, aktualizację oprogramowania, itd. zgromadzone dane z pracy całego systemu służą do

tworzenia różnorodnych raportów (możliwość przesyłania predefiniowanych raportów w określonym czasie na ustalone adresy e-mail), wykorzystywanych przez specjalistyczne komórki MUW.;

- 6) Aplikacja powinna zapewniać dostęp do zintegrowanego systemu bezpieczeństwa MUW również z poziomu przeglądarek internetowych (Chrome, Firefox, Edge w wersjach aktualnych oraz 2 poprzednich), zakres zostanie doprecyzowany w toku realizacji;
- 7) Aplikacja musi posiadać mechanizmy zabezpieczające przed nieuprawnionym dostępem z zewnątrz. System powinien posiadać mechanizm autoryzacji użytkowników kompatybilny z ActiveDirectory posiadanym przez Zamawiającego.;
- 8) Aplikacja musi być dostępna poprzez sieć LAN (intranet);
- 9) Aplikacja musi zapewniać monitorowanie i zarządzanie sygnałami z podsystemu sygnalizacji włamania i napadu, może wykorzystywać istniejące struktury sieci LAN do zapewnienia pełnej integracji obiektowych systemów zabezpieczeń, takich jak: system CCTV, SSWIN, SKD, sygnalizacji pożaru (system wizualizacji);
- 10) Aplikacja musi zapewniać zdalne zarządzanie strefami ochrony (wył/wł);
- 11) Aplikacja zapewni obsługę kontroli pracy firm realizujących usługi ochrony na podstawie generowanych raportów (system patrolowania);
- 12) Aplikacja zapewni wizualizację stanów alarmowych;
- 13) Aplikacja musi zapewniać dostęp do danych systemu poprzez sieć LAN – MUW oprogramowanie winno umożliwiać monitorowanie przejść on-line - kontrolę czytników kart elektronicznych sprzężonych z zamkami otwierającymi drzwi, predefiniowanie reguł dostępu poszczególnych pracowników do stref chronionych;
- 14) Aplikacja powinna analizować istotne z punktu widzenia użytkownika informacje, zapewniać ich podgląd i wydruk. W szczególności powinna umożliwiać sprawdzenie, kto i kiedy otwierał dane przejście (w szczególności w strefach specjalnych wskazanych przez Zamawiającego na etapie realizacji).
- 15) Projektant powinien zaplanować stanowisko wydawania przepustek (wejście C + dodatkowe / okazjonalne w wejściu B). Stanowisko takie ma służyć edycji przepustek oraz może spełniać funkcje wizualizacji stanu systemu (wizualizacja nie dotyczy wejścia B).
- 16) Projektant uwzględni także kwestie drukowania etykiet na karty oraz nadawanie i odbieranie stałych uprawnień dla pracowników. Zamawiający jest w posiadaniu urządzeń do personalizacji kart (Zebra ZXP1 oraz Fargo HDP5600).
- 17) Projektant powinien zaplanować utworzenie stanowiska dowódcy ochrony (we wskazanym przez Zamawiającego pomieszczeniu) wraz z jego całkowitym wyposażeniem (monitory, itd.)
- 18) Projektant powinien zaplanować stanowisko administratora systemu, które obsługiwane będzie przez pracownika urzędu (w lokalizacji wskazanej przez Zamawiającego).

Wymagania w zakresie systemu kontroli dostępu (SKD)

- 1) Projektant zaprojektuje obustronną kontrolę dostępu w następujących lokalizacjach:
 - drzwi zewnętrzne wejście A (dziejniec od ul. Elektoralnej);
 - drzwi zewnętrzne w przejściu pomiędzy dziedzińcem głównym a dziedzińcem od ul. Elektoralnej - 2 szt.;
 - drzwi zewnętrzne w bramie dziedzińca głównego (klatka schodowa K9);
 - drzwi zewnętrzne wejście E tj. klatka schodowa K14 (2 sztuki), wejście na klatkę schodową K10 (od pl. Bankowego); wejście na klatkę schodową k11 od strony dziedzińca przy al. Solidarności;
 - furtka w bramie wjazdowej od ul. Solidarności;
 - drzwi na I piętrze (wygrózenie klatek schodowych K7 i K9 od strony korytarza VIP)Projektant zaprojektuje/dokona zmian dokumentacji projektowej otrzymanej przez Zamawiającego:
 - bramki w wejściu B (2 szt.);
 - bramki w wejściu C (5 szt.);
 - bramka w wejściu D (1 lub 2 szt.) – w danej lokalizacji istnieje bramka kontroli dostępu, w przypadku braku możliwości włączenia urządzenia do systemu, bądź braku możliwości instalacji urządzenia o zbliżonych parametrach wizualnych należy przewidzieć wymianę urządzenia na nowe ;
 - włączenie do systemu SKD systemu obecnie funkcjonującego w Punkcie Obsługi Klienta MUW zlokalizowanym w wejściu F (ul. Solidarności)
- 2) Projektant zaprojektuje w holu budynku B w wejściu C „punkt recepcyjny” zapewniający kontakt z klientami i wydawanie „kart gościa” (nie dotyczy aranżacji recepcji). Projekt ma zapewnić, aby klienci wchodzili wejściem C, a doraźnie istniała możliwość, w przypadku organizacji uroczystości objętych systemem zaproszeń, uruchomienia wejścia B;
- 3) Projekt musi zapewnić, aby wejścia zewnętrzne (poza wejściem C) były wejściami dostępnymi wyłącznie dla pracowników z selektywną możliwością tworzenia uprawnień dostępu do poszczególnych przejść;
- 4) Projektant uwzględni dla SKD możliwość przydzielania czasowego dostępu do wybranych stref w obiekcie;
- 5) Projektant uwzględni projektując SKD konieczność zapewnienia współpracy z istniejącymi lokalnymi systemami kontroli dostępu (pomieszczenia Punktu Obsługi Klienta, Biuro Ochrony, WBZK, Serwerownie, pomieszczenia socjalne, itd.) w tym celu należy uwzględnić aby System obsługiwał karty o parametrach wskazanych w załączonym do opz dokumencie (CryptoCertum 3.2.). Dodatkowo należy przewidzieć dostawę 400 kart;
- 6) Karty SKD będą obsługiwane systemem elektronicznych depozytorów kluczy;
- 7) SKD musi być administrowane poprzez aplikację, gwarantując efektywny mechanizm przydzielania i migracji uprawnień w zależności od przydzielonej roli użytkownika;
- 8) SKD ma mieć możliwość rozbudowy o funkcję rejestracji czasu pracy;

- 9) Przy wszystkich przejściach należy zaprojektować urządzenia umożliwiające otwarcie w sytuacji awaryjnej (np. pożaru);
- 10) Projektant zaprojektuje SKD tak aby wskazane przez Zamawiającego strefy miały możliwość dualnego lub alternatywnego do karty potwierdzenia identyfikacji;

Wymagania w zakresie depozytorów kluczy

- 1) Projektant zaplanuje system elektronicznych depozytorów kluczy z zachowaniem zasady jednej karty;
- 2) Planowana liczba depozytorów min. 6 szt. (z przeznaczeniem na ok. 420 kluczy) w lokalizacjach uzgodnionych z Zamawiającym;
- 3) Depozytory powinny być wyposażone w kamery zintegrowane z systemem CCTV;.
- 4) Depozytory powinny być wyposażone w podtrzymanie zasilania gwarantujące min. 12 godzin pracy.

Wymagania w zakresie współpracy z istniejącym systemem IP CCTV

- 1) Istniejący system IP CCTV oparty jest na oprogramowaniu GeoVision oraz Hikvision DS. 9632NI-I8 (dane w załączeniu do OPZ). Od Projektanta wymaga się zaplanowania (w uzgodnieniu z Zamawiającym – poglądowe lokalizacje wskazane na załączonym do OPZ rysunku) niezbędnego zakresu rozbudowy Systemu IP CCTV ze względu na potrzeby Zintegrowanego Systemu Bezpieczeństwa;
- 2) Zamawiający oczekuje w zakresie planowanych rozwiązań technicznych, aby Projektant, uwzględnił współdziałanie z integrowanymi podsystemami ochrony: np. dowiązania do zdarzeń alarmowych (kontaktrony w drzwiach zewnętrznych), , wsparcie weryfikacji użytkowników SSWiN i SKD, itd.;
- 3) Zamawiający oczekuje, aby Projektant uwzględnił w projekcie rozbudowę systemu o lokalizacje min. 25 kamer oraz kamer przewidzianych dla depozytorów kluczy oraz wymianę kamer, których nie można włączyć do projektowanego systemu;
- 4) Projektowany system CCTV ma integrować wszystkie urządzenia monitorujące w obiekcie;
- 5) Zamawiający oczekuje monitorowania wszystkich wejść do budynku (wejście i wyjście).

Wymagania w zakresie systemu monitoringu stanu zamknięcia/otwarcia drzwi

- 1) Projektant zaprojektuje system monitoringu stanu zamknięcia drzwi zewnętrznych (kontaktrony bądź rozwiązanie alternatywne), w taki sposób aby wizualizacja systemu (w portierni wejście C oraz pomieszczenie ochrony) sygnalizowała stan zamknięcia poszczególnych drzwi (na wizualizacji oraz dźwiękowo).
- 2) Projektant zaprojektuje system monitoringu stanu zamknięcia drzwi na I piętrze (wygródenie klatek schodowych K7 i K9 od strony korytarza VIP), w taki sposób aby

wizualizacja systemu (w portierni wejście C oraz pomieszczenie ochrony) sygnalizowała ich stan (na wizualizacji).

Wymagania w zakresie SSWIN

- 1) Projektant zaprojektuje integrację istniejących systemów WiN bądź w przypadku braku możliwości integracji zaplanuje wymianę na nowy (9 lokalizacji);
- 2) Projektant zaplanuje System tak, aby istniała możliwość przyjmowania informacji z wydzielonych systemów alarmowych;

Wymagania w zakresie współpracy z SAP

- 1) MUW posiada w obiekcie system ppoż., w związku z powyższym Projektant skoreluje planowane rozwiązania projektowe z funkcjonującymi rozwiązaniami ppoż.;
- 2) Projektant zintegruje pozostałe elementy systemu z funkcjonującą w obiekcie wizualizacją sygnałów sygnalizacji pożaru;
- 3) Projektant uwzględni współdziałania systemu ppoż. z systemami kontroli dostępu w przypadkach pożaru i ewakuacji.

Inne wymagania

- 1) Projektant zaplanuje również kwestie energetyczne w zakresie podtrzymania napięcia dla elementów Systemu na co najmniej 30 minut (utrzymanie zamknięcia stref specjalnych tj. BO, serwerownia oraz podtrzymanie systemu w czasie pozwalającym na bezpieczne zamknięcie aplikacji); Nie dotyczy zaniku napięcia w przypadku alarmu pożaru.
- 2) System Kontroli Dostępu w obiekcie MUW zaliczać się będzie do systemów dużych. Należy do celów projektowych przyjąć, że system musi obsłużyć co najmniej 2000 użytkowników;
- 3) Realizacja projektu powiązana jest z ingerencją w sieć LAN MUW. Projektant winien pamiętać o uwzględnieniu prawidłowego zaprojektowania sieci LAN przewidzianej do funkcjonowania Systemu, a w tym CCTV IP. Projektant zaprojektuje włączenia do istniejącej sieci, bądź w razie konieczności rozbudowę istniejącej sieci.
- 4) Zadaniem Projektanta będzie zaprojektowanie rozbudowy okablowania LAN w ramach systemu;
- 5) Projektant winien szczególnie uwzględnić następujące normy: PN-EN 50174-2:2002 Technika informatyczna -- Instalacja okablowania -- Część 2: Planowanie i wykonawstwo instalacji wewnątrz budynków, PN-EN 50173-1:2007 (U) Technika informatyczna -- Systemy okablowania strukturalnego -- Część 1: Wymagania ogólne, PN-EN 50174-3:2005 Technika informatyczna -- Instalacja okablowania -- Część 3: Planowanie i wykonawstwo instalacji na zewnątrz budynków;
- 6) Projekt winien oprzeć System o węzły sieci LAN w budynkach MUW – w razie konieczności zaplanować zmianę lokalizacji węzłów lub ich rozbudowę, w węzłach sieci zaplanować

w miarę możliwości oddzielne separowane szafy, dedykowane na potrzeby Zintegrowanego Systemu Bezpieczeństwa MUW lub zaplanować umieszczenie elementów aktywnych w części istniejących szaf rackowych jak również przewidzieć zakup wszelkiego niezbędnego wyposażenia;

- 7) Projektant zaprojektuje System dla przyjętego czasu przechowywania zdarzeń w Systemie tj. 3 miesiące z uwzględnieniem wykorzystania macierzy dyskowych, których dostawę należy przewidzieć;
- 8) Projektant zaplanuje integrację z posiadanymi przez Zamawiającego urządzeniem – bramką detekcji materiałów metalowych.
- 9) Dokumentacja musi być sporządzona z uwzględnieniem wymagań w zakresie dostępności dla osób niepełnosprawnych lub projektowania z przeznaczeniem dla wszystkich użytkowników.
- 10) Z uwagi na fakt, iż obiekt w który realizowana będzie inwestycja jest obiektem zabytkowym należy w miarę możliwości przewidzieć bezprzewodową komunikację urządzeń minimalizując tym samym ingerencję w substancję zabytkową;
- 11) Projektant w przypadku konieczności opracuje zamienny projekt budowlany, obejmujący wszelkie wymagania Zamawiającego zawarte w niniejszym OPZ, a wykraczające poza przekazany z SIWZ projekt, zgodnie z wymaganiami ustawy Prawo Budowlane.
- 12) Przy projektowaniu elektronicznych systemów wspomagających ochronę informacji niejawnych należy uwzględnić zasady określone w:
 - ROZPORZĄDZENIU RADY MINISTRÓW z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. z 2012 r., poz. 683 z późn. zm), w szczególności:
 - elektroniczne systemy pomocnicze (system kontroli dostępu, system sygnalizacji napadu i włamania) używane do ochrony informacji niejawnych należy wykonywać zgodnie z zasadami sztuki inżynierskiej i aktualnym poziomem wiedzy technicznej, opisanym w szczególności w odpowiednich Polskich Normach.”,
 - elektroniczne systemy pomocnicze (system kontroli dostępu, system sygnalizacji napadu i włamania) powinny posiadać wydane przez dostawcę, z uwzględnieniem przepisów o systemie oceny zgodności, poświadczenia zgodności z wymogami określonymi w rozporządzeniu
 - ROZPORZĄDZENIU RADY MINISTRÓW z dnia 13 marca 2017 r. zmieniające rozporządzenie w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. z 2017 r., poz. 522) opisane w Kategorii K4: kontrola dostępu – Środek bezpieczeństwa K4S1 – System kontroli dostępu Typ 3.

REALIZACJA

- 1) Wykonawca w przypadku konieczności jest zobowiązany do uzyskania wszystkich decyzji, opinii, uzgodnień i pozwoleń właściwych organów niezbędnych do wykonania i odbioru całości zadania, w tym pozwolenia na prowadzenie robót budowlanych w obiekcie zabytkowym oraz pozwolenia na budowę oraz wykonania robót budowlanych zgodnie z przygotowaną dokumentacją projektową oraz wymaganiami określonymi powyżej.
- 2) Wykonawca jest zobowiązany do dostawy wszelkich urządzeń i wyposażenia niezbędnych do osiągnięcia funkcjonalności opisanej w niniejszym OPZ.
- 3) Z uwagi na bezpieczeństwo wewnętrzne MUW szczegółowe informacje dotyczące stopnia zabezpieczenia poszczególnych pomieszczeń zostaną przekazane na etapie realizacji.