Szczecin, dnia 21 października 2021 r.

PROKURATURA REGIONALNA
W SZCZECINIE
ul. Mickiewicza 153
71-260 SZCZECIN
tel. (91) 441-09-57, fax.(91) 441-09-44

200-7.262.12.2021

ZAPROSZENIE DO ZŁOŻENIA OFERTY

Prokuratura Regionalna w Szczecinie zaprasza do złożenia oferty na: ***Wykonanie dokumentacji projektowo-kosztorysowej wraz z pełnieniem nadzoru autorskiego dla zadania: modernizacja systemu bezpieczeństwa który realizował będzie funkcje SSWiN, SKD, CCTV, ANTY-NAPADOWE w budynku Prokuratury Regionalnej w Szczecinie przy ul. Mickiewicza 153.***
Ofertę należy złożyć na formularzu ofertowym – **załącznik nr 1** do niniejszego zaproszenia (lub w oparciu o jego wzór) i przesłać do Zamawiającego mailem na adres: ksiegowosc@szczecin.pr.gov.pl lub marek.talaga@szczecin.pr.gov.pl lub złożyć w pok. nr 131 (I piętro) w terminie do **dnia 2 listopada 2021 r. do godz. 10.00** Wykonawca określa cenę brutto oraz VAT za cały przedmiot zamówienia.
Zamawiający zaleca wykonanie wizji lokalnej przed przystąpieniem do złożenia oferty. Zamawiający wyznacza w tym celu termin 27 października 2021r. w godzinach 10.00-13.00 po wcześniejszym skontaktowaniu się z przedstawicielem Zamawiającego, Panem Markiem Talaga – tel. (91) 441-09-57, kom. 667-084-317.

Zamawiający informuje jednocześnie, iż zamówienie zostanie udzielone Wykonawcy, który zaoferuje najniższą cenę brutto za całość zamówienia. Projekt umowy stanowi **załącznik nr 3** do niniejszego zaproszenia.

Szczegółowy opis przedmiotu zamówienia ujęty został w **załączniku nr 2 umowy** do niniejszego zaproszenia.

Osobą upoważnioną do kontaktów (w tym w zakresie zamiaru przeprowadzenia wizji lokalnej) jest p. Marek Talaga – tel. (91) 441-09-57, kom. 667-084-317.

Zamawiający zastrzega sobie możliwość unieważnienia postępowania bez podawania przyczyny. W takiej sytuacji Wykonawcy nie przysługuje roszczenie o zawarcie umowy oraz roszczenia odszkodowawcze.

Klauzula informacyjna dotycząca ochrony danych osobowych zgodnie z art. 13 RODO w związku z niniejszym postępowaniem o zamówienie publiczne

Zgodnie z art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej RODO, informuję, że:

1. Administratorem , w rozumieniu art. 4 pkt 7 RODO, danych osobowych jest Prokuratura Regionalna w Szczecinie z siedzibą przy ul. Mickiewicza 153, 71 – 260
w Szczecinie, tel. 91 441 09 79, e-mail. sekretariat@szczecin.pr.gov.pl.
2. Dane kontaktowe inspektora ochrony danych: tel. 91 441 09 72, e-mail iod@szczecin.pr.gov.pl
3. Podstawę prawną przetwarzania danych stanowi art.6 ust.1 lit. c) RODO w związku z przepisami ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021r. poz. 1129 t.j.), zwanej dalej ustawą PZP.
4. Dane osobowe przetwarzane będą w celu związanym z niniejszym postępowaniem
o udzielenie zamówienia publicznego i jego późniejszą realizacją (w tym zawarciem umowy lub udzieleniem zlecenia/zamówienia).

5. Dane osobowe są przechowywane przez okres nie dłuższy niż jest to niezbędne do realizacji celów, w których są przetwarzane, a po tym czasie przez okres oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa, w szczególności zgodnie z Zarządzeniem Nr 84/16 Prokuratora Generalnego z dnia 29 grudnia 2016 r. w sprawie wprowadzenia jednolitego rzeczowego wykazu akt powszechnych jednostek organizacyjnych prokuratury oraz przepisami określającymi zasady przechowywania przez zamawiających dokumentacji w sprawach związanych z postępowaniem o udzielenie zamówienia publicznego.
6. Dane osobowe mogą być przekazywane innym podmiotom, które będą je przetwarzały, w szczególności: osobom lub podmiotom, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy PZP, podmiotom prowadzącym działalność pocztową, kurierską, bankom, a w przypadku konieczności prowadzenia rozliczeń, organom państwowym lub innym podmiotom uprawnionym na podstawie przepisów prawa, celem wykonania ciążących na nas obowiązków (Urząd Skarbowy, PIP, ZUS), podmiotom wspierającym Administratora w prowadzonej działalności na jego zlecenie, w szczególności radcom prawnym, podmiotom świadczącym usługi ochrony oraz dostawcom zewnętrznych systemów wspierającym naszą działalność.
7. Osobie, której dane są przetwarzane przysługuje prawo:

a) na podstawie art. 15 RODO żądania od administratora dostępu do danych osobowych;
b) na podstawie art. 16 RODO żądania od administratora sprostowania lub uzupełnienia danych osobowych;
c) na podstawie art. 18 RODO żądania od administratora ograniczenia przetwarzania danych osobowych;
wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

8. Administrator informuje, że przepisy ustawy PZP ograniczają prawo do skorzystania:

- ze sprostowania lub uzupełnienia danych (art. 16 RODO), jeżeli zrealizowanie tego prawa mogłoby skutkować zmianą wyniku postępowania o udzielenie zamówienia lub zmianą postanowień umowy w sprawie zamówienia publicznego w zakresie niezgodnym z ustawą PZP;
- z ograniczenia przetwarzania (art. 18 RODO), które nie może zostać zrealizowane do czasu zakończenia tego postępowania, z zastrzeżeniem przypadków określonych w art. 18 ust. 2 RODO.

9. Osobie, której dane są przetwarzane nie przysługuje prawo:

a) usunięcia danych osobowych – art. 17 ust. 3 lit. b, d lub e RODO;
b) przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
c) wniesienia sprzeciwu wobec przetwarzania danych osobowych, o którym mowa w art. 21 RODO, gdyż podstawą prawną przetwarzania danych osobowych jest art. 6 ust. 1 lit. c RODO.

10. W celu skorzystania z praw, o których mowa w pkt 7 ppkt 1-3 należy skontaktować się z administratorem lub inspektorem ochrony danych, korzystając ze wskazanych wyżej danych kontaktowych.
11. Podanie danych jest dobrowolne, niemniej ich niepodanie skutkować będzie brakiem możliwości udziału w postępowaniu o udzielenie zamówienia publicznego, o którym mowa w pkt. 4.
12. Administrator nie dokonuje zautomatyzowanego podejmowania decyzji, w tym profilowania, o którym mowa w art. 22 RODO.
13. Jednocześnie Zamawiający przypomina o ciążącym na Państwie obowiązku informacyjnym wynikającym z art. 14 RODO względem osób fizycznych, których dane przekazane zostaną Zamawiającemu w związku z prowadzonym postępowaniem i które Zamawiający pośrednio pozyska od wykonawcy biorącego udział w postępowaniu, chyba że ma zastosowanie co najmniej jedno z wyłączeń, o których mowa w art. 14 ust. 5 RODO.

PROKURATOR REGIONALNY

Artur Maludy

Załączniki:

1. Formularz ofertowy
2. Opis przedmiotu zamówienia
3. Projekt umowy
4. Wytyczne dotyczące zabezpieczenia technicznego

/gd

2009-7.262. 12 .2021

Załącznik nr 1 do zaproszenia

Zamawiający
Prokuratura Regionalna w Szczecinie
ul. Adama Mickiewicza 153
Szczecin
tel. (91) 441-09-57, fax.(91) 441-09-44

Formularz ofertowy

Imię i nazwisko i/lub.....
nazwa (firma) .....
Wykonawcy .....
Adres Wykonawcy:
kod, miejscowość, ...
województwo, kraj: .....
ulica, nr domu, nr lokalu .....
Nr telefonu: ..... Nr faksu.....
e-mail.....
NIP: .....REGON: .....
Bank: .....Nr rachunku: .....

1. Odpowiadając na zaproszenie do złożenia oferty w postępowaniu o zamówienie publiczne o wartości zamówienia nie przekraczającej 130 000.00 zł netto tj. poniżej progu stosowania ustawy z dnia 11 września 2019r. - Prawo zamówień publicznych (Dz. U. z 2021 r., poz. 1129) na: ***Wykonanie dokumentacji projektowo-kosztorysowej wraz z pełnieniem nadzoru autorskiego dla zadania: modernizacja systemu bezpieczeństwa który realizował będzie funkcje SSWiN, SKD, CCTV, ANTY-NAPADOWE w budynku Prokuratury Regionalnej w Szczecinie przy ul. Mickiewicza 153***, składam niniejszą ofertę na cenę brutto:

..... (słownie złotych: .....)

1. Akceptujemy warunki płatności dni określone we wzorze umowy.
2. Oświadczam(my), że jestem(śmy) związany(i) ofertą - 28 dni.
3. Oświadczam(y), że cena uwzględnia wszystkie koszty wykonania zamówienia.
4. Oświadczam(my), że posiadamy uprawnienia do wykonywania przedmiotowej działalności
5. Zamówienie zrealizuję(emy) – sam(i) / z udziałem podwykonawców (niepotrzebne skreślić).
6. W przypadku zatrudnienia podwykonawców wskazuję(emy) części zamówienia: .....
   ..... których wykonanie zamierzam(y) powierzy następującym podwykonawcom: .....
7. W przypadku zatrudnienia podwykonawców, odpowiadam(y) za ich pracę jak za swoją własną.

8. Zapoznałem (liśmy) się z wzorem przyszłej umowy i nie wnoszę(simy) w stosunku do nich żadnych uwag, a w przypadku wyboru mojej / naszej oferty podpiszę(emy) ją w miejscu i terminie wskazanym przez Zamawiającego.
9. Oświadczam(my), że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.
10. W przypadku wyboru naszej oferty:

a) Osobą odpowiedzialną ze strony Wykonawcy za realizację przedmiotu umowy będzie (imię, nazwisko, telefon, e-mail): .....
.....
.....

b) Umowę w imieniu Wykonawcy podpisywać będą (imię, nazwisko, stanowisko): .....

c) Inne wymagania zamawiającego:

Wykonanie przedmiotu zamówienia do 28 dni od dnia podpisania umowy

....., dn. .....

.....
(podpis(y) osób uprawnionych)

2009-7.262.12.2021

Załącznik nr 2 do zaproszenia

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest wykonanie dokumentacji projektowo-kosztorysowej wraz z pełnieniem nadzoru autorskiego dla zadania: *modernizacja systemu bezpieczeństwa który realizował będzie funkcje SSWiN, SKD, CCTV, ANTY-NAPADOWE" w budynku Prokuratury Regionalnej w Szczecinie przy ul. Mickiewicza 153.*
2. Przygotowana dokumentacja musi uwzględniać wytyczne Ministerstwa Sprawiedliwości (w załączeniu).
3. Przygotowana dokumentacja musi zawierać :
   a) projekt wykonawczy
   b) kosztorys inwestorski
   c) przedmiar robót
4. Dokumentacja projektowo-kosztorysowa powinna być dostarczona Zamawiającemu w formie papierowej w 2 egz. oraz na nośniku w postaci płyty DVD – 1 szt.
5. Ww. projekt wykonawczy musi być uzgodniony i zaparafowany przez rzeczoznawcę ds. ppoż.

Wymagania ogólne

1. Projekt Systemu musi być wykonany w oparciu o wymagania norm:
   - PN-EN 50131-1 Systemy Alarmowe. Systemy Sygnalizacji Włamania i Napadu,
   - PN-EN 50133-1 Systemy Alarmowe. System Kontroli Dostępu
2. Wykonawca przeprowadzi audyt obecnie funkcjonującego systemu alarmowego celem zapoznania się z używanym rejestratorem, okablowaniem, rodzajem używanych kamer oraz czujek. Na bazie tej wiedzy określi, które z wymienionych składowych Systemu będzie możliwe uwzględnić w projekcie;
3. Dobór rozwiązań technicznych każdego systemu zostanie uzgodniony z Zamawiającym po zawarciu umowy w formie protokołu uzgodnień, przy czym projektując system uwzględnione zostaną możliwości finansowe Zamawiającego, a także koszty eksploatacyjne systemu po jego instalacji.
4. Na dokumentację będącą przedmiotem zamówienia składać się będzie:
   a) dokumentacja projektowa opisowa wraz z częścią rysunkową,
   - 2 egzemplarze w wersji drukowanej oraz 1 egz. w wersji elektronicznej w formacie .pdf
   b) kosztorys i przedmiar w formie elektronicznej: .pdf
5. Po zawarciu umowy Zamawiający udostępni rzuty kondygnacji budynku, w których instalowane będą systemy. Zamawiający jest w posiadaniu powykonawczej dokumentacji instalacji elektrycznej i logicznej, którą w razie konieczności udostępni wybranemu wykonawcy celem realizacji przedmiotu zamówienia.

Wymagania w zakresie możliwości Systemu i aplikacji obsługującej System

1. Urządzenia stanowiące centrum Systemu, jak: centralka alarmowa, zasilenie rezerwowe, macierz dyskowa oraz inne urządzenia zamontowane powinny być w szafie typu RACK we wskazanym przez Zamawiającego pomieszczeniu. Pomieszczenie te wyposażone jest w klimatyzację i ulokowane jest na poziomie przyziemia budynku.
2. Wykonawca zaplanuje czujniki kontrolujące warunki środowiskowe pomieszczenia Centrali podłączone do Systemu mierzące: temperaturę, zadymienie, zalanie tak by w razie wystąpienia zagrożenia dla pracujących urządzeń Centrali powiadomieni zostali pracownicy ochrony.
3. Aplikacja monitorująca funkcje systemu na bazie, której Wykonawca zaprojektuje System jak i urządzenia wchodzące w skład Systemu jak: kamery, czujki, czytniki i in oraz okablowanie, muszą zostać opisane przez Projektanta w taki sposób aby nie narzucać konkretnego rozwiązania producenta i zachować możliwość konkurencyjności.
4. Aplikacja ma cechować się otwartą architekturą tj. podatnością na rozszerzenia, możliwością rozbudowy systemu zarówno pod względem sprzętowym, jak i oprogramowania.

5. Aplikacja musi obligatoryjnie wykorzystywać interfejs w języku polskim.
6. 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.
7. 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.
8. Aplikacja powinna zapewniać dostęp do zintegrowanego systemu bezpieczeństwa również z poziomu przeglądarek internetowych.
9. Aplikacja musi posiadać mechanizmy zabezpieczające przed nieuprawnionym dostępem z zewnątrz.
10. Aplikacja musi zapewniać możliwości obsługi systemu CCTV w tym możliwość pobierania nagrań CCTV.
11. Aplikacja zapewni wizualizację stanów alarmowych.
12. Aplikacja musi zapewniać dostęp do danych systemu poprzez sieć LAN.
13. 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.
14. Projektant powinien zaplanować stanowisko wydawania przepustek. Stanowisko takie ma służyć edycji przepustek oraz może spełniać funkcje wizualizacji stanu systemu.
15. Projektant uwzględni także kwestie drukowania etykiet na karty oraz nadawanie i odbieranie stałych uprawnień dla pracowników.
16. Projektant zaplanuje w Systemie czas przechowywania zdarzeń dla: SKD i SSWiN, na 250.000 zdarzeń, a dla CCTV 30 dni z uwzględnieniem wykorzystania macierzy dyskowych.

Wymagania w zakresie CCTV

1. System monitoringu wizyjnego swoim zasięgiem ma obejmować określone przez Zamawiającego pomieszczenia i korytarze wewnątrz budynku oraz teren wokół budynku.
2. Projektant zaplanuje kamery o parametrach przy których kamery będą poprawnie działać i funkcjonować w oświetleniu dziennym i nocnym pochodzącym od istniejących lamp ulicznych oraz kamer z promiennikami IR.
3. Projektant zaplanuje możliwość rejestrowania osób, które zgrywały materiał video oraz zakres danych jaki został zgrany.

Wymagania w zakresie SKD

1. SKD szacujemy, że obejmie około 150 użytkowników. Należy jednak do celów projektowych przyjąć, że system musi obsłużyć co najmniej 200 użytkowników.
2. Przy każdych przejściach należy zaprojektować urządzenia umożliwiające otwarcie w sytuacji awaryjnej (np. pożaru) – należy dążyć do unikania projektowania urządzeń drogich w serwisowaniu opartych o akumulatory wymagające wymiany.

Wymagania w zakresie SSWiN

1. Projektant zaplanuje System tak, aby istniała możliwość jego rozbudowy o elementy SSWIN w późniejszych etapach rozwoju Systemu.

Wymagania w zakresie instalacji napadowej

1. Projektant zaplanuje w określonych pomieszczeniach przez Zamawiającego urządzenia pozwalające na sygnalizację napadu lub samego zagrożenia napadem. Sygnalizacja o wystąpieniu wezwania powinna powiadomić pracowników ochrony w budynku.

Inne wymagania

1. Projektant zaplanuje również kwestie energetyczne w zakresie podtrzymania zasilania dla elementów Systemu na co najmniej 120 minut w przypadku jego zaniku;

2009-7.262.12.2021

Załącznik nr 3 do zaproszenia

- PROJEKT UMOWY –

UMOWA Nr ...../...../2021

zawarta w dniu **października 2021** roku pomiędzy:
Prokuraturą Regionalną w Szczecinie z siedzibą w Szczecinie przy ul. Adama Mickiewicza 153, (71-260 Szczecin), posiadającą numer NIP: 852-261-92-28, posiadającą numer REGON: 363868183, reprezentowaną przez:

Artura Maludy - Prokuratora Regionalnego
Zwaną dalej **Zamawiającym**

a

Zwaną dalej **Wykonawcą**

W wyniku przeprowadzonego postępowania o udzielenie zamówienia publicznego, do którego z uwagi na wartość zamówienia nie stosuje się ustawy z dnia 11 września 2019 r. - Prawo Zamówień Publicznych (tj. Dz. U. z 2021 r. poz. 1129 z późn. zm.), została zawarta umowa następującej treści:

§ 1.

1) Wykonawca zobowiązuje się do wykonania dokumentacji projektowo- kosztorysowej modernizacji istniejącego systemu bezpieczeństwa, który realizował będzie funkcje SSWiN, SKD, CCTV, antynapadowe w budynku Prokuratury Regionalnej w Szczecinie przy ul. Mickiewicza 153. Przedmiot zamówienia jest realizowany w formie opracowania dokumentacji projektowo kosztorysowej wraz z pełnieniem nadzoru autorskiego.
2) Wykonawca zobowiązuje się do opracowania dokumentacji projektowej zgodnie z Rozporządzeniem Ministra Infrastruktury z dnia 02.09.2004r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego (t.j. Dz.U. 2013, poz. 1129), z obowiązującymi Polskimi Normami, aktualnym poziomem wiedzy technicznej oraz ustaleniami określonymi w wymaganych warunkach technicznych i decyzjach administracyjnych.
3) Projekt Systemu musi być wykonany w oparciu o wymagania norm:
   a) - PN-EN 50131-1 Systemy Alarmowe. Systemy Sygnalizacji Włamania i Napadu,
   b) - PN-EN 50133-1 Systemy Alarmowe. System Kontroli Dostępu.
4) Wykonawca przeprowadzi audyt obecnie funkcjonującego systemu alarmowego celem zapoznania się z używanym rejestratorem, okablowaniem, rodzajem używanych kamer oraz czujek. Na bazie tej wiedzy określi, które z wymienionych składowych systemu będzie możliwe uwzględnić w projekcie. Dobór rozwiązań technicznych każdego systemu zostanie uzgodniony z Zamawiającym po zawarciu umowy w formie protokołu uzgodnień, przy czym projektując system uwzględnione zostaną możliwości finansowe Zamawiającego, a także koszty eksploatacyjne systemu po jego instalacji.
5) Na dokumentację będącą przedmiotem zamówienia składać się będzie:
   a) dokumentacja projektowa opisowa wraz z częścią rysunkową,
   b) 2 egzemplarze w wersji drukowanej oraz 1 egz. w wersji elektronicznej w formacie .pdf
   c) kosztorys i przedmiar w formie elektronicznej: .pdf
6) Po zawarciu umowy Zamawiający udostępni rzuty kondygnacji budynku, w których instalowane będą systemy. Zamawiający jest w posiadaniu dokumentacji powykonawczej, którą w razie konieczności udostępni wybranemu wykonawcy celem realizacji przedmiotu zamówienia.

7) Przed przystąpieniem do opracowania koncepcji rozwiązań projektowych, Wykonawca zobowiązany jest do oględzin obiektu z przedstawicielem Zamawiającego w celu dokonania ustaleń z Użytkownikiem końcowym obiektu. Koncepcję zaproponowanych rozwiązań projektowych dla każdej części dokumentacji Wykonawca powinien bezwzględnie pisemnie uzgodnić z Zamawiającym przed przystąpieniem do projektowania szczegółów. W celu uzgodnienia, Wykonawca powinien przedłożyć Zamawiającemu w wersji papierowej i elektronicznej zaproponowany wariant rozwiązań oparty na opisie przedmiotu zamówienia.
8) Termin uzgodnienia przez Zamawiającego koncepcji rozwiązań projektowych wynosi do 7 dni od daty wpływu dokumentacji koncepcji do Zamawiającego. Termin ten pozostaje bez wpływu na termin realizacji zamówienia, o którym mowa w § 3 umowy.
9) Każda część dokumentacji projektowo – kosztorysowej powinna być pisemnie uzgodniona z Zamawiającym pod względem rozwiązań technicznych. W tym celu Wykonawca powinien przedłożyć Zamawiającemu w wersji papierowej i elektronicznej po jednym egzemplarzu każdej części dokumentacji projektowo – kosztorysowej. Termin uzgodnienia przez Zamawiającego dokumentacji projektowo – kosztorysowej wynosi do 7 dni od daty wpływu dokumentacji do Zamawiającego. Termin ten pozostaje bez wpływu na termin realizacji zamówienia, o którym mowa w § 3 umowy.

§2

1) Wykonawca zobowiązuje się do traktowania jako poufne dokumentów oraz informacji dotyczących Zamawiającego oraz przedmiotu niniejszej umowy uzyskanych w związku z jej wykonywaniem oraz do ich nieujawniania osobom trzecim, zarówno w trakcie realizacji umowy, jak i po jej zakończeniu, za wyjątkiem osób, których udział w realizacji przedmiotu umowy jest niezbędny, przy czym ujawnienie tych informacji powinno zostać poprzedzone przeszkoleniem tych osób w zakresie obowiązku poufności, a nadto osoby te powinny przed przystąpieniem do realizacji umowy podpisać oświadczenie w przedmiocie obowiązku poufności, stanowiące załącznik nr 4 do umowy. Wykonawca zobowiązany jest dostarczyć podpisane oświadczenia Zamawiającemu przed terminem rozpoczęcia wykonywania czynności przez poszczególne osoby.
2) Za informacje poufne uważa się wszelkie informacje pisemne lub ustne, a także zapisane na nośnikach informacji odnoszące się do Stron umowy, w szczególności techniczne, know-how, organizacyjne, finansowe, prawne i inne mające wartość ekonomiczną, jak i informacje uzyskane w toku analizowania lub przetwarzania informacji udostępnionych, niezależnie od sposobu w jaki zostały udostępnione Stronie lub osobie trzeciej działającej w imieniu Strony przed jak i po dacie niniejszej umowy, z wyłączeniem informacji lub danych:
   a) które są publicznie dostępne bez naruszania niniejszej umowy,
   b) które zostaną ujawnione przez stronę otrzymującą po uprzednim uzyskaniu pisemnej zgody.
3) Wykonawca ponosi odpowiedzialność za wszelkie przypadku naruszenia poufności, w tym także dokonane przez swoich pracowników lub osoby świadczące na rzecz Wykonawcy usługi na podstawie umów cywilnoprawnych.
4) W przypadku ujawnienia osobom nieuprawnionym informacji poufnych przez Wykonawcę lub osoby za które ponosi on odpowiedzialność, Wykonawca zapłaci na rzecz Zamawiającego karę umowną w wysokości 20% wynagrodzenia brutto, o którym mowa w § 4 ust. 1 za każde naruszenie.

§3

1) Umowa zostaje zawarta na czas określony, tj. od dnia października 2021 r. do dnia grudnia 2022 r.
2) Dokumentację projektową Wykonawca przekaże protokolarnie Zamawiającemu w terminie **28 dni od daty zawarcia umowy.**
3) Zamawiający dokonuje protokolarnego przyjęcia przedłożonej dokumentacji w terminie 4 dni od daty protokołu przekazania, przy czym jeśli dokumentacja ma wady spisuje protokół i wyznacza termin usunięcia stwierdzonych braków i/lub usterek. Sporządzony protokół Zamawiający przekazuje Wykonawcy.

§4

1) Za wykonanie przedmiotu umowy strony ustaliły ryczałtowe wynagrodzenie miesięczne w wysokości ..... **zł brutto** (słownie: ..... 00/100).
2) Ustalone wynagrodzenie obejmuje wszystkie należne podatki, opłaty i zaspokaja wszystkie roszczenia Wykonawcy z tytułu wykonywania niniejszej umowie.
3) Rozliczenie za wykonanie przedmiotu niniejszej umowy nastąpi na podstawie faktury wystawionej po wykonaniu usługi w danym miesiącu.
4) Należne Wykonawcy wynagrodzenie płatne będzie przelewem na konto Wykonawcy, na podstawie prawidłowo wystawionej faktury, w terminie 30 dni od daty jej wystawienia.

§5

1. Wykonawca oświadcza, że
   c) Przysługują mu autorskie prawa majątkowe do przedmiotu umowy stanowiącego dokumentację projektowo- kosztorysową modernizacji istniejącego systemu bezpieczeństwa u Zamawiającego, zwanego dalej utworem;
   d) autorskie prawa majątkowe do utworu nie są w żaden sposób ograniczone ani obciążone na rzecz osób trzecich;
   e) Przeniesienie na Zamawiającego autorskich praw majątkowych nie narusza jakichkolwiek praw osób trzecich.
2. Wykonawca przenosi na Zamawiającego majątkowe prawa autorskie do utworu w zakresie wszystkich znanych w chwili zawarcia umowy pól eksploatacji, a w szczególności:
   a) w zakresie utrwalania i zwielokrotniania utworu – wytwarzanie określoną techniką egzemplarzy utworu, w tym techniką drukarską, reprograficzną oraz techniką cyfrową;
   b) w zakresie obrotu oryginałem albo egzemplarzami, na których utwór utrwalono – wprowadzenie do obrotu, użyczenie lub najem oryginału albo egzemplarzy.
3. Strony postanawiają, że autorskie prawa majątkowe do utworu przechodzą na Zamawiającego w chwili wydania utworu.
4. Z chwilą wydania utworu Zamawiający nabywa prawo własności egzemplarza utworu oraz nośników, na których został utrwalony.
5. Wykonawca wyraża zgodę na dokonywanie przez Zamawiającego wszelkich zmian, uzupełnień i aktualizacji utworu.
6. Strony zgodnie oświadczają, iż wynagrodzenie, o którym mowa w § 4 ust. 1 umowy obejmuje również wynagrodzenie Wykonawcy z tytułu przeniesienia autorskich praw majątkowych na wszystkich wskazanych w umowie polach eksploatacji, w tym wyczerpuje w całości należności przysługujące Wykonawcy w związku z zawarciem niniejszej umowy, z tytułu korzystania z utworu na wszystkich wskazanych polach eksploatacji, z tytułu przeniesienia prawa własności egzemplarza utworu oraz nośników, na których utwór został utrwalony oraz za udzielenie zgody na wykonywanie praw zależnych, a także z tytułu pełnienia nadzoru autorskiego.
7. Wykonawca zezwala Zamawiającemu na wykonywanie zależnych praw autorskich do opracowań utworu oraz przenosi na nabywcę wyłączne prawo zezwalania na wykonywanie zależnych praw autorskich.
8. Zamawiający nie jest zobowiązany do każdorazowego oznaczania autorstwa utworu/egzemplarza utworu.

§6

1. Wykonawca zapłaci Zamawiającemu karę umowną:
   a) za zwłokę w wykonaniu przedmiotu umowy - w wysokości 10 % wynagrodzenia brutto, o którym mowa w § 4 ust. 1 za każdy rozpoczęty dzień opóźnienia,
   b) za zwłokę w okresie gwarancji - w wysokości 1% wynagrodzenia brutto, o którym mowa w § 4 ust. 1 za każdy rozpoczęty dzień zwłoki liczony od dnia wyznaczonego na usunięcie wad,
   c) za odstąpienie od umowy z przyczyn zawinionych przez Wykonawcę - w wysokości wynagrodzenia brutto, o którym mowa w § 4 ust. 1.
2. Jeżeli wysokość zastrzeżonych kar umownych nie pokrywa poniesionej szkody strony mogą dochodzić odszkodowania uzupełniającego na zasadach ogólnych.

3. Kary umowne mogą być potrącane przez Zamawiającego z przysługującego Wykonawcy wynagrodzenia brutto, na co Wykonawca wyraża zgodę.
4. Kary umowne są niezależne od siebie i kumulują się.

§7

1) Zamawiającemu przysługuje prawo rozwiązania umowy w trybie natychmiastowym:
a) gdy zostanie ogłoszona likwidacja firmy Wykonawcy,
b) zostanie wydany nakaz zajęcia majątku Wykonawcy,
c) Wykonawca nie rozpoczął realizacji umowy bez uzasadnionej przyczyny,
d) Zamawiający poniósł szkodę w wyniku działania lub zaniechania Wykonawcy;
e) Wykonawca w sposób nienależyty realizuje przedmiot umowy.
2) Zamawiający może odstąpić od umowy w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, w terminie 30 dni od powzięcia wiadomości o tych okolicznościach.
3) Rozwiązanie umowy oraz odstąpienie od umowy, powinno nastąpić w formie pisemnej i powinno zawierać uzasadnienie pod rygorem nieważności takiego oświadczenia.
4) W przypadku wypowiedzenia lub odstąpienia od umowy, Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu faktycznie wykonanej części umowy.

§8

1. Wykonawca udziela Zamawiającemu gwarancji jakości na przedmiot umowy. Wykonawca jest odpowiedzialny względem Zamawiającego za wady przedmiotu umowy istniejące w czasie jego wydania oraz za wady powstałe po jego przyjęciu, lecz z przyczyn tkwiących w przedmiocie umowy w chwili wydania, zmniejszające jego wartość lub użyteczność ze względu na cel oznaczony w umowie albo wynikający z przeznaczenia. Wykonawca odpowiada w szczególności za rozwiązania przyjęte w przedmiocie umowy niezgodnie zobowiązującymi normami i przepisami, za nieprzydatność przedmiotu umowy dla realizacji celu, jakiemu służy lub jego niewłaściwość czy nieodpowiedniość.
2. Zamawiający nie jest zobowiązany do sprawdzania przedmiotu umowy pod względem jego zgodności z obowiązującymi normami i przepisami oraz pod względem kompletności, a tym samym Wykonawca nie może zwolnić się z odpowiedzialności za nieprawidłowość i niekompletność wykonanego przedmiotu umowy.
3. Gwarancja jakości obowiązuje przez okres 24 **miesięcy** od chwili podpisania przez strony protokołu odbioru końcowego bez zastrzeżeń.
6. W okresie gwarancji Wykonawca zobowiązuje się do usunięcia usterek w terminie 7 dni od dnia zgłoszenia wady przez Zamawiającego.

§ 9

Zgodnie z art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej RODO, informuję, że:
1. Administratorem , w rozumieniu art. 4 pkt 7 RODO, danych osobowych jest Prokuratura Regionalna w Szczecinie z siedzibą przy ul. Mickiewicza 153, 71 – 260
w Szczecinie, tel. 91 441 09 79, e-mail. sekretariat@szczecin.pr.gov.pl.
2. Dane kontaktowe inspektora ochrony danych: tel. 91 441 09 72, e-mail iod@szczecin.pr.gov.pl
3. Podstawę prawną przetwarzania danych stanowi art.6 ust.1 lit. c) RODO w związku z przepisami ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021r. poz. 1129 t.j.), zwanej dalej ustawą PZP.
4. Dane osobowe przetwarzane będą w celu związanym z niniejszym postępowaniem
o udzielenie zamówienia publicznego i jego późniejszą realizacją (w tym zawarciem umowy lub udzieleniem zlecenia/zamówienia).

5. Dane osobowe są przechowywane przez okres nie dłuższy niż jest to niezbędne do realizacji celów, w których są przetwarzane, a po tym czasie przez okres oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa, w szczególności zgodnie z Zarządzeniem Nr 84/16 Prokuratora Generalnego z dnia 29 grudnia 2016 r. w sprawie wprowadzenia jednolitego rzeczowego wykazu akt powszechnych jednostek organizacyjnych prokuratury oraz przepisami określającymi zasady przechowywania przez zamawiających dokumentacji w sprawach związanych z postępowaniem o udzielenie zamówienia publicznego.
6. Dane osobowe mogą być przekazywane innym podmiotom, które będą je przetwarzały, w szczególności: osobom lub podmiotom, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy PZP, podmiotom prowadzącym działalność pocztową, kurierską, bankom, a w przypadku konieczności prowadzenia rozliczeń, organom państwowym lub innym podmiotom uprawnionym na podstawie przepisów prawa, celem wykonania ciążących na nas obowiązków (Urząd Skarbowy, PIP, ZUS), podmiotom wspierającym Administratora w prowadzonej działalności na jego zlecenie, w szczególności radcom prawnym, podmiotom świadczącym usługi ochrony oraz dostawcom zewnętrznych systemów wspierającym naszą działalność.
7. Osobie, której dane są przetwarzane przysługuje prawo:
a) na podstawie art. 15 RODO żądania od administratora dostępu do danych osobowych;
b) na podstawie art. 16 RODO żądania od administratora sprostowania lub uzupełnienia danych osobowych;
c) na podstawie art. 18 RODO żądania od administratora ograniczenia przetwarzania danych osobowych;
wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
8. Administrator informuje, że przepisy ustawy PZP ograniczają prawo do skorzystania:
- ze sprostowania lub uzupełnienia danych (art. 16 RODO), jeżeli zrealizowanie tego prawa mogłoby skutkować zmianą wyniku postępowania o udzielenie zamówienia lub zmianą postanowień umowy w sprawie zamówienia publicznego w zakresie niezgodnym z ustawą PZP;
- z ograniczenia przetwarzania (art. 18 RODO), które nie może zostać zrealizowane do czasu zakończenia tego postępowania, z zastrzeżeniem przypadków określonych w art. 18 ust. 2 RODO.
9. Osobie, której dane są przetwarzane nie przysługuje prawo:
a) usunięcia danych osobowych – art. 17 ust. 3 lit. b, d lub e RODO;
b) przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
c) wniesienia sprzeciwu wobec przetwarzania danych osobowych, o którym mowa w art. 21 RODO, gdyż podstawą prawną przetwarzania danych osobowych jest art. 6 ust. 1 lit. c RODO.
10. W celu skorzystania z praw, o których mowa w pkt 7 ppkt 1-3 należy skontaktować się z administratorem lub inspektorem ochrony danych, korzystając ze wskazanych wyżej danych kontaktowych.
11. Podanie danych jest dobrowolne, niemniej ich niepodanie skutkować będzie brakiem możliwości udziału w postępowaniu o udzielenie zamówienia publicznego, o którym mowa w pkt. 4.
12. Administrator nie dokonuje zautomatyzowanego podejmowania decyzji, w tym profilowania, o którym mowa w art. 22 RODO.
13. Jednocześnie Zamawiający przypomina o ciążącym na Państwie obowiązku informacyjnym wynikającym z art. 14 RODO względem osób fizycznych, których dane przekazane zostaną Zamawiającemu w związku z prowadzonym postępowaniem i które Zamawiający pośrednio pozyska od wykonawcy biorącego udział w postępowaniu, chyba że ma zastosowanie co najmniej jedno z wyłączeń, o których mowa w art. 14 ust. 5 RODO.
14. Umowa nie obejmuje swoim zakresem przetwarzania danych osobowych pracowników Zamawiającego w rozumieniu przepisów o ochronie danych osobowych i nie przewiduje takich działań.

§ 10

1) Zamawiający nie przewiduje indeksacji cen i udzielenia zaliczki.
2) Zamawiający nie wyraża zgody na przelew wierzytelności z niniejszej umowy na osobę trzecią.
3) Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.
4) Wykonawca zobowiązany jest do pisemnego informowania Zamawiającego o każdej zmianie swojej siedziby, konta bankowego, nr tel. oraz nr NIP i REGON-u.
5) Nie stanowi zmiany umowy:
6) zmiana danych związanych z obsługą administracyjno-organizacyjną umowy (np. zmiana nr rachunku bankowego)
7) zmiana danych teleadresowych, zmiany osób wskazanych do kontaktów między Stronami.
8) Ewentualne spory, jakie mogą wyniknąć w związku z wykonywaniem niniejszej umowy, strony będą w pierwszej kolejności rozstrzygać polubownie w drodze negocjacji.

9) Sprawy sporne nie rozstrzygnięte polubownie strony poddają orzecznictwu sądom powszechnym właściwym miejscowo dla siedziby Zamawiającego.
10) W sprawach nie uregulowanych niniejszą umową stosuje się przepisy powszechnie obowiązujące.
11) Załączniki stanowią integralna część niniejszej umowy.
12) Umowa sporządzona została w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

WYKONAWCA: **ZAMAWIAJĄCY:**

Załączniki do umowy:
Załącznik nr 1: Formularz ofertowy (kserokopia Wykonawcy)
Załącznik nr 2: Opis przedmiotu zamówienia
Załącznik nr 3: Wytyczne dot. zabezpieczenia technicznego
Załącznik nr 4: Oświadczenie o zachowaniu poufności danych

2009-7.262.12.2021

Szczecin,
dnia.....2021 r.

OŚWIADCZENIE

Ja niżej podpisany, ...legitymująca/y się dowodem osobistym nr ....., oświadczam, że:

- zobowiązuję się do zachowania w poufności wszelkich informacji , które pozyskam w toku realizacji umowy zawartej na skutek przeprowadzonego postępowania nr 2009-7.262.12.2021 na usługę: Wykonania dokumentacji projektowo-kosztorysowej wraz z pełnieniem nadzoru autorskiego dla zadania *Modernizacja systemu bezpieczeństwa który realizował będzie funkcje SSWiN, SKD, CCTV, ANTY-NAPADOWE w budynku Prokuratury Regionalnej w Szczecinie przy ul. Mickiewicza 153*, zarówno w trakcie realizacji umowy, jak i po jej zakończeniu;
- zapoznałam/ em się z przepisami o ochronie danych osobowych, a także bezpieczeństwa informacji, tj. Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych, ustawą z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,

.....
(Podpis osoby składającej oświadczenie)

2009-7.262.12.2021

Załącznik nr 4 do zaproszenia

WYTYCZNE DOTYCZĄCE ZABEZPIECZENIA TECHNICZNEGO

Wszystkie rozwiązania systemu kontroli dostępu (SKD) muszą być uzgodnione z rzeczoznawcą ds. zabezpieczeń przeciwpożarowych a wprowadzone rozwiązania nie mogą utrudniać ewakuacji osób i mienia.

Zastosowany system powinien być zgodny z zaleceniami normy PN-EN 60839-11-1 *Systemy alarmowe i elektroniczne systemy zabezpieczeń, część 11-J: Elektroniczne systemy kontroli dostępu, wymagania dotyczqce systemów i komponentów.* System kontroli dostępu jako minimalne powinien spełniać wymagania stopnia 2. Zaleca się stosowanie systemu spełniającego wymagania stopnia 3. Wymagania powinny zostać sformułowane w drodze analizy zagrożeń przeprowadzonej dla każdego obiektu.

Wprowadzone i już funkcjonujące w budynku prokuratury SKD nie spełniające wymagań, należy dostosowywać uwzględniając te wytyczne w trakcie planowanych lub prowadzonych prac modernizacyjnych.

System musi zawierać możliwość integracji z systemem rejestracji czasu pracy w postaci automatycznego eksportu zdarzeń oraz spełniać wymagania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych - RODO, w zakresie anonimizacji danych osobowych (zalecana automatyczna anominizacja).

Poniższe wymagania mogą być stosowane jako wytyczne i nie zastępują specyfikacji technicznej, która musi być dostosowana do struktury architektonicznej, organizacyjnej oraz uwarunkowań innych systemów teletechnicznych dla każdego obiektu.

Wymagania techniczne systemu kontroli dostępu.

1. **Interfejs użytkownika.**
    a. ***Tożsamość:***

Podstawowym nośnikiem tożsamości w SKD powinien być identyfikator w postaci karty wykonanej w technologii zapewniającej szyfrowanie informacji na karcie oraz szyfrowaną transmisję z czytnikiem.

W normalnym trybie działania system powinien wykorzystywać do rozpoznania pełną

informację identyfikatora (kod obiektu i numer karty lub niepowtarzalny numer karty).

W awaryjnym trybie pracy system może wykorzystywać do rozpoznania jedynie część informacji identyfikatora (np. tylko kod obiektu).

Numer identyfikacyjny identyfikatora dający się odczytać z identyfikatora nie może być bezpośrednią reprezentacją pełnego kodowania.

W przypadku wykorzystania rozpoznania za pomocą, informacji zapamiętanej w połączeniu z identyfikatorem lub biometryką, informacja zapamiętana (kod PIN) wymaga minimum 4 cyfr. System powinien umożliwiać wykorzystanie czytników biometrycznych. W systemie można stosować wyłącznie czytniki pozwalające na rozpoznanie żywego organizmu. Współczynnik błędnych akceptacji określony na podstawie dokumentacji dostarczonej przez producenta nie powinien być niższy niż 0,3%[1].

b. ***Wymagania dotyczące rozpoznania tożsamości:***

System powinien umożliwiać przyznawanie praw dostępu grupie danych identyfikacyjnych i powinien umożliwiać zmianę, praw dostępu grupy danych identyfikacyjnych.

c. ***Czytniki kontroli dostępu powinny spełniać następujące wymagania:***

- wykorzystywać protokół Wiegand-37 lub dłuższy do komunikacji,
- odporny na działanie czynników atmosferycznych, minimum IP55,
- częstotliwość pracy 13,5 6MHz,
- kodowana transmisja danych pomiędzy czytnikiem i kartą, klucz kodowania 64 bit,
- audiowizualna sygnalizację stanu drzwi (buzzer i/lub diody LED). .
- zabezpieczenie przed odwrotną polaryzacją styków zasilających.

2. Kontroler, Interfejs przejścia kontrolowanego,

SKD powinien mieć wyjścia zdolne do sterowania elektromagnesów drzwiowych, zaczepów elektrycznych, aktywatorów montowanych w ościeżnicy, rygli sterowanych elektrycznie, hydraulicznie albo pneumatycznie i/lub innych typów zamków elektromechanicznych oraz elektrycznych dźwigni przeciwpanicznych.

System powinien umożliwić dostęp przyznany warunkowo zależnie od stanu danych identyfikacyjnych (zablokowany, zawieszony, unieważniony).

Kontrolery (sterowniki) współpracujące z czytnikami danych oraz pozostałymi elementami (zamki elektryczne, zwory, rygle, szlabany, triody, bramki, przyciski, czujniki stanu drzwi itp.) powinny posiadać możliwość pracy w trybie sieciowym (ON-LINE) i autonomicznym (OFF-

[1] Zasadność wykorzystania biometrykl w SKD należy do decyzji każdego administratora budynku, jednak w obecnej chwili wskazane jest, aby systemy były przygotowane na taką ewentualność, na poziomie zapewniającym odpowiednie bezpieczeństwo przechowywanym danym biometrycznym.

LINĘ - samodzielna praca kontrolerów SKD tj. bez komunikacji z serwerem, w oparciu o posiadane dane konfiguracyjne w pełnym zakresie funkcjonalnym, buforowanie i rejestracja w pamięci nieulotnej zdarzeń do momentu odzyskania komunikacji z serwerem - wielkość bufora, co najmniej 16000 zdarzeń w każdym sterowniku[2]. Praca w trybie autonomicznym każdego kontrolera (sterownika) powinna zapewniać zachowanie w pamięci nieulotnej uprawnień w zakresie dostępu dla użytkowników, oraz pozostałych parametrów związanych z działaniem kontrolowanego przejścia,

Każdy kontroler winien być wyposażony w dualną pamięć umożliwiającą wykonanie synchronizacji danych kontrolera z serwerem bez konieczności blokowania urządzań SKD (drzwi, kołowrotów, szlabanów) i użytkowników. Jeden kontroler (sterownik) powinien obsługiwać maksymalnie 1 przejście np, drzwi, tripod, bramkę, szlaban bez względu na to czy jest to przejście jedno- (jeden czytnik) czy dwustronnie kontrolowane (dwa czytniki).

Obudowa kontrolera (sterownika) powinna uniemożliwiać bezpośredni dostęp osobom nieuprawnionym. Kontroler winien posiadać możliwość wyposażenia go w dodatkowe wejścia/ wyjścia cyfrowe umożliwiające współpracę z innymi elementami. SKD powinien zapewniać realizacji funkcji antypassback. Obszary kontrolowane, dla których włączona będzie funkcja antypassback muszą posiadać zdefiniowane czytniki wyjścia. Użytkownicy opuszczający obszar kontrolowany mają obowiązek użycia karty. Ponowne wejście do obszaru kontrolowanego bez uprzedniego zarejestrowania wyjścia nie będzie możliwe.

3. **Konsola obsługi,**

a. Wymagania w *zakresie sygnalizacji i powiadamiania:*

- sygnalizacja wizualna i/lub dźwiękowa stanu zarygłowania przejścia, aż do chwili przyznania dostępu,
- powiadamianie wizualne, gdy jest przyznany dostęp,
- rejestracja zdarzeń, gdy jest przyznany dostęp,
- powiadamianie wizualne, ostrzeganie i rejestracja zdarzeń, gdy odmowa dostępu nastąpiła w wyniku próby użycia przedawnionego identyfikatora,
- powiadamianie wizualne, ostrzeganie i rejestracja zdarzeń w przypadku odmowy dostępu w wyniku konfigurowalnej liczby prób użycia uprawnionego identyfikatora z nieuprawnioną informacją zapamiętaną,
- możliwość śledzenia karty (wyświetlanie, rejestracja),

2liczba zdarzeń bufora w przypadku utraty połączenia z serwerem, powinna być dostosowana do możliwości reakcji na awarie w SKD. im dłuższy przewidywany czas reakcji i więcej zdarzeń (przejść) tym bufor powinien być większy. Zaproponowane 16000 jest rozwiązaniem dla budynków o dużym nasileniu ruchu i możliwościach reagowania na awarię w przeciągu 24 godzin od wystąpienia.

- możliwość śledzenia czytnika (wyświetlanie, rejestracja),

Wszystkie zmiany inicjowane przez operatora powinny być rejestrowane z uwzględnieniem: typu, ID operatora, czasu i daty wystąpienia.

b. Program nadzorczy systemu kontroli dostępu powinien zapewniać:

- możliwość ograniczania praw dostępowych - okres ważności karty,
- możliwość podglądu ruchu osobowego na wybranych przejściach w trybie on-line, dla wybranych typów zdarzeń (alarmowych) oraz przejść,
- współpracować ze skanerem dowodów osobistych i paszportów, dla kart gości,
- umożliwiać definiowanie kart dla gości, kart jednodniowych, kart okresowych,
- umożliwiać generowanie raportów ewakuacyjnych z uwzględnieniem ostatniej lokalizacji wszystkich pracowników i zarejestrowanych gości, obecnych na terenie budynku sądu,
- umożliwiać integrację z systemem depozytorów kluczy.

4. **Wymagania dotyczące zasilania**

Centrala kontroli dostępu powinna być wyposażona w rezerwowe źródło zasilania zdolne do obsługi centrali i jej akcesoriów w określonych warunkach pełnego obciążenia przez czas min. 2 godzin[3]. Warunki obciążenia nie dotyczą konsoli obsługi ani aktywatorów przejścia kontrolowanego.

5. **Elementy zabezpieczenia mechanicznego (kołowroty, bramki itp.) powinny spełniać następujące wymagania:**

- potwierdzenie pełnego obrotu w SKD,
- wspomaganie przejścia,
- blokada przed ruchem powrotnym,
- przycisk ewakuacyjny z sygnalizacją led potwierdzającą użycie,
- użycie przycisku ewakuacyjnego odnotowane zostaje w SKD,
- drzwi objęte kontrolą dostępu powinny być wyposażone w czujniki kontaktu potwierdzające otwarcie drzwi (np. kontaktrony),

6. **Dodatkowe funkcje, które powinien zapewniać system kontroli dostępu:**

Pełna otwartość sprzętowa i programowa tj.

- możliwość dodawania kolejnych urządzeń w związku z rozbudową systemu,
- możliwość definiowania, dodawania oraz integracji z innymi urządzeniami związanych z automatyczną identyfikacją,
- możliwość integracji fragmentów systemu w sieciach LAN / WAN tj,
    - jednolite zarządzanie elementami systemu rozmieszczonymi w różnych punktach,

---

3Czas pracy w przypadku awarii zasilania należy dostosować do możliwości reakcji na awarię.

- możliwość obsługi dowolnej liczby obiektów.

- architektura oprogramowania typu Klient - Serwer,
- zabezpieczenie przed wczytywaniem niezaprogramowanych kart (np. kart płatniczych, urządzeń NFC).

7, Integracja z systemem Rejestracji Czasu Pracy (RCP)

W związku z projektem wdrożenia w prokuraturze systemu RCP w specyfikacji technicznej kontroli dostępu należy uwzględnić fałd, że funkcjonalność systemu RCP w zakresie ewidencjonowania i rozliczania czasu pracy zostanie zaimplementowana do Zintegrowanego Systemu Rachunkowo Kadrowego (ZSRK) a co za tym idzie wymiana danych będzie następowała pomiędzy SKD i ZSRK za pośrednictwem szyny danych.

W celu zapewnienia wymiany odpowiednich danych w specyfikacji technicznej SKD należy uwzględnić poniższe informacje:

a) ***Minimalne zdarzenia, które system ZSRK będzie mógł przyjmować po wdrożeniu „Rozliczania czasu pracy"[1];***

- Rodzaj zdarzenia czasowego:
    - Kod Nazwa (maksymalnie 25 znaków)
    - PIO Wejście
    - P15 Wyjście na przerwę
    - P20 Wyjście
    - P30 Wyjście służbowe

b) ***SKD nie będzie poddawał danych agregacji.***

- Dane powinny zawierać:
    - Kod zdarzenia (słownik: P10, P15, P20, P3 0),
    - Numer karty (maksymalnie 8 znaków numerycznych np. 00239223),
    - Data zdarzenia (data w formacie RRRRMMDD),
    - Czas zdarzenia (godzina, minuta, sekunda w formacie HHMMSS),

c) ***Dane z SKD mają być przekazywane postaci pliku.***

- Plik o strukturze jak w punkcie 1,
- plik w formacie ,txt lub .csv. Kolumny rozdzielone średnikiem (znakiem średnika „;"),
- kolejne kolumny powinny zawierać informacje:
    - Kod zdarzenia (słownik: PIO, P15, P20, P30),
    - Numer karty (maksymalnie 8 znaków numerycznych np. 239223),
    - Data zdarzenia (data w formacie RRRR-MM-DD),
    - Czas zdarzenia (godzina, minuta, sekunda w formacie HH:MM:SS),

d) Udostępnienie bazy danych w SKD, ma się odbywać w formie Online za pośrednictwem

szyny danych. Zgodnie z wypracowanym zestawem konwencji integracyjnych cała komunikacja w pierwszej kolejności powinna odbywać się w oparciu o WebService'y eksponowane SOAPem 1.1 na chwilę obecną. Komunikacja pomiędzy SKD a szyną powinna następować przez WebSeryice. Pomiędzy szyną danych a ZSRK również przez WebService.

e) SKD powinien dawać możliwość automatycznej wymiany Online lub w odstępach czasowych, które można zdefiniować na poziomie prokuratury. SKD powinien sam inicjować wysłanie danych na szynę danych bez zapytania ze strony ZSRK.

8. Dodatkowe informacje:

- w nowo budowanych systemach kontroli dostępu należy stosować do komunikacji protokół OSDP (np. AES 128.),