

## Szczegółowy opis przedmiotu zamówienia

Przedmiotem zamówienia jest wykonanie projektu i instalacja elementów Elektronicznego Systemu Bezpieczeństwa (ESB) w jednostkach KRUS w Poznaniu, Koninie, Ostrowie Wlkp., Rawiczu i Pile w różnym zakresie, pracujących w sieci korporacyjnej WAN/LAN.

## Ogólna charakterystyka Elektronicznego Systemu Bezpieczeństwa

## 1. Centralka do Systemu Monitoringu Infrastruktury Technicznej w 5 lokalizacjach

- monitorować parametry w reżimie 7x24,
- ma mieć awaryjne podtrzymanie zasilania z akumulatora(ów) na wypadek zaniku zasilania sieciowego, zapewniającego poprawne funkcjonowanie w czasie nie krótszym niż 24 godziny po zaniku zasilania,
- możliwość przechowywania informacji ( ok. 5000 rekordów) o monitorowanych parametrach obiektu, wykrytych zdarzeniach alarmowych,
- obsługa 1 dualna czujka ruchu i zbitcia szyby,
- obsługa 1 czujnika/kontrolera temperatury i wilgotności w pomieszczeniu,
- układ dla 1 fazy zaniku i powrotu napięcia zasilania z sieci 230VAC,
- obsługa 1 czujnika zalania,
- zarządzanie stanem rolet antywłamaniowych (rolety są sterowane elektrycznie),
- zarządzanie pracą klimatyzatorów ( są wyposażone w dedykowany sterownik do pracy turnusowej),
- współpraca z systemem nadzoru i monitoringu,
- ma mieć moduł GSM/SMS do powiadamiania wyznaczonych pracowników poprzez wysyłanie komunikatów za pośrednictwem SMS oraz za pośrednictwem poczty elektronicznej z każdej lokalizacji (np. w przypadku wystąpienia zdarzenia alarmowego typu: 'wysoka temperatura w pomieszczeniu serwerowni'),
- funkcja zdalnej bramy GSM,
- możliwość ustawienia opóźnienia dla sygnałów alarmowych (czas od wystąpienia alarmu do wysłania powiadomienia),
- możliwość blokady alarmowania danego sygnału,
- możliwość zdalnej aktualizacji oprogramowania (Upgrade),
- wizualizacja stanu pracy centralki/kontrolera poprzez diody LED: ALARM, PRACA,
- konfiguracja centralki/kontrolera w języku polskim,
- powiadomienia: E-mail, SMS w języku polskim,
- możliwość Upgrade do wyższej wersji (zwiększenie funkcjonalności),
- Zegar RTC - automatyczna synchronizacja z serwerem SNTP, automatyczna zmiana czas letni, strefa czasowa, możliwość ręcznego żądania synchronizacji,
- możliwość współpracy z systemem nadrzędnym (np. systemem nadzoru i monitoringu),

## 2. System Kontroli Dostępu w 4 lokalizacjach

- kontrola dostępu realizująca w sposób jednoznacznie identyfikujący osobę wchodzącą –autoryzacja przy pomocy karty zblizeniowej z możliwością wpisania kodu PIN – czytniki zblizeniowe z klawiaturą,
- ma mieć awaryjne podtrzymanie zasilania z akumulatora(ów) na wypadek zaniku zasilania sieciowego, zapewniającego poprawne funkcjonowanie w czasie nie krótszym niż 12 godzin po zaniku zasilania,
- brak ograniczenia liczby kontrolerów pracujących w jednym sieciowym systemie (możliwość zabudowy systemu rozproszonego (min. kilkadziesiąt obiektów),
- rejestrację godzin oraz informacji o otwierającym drzwi,
- zdalne otwarcie drzwi przez administratora,
- 2 przyciski do otwierania drzwi w pokoju informatyków przy ich biurkach,
- 20 szt. kart zblizeniowych (po 5 szt. dla Konina, Ostrowa, Piły i Rawicza),
- wysłanie powiadomienia o zdarzeniu np. każdorazowe wpisanie złego kodu PIN, każdorazowe odczytanie nieważnej karty, otwarcie drzwi siłą, zbyt długie pozostawienie otwartych drzwi, itp.,
- obsługa kart standardu Wiegand lub Clock&Data,
- możliwość wymiany oprogramowania Upgrade – zwiększenie funkcjonalności,
- możliwość zdalnej konfiguracji,
- możliwość przechowywania informacji (rejestr zdarzeń, min. 5000 rekordów),
- możliwość współpracy z systemem nadrzędnym (np. systemem nadzoru i monitoringu),

## 3. Oprogramowanie (System Centralny)

- System powinien być zbudowany w architekturze klient-serwer aby zapewnić dostępność danych on-line i archiwalnych o stanie infrastruktury technicznej wielu rozproszonych serwerowni (obiektów) dla wielu użytkowników odpowiedzialnych za ich prawidłowe funkcjonowanie,
- Zarządzanie i konfigurowanie w języku polskim,
- System powinien zapewnić wysyłanie powiadomień w technologii SMS GSM, e-mail, trap SNMP wg harmonogramów czasowych dla grup alarmów i grup odbiorców SMS,
- System powinien zapewniać dwustronne inicjowanie komunikacji: samoczynnie przez lokalną jednostkę kontrolną w przypadku wystąpienia zdarzenia alarmowego lub na polecenie operatora w celu sprawdzenia stanu obiektu,

- Możliwość komunikacji z lokalnymi jednostkami kontrolnymi z wykorzystaniem sieci Ethernet i protokołu TCP/IP,
- Oprogramowanie powinno zapewniać zarządzanie użytkownikami systemu i gromadzenie historii o ich aktywności (logowanie, wylogowanie, odebranie alarmu),
- Oprogramowanie musi umożliwiać blokowanie dostępu do danych urządzenia osobom niepożądanym poprzez zastosowanie uprawnień,
- Grupowanie użytkowników i przydzielanie uprawnień grupom,
- Możliwość wydzielenia stref w obiekcie i przyznawania uprawnień do całych stref,
- Sterowanie zdalne obiektem (kasowanie alarmów, otwarcie drzwi, uzbrajanie/rozbrajanie systemu),
- Zdalna aktualizacja oprogramowania (firmware) sterowników zainstalowanych na obiekcie oraz ich konfiguracja,
- Integracja istniejących central alarmowych pożaru, włamania i napadu,
- Monitorowanie i zarządzanie systemami sygnalizacji pożaru, włamania i napadu,
- Wdrożone mechanizmy szyfrowania przesyłanych danych,
- Zarządzanie i monitorowanie systemami kontroli dostępu zapewniający,
  - możliwość integracji z depozytariuszami kluczy w lokalizacjach
  - jednoznaczną identyfikację osoby oraz rejestracja czasu wejścia do pomieszczenia
- Obsługa systemów telewizji dozorowej – możliwość wywołania „okna” obrazem na żywo z zainstalowanej kamery oraz automatyzacja procesów pobierania nagrań,
- Zapewnienie współdziałania z integrowanymi podsystemami ochrony np. dowiązania do zdarzeń alarmowych, weryfikacja alarmów pożarowych, wsparcie weryfikacji alarmów (SSWiN i SKD, SSP) przez Operatora systemu Centrum Nadzoru (np. pracownika ochrony).

Wydruk raportów dla poszczególnych elementów systemu oraz możliwość eksportu do XLS, np.

- o konfiguracji dostępu do obiektów,
- o posiadanych uprawnień dla osoby,
- o zdarzeń dla wybranego obiektu – kontrola dostępu dla wybranego przedziału czasu,
- o stanu obiektu na wybrany dzień.

### Szczegóły dotyczące poszczególnych lokalizacji

#### 1. Poznań – jednostka nadrzędna, (w budynku jest system kontroli dostępu)

Dostawa, montaż i konfiguracja w serwerowni:

- 1 dualna czujka ruchu i stłuczenia szyby,
- 1 czujnika/kontroler temperatury i wilgotności w pomieszczeniu,
- układ dla 1 fazy zaniku i powrotu napięcia zasilania z sieci 230VAC,
- 1 czujnika zalania,
- moduł GSM/SMS.

#### 2. Ostrów Wielkopolski – jednostka podrzędna

Dostawa, montaż i konfiguracja w serwerowni:

- 1 dualna czujka ruchu i stłuczenia szyby,
- 1 czujnika/kontroler temperatury i wilgotności w pomieszczeniu,
- układ dla 1 fazy zaniku i powrotu napięcia zasilania z sieci 230VAC,
- moduł GSM/SMS,
- elementy do jednostronnej kontroli dostępu w 3 pomieszczeniach,
- 2 przyciski do otwierania drzwi w pokoju informatyków przy ich biurkach.

*Dodatkowe informacje do kontroli dostępu:*

- *drzwi do serwerowni są nowe i wyposażone w samozamykacz, elektrozaczep z sygnalizacją otwarcia i zamknięcia,*
- *drzwi do pomieszczenia technicznego i do pomieszczenia informatyków nie mają wyposażenia KD,*
- *wszystkie pomieszczenia znajdują się blisko siebie.*

#### 3. Pila – jednostka podrzędna

Dostawa, montaż i konfiguracja w serwerowni:

- 1 dualna czujka ruchu i stłuczenia szyby,
- 1 czujnika/kontroler temperatury i wilgotności w pomieszczeniu,
- układ dla 1 fazy zaniku i powrotu napięcia zasilania z sieci 230VAC,
- moduł GSM/SMS,
- elementy do jednostronnej kontroli dostępu w 2 pomieszczeniach, jeśli istnieje taka potrzeba
- 2 przyciski do otwierania drzwi w pokoju informatyków przy ich biurkach.

*Dodatkowe informacje:*

- *drzwi do serwerowni są nowe i wyposażone w samozamykacz, elektrozaczep z sygnalizacją otwarcia i zamknięcia,*
- *drzwi do pokoju informatyków mają elementy kontroli dostępu wraz z czytnikiem (do ewentualnej wymiany),*
- *pomieszczenia znajdują się blisko siebie.*

#### 4. Rawicz – jednostka podrzędna

Dostawa, montaż i konfiguracja w serwerowni:

- 1 dualna czujka ruchu i stłuczenia szyby,
- 1 czujnika/kontroler temperatury i wilgotności w pomieszczeniu,
- układ dla 1 fazy zaniku i powrotu napięcia zasilania z sieci 230VAC,
- 1 czujnika zalania,
- moduł GSM/SMS,
- elementy do jednostronnej kontroli dostępu w 2 pomieszczeniach,
- 2 przyciski do otwierania drzwi w pokoju informatyków przy ich biurkach.

*Dodatkowe informacje:*

- *drzwi do serwerowni są nowe i wyposażone w samozamykacz, elektrozaczep z sygnalizacją otwarcia i zamknięcia,*
- *drzwi do pomieszczenia informatyków nie mają wyposażenia w elementy KD,*
- *pomieszczenia znajdują się blisko siebie.*

#### 5. Konin – jednostka podrzędna

Dostawa, montaż i konfiguracja w serwerowni:

- 1 dualna czujka ruchu i stłuczenia szyby,
- moduł GSM/SMS,
- elementy do jednostronnej kontroli dostępu w 2 pomieszczeniach, jeśli istnieje taka potrzeba,
- 2 przyciski do otwierania drzwi w pokoju informatyków przy ich biurkach.

*Dodatkowe informacje:*

- *drzwi w serwerowni i pomieszczeniu informatyków są wyposażone w kontrolę dostępu typu KD-01,*
- *pomieszczenia te znajdują się na różnych kondygnacjach i różnych częściach budynku,*
- *w serwerowni zainstalowane są elementy monitoringu infrastruktury technicznej, tj.*
  - a. kontroler ITsupervisor standard 1.7.4,*
  - b. czujka temperatury i wilgotności KTW-2 z LCD na ścianie,*
  - c. czujka CHT-RS485 BOX w szafie rack ,*
  - d. czujka zaniku zasilania z sieci energetycznej i powrotu UKZA\_3x.*