Podlaski Oddział Regionalny
ul. Nowa 2
18-400 Łomża

Wymagania techniczne Systemu Kontroli Dostępu (SKD)

Obiekt musi być wyposażony w system kontroli dostępu firmy ROGER RACS 4 ze względu na kompatybilność posiadanych elementów zastępczych, a także na obowiązujące umowy serwisowe z firmą ochraniarską (m.in. konieczność posiadania na magazynie odpowiednich zamienników).
* centrala systemu SKD CPR32-NET-BRD ROGER powinna zostać zamontowana w pomieszczeniu serwerowni,
* pomiędzy centralą SKD, a panelem krosowniczym w szafie dystrybucyjnej SD należy ułożyć przewód połączeniowy w celu zapewnienia komunikacji (przewód musi być poprowadzony w listwach ochronnych uniemożliwiający przypadkowe jego uszkodzenie),
* w celu poprawnej komunikacji centrala SKD zostanie skonfigurowana z następującymi ustawieniami: IP: 10.25.32.195, Maska: 255.555.255.0, Brama: 10.25.32.1,
* System kontroli dostępu powinien zostać skonfigurowany pod względem:
(a) podziału na grupy zabezpieczeń z przypisanymi do nich odpowiednimi kontrolerami KD zgodnie z poniższymi wytycznymi:
- BP189_serwerownia (tryb autoryzacji: karta, pastylka) - pomieszczenie serwerowni BP,
- BP189_archiwum (tryb autoryzacji: karta, pastylka) - wszystkie pomieszczenia archiwum BP, składnicy akt BP, tymczasowego miejsca przechowywania dokumentów BP),
- BP189_strefa (tryb autoryzacji: karta, pastylka) - wszystkie wejścia z zewnątrz do strefy administracyjnej BP.
- BWI_serwerownia (tryb autoryzacji: karta, pastylka) - pomieszczenie serwerowni BWI,
- BWI_archiwum (tryb autoryzacji: karta, pastylka) - wszystkie pomieszczenia archiwum BWI, składnicy akt BWI, tymczasowego miejsca przechowywania dokumentów BWI),
- BWI_strefa (tryb autoryzacji: karta, pastylka) - wszystkie wejścia z zewnątrz do strefy administracyjnej BWI.
(b) podziału na grupy dostępu:
- BP189_strefa_przejscia (użytkownicy przypisani do tej grupy mają dostęp tylko do strefy dostępu Biura Powiatowego. Strefa BP189 – podstawowa grupa nieobejmująca kontrolerów w serwerowni i archiwach BP),
- BP189_archiwum_przejscia (użytkownicy przypisani do tej grupy mają dostęp do stref dostępu: BP189_archiwum i BP189_strefa, np. archiwista),
- BP189_serwerownia_przejscia (użytkownicy przypisani do tej grupy mają dostęp do stref dostępu: BP189_serwerownia i BP189_strefa, np. informatyk)
- BP189_pelen_dostep (użytkownicy przypisani do tej grupy mają dostęp do wszystkich kontrolerów w danym BP; np. kierownik BP189),
- BP189_brak_dostepu (użytkownicy przypisani do tej grupy nie mają dostęp do kontrolerów w BP; np. byli pracownicy BP, osoby nieobecne ponad 30 dni w pracy).
- BWI_strefa_przejscia (użytkownicy przypisani do tej grupy mają dostęp tylko do strefy dostępu BWI. Strefa BWI – podstawowa grupa nieobejmująca kontrolerów w serwerowni i archiwach BWI),
- BWI_archiwum_przejscia (użytkownicy przypisani do tej grupy mają dostęp do stref dostępu: BWI_archiwum i BWI_strefa, np. archiwista),
- BWI_serwerownia_przejscia (użytkownicy przypisani do tej grupy mają dostęp do stref dostępu: BWI_serwerownia i BWI_strefa, np. informatyk)
- BWI_pelen_dostep (użytkownicy przypisani do tej grupy mają dostęp do wszystkich kontrolerów w BWI; np. kierownik BWI),
- BWI_brak_dostepu (użytkownicy przypisani do tej grupy nie mają dostęp do kontrolerów w BWI; np. byli pracownicy BWI, osoby nieobecne ponad 30 dni w pracy).
W pastylkę/kartę zbliżeniową w standardzie EM 125 kHz wyposażony będzie każdy z pracowników i należy go przypisać w zależności od pełnionych zadań do jednej z powyższych grup.
Zainstalowany system kontroli dostępu musi być kompatybilny z kartami/pastylkami zbliżeniowymi firmy ROGER, w które wyposażyć należy pracowników BP ARiMR,

* zastosowane kontrolery KD (niedopuszczalne jest zastosowanie czytników, które do działania wymagają ciągłej komunikacji z centralą KD – kontrolery muszą działać w trybie autonomicznym np. ROGER PR311SE) i muszą być kompatybilne z centralą systemu kontroli dostępu, posiadać atesty dopuszczające do użytkowania na terytorium Polski,
* zastosowane czujniki otwarcia drzwi KD muszą być kompatybilne z centralą systemu kontroli dostępu i posiadać atesty dopuszczające użytkowania na terytorium Polski,
* zastosowane przyciski wyjścia KD muszą być kompatybilne z centralą systemu kontroli dostępu i posiadać atesty dopuszczające do użytkowania na terytorium Polski, dodatkowo powinny być dostosowane do dużego obciążenia,
* zastosowane przyciski awaryjnego wyjścia KD muszą być kompatybilne z centralą systemu kontroli dostępu i posiadać atesty dopuszczające użytkowania na terytorium Polski,
* system kontroli dostępu musi zostać zamontowany na każdych drzwiach będących wejściem do strefy administracyjnej, jak i każdego pomieszczenia archiwum, składnicy akt, tymczasowego miejsca przechowywania dokumentów i serwerowni (są to strefy zabezpieczeń do których wchodzi się ze strefy administracyjnej). Wejście dowolnego użytkownika, po użyciu karty musi być rejestrowane w logach systemu kontroli dostępu, wyjście z dowolnej strefy następuje po naciśnięciu przycisku wyjścia lub klamki – brak konieczności rejestrowania wyjścia z pomieszczenia w logach systemu.
* Każde drzwi chronione systemem kontroli dostępu muszą być wyposażone w wewnętrzny przycisk awaryjnego otwarcia drzwi (z możliwością resetowania przycisku z użyciem kluczyka np. przycisk awaryjnego otwarcia drzwi APKW, niedopuszczalne jest montaż przycisków ze zbijaną szybką).
* Wykonawca zobowiązuje się do przekazania dokumentacji technicznej systemu kontroli dostępu, w przekazywanej dokumentacji muszą być spełnione następujące warunki:
- informacje o podziale na grupy zabezpieczeń,
- informacje o podziale na grupy dostępu,
- wykaz wszystkich kontrolerów KD (nr linii, opis, grupa zabezpieczeń, lokalizacja, nr pomieszczenia),
- wykaz wszystkich urządzeń zainstalowanych na obiekcie (model urządzenia, typ, ilość),
- bilans mocy (nazwa urządzenia, producent, pobór mocy, suma poboru),
- zaznaczone wszystkie zamontowane elementy na aktualnych rzutach obiektu z legendą umożliwiającą w jednoznacznym sposób zlokalizowanie miejsca montażu elementu,
- schemat podłączenia.

W przypadku braku, któregokolwiek z wymienionych punktów Wykonawca zobowiązuje się do usunięcia w terminie 2 tygodni od momentu poinformowania o nieprawidłowościach i dostarczenia zaktualizowanej dokumentacji do ARiMR.

Po skutecznym odbiorze Wykonawca przekaże w wersji elektronicznej na nośniku optycznym w osobnych katalogach:
- pliki konfiguracyjne i dokumentację systemu kontroli dostępu obiektu,
- rzuty obiektu w formacie AutoCAD