1. OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest: sprzedaż, dostawa, instalacja, konfiguracja i uruchomienie systemu kontroli dostępu oraz systemu wideo-domofonowego w budynku Rektoratu przy ul. Banacha 11 należącym do Akademii Wychowania Fizycznego we Wrocławiu, przy al. I.J. Paderewskiego 35

W ramach wykonania przedmiotu zamówienia Wykonawca zobowiązany jest zrealizować:

- Instalację Systemu Kontroli Dostępu do budynku opierającego się o dwa moduły zewnętrzne wyposażone w kamery,
- Instalację zasilania elektrycznego na potrzeby systemu kontroli dostępu oraz wideo-domofonów,
- Instalację okablowania LAN koniecznego do uruchomienia systemu oraz integrację z istniejącymi systemami informatycznymi w zakresie kontroli dostępu (w tym dokonanie niezbędnych połączeń pomiędzy szafami dystrybucyjnymi w budynku,
- Integracja musi opierać na istniejących bazach kart pracowniczych i studenckich
- Instalację Systemu Wideo-domofonu ma opierać się o (dwa moduły stacji zewnętrznej, osiem modułów stacji wewnętrznych, umożliwiających podgląd i autoryzację dostępu do budynku)

2. WYMAGANIA ZAMAWIAJĄCEGO

Wymagana dokumentacja powykonawcza – w wersji papierowej w 1 egz. oraz w wersji elektronicznej (.pdf) w 1 egz.

2.1 Przewidywany zakres dokumentacji:

Po zakończeniu prac sporządzenie dokumentacji powykonawczej zawierającej co najmniej:

- instrukcje obsługi i gwarancje urządzeń dostarczonych i zainstalowanych przez Wykonawcę (w wersji elektronicznej oraz 1 egzemplarz w wersji papierowej),
- specyfikacja techniczna zainstalowanego sprzętu i użytych materiałów,
- opis systemu – zawierający co najmniej wykaz urządzeń wchodzących w skład systemu, użytych materiałów, schemat kreskowy z zaznaczonymi miejscami instalacji elementów systemów naniesiony na schemacie budynkowym,
- opis połączeń kablowych oraz odpowiednie oznaczenie gniazd i patchpanelu

2.2 Specyfikacja techniczna i funkcjonalna systemu kontroli dostępu.

1. W ramach zamówienia Wykonawca dostarczy niezbędne, dożywotnie licencje dla oprogramowania systemu Kontroli Dostępu z możliwością przyszłej rozbudowy systemu, z zapewnieniem:
   a) jednoczesnej obsługi do 10 000 użytkowników/kart, przy czym zmiana parametrów jednego użytkownika/karty (np. zastąpienie jednej osoby inną dla tej samej karty), nie jest uważane za zwiększenie liczby użytkowników. Ponadto system musi umożliwiać usuwanie nieaktywnych (zgubionych lub uszkodzonych) kart,
   b) jednoczesne użytkowanie systemu (tj. konfigurację systemu, nadawanie uprawnień dla użytkowników, raportowanie zdarzeń itp.) na dowolnej liczbie stanowisk komputerowych co najmniej na poziomach:
      - Administratora – umożliwiającym pełne zarządzanie, kontrola, raportowanie i konfiguracja systemu,
      - Administratora Grupowego – umożliwiającym pełne zarządzanie, kontrola, raportowanie i konfiguracja systemu wyłącznie w wydzielonej strefie (grupie przejść),
      - Administratorów Dostępów - umożliwiającym nadawanie uprawnień użytkownikom oraz raportowanie,

- Operatorów Raportów - umożliwiającym raportowanie,
- Portierów - umożliwiającym podgląd wybranych zdarzeń i alarmów.

2. Scentralizowana obsługa i zarządzanie infrastrukturą oraz użytkownikami, z możliwością wydzielenia stref (grup przejść) do niezależnej obsługi i administracji.
3. Infrastruktura systemu oparta o technologię IP - komunikacja pomiędzy urządzeniami systemu tj. serwer, stanowiska administratorów i operatorów, kontrolery, moduły sterujące musi odbywać się za pośrednictwem sieci LAN i standardowego protokołu TCP/IP.
4. System musi zapewniać m.in.:
   a) monitorowanie i rejestrację zdarzeń zachodzących w systemie,
   b) zarządzanie pełna kontrola i konfiguracja systemu,
   c) zarządzanie alarmami,
   d) raportowanie,
   e) działanie w trybie zasilania awaryjnego z akumulatorów.
5. Obsługa minimum 10 tys. użytkowników
6. Obsługa nieograniczonej liczby zdarzeń, jedyne dozwolone ograniczenie, to ilość dostępnego miejsca na dysku twardym.
7. Monitorowanie stanu zabezpieczonych drzwi.
8. Monitorowanie anty-sabotażowe urządzeń.
9. Automatyczne odczytywanie zaszyfrowanych danych sektorowych w przypadku kart pracowników z użyciem klucza oraz numeru seryjnego kart studenckich w standardzie Mifare:
   a) w przypadku obecności zaszyfrowanej zawartości na kartach pracowników dane te powinny być użyte do identyfikacji użytkownika,
   b) w przypadku braku obecności zaszyfrowanej zawartości na kartach do identyfikacji powinien zostać użyty numer seryjny karty/ lub numer legitymacji potwierdzony z bazą danych studentów/doktorantów
10. Funkcja automatycznego powiadomienia e-mail dla wybranych zdarzeń alarmowych oraz przejść.
11. Funkcja raportowania o zdarzeniach z wykorzystaniem rozbudowanych filtrów umożliwiająca prezentację danych dotyczących przejścia, karty(użytkownika), grupy przejść lub kart użytkowników w zadanym okresie czasu itp.
12. Możliwość eksportu raportów do plików typu pdf, html, xlsx, csv.
13. Definiowanie kalendarza świąt (z opcją automatycznego nadawania/blokowania dostępu do przejść).
14. Rejestracja operacji wykonywanych przez administratorów.
15. Możliwość monitorowania stanu systemu poprzez przygotowane rozszerzenia i integrację z istniejącym systemem Zabbix

Wymogi oprogramowania.

1. Oprogramowanie systemu Kontroli Dostępu musi być wykonane w technologii klient-serwer. Oprogramowanie klienckie dostarczonego systemu Kontroli Dostępu nie może przechowywać danych na stanowiskach komputerowych, na których jest zainstalowane lub uruchomione.
2. Aplikacje muszą działać pod kontrolą systemu Windows w wersji 64-bit (wsparcie dla systemów operacyjnych Windows 7, 8, 10,11 oraz systemów z rodziny Windows Server od wersji 2008 w górę.
3. Wszystkie aplikacje powinny zapewniać mechanizm uwierzytelniania i autoryzacji użytkowników. W związku z tym administrator (z odpowiednimi uprawnieniami)

może zdefiniować określone prawa dostępu i uprawnienia dla każdego użytkownika w systemie.
4. Pełna obsługa aplikacji w języku polskim.
5. Oprogramowanie zainstalowane na serwerze musi utrzymywać łącze komunikacyjne z kontrolerami sprzętowymi, w sposób ciągły monitorować, czy kontrolery są w trybie online, czy offline oraz sygnalizować stan pracy systemu, w tym na przykład brak połączenia z elementami systemu lub awarie.
6. Nadawanie uprawnień poszczególnym użytkownikom systemu zarządzania w zależności od stanowiska (administrator, administrator grupy, operator raportów, portier itp.).
7. Zarządzanie uprawnieniami użytkownika(karty) typu gość.
8. Opcja aktywacji lub wyłączenia profilu posiadacza karty: profil posiadacza karty aktywny do zadanej daty, wygaśnięcie w dniu zdefiniowanym przez uprawnionego Administratora.
9. Możliwość tworzenia polityk haseł dla użytkowników.
10. Konfiguracja grup uprawnień z jednoczesną możliwością nadawania dodatkowych, indywidualnych, uprawnień poza grupami.
11. Zarządzanie alarmami w oprogramowaniu musi umożliwiać:
    a) zmianę typu alarmów i ostrzeżeń,
    b) przypisanie akcji dla służb ochrony po odebraniu alarmu,
    c) przypisanie harmonogramów powiadomień email dla alarmów i ostrzeżeń,
    d) określenie odbiorców alarmów i ostrzeżeń,
    e) potwierdzanie odbioru alarmów i ostrzeżeń przez Użytkowników w oprogramowaniu do odbioru alarmów online.

Integracje z systemami zewnętrznymi.
System musi docelowo umożliwiać wsparcie i możliwość integracji innych systemów zewnętrznych. Powinien zawierać funkcje i cechy umożliwiające obsługę dodawanych w przyszłości nowych elementów do integracji z systemami zewnętrznymi, takimi jak:
a) zewnętrzne systemy nadzoru wizyjnego,
b) zewnętrzne systemy kontroli dostępu.

Kontrolery i urządzenia sterujące.
Wymagane cechy techniczne, jakościowe i funkcjonalne kontrolerów:
a) komunikacja w serwerem w ramach systemu Kontroli Dostępu w oparciu o protokoły IP w sieci Ethernet.
b) kontrola dostępu do sieci z wykorzystaniem standardu 802.1X,
c) obsługa protokołu OSDP umożliwiającego bezpieczną komunikację pomiędzy kontrolerem a czytnikiem,
d) ochronę komunikacji z hostem z wykorzystaniem standardów AES-256,
e) wsparcie dla OpenSSL.

Czytniki kart.
Wymagane cechy techniczne, jakościowe i funkcjonalne czytników kart:
a) zakres temperatur pracy: nie węższy niż od -20℃ do 50℃,
b) klasa środowiskowa IP65,
c) współpraca z kartami 13,56 MHz,
d) obsługa technologii MIFARE Classic, MIFARE DESFire EV1 i iCLASS,
e) zgodność z stosownymi normami ISO,
f) posiadać czujnik antysabotażowy.

Przejścia.

1. Przejścia kontrolowane w ramach systemu Kontroli Dostępu muszą być zabezpieczone blokadami typu elektrozaczep lub zworą elektromagnetyczną
2. Przejścia jednostronne muszą zostać zamontowane w taki sposób, aby wejście do pomieszczenia było możliwe dzięki użyciu karty z odpowiednimi uprawnieniami, przycisku zwalniającego zaworę z systemu wideodomofonowego lub klucza dopasowanego do istniejącej wkładki, natomiast wyjście umożliwiać będzie klamka lub przycisk zwalniający blokadę. W przejściu należy zainstalować kontaktrony przekazujące do systemu informacje o otwarciu drzwi.

Elektrozaczepy.
Wymagane cechy techniczne, jakościowe i funkcjonalne elektrozaczepów:
Dla przejść wymagany jest montaż elektrozaczepu normalnie zamkniętego - rewersyjnego (NO):

a) możliwość montażu do drzwi lewych i prawych oraz montażu w poziomie,
b) siła trzymania 3000N,
c) głębokość zachodzenia zapadki 6mm,
d) zakres temperatury pracy: -15 °C +40 °C,
e) certyfikowany na zgodność z normą PN-EN 13637.

Zwory elektromagnetyczne.
Montowane elementy tego typu powinny spełniać poniższe wymagania:

a) montaż nawierzchniowy,
b) siła przyciągania dla drzwi jednostronnych ma być nie mniejsza niż 270 kg, a dla drzwi dwuskrzydłowych 540 kg,

2.3 BUDOWA SYSTEU WIDEODOMOFONOWEGO
Budowa systemów będzie polegała na instalacji dwóch paneli zewnętrznych wyposażonych:

- kamery min. 2 Mpx ,
- dwukierunkowego systemu komunikacji głosowej,
- modułów klawiatury numerycznej,
- modułów wizytownika,
- samozamykaczy.

Montażu ośmiu dotykowych paneli wewnętrznych:

- kolorowy ekran dotykowy min. 7 in w rozdzielczości 1024x600,
- głośnik i mikrofon, komunikacja dwustronna,
- standard PoE,
- TCP/IP, SIP, RTSP.

Montaż dedykowanej szafy RACK na potrzeby systemu wideo domofonowego oraz systemu kontroli dostępu:

- Szafa Rack 9U - 19 cali,
- PatchPanel,
- Zasilacz Awaryjny UPS,
- Switch sieciowy POE zarządzalny z obsługą VLAN,
- Połączenie światłowodowe do istniejącej szafy dystrybucyjnej znajdującej się w budynku.

Montaż szafy RACK i zasilacza awaryjnego UPS umożliwiającego potrzymanie systemów powyżej 5 godzin i ułożeniu nowej instalacji pod urządzenia. Dokładny przebieg tras

kablowych i ich długość zostanie ustalona przed realizacją zadania w trybie konsultacji w oparciu o ustalenia przeprowadzone w trakcie wizji lokalnej na obiekcie oraz posiadanej dokumentacji. Kable połączeniowe do modułów powinny zostać zakończone w przypadku szafy Rack w PatchPanelu a w przypadku końcówek opisanymi gniazdkami RJ45. Zakup, dostawa i montaż niezbędnego materiału i sprzętu do budowy systemów, należy do Wykonawcy. W przypadku realizacji przedmiotu zamówienia powiązanej z dostawą nowego wyposażenia systemów, oferowany sprzęt musi być fabrycznie nowy (nieregenerowany), pochodzący z oficjalnego źródła dystrybucji, wyposażony w aktualne oprogramowanie producenta i pełną gwarancję. Wykonawca udzieli gwarancji na dostarczone urządzenia oraz wykonane instalacje na okres min. 36 m-cy. W okresie objętym gwarancją Wykonawca w ramach przedmiotu zamówienia dokona przeglądów gwarancyjnych. Okresowe przeglądy gwarancyjne muszą być wykonane nie rzadziej niż co 6 miesięcy.
W przypadku budowy tras kablowych należy je wykonać w rurach karbowanych i korytkach elektroinstalacyjnych zgodnie z uzyskanymi uzgodnieniami. Ułożenie należy wykonać w sposób nie powodujący uszkodzeń istniejącej infrastruktury teletechnicznej. Wykonawca ponosi odpowiedzialność za prawidłowy montaż urządzeń zgodnie ze sztuką budowlaną. Szczegółowe warunki montażu będą uzgadniane z Zamawiającym.
Montaż urządzeń powinien zostać wykonany przez pracowników wykwalifikowanych (licencja pracowników zabezpieczenia technicznego).
UWAGI:
1. Przed przystąpieniem do złożenia oferty zaleca się dokonać wizji lokalnej w miejscu planowanego montażu elementów systemu kontroli dostępu.
Kontakt w sprawie terminu wizji – Akademia Wychowania Fizycznego we Wrocławiu:
Marian Grabarski tel. 713473171, 665770610 mail: marian.grabarski@awf.wroc.pl
Wiesław Stonoga tel. 713473400: 609109765 mail: wieslaw.stonoga@awf.wroc.pl
Robert Gdula tel. 713473316, 885883375 mail: Robert.gdula@awf.wroc.pl

W przypadku nie przeprowadzenia wizji lokalnej Wykonawca ponosi pełną odpowiedzialność za treść złożonej oferty.
2.4 WYMAGANIA DOTYCZĄCE ROZWIĄZAŃ TECHNICZNO – MATERIAŁOWYCH
Parametry kabli:
Wszystkie kable użyte do ułożenia niezbędnej infrastruktury muszą posiadać parametry zgodne z polskimi normami i zaleceniami europejskimi. Powinny być dobrane do warunków pracy zgodnych z oświadczeniem producenta instalowanego sprzętu. Zamawiający wymaga aby użyty kabel UTP (wewnętrzna instalacja) lub FTP (zewnętrzna instalacja) zastosowany do podłączenia elementów systemów był co najmniej kat. 6. (żyły kabla wykonane w 100% z miedzi)Oświadczenie producenta lub kartę katalogową kabla należy dołączyć do dokumentacji powykonawczej.