



PROGRAM FUNKCJONALNO - UŻYTKOWY

ZAMAWIAJACY: Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego
ul. gen. Sylwestra Kaliskiego 2
00-908 Warszawa 49, skr. poczt. 50
NIP: 527-020-63-00
REGON: 012122900
tel. 261 839 041
fax. 261 839 179
www.wat.edu.pl

NAZWA ZADANIA: „Budowa systemu kontroli dostępu na obszarze Wojskowej Akademii Technicznej wraz z przebudową wejść na teren Studium Wychowania Fizycznego w formule „zaprojektuj i wykonaj”.

BRANŻA: Budowlana, sanitarna, elektryczna, teletechniczna.

ADRES OBIEKTU: ul. gen. Sylwestra Kaliskiego 2
00-908 Warszawa, Dzielnica Bemowo

KOD CPV:

| | |
|------------|---|
| 42961100-1 | Systemy kontroli dostępu. |
| 35121000-8 | Urządzenia bezpieczeństwa |
| 35120000-1 | Systemy nadzoru i bezpieczeństwa |
| 31711310-0 | Roboty instalacyjne elektryczne |
| 45315600-4 | Karty magnetyczne do kontroli dostępu |
| 45312200-9 | Instalowanie systemów alarmowych i antywłamaniowych |
| 51110000-6 | Usługi instalowania sprzętu elektrycznego |
| 72260000-6 | Usługi wdrażania oprogramowania |
| 31700000-3 | Urządzenia elektroniczne |
| 30237110-0 | Czytniki kart magnetycznych |

DATA OPRACOWANIA: 28.10.2025 r.

| Wyszczególnienie | Imię i nazwisko | Podpis |
|--|-------------------|-------------------|
| 1 | 2 | 3 |
| Przygotował | mjr Cezary Rams | mjr Cezary RAMS |
| Przygotował | Krzysztof Dybicz | Krzysztof Dybicz |
| Przygotował | Ewa Malinowska | Malinowska Ewa |
| Sprawdził | Grzegorz Bobiński | Grzegorz Bobiński |
| Uzgodnił w zakresie budowlanym | Marek Kliszczyk | Marek Kliszczyk |
| Uzgodnił w zakresie instalacji telekomunikacyjnych | Ewa Kaczmarek | Ewa Kaczmarek |
| Uzgodnił w zakresie instalacji elektrycznych | Konrad Graboś | Konrad Graboś |
| Uzgodnił w zakresie sanitarnym | Adam Zajęzkowski | Adam Zajęzkowski |
| Uzgodnił w zakresie ppoż. | Sławomir Rapala | Sławomir Rapala |

Spis treści

| | | |
|------|---|----|
| 1. | WPROWADZENIE | 4 |
| 2. | ZAKRES PRZEDMOTU ZAMÓWIENIA | 5 |
| 2.1. | Zestawienie ilościowe | 5 |
| 2.2. | Stacje robocze wchodzących w zakres przedmiotu zamówienia..... | 5 |
| 2.3. | Stanowisko do personalizacji kart zbliżeniowych | 5 |
| 2.4. | Opis przejść podlegających modernizacji..... | 5 |
| | Schemat blokowy systemu kontroli dostępu..... | 8 |
| 3. | SPECYFIKACJA TECHNICZNA WARUNKÓW ZAMÓWIENIA | 9 |
| 3.1. | Przedmiot zamówienia..... | 9 |
| 3.2. | Zakres zamówienia | 9 |
| 3.3. | Wymagania dotyczące systemu kontroli dostępu | 10 |
| 3.4. | Wymagania dotyczące wykonania prac | 11 |
| 3.5. | Zakres prac budowlanych w obrębie przejścia nr 28..... | 12 |
| 3.6. | Wymagania dotyczące urządzeń systemu kontroli dostępu..... | 14 |
| 3.7. | Wymagania funkcjonalne systemu kontroli dostępu | 18 |
| 3.8. | Bezpieczeństwo i redundancja systemu | 21 |
| 3.9. | Wymagania dla SKD w zakresie ochrony danych..... | 21 |
| 4. | INTEGRACJA SYSTEMU KONTROLI DOSTĘPU Z INNYMI SYSTEMAMI..... | 22 |
| 4.1. | Integracja z systemami SSWiN, CCTV, SSP, depozytorem kluczy..... | 22 |
| 4.2. | Integracja w Lokalnym Centrum Nadzoru | 23 |
| 4.3. | Integracja SKD z bazą pośrednią systemów z danymi pracowników i studentów | 23 |
| 5. | ZAKRES DOKUMENTACJI..... | 24 |
| 6. | RÓWNOWAŻNOŚĆ | 25 |
| 7. | WIZJA LOKALNA | 25 |
| 8. | TERMIN REALIZACJI PRAC | 25 |
| 9. | WARUNKI GWARANCJI I SERWISU | 25 |

1. WPROWADZENIE

1. Podstawa prawną realizacji przedmiotu zamówienia jest ustawa z dnia 30.08.2024 Prawo zamówień publicznych (Dz. U. 2024 poz. 1320).
2. Przedmiot zamówienia należy wykonać w formule „zaprojektuj i wykonaj”.
3. Program Funkcjonalno – Użytkowy określa:
 - 1) podstawowe wymagania dla projektowanego przedmiotu zamówienia umożliwiające sporządzenie dokumentacji projektowej budowlanej i technicznej, na podstawie, której będzie można wykonać roboty budowlane spełniające oczekiwania Zamawiającego określone w niniejszym opracowaniu;
 - 2) wymagane zakresy robót;
 - 3) standardy Zamawiającego dotyczące wykonania przedmiotu zamówienia;
4. Projektant powinien przewidzieć rozwiązania, z zastosowaniem atestowanych urządzeń i instalacji, ich montażu wraz z uruchomieniem, zgodnego z wymaganiami DTR producenta, z zapewnieniem niezbędnego serwisu oraz konserwacji urządzeń i instalacji. Wszelkie niezbędne materiały, części zamienne i eksploatacyjne, użyte podczas serwisowania w/w. urządzeń i instalacji, w okresie obowiązywania gwarancji Wykonawcy, uwzględnione powinny być w zakresie ceny ofertowej, wraz z dostawą i montażem.
5. Ze względu na krytyczne znaczenie Systemu Kontroli Dostępu (SKD) w WAT i zachowania ciągłości jego działania, Zamawiający oczekuje właściwej wiedzy i doświadczenia od Wykonawcy realizującego usługę modernizacji wraz z dostawą niezbędnych urządzeń i oprogramowania.
6. Wykonawca powinien posiadać świadectwo bezpieczeństwa przemysłowego.
7. Wykonawca systemu powinien posiadać koncesję MSWiA na montaż, konserwację, naprawę systemu kontroli dostępu.
8. Poprawne działanie SKD wpływa bezpośrednio na ciągłość funkcjonowania / realizację zadań instytucji zlokalizowanych na terenie kompleksu WAT. Zamawiający oczekuje wykonania przedmiotu umowy przez Wykonawcę w sposób gwarantujący zapewnienie wysokiego poziomu niezawodności i ciągłej dostępności SKD.
9. Przed realizacją zadania Wykonawca przekaże do Działu Informatyki (DIN) i Sekcji Ochrony Obiektów (SOO) do uzgodnienia dokumentację techniczną, na podstawie, której zostanie wykonana realizacja. Dokumentacja techniczna musi być zgodna z aktualnymi:
 - 1) „Warunkami do projektowania i budowy sieci strukturalnych dla potrzeb systemów w Wojskowej Akademii Technicznej” (<https://www.wojsko-polskie.pl/wat/regulacje-it/>);
 - 2) Wymaganiami eksploatacyjno-technicznymi dla XIX grupy SpW – Systemy i urządzenia specjalistyczne do ochrony obiektów;
 - 3) Instrukcją o ochronie obiektów wojskowych i konwojowanego mienia DU-3.14.3 (A).
10. Ze względu na krytyczną infrastrukturę obiektu przewidziany jest najwyższy poziom bezpieczeństwa, zastosowanie certyfikowanych urządzeń systemu kontroli dostępu zdefiniowanych w klasie 3 wg. normy PN-EN-60839-11.
11. W trakcie realizacji:
 - 1) Wykonawca zapewni obecność Kierownika Robót Branży: Budowlanej, Telekomunikacyjnej, Elektrycznej z uprawnieniami budowlanymi do kierowania robotami bez ograniczeń w każdej realizowanej branży;
 - 2) Wykonawca powinien dysponować osobami posiadającymi uprawnienia do projektowania bez ograniczeń w każdej z występujących branż;

- 3) Wszystkie prace należy wykonać pod nadzorem inspektorów WAT właściwych dla określonych branż;
- 4) Wykonawca przygotowuje szczegółowe Specyfikacje Techniczne Wykonania i Odbioru Robót (STWiOR) zgodnie z zakresem ujętym w dokumentacji projektowej zatwierdzonej przez Zamawiającego;
- 5) Wykonawca opracuje informację dotyczącą Bezpieczeństwa i Ochrony Zdrowia dla przedmiotowych robót budowlanych (prześle Zamawiającemu w formacie doc i pdf);
- 6) Wykonawca zaktualizuje Instrukcję Bezpieczeństwa Pożarowego (w przypadku, gdy będzie wymagana) i prześle Zamawiającemu w formacie doc i pdf;
- 7) Zamawiający wymaga sprawowania nadzoru autorskiego nad realizacją zadania (koszt nadzoru autorskiego po stronie Wykonawcy);
- 8) Zamawiający przewiduje organizację cotygodniowych koordynacji (uczestnictwo Wykonawcy w koordynacjach jest obowiązkowe).

2. ZAKRES PRZEDMOTU ZAMÓWIENIA

2.1. Zestawienie ilościowe

| Lp. | Opis | Ilość |
|-----|-----------------|-------|
| 1 | Ilość przejść | 69 |
| 2 | Ilość czytników | 133 |

2.2. Stacje robocze wchodzących w zakres przedmiotu zamówienia

| Lp. | Urządzenie | Przeznaczenie | Ilość | Uwagi |
|-----|--------------------------------------|--------------------------------|-------|--------------------------------------|
| 1 | Stacja robocza z możliwością wydruku | Pomieszczenia biura przepustek | 4 | Komputer, mysz, klawiatura + monitor |

2.3. Stanowisko do personalizacji kart zbliżeniowych

| Lp. | Urządzenie | Ilość | Uwagi |
|-----|---|--------|-----------------|
| 1 | Drukarka termotransferowa ze zbliżeniowym modułem kodującym | 2 | druk dwustronny |
| 2 | Materiały eksploatacyjne na 20 000 wydruków do w/w drukarek | 1 | |
| 3 | Karty zbliżeniowe | 25 000 | |

2.4. Opis przejść podlegających modernizacji

1. Przejście nr 1

Wejście/wyjście na teren uczelni realizowane w oparciu o cztery niskie bramki obrotowe. Wjazd/wyjazd realizowany w oparciu o 2 szlabany z SKD.

Zamawiający oczekuje modernizacji przejścia pieszego poprzez zainstalowanie dwóch (podwójnych, dwukierunkowych) wysokich kołowrotów wraz z wymianą istniejącego okablowania. Szlabany należy dostosować do instalowanego rozwiązania.

2. Przejście nr 2

Wejście/wyjście na teren uczelni realizowane w oparciu o dwie niskie bramki obrotowe. Wjazd/Wyjazd realizowany w oparciu o dwa szlabany z SKD.

Zamawiający oczekuje modernizacji przejścia pieszego poprzez zainstalowanie jednego (pojedynczego, dwukierunkowego) wysokiego kołowrotu wraz z wymianą istniejącego okablowania. Szlabany należy dostosować do instalowanego rozwiązania.

3. Przejście nr 3

Wejście/wyjście na teren uczelni realizowane w oparciu o cztery niskie bramki uchylne oraz drzwi przesuwne.

Zamawiający oczekuje dostosowania przejść do instalowanego rozwiązania z zachowaniem bramek i drzwi wraz z wymianą okablowania.

4. Przejście nr 4

Wejście/wyjście na teren uczelni realizowane w oparciu o jeden (podwójny, dwukierunkowy) wysoki kołowrót.

Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania z zachowaniem kołowrotów oraz wymianą istniejącego okablowania.

5. Przejście nr 5

Wejście/wyjście na teren uczelni realizowane w oparciu o dwa (podwójne, dwukierunkowe) wysokie kołowroty.

Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania z zachowaniem kołowrotów oraz wymianą istniejącego okablowania. Dodatkowo należy rozszerzyć wejście na teren uczelni o dwa (podwójne, dwukierunkowe) wysokie kołowroty.

6. Przejście nr 6

Wejście/wyjście na teren uczelni realizowane w oparciu o jeden (podwójny, dwukierunkowy) wysoki kołowrót.

Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania z zachowaniem kołowrotów oraz wymianą istniejącego okablowania.

7. Przejście nr 7

Wejście/wyjście na teren uczelni realizowane w oparciu o dwa (podwójne, dwukierunkowe) wysokie kołowroty.

Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania z zachowaniem kołowrotów oraz wymianą istniejącego okablowania.

8. Przejście nr 8

Wejście/wyjście na teren uczelni realizowane w oparciu o jeden (podwójny, dwukierunkowy) wysoki kołowrót.

Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania z zachowaniem kołowrotu oraz wymianą istniejącego okablowania.

9. Przejście nr 9

Wejście/wyjście na teren uczelni realizowane w oparciu o jeden (pojedynczy, dwukierunkowy) wysoki kołowrót.

Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania z zachowaniem kołowrotu oraz wymianą istniejącego okablowania.

10. Przejście nr 10

Wejście/wyjście na teren uczelni realizowane w oparciu o jeden (podwójny, dwukierunkowy) wysoki kołowrót.

Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania z zachowaniem kołowrotów oraz wymianą istniejącego okablowania.

11. Przejście nr 11

Wejście/wyjście na teren akademika realizowane w oparciu o dwoje jednoskrzydłowych drzwi.
Zamawiający oczekuje wymiany drzwi i dostosowania przejścia do instalowanego rozwiązania.

12. Przejście nr 12

Wejście/wyjście na teren akademika realizowane w oparciu o dwuskrzydłowe drzwi.
Zamawiający oczekuje wymiany drzwi i dostosowania przejścia do instalowanego rozwiązania.

13. Przejście nr 13

Wejście/wyjście na teren akademika realizowane w oparciu o dwoje dwuskrzydłowych drzwi.
Zamawiający oczekuje wymiany drzwi i dostosowania przejścia do instalowanego rozwiązania.

14. Przejście nr 14

Wejście/wyjście na teren akademika realizowane w oparciu o dwoje dwuskrzydłowych drzwi.
Zamawiający oczekuje wymiany drzwi i dostosowania przejścia do instalowanego rozwiązania.

15. Przejście nr 15

Wejście/wyjście na teren akademika realizowane w oparciu o dwuskrzydłowe drzwi.
Zamawiający oczekuje wymiany drzwi i dostosowania przejścia do instalowanego rozwiązania.

16. Przejście nr 16

Wejście/wyjście na teren akademika realizowane w oparciu o dwuskrzydłowe drzwi.
Zamawiający oczekuje wymiany drzwi i dostosowania przejścia do instalowanego rozwiązania.

17. Przejście nr 17

Wejście/wyjście na teren akademika realizowane w oparciu o dwuskrzydłowe drzwi.
Zamawiający oczekuje dostosowanie przejścia do instalowanego rozwiązania. Budynek objęty jest gwarancją. Zmiany należy uzgodnić z gwarantem.

18. Przejście nr 18

Wejście/wyjście na teren budynku w oparciu o cztery dwukierunkowe niskie kołowrotki oraz bramkę uchylną.
Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania.

19. Przejście nr 19

Wejście/wyjście na teren budynku w oparciu o pojedyncze drzwi.
Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania.

20. Przejście nr 20

Wejście/wyjście na teren budynku w oparciu o dwuskrzydłowe drzwi.
Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania.

21. Przejście nr 21

Wejście/wyjście na teren budynku w oparciu o dwuskrzydłowe drzwi.
Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania.

22. Przejście nr 22

Wejście/wyjście na teren budynku w oparciu o dwoje dwuskrzydłowych drzwi.
Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania.

23. Przejście nr 23

Wejście/wyjście na teren budynku w oparciu o dwoje dwuskrzydłowych drzwi.
Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania.

24. Przejście nr 24

Wejście/wyjście na teren budynku w oparciu o dwoje dwuskrzydłowych drzwi.
Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania. Budynek objęty jest gwarancją. Zmiany należy uzgodnić z gwarantem.

25. Przejście nr 25

Wejście/wyjście do działu w oparciu o dwuskrzydłowe drzwi.
Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania.

26. Przejście nr 26

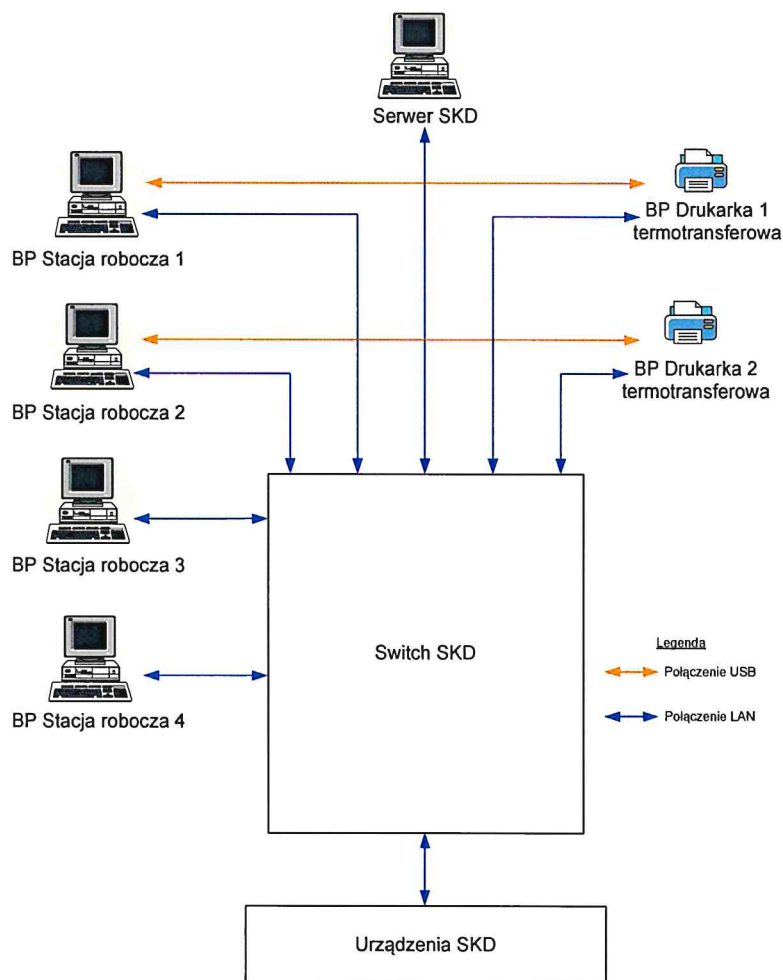
Wejście/wyjście na teren budynku w oparciu o dwuskrzydłowe drzwi.
Zamawiający oczekuje dostosowania przejścia do instalowanego rozwiązania.

27. Przejście nr 27

Wejście/wyjście do 8 pomieszczeń wewnątrz budynku.
Zamawiający oczekuje wymiany drzwi i dostosowania przejść do instalowanego rozwiązania.

28. Przejście nr 28

Zamawiający oczekuje wykonania zakresu prac opisanego w rozdziale 3.5.



Rysunek 1 Schemat blokowy systemu kontroli dostępu

3. SPECYFIKACJA TECHNICZNA WARUNKÓW ZAMÓWIENIA

3.1. Przedmiot zamówienia

Przedmiotem zamówienia jest kompleksowe wykonanie prac w zakresie zaprojektowania, dostawy, uruchomienia oraz utrzymania w okresie gwarancji Systemu Kontroli Dostępu (dalej: SKD).

3.2. Zakres zamówienia

Zakres zamówienia obejmuje:

1. Wykonanie projektu SKD. Projekt w podziale na branże, ma obejmować m.in. część budowlaną, teletechniczną i elektryczną. Wykonawca powinien dysponować osobami posiadającymi uprawnienia do projektowania bez ograniczeń w każdej z występujących branż. W dokumentacji projektowej należy uwzględnić nowoczesne rozwiązania technologiczne zgodne z opisem w PFU. Na etapie opracowywania dokumentacji projektant jest zobligowany do przeprowadzenia wizji lokalnej, analizy uwarunkowań lokalizacyjnych oraz uwzględnienia szczegółowych wytycznych Zamawiającego dotyczących lokalizacji montażu oraz specyfikacji technicznej urządzeń. Celem tych działań jest dobór optymalnych rozwiązań projektowych w kontekście kompleksowego działania systemu SKD.
2. Wykonanie i zatwierdzenie szczegółowego harmonogramu prac.
3. Wykonanie przedmiaru robót (format plików edytowalnych rozpoznawany przez program Norma) i kosztorysów ofertowych z podziałem na występujące branże wraz z zestawieniem kosztów zadania (ZKZ) całości przedmiotu zamówienia.
4. Wykonanie szczegółowych kosztorysów ofertowych wykonania robót (z aktualnymi cenami i podziałem na branże z ZKZ Oferty przetargowej) zgodnie z zakresem robót ujętym w dokumentacji projektowej, technicznej i wykonawczej, po zatwierdzeniu rozwiązań projektowych przez Zamawiającego.
5. Opracowanie Specyfikacji Technicznej Wykonania i odbioru Robót (STWiOR) i informacji dotyczącej Bezpieczeństwa i Ochrony Zdrowia dla przedmiotowych robót budowlanych.
6. Dostawę urządzeń (w tym przełączników sieciowych), instalację oraz uruchomienie systemu wraz z odpowiednią liczbą licencji.
7. Dostawę i instalację zestawów drzwiowych i kołowrotów mechanicznych przejść objętych elektroniczną kontrolą dostępu.
8. Wykonanie prac budowlanych w miejscach budowy nowych kołowrotów (szczególnie w miejscu modernizacji przejścia nr 28), opisanych w punkcie 3.5.
9. Wykonanie zasilania urządzeń kontroli dostępu.
10. Dostawę 25 000 kart zbliżeniowych oraz wykonanie personalizacji dla około 10 000 sztuk, podzielone na pięć odrębnych grup użytkowników.
11. Testy systemu.
12. Zaktualizowanie Instrukcji Bezpieczeństwa Pożarowego w obiektach, w których jest wymagana.
13. Szkolenie z obsługi SKD dla personelu.
14. Sporządzenie dokumentacji powykonawczej dla w/w prac.
15. Demontaż zbędnego lub nieczynnego / nieużywanego okablowania będącego w zakresie prac.
16. Wykonanie prac przygotowawczych związanych z wyniesieniem a po wykonaniu prac z wniesieniem lub zabezpieczeniem urządzeń / instalacji znajdujących się w obrębach prowadzenia prac i wskazanych przez Zamawiającego.

17. Wywóz i utylizacja odpadów i zdemontowanych urządzeń zgodnie z obowiązującymi przepisami w tym zakresie. Zamawiający zastrzega sobie prawo do zachowania wybranych demontowanych materiałów i urządzeń.
18. Zabezpieczenie miejsca wykonywania prac.
19. Złożenie wniosku o pozwolenie na budowę lub dokonanie zgłoszenia wykonania robót budowlanych i uzyska decyzję o pozwoleniu na budowę (w przypadku, gdy będzie wymagane).
20. Opis prac będących w zakresie Przejścia nr 28:
 - 1) Montaż kontroli dostępu wraz przebudową głównego wejścia i:
 - a) dostawą i montażem wysokich bramek obrotowych;
 - b) dostawą i montażem furtek ogrodzenia;
 - c) dostawą i montażem systemów wspomagających ochronę obiektu, CCTV oraz video-domofonu, kompatybilnych z obowiązującymi w Wojskowej Akademii Technicznej, zapewniając doświetlenie obszaru wejścia poprzez nowe oprawy oświetleniowe na słupach;
 - d) przeniesienie istniejącego kontenera służby wartowniczej wraz z zasilaniem elektrycznym i telekomunikacyjnym.
 - 2) Prace w budynku wskazanym na etapie projektu wykonawczego Przejścia nr 28:
 - a) dostawa, montaż i uruchomienie elektronicznego depozytora na min. 100 kluczy;
 - b) montaż instalacji klimatyzacji wraz z zasilaniem elektrycznym i instalacją odprowadzenia skroplin a w tym: Instalację chłodniczą freonową należy wykonać z rur miedzianych chłodniczych, izolowanych dla instalacji klimatyzacyjnych. W przypadku połączeń, należy wykonać je lutem twardym. Wszystkie przejścia przewodów przez przegrody budowlane należy wykonać w tulejach ochronnych utwierdzonych w przegrodzie, umożliwiających wzdlużne przemieszczanie się przewodu. Przestrzeń pomiędzy tuleją a przewodem należy wypełnić materiałem plastycznym lub elastycznym, nie powodującym uszkodzenia przewodu. Izolację rurociągów należy wykonać z otulin z pianki z kauczuku syntetycznego o grubości 19 mm. Powierzchnie izolowane powinny być suche i czyste. Izolację rurociągów prowadzonych na zewnątrz budynku należy zabezpieczyć przed wpływem warunków atmosferycznych za pomocą obudowy. Instalacje skroplin wykonać jako grawitacyjne z rur pcv. Podłączenia wykonywać z zastosowaniem syfonu;
 - c) remont pomieszczenia Punktu Dystrybucyjnego w bud. nr 19 w tym: usunięcie spękań i odnowienie powłok malarskich ścian i sufitu;
 - d) montaż szafy teletechnicznej 42U oraz instalacja systemu kontroli dostępu i CCTV dla pomieszczenia wskazanego przez Zamawiającego na etapie projektu wykonawczego.
 - 3) Remont bram wjazdowych ogrodzenia terenu obejmujący:
 - a) wykonanie dodatkowej furtki, przy bramie, w centralnej części ośrodka;
 - b) dostawa i montaż, do nowej i istniejącej furtki, systemu kontroli dostępu;
 - c) dostawa i montaż systemu nadzoru CCTV, z włączeniem do systemu WAT, oraz doświetlenie obszaru wejść, poprzez nowe oprawy oświetleniowe na słupach przy obu bramach.

3.3. Wymagania dotyczące systemu kontroli dostępu

W ramach modernizacji Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego (WAT), jako jednostki nadzorowanej przez Ministra Obrony Narodowej, należy przeprowadzić kompletną modernizację środków ochrony elektronicznej w zakresie systemu kontroli dostępu (SKD). System ma być kompatybilny z systemem używanym w MON i opierać się na koncepcji inteligencji rozproszonej, gdzie wszystkie uprawnienia dostępu oraz funkcje systemowe mają być zarządzane bezpośrednio na najniższym poziomie — przez kontrolery.

System Kontroli Dostępu ma być zaprojektowany w oparciu o otwartą, modułową i skalowalną architekturę, która ma zapewnić elastyczność i łatwość integracji z innymi systemami bezpieczeństwa, ale również umożliwić przyszły rozwój i rozbudowę w odpowiedzi na zmieniające się potrzeby organizacji. Otwartość architektury ma pozwalać na płynne połączenie SKD z kluczowymi elementami infrastruktury budynku, takimi jak system sygnalizacji włamania i napadu (SSWiN), system telewizji dozorowej (CCTV), a także z innymi systemami automatyki budynkowej, co stworzy kompleksowe i zintegrowane środowisko zarządzania bezpieczeństwem.

Podstawą systemu ma być dedykowany zestaw do rozwoju oprogramowania (SDK) oraz certyfikowany interfejs programistyczny API, które umożliwią wykwalifikowanym integratorom dostosowanie i rozbudowę funkcjonalności systemu zgodnie z indywidualnymi wymaganiami projektu. Dzięki temu ma być stworzenie rozwiązań precyzyjnie dopasowanych do specyfiki obiektu, niezależnie od jego wielkości, stopnia skomplikowania czy branży. Implementacja SDK i API ma zagwarantować, że wszystkie elementy systemu – od czytników kart, przez kontrolery dostępu, aż po oprogramowanie zarządzające – będą współpracować ze sobą w sposób spójny, bezpieczny i stabilny.

3.4. Wymagania dotyczące wykonania prac

1. Dostarczone urządzenia muszą być fabrycznie nowe i pochodzić z seryjnej produkcji.
2. Użyte materiały między innymi kable, kanały kablowe itp. powinny być bezhalogenowe, trudnopalne, nierozprzestrzeniające ognia i emitujące niewielkie ilości dymu.
3. Po wykonaniu robót budowlanych budynku muszą spełniać wymagania wynikające z norm i obowiązujących przepisów w zakresie bezpieczeństwa nośności konstrukcji, ochrony pożarowej, bezpieczeństwa i higieny pracy, warunków sanitarno-epidemiologicznych, ochrony środowiska.
4. Wykonawca zapewni dostawę sprzętu do wskazanej lokalizacji w siedzibie Zamawiającego.
5. Wykonawca przedstawi Zamawiającemu harmonogram prowadzenia prac. Warunkiem koniecznym, aby prace mogły się rozpocząć, jest zatwierdzenie harmonogramu przez Zamawiającego. Harmonogram powinien obejmować szczegółowy opis poszczególnych etapów prac.
6. Przed rozpoczęciem prac budowlano - modernizacyjnych przejść wskazanych w punkcie 2.1 Wykonawca skonfiguruje i uruchomi serwer, stacje robocze systemu kontroli dostępu, przygotuje karty dostępowe zgodnie z wytycznymi Zamawiającego.
7. Wykonawca będzie odpowiedzialny za prawidłowe skonfigurowanie połączeń fizycznych i logicznych, podłączenie urządzeń oraz ich konfigurację umożliwiającą niezakłóconą pracę systemu.
8. Prace instalacyjne mają być prowadzone wyłącznie w terminach wcześniej uzgodnionych z Zamawiającym. Prace na danym przejściu Wykonawca ma obowiązek zgłosić z co najmniej dwutygodniowym wyprzedzeniem. Prace mogą rozpocząć się po uzyskaniu zatwierdzenia prowadzenia prac przez Zamawiającego.
9. Wykonawca uzgodni z Zamawiającym sposób zabezpieczenia miejsca prowadzenia prac, w szczególności w obrębie wejść ze obszaru ogólnodostępnego do obszaru chronionego (m. in. wykonanie tymczasowego ogrodzenia miejsca pracy, monitoringu itp.). Koszt zabezpieczeń po stronie Wykonawcy.
10. Wykonawca uzgodni z Zamawiającym projekt organizacji ruchu na czas prowadzenia prac w miejscach o zwiększonym natężeniu ruchu, miejsca zostaną wskazane przez Zamawiającego.
11. Zamawiający nie dopuszcza wyłączenia z użytkowania więcej niż jednego przejścia o zwiększonym natężeniu ruchu (dotyczy przejść ze obszaru ogólnodostępnego do obszaru chronionego).
12. W tym samym czasie nie można prowadzić prac na przejściach oznaczonych w tabeli: Wykaz przejść wchodzących w zakres przedmiotu zamówienia” (punkt 2.1) numerami:
 - 1) 1 i 2;

- 2) 1 i 5;
 - 3) 1 i 6;
 - 4) 2 i 8;
 - 5) 5 i 7;
 - 6) 9 i 10;
 - 7) 18, 19 i 20.
13. Zamawiający wymaga uruchomienia przejścia od razu po jego wybudowaniu i skonfigurowaniu w systemie (po przeprowadzeniu odbioru częściowego).
14. Zamawiający wymaga od Wykonawcy:
- 1) Bieżącego utrzymywania porządku na drogach komunikacyjnych oraz w obszarach, z których będzie korzystać w trakcie wykonywania prac;
 - 2) Prawidłowego wykonania, odtworzenia wszystkich elementów budowlanych, które zostały zniszczone, rozebrane, uszkodzone w trakcie realizacji prac a nie były w zakresie zadania.

3.5. Zakres prac budowlanych w obrębie przejścia nr 28

1. Wejście główne

- 1) usunąć fragment żywopłotu (ok. 10mb);
- 2) za istniejącym ogrodzeniem przygotować podbudowę (pow. ok. 2,5 x 6m z bloczków fundamentowych lub kostki brukowej) i przenieść kontener służby wartowniczej,
- 3) ~~wraz z kontenerem należy przenieść wszystkie przyłączone instalacje telekomunikacyjne i zasilające, połączone z budynkiem SWF i siecią WAT (kabel UTP z zaporą przeciwwilgociową 4x2x0,5 i światłowodowego 6J). Istniejące kable należy wycofać i ponownie wprowadzić do kontenera zakańczając w istniejącej skrzynce w kontenerze. Nie dopuszcza się przedłużania kabli. W przypadku zbyt krótkich kabli należy wymienić całe odcinki między istniejącymi złączami,~~
- 4) wykonać fragment chodnika (powierzchnia ok 2 x 3m z kostki betonowej typu „Holand” na podbudowie stabilizowanej klasy min, RM5, grubość kostki 8cm, obrzeża 8x25) łączący istniejący chodnik z wejściem do przeniesionego kontenera,
- 5) w miejscu obecnego wejścia głównego przygotować odpowiedni fundament (wymiary i głębokość fundamentu zgodnie z wytycznymi producenta zestawu, beton klasy min. B30 W8 zbrojony góra i dołem siatkami z drutu #8 w rozstawie 15x15cm) z doprowadzeniem zasilania i przewodów sterujących do montażu kołowrotów,
- 6) zamontować wysoką bramkę obrotową, na 4 przejścia (sugerowany montaż dwóch podwójnych zestawów analogicznie jak przy budynku głównym WAT), z kontrolą dostępu, kompatybilną z systemem przepustkowym WAT oraz systemem nadzoru CCTV (kamer wideo z doświetleniem wejścia),
- 7) istniejący chodnik z kostki brukowej należy poszerzyć tak, by zapewniał swobodne przejście do systemu bramkowego (do wykonania ok 30m² nowego chodnika z kostki betonowej typu „Holand” na podbudowie stabilizowanej klasy min, RM5, grubość kostki 8cm, obrzeża 8x25),
- 8) obok przejścia należy wykonać dodatkowe ogrodzenie panelowe, wraz z fundamentem, dopasowane wizualnie do istniejącego (wysokość ogrodzenia i furtek ok. 180cm, wzmacniane słupki, panele zgrzewane 3D z drutu o grubości min. 4mm – całość ocynkowana i malowana proszkowo),
- 9) zamontować dwie furtki szer. min. 120 cm (pierwsza od ulicy Kartezjusza z wideodomofonem, druga od strony przejścia otwierana przyciskiem przez służbę wartowniczą) wyposażone

- w CCTV, sterowane z wartowni przeznaczone dla osób nieposiadających przepustek, dostawców przesyłek, zaopatrzenia, itp., furtki i słupki wyposażone w zamki magnetyczne,
- 10) w miejscu wygradzenia, wykonać fragment chodnika, łączący wejście do wartowni z furtką i istniejącym chodnikiem (powierzchnia ok. 4x3m z kostki betonowej typu „Holand” na podbudowie stabilizowanej klasy min, RM5, grubość kostki 8cm, obrzeża 8x25).

2. Remont bram wjazdowych ogrodzenia terenu

1) Brama pierwsza:

- a) przy istniejącej furtce, w odległości ok. 3m montaż metalowego słupa latarni oświetlającej wejście (wysokość latarni od 3 do 5m) wraz z fundamentem i doprowadzeniem przewodów (peszli) zasilających i telekomunikacyjnych;
- b) montaż kamery umożliwiającej identyfikację osób wchodzących i nadzór nad obszarem wejścia;
- c) wyposażenie furtki w zamek magnetyczny.

2) Brama druga:

- a) zabezpieczenie, oczyszczenie istniejącej bramy;
- b) rozebranie fragmentu ogrodzenia wraz z fundamentem, słupkami, panelami;
- c) wykonanie, obniżonego do poziomu istniejącego terenu, fundamentu, pod słupki i furtkę (furtka szerokości 120 cm wysokości 180 cm wykonana na wzór furtki z pierwszej bramy) z montażem kanałów/peszli, umożliwiających doprowadzenie zasilania i przewodów sterowniczych do systemu kontroli dostępu i kamer;
- d) dostawy i montażu dodatkowej furtki szerokości 1,2m (wykonanej na wzór furtki z bramy nr 1 wyposażonej w zamek magnetyczny) oraz dodatkowego, niezbędnego do montażu furtki, słupka ogrodzenia;
- e) przy nowej furtce, w odległości ok. 3m montaż metalowego słupa latarni, oświetlającej wejście (wysokość latarni od 3 do 5m) wraz z fundamentem i doprowadzeniem przewodów (peszli) zasilających i telekomunikacyjnych;
- f) montaż kamery umożliwiającej identyfikację osób wchodzących i nadzór nad obszarem wejścia.

3) Ponadto:

- a) Wykonanie niezbędnych odcinków przyłączy do istniejącej kanalizacji telekomunikacyjnej na terenie Studium Wychowania Fizycznego WAT należy zrealizować poprzez ułożenie rurociągu ziemnego HDPE 2x40/3,7 mm do najbliższej, uzgodnionej z Zamawiającym studni kablowej wraz z uwzględnieniem posadowienia niezbędnej liczby studni kablowych. Długość sumaryczna ok. 150 mb,
- b) Nowo projektowane punkty kamerowe (kołowrót, furtki, drzwi do PD) należy podłączyć nowego 16-kanałowego rejestratora, który należy zamontować w nowej szafie w pomieszczeniu PD w budynku nr 19 Studium Wychowania Fizycznego WAT. Istniejącą kamerę w holu obrócić tak, aby polem widzenia objęła depozytor kluczy. Nowy rejestrator należy podłączyć do podsieci systemów bezpieczeństwa WAT poprzez istniejący przełącznik w szafie rack w pomieszczeniu PD. Zobrazowanie z kamer wyprowadzić w pomieszczeniu portierni w budynku nr 19 na istniejącą stację z monitorem,
- c) Specyfikacja minimalnych wymagań dla urządzeń kamerowych znajduje się w Wymaganiach eksploatacyjno-technicznych dla XIX grupy SpW – systemy i urządzenia specjalistyczne do ochrony obiektów (załącznik nr 2) – kamery wyposażone w motozoom oraz min. 8Mpx z doświetlaczem oraz zasilaniem awaryjnym na min. 36h w przypadku zaniku zasilania;
- d) Należy zapewnić szkolenie dla administratorów lokalnych systemu CCTV w SWF WAT.

- e) Zasilanie do bramek obrotowych, furtek oraz kontenera służby dyżurnej prowadzić trasami podziemnymi w rurach ochronnych. Po zmianie lokalizacji kontenera służby dyżurnej zaprojektować i wykonać oświetlenie strefy kontrolowanej przy kontenerze – oprawami LED z czujkami ruchu, z możliwością wyłączenia czujek ruchu (z kontenera służby dyżurnej).

3.6. Wymagania dotyczące urządzeń systemu kontroli dostępu

1. Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nie może nosić żadnych śladów użytkowania. Wymaga się, aby sprzęt był fabrycznie nowy, pochodził z oficjalnego kanału sprzedaży producenta dedykowanego na rynek polski oraz był wyprodukowany seryjnie, z uwzględnieniem wszystkich opcji konfiguracyjnych przewidzianych dla oferowanego modelu. Niedopuszczalne są produkty prototypowe, urządzenia długo magazynowane lub pochodzące z programów wyprzedażowych producenta. Sprzęt nie może znajdować się na listach „end-of-sale” ani „end-of-support” producenta.
 2. Wykonawca powinien posiadać autoryzację producenta potwierdzoną aktualnym certyfikatem serwisowym (min. 2 osoby przeszkolone) w celu zachowania pełnych warunków gwarancji producenta.
 3. Producent powinien posiadać certyfikat ISO 9001 w zakresie sprzedaży i serwisu urządzeń drukujących do kart PVC oraz systemów identyfikacji i kart elektronicznych.
 4. Wymagana liczba oraz rozmieszczenie portów na obudowie urządzeń nie może być osiągnięta poprzez stosowanie konwerterów, przejściówek ani innych zewnętrznych akcesoriów tego typu.
 5. Do dostawy dołączona zostanie odpowiednia liczba kabli zasilających i połączeniowych niezbędnych do uruchomienia sprzętu.
-
6. Konfiguracja zamawianego sprzętu będzie realizowana w ścisłej współpracy i uzgodnieniu z Zamawiającym, ze szczególnym uwzględnieniem obowiązującej w Wojskowej Akademii Technicznej polityki bezpieczeństwa informacji oraz istniejących zasobów IT.
 7. Po zakończeniu instalacji Wykonawca zobowiązany będzie do przekazania dokumentacji powykonawczej, która obejmie w szczególności komplet danych dostępowych do urządzeń i oprogramowania używanego podczas instalacji i konfiguracji.
 8. W przypadku dostawy sprzętu komputerowego z preinstalowanym systemem operacyjnym, Zamawiający wymaga dostarczenia systemu fabrycznie nowego, nigdy wcześniej nieużywanego ani nieaktywowanego na innym urządzeniu, pochodzącego wyłącznie z legalnego źródła sprzedaży oraz posiadającego certyfikat autentyczności dla każdej licencji, o ile producent stosuje takie certyfikaty. Naklejka hologramowa systemu operacyjnego powinna być zabezpieczona zgodnie ze standardami producenta przed możliwością odczytania klucza licencyjnego. Zamawiający zastrzega sobie prawo do weryfikacji legalności dostarczonego oprogramowania zarówno na etapie oceny ofert, jak i podczas odbioru sprzętu, bezpośrednio u producenta oprogramowania. Wykonawca będzie zobowiązany do przedstawienia dokumentów potwierdzających zakup oprogramowania w autoryzowanym kanale dystrybucyjnym producenta na żądanie Zamawiającego.
 9. Opis minimalnych parametrów wybranych urządzeń systemu kontroli dostępu:
 - 1) Serwer - Środowisko serwerowe zabezpiecza Zamawiający.
 - 2) Kontrolery:
 - a) Kontrolery muszą posiadać zdolność podejmowania autonomicznych decyzji autoryzacyjnych, z lokalnym przechowywaniem danych autoryzacyjnych oraz synchronizacją z serwerem SKD;
 - b) Kontrolery muszą być standardowymi urządzeniami sieciowymi z komunikacją w protokole TCP/IP, bez konieczności stosowania konwersji sygnału;
 - c) Komunikacja między kontrolerami odbywać się musi w trybie „peer-to-peer”, bez udziału serwera;

- d) Minimalne parametry techniczne kontrolerów: CPU 800 MHz, 256 MB SDRAM, 2 GB pamięci Flash;
 - e) Buforowanie zdarzeń w kontrolerze musi obejmować minimum 1 000 000 wpisów, z automatycznym nadpisywaniem najstarszych w przypadku przepełnienia;
 - f) W przypadku utraty łączności z serwerem, kontrolery muszą kontynuować pracę w trybie autonomicznym, przysyłać zgromadzone zdarzenia po przywróceniu połączenia, samodzielnie podejmować decyzję o udzielaniu bądź blokowaniu dostępu, a także współdziałać z innymi systemami zabezpieczeń;
 - g) Kontrolery SKD muszą posiadać własne zasilanie awaryjne z akumulatorem.
- 3) Czytniki:
- a) Obudowa czytników min. IP54;
 - b) Wskazanie statusu sygnałem dźwiękowym lub za pomocą diody LED;
 - c) Wbudowane czujniki sabotażu;
 - d) Czytniki muszą umożliwiać określenie stanu aktywności oraz roli przy utracie połączenia z kontrolerem.
- 4) Moduły rozszerzeń:
- a) Otwarta architektura umożliwiająca wybór oprogramowania bez wymiany sprzętu;
 - b) Komunikacja zabezpieczona TLS 1.2 lub AES-256, obsługa minimum 4 czytników, port OSDP (RS-485), zasilanie 12V DC i PoE/PoE+;
 - c) Nadzorowane i nienadzorowane wejścia, przekaźniki, praca w szerokim zakresie temperatur;
 - d) Certyfikaty UL294, FCC Part 15 Class A, CE, RoHS oraz szyfrowanie zgodne z NIST.
- 5) Zasilacze:
- a) zasilacz buforowy przeznaczony do nieprzerwanego zasilania urządzeń wymagających stabilnego napięcia;
 - b) zasilanie 200-240V AC;
 - c) prąd wyjściowy 2,5A;
 - d) częstotliwość zasilania 50/60Hz;
 - e) regulacja napięcia wyjściowego DC;
 - f) regulacja napięcia wejściowego;
 - g) zabezpieczenie przed rozładowaniem i odwrotnym podłączeniem akumulatora;
 - h) sygnalizacja pracy diody LED;
 - i) sygnał alarmowy o niskim stanie naładowania akumulatora;
 - j) zabezpieczenie przeciwzwarciowe, przeciwprzepięciowe, przeciążeniowe;
 - k) zabezpieczenie antysabotażowe obudowy chroniące przed nieuprawnionym otwarciem.
- 6) Przełączniki sieciowe:
- a) zarządzalny przełącznik Gigabit Ethernet wyposażony w 24/48 portów 10/100/1000BaseT;
 - b) porty uplink muszą umożliwiać obsadzenie modułami Gigabit Ethernet SFP (co najmniej 1000Base-T, 1000Base-SX, 1000Base-LX/LH), 10Gigabit Ethernet (co najmniej 10GBase-SR, 10GBase-LR,) lub SFP28 (co najmniej 25GBASE-SR, 25GBASE-SL, 25GBASE-LR);
 - c) możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU;
 - d) slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb):
 - 25G/10G SFP28,
 - 1G SFP,
 - 10G SFP+,
 - e) porty SFP/SFP+/QSFP możliwe do obsadzenia wkładkami zależnie od potrzeb:

- porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U,
 - porty SFP+ – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax,
- f) zasilacz prądem naprzemiennym 230V, możliwość instalacji zasilacza redundantnego,
- g) redundantne i wymienne moduły wentylatorów,
- h) przełącznik wspiera IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności).
- 7) Stacja robocza: komputer typu AllinOne 27'' o parametrach:
- a) procesor 10 rdzeni, 2.4 GHz, 4.9 GHz Turbo, 24MB Cache;
 - b) Karta graficzna zintegrowana, 1x wyjście HDMI lub 1x DP,
 - c) pamięć RAM 32GB;
 - d) dysk SSD 2000 GB;
 - e) złącza na tylnym panelu 1x RJ45, 1x USB 3.2 Gen 2, 2x USB;
 - f) Złącza na przednim panelu 1x USB 3.2 Gen 2, audio;
 - g) matryca 27";
 - h) standard łączności bezprzewodowej min. WiFi 6 oraz Bluetooth 5.2, szyfrowanie TPM 2.0;
 - i) kamera internetowa, mikrofon, wbudowany napęd DVD-RW lub dołączany pod USB;
 - j) Windows 11 PRO PL;
 - k) Klawiatura i mysz przewodowa lub bezprzewodowa.
-
- 8) Drukarki termotransferowe:
- a) Drukarka do kart PVC z funkcją odczytu i kodowania kart RFID oraz smart card produkcji/dostosowany do wybranego SKD;
 - b) Metoda nadruku: Dye-Sublimation and Resin Retransfer High-Definition Printing, poza krawędzie karty (Over-the-edge on CR-80 cards);
 - c) Typ nadruku: dwustronny z funkcją obsługi układów elektronicznych w jednym przebiegu karty;
 - d) Rozdzielczość druku 300 dpi (11.8 punktów/mm);
 - e) Ilość kolorów: 16.7 mln / 256 odcieni na pixel;
 - f) Przygotowana do obsługi taśm drukujących typu YMC min. 750 wydruków, YMCK in. 500 wydruków, YMCKK min. 500 wydruków, YMCFFK na 500 wydruków, • Resin K na 3000 wydruków, Film retransferowy Clear 1500 wydruków, Film Standard Holographic na 500 wydruków oraz taśm laminacyjnych: typu TTF Thermal Transfer Overlamine 0.25 mil na 500 wydruków oraz taśm typu PolyGuard® 1.0 mil oraz 0.6 mil na 250 wydruków;
 - g) Prędkość wydruku:
 - 27 sekund na kartę / 133 karty na godz. (YMCK);
 - 33 sekundy na kartę / 109 kart na godz. (YMCKK);
 - 33 sekundy na kartę / 109 kart na godz. (YMCK z laminacją dwustronną);
 - 44 sekundy na kartę / 82 karty na godz. (YMCKK z laminacją dwustronną);
 - h) Akceptowane rozmiary kart: CR-80 (85.6mm x 54mm);
 - i) Akceptowane grubości kart: zakres .030" (30 mil) - .050" (50 mil) / .762mm to 1.27mm;
 - j) Akceptowane typy kart: ABS, Laminowane PVC, PET, PETG, Poliwęglan 100%, optyczne karty pamięciowe, zbliżeniowe, stykowe, z paskiem magnetycznym, karty samoprzylepne z podkładem typu papier lub Mylar;

- k) Pojemność minimalna podajnika kart: 100 kart (o grubości .030" / .762mm) z opcjonalną możliwością rozbudowy do 200 kart; pojemność minimalna odbiornika kart: 200 kart (o grubości .030" / .762mm);
 - l) Wymagana dostępność rolki czyszczącej w komplecie z każdą taśmą drukującą barwną;
 - m) Wyświetlacz: Graficzny typu OLED;
 - n) Pamięć podręczna RAM (minimalna wbudowana): 1GB;
 - o) Wymagane sterowniki: Windows® 10 / 11 / Server 2016 / Server 2019 / Server 2022;
 - p) Wymagane funkcjonalności minimalne w standardzie: odczyt/zapis kart zbliżeniowych (dostosowany do wybranego SKD), odczyt/zapis kart stykowych ISO 7816;
 - q) Wbudowane porty komunikacyjne: USB 2.0 HS (typu High Speed) oraz Ethernet z wewnętrznym serwerem wydruku;
 - r) Zakres temperatur pracy drukarki: 65° to 90° F / 18° to 32° C;
 - s) Zakres wilgotności pracy drukarki: 20 - 80% bez kondensacji pary wodnej;
 - t) Wymiary maksymalne i waga maksymalna urządzenia:
 - Drukarka z modulem obracającym karty (druk dwustronny): 12"H x 22"W x 11"D / 30.5cm x 55.9cm x 27.9cm, waga do 13,5kg;
 - u) Certyfikaty bezpieczeństwa: UL, CE, FCC, IC, IFTEL, KC, VCCI, MIC, NCC, WPC, BIS, ENACOM;
 - v) Zasilanie: 100-240 VAC, 1.6A, częstotliwość prądu zasilającego: 50 Hz / 60 Hz;
 - w) Gwarancja (wymagania minimalne): Drukarka - 4 lata gwarancji producenta,
 - x) Głowica drukująca – gwarancja producenta typu Lifetime (z nieograniczonym limitem wydruków na oryginalnych taśmach i kartach HID/FARGO);
 - y) Funkcjonalności dotyczące bezpieczeństwa przesyłanych do drukarki i drukowanych danych:
 - funkcja wymazywania/usuwania danych z panelu resinowego taśmy drukującej;
 - funkcja szyfrowania przesyłanych danych w standardzie min. AES-256;
 - wbudowane w sterownik narzędzie diagnostyczne typu Workbench do zarządzania procesem nadruku oraz zarządzania kolorami;
 - z) Wymagane z urządzeniem - komplet bibliotek SDK.
- 9) Kołowroty:
- a) Urządzenie sterowane logicznie dwukierunkowo z możliwością indywidualnego programowania;
 - b) Konstrukcja wykonana ze stali nierdzewnej;
 - c) Praca w trudnych warunkach atmosferycznych;
 - d) Temperatura pracy -20°C - +70°C;
 - e) IP 54;
 - f) Średnia ilość cykli 5 000 000 / 10 000 000;
 - g) Czas zwolnienia 5 sek;
 - h) Przepustowość praktyczna 2x1000 os. na godz.;
 - i) Pobór mocy 80W na jedno przejście;
 - j) Zadaszenie;
 - k) Ramka montażowa do montażu wpuszczanego;
 - l) Blokowanie się w przypadku awarii lub w czasie przerwy z dostawie prądu;
 - m) Konfigurowalne wskaźniki LED sygnalizujące stan przejścia;
 - n) Zapasowa bateria;
 - o) Możliwość integracji z kontrolą dostępu. Przygotowane miejsca pod montaż czytników;
 - p) Zabezpieczenie układu mechaniczno - programowalnego przed dostępem osób nieuprawnionych;

- q) Wyjście serwisowe sygnalizujące prawidłową pracę urządzenia lub awarię;
- r) Zabezpieczenie przed uszkodzeniem mechanicznym;
- s) Uniemożliwienie wejścia więcej niż jednej osobie jednocześnie;
- t) Blokowanie, gdy nie nastąpi przejście po upływie określonego czasu;
- u) Wbudowany system antykradzieżowy.

10) Drzwi:

- a) Należy zastosować drzwi wraz z okuciami posiadającymi odpowiednie certyfikaty, fabrycznie przystosowane do integracji z systemem kontroli dostępu;
- b) Otwarcie drzwi od strony wewnętrznej musi spełniać funkcję wyjścia ewakuacyjnego pożarowego;
- c) Drzwi mają być wyposażone w samozamykacz dostosowany do ciężaru drzwi;
- d) Drzwi dwuskrzydłowe na etapie produkcji mają być wyposażone w przepust w skrzydle biernym;
- e) Po montażu urządzeń kontroli dostępu należy zachować „światło” drzwi zgodne z przepisami ppoż.

3.7. Wymagania funkcjonalne systemu kontroli dostępu

1. System kontroli dostępu (SKD) musi gwarantować skalowalność oraz możliwość rozbudowy w następującym zakresie:
 - 1) liczba kontrolowanych przejść: minimum 1500;
 - 2) liczba rekordów w bazie danych: minimum 200 000;
 - 3) liczba użytkowników systemu: minimum 20 000.
2. Dostępność i tryb pracy: system musi działać w trybie ciągłej dyspozycyjności 24/7, 365 dni w roku.
3. Monitorowanie urządzeń musi odbywać się przy użyciu protokołu SNMPv3 lub równoważnego.
4. Logowanie do systemu musi odbywać się z wykorzystaniem indywidualnych loginów i haseł, z możliwością wymuszania przez administratora stosowania haseł o określonej sile oraz okresowej ich zmiany.
5. System powinien wspierać mechanizm uwierzytelniania dwuskładnikowego (2FA).
6. Programowanie funkcjonalności kontrolerów powinno odbywać się z poziomu aplikacji graficznej metodą „drag and drop”.
7. Konfiguracja systemu powinna być możliwa z poziomu jednego centralnego punktu lub lokalnie w kontrolerze, z synchronizacją do serwera.
8. System musi umożliwiać zdalny dostęp do pełnej konfiguracji kontrolera.
9. Architektura SKD powinna opierać się na topologii gwiazdy z bezpośrednim połączeniem kontrolerów do przełączników sieciowych, z możliwością zastosowania magistrali rozszerzającej wejścia/wyjścia.
10. System musi być zintegrowany z platformą Venom PSIM działającą w LCN WAT, z dostarczeniem SKD/API umożliwiającego wizualizację stanów i sterowanie przejściami.
11. Zasilanie i monitoring:
 - 1) System musi monitorować zasilanie 230 V AC oraz stan akumulatora, prezentując te informacje w systemie SKD i systemach zintegrowanych.
12. Monitorowanie w czasie rzeczywistym uprawnień dostępowych, identyfikacja osób, czasu oraz miejsca uzyskania dostępu.
13. Raportowanie:

- 1) System musi umożliwiać tworzenie nowych, konfigurowalnych raportów oraz generowanie logów systemowych do celów analitycznych;
- 2) System musi umożliwiać generowanie raportów w formatach PDF i Excel lub równoważnych, z możliwością zapisu i wydruku lokalnego oraz sieciowego;
- 3) Raporty muszą być konfigurowalne pod względem zakresu danych i zawierać m.in.:
 - a) informacje o zdalnym otwarciu drzwi;
 - b) dane o grupach dostępu;
 - c) zdarzenia systemowe i alarmowe;
 - d) konfigurację sprzętu i drzwi;
 - e) szczegółowe dane o zdarzeniach, w tym priorytet i harmonogram.
14. Zarządzanie alarmami i zdarzeniami:
 - a) Administrator ma możliwość konfigurowania nazw, wyświetlania, maskowania alarmów, definiowania instrukcji obsługi zdarzeń, wysyłania powiadomień e-mail oraz zarządzania schematami postępowania;
 - b) System musi wspierać synchronizację alarmów wyświetlanych na wielu stanowiskach, z przypisanymi instrukcjami tekstowymi (minimum 250 znaków);
 - c) Możliwość tworzenia alarmów podczas instalacji z konfigurowalnymi parametrami (priorytet, maskowanie, raportowanie);
 - d) Alarmy i zdarzenia muszą być widoczne i zarządzane także w trybie offline.
15. Zarządzanie uprawnieniami użytkowników poprzez odpowiednią strukturę ról z wyróżnieniem poziomów uprawnień przynajmniej dla administratora i użytkownika.
16. Logowanie zdarzeń na poziomie umożliwiającym przeprowadzenie dokładnej analizy w przypadku kompromitacji systemu.
17. Możliwość edycji, usuwania, anonimizacji i pseudoanonimizacji przetwarzanych danych osobowych oraz wygenerowanie raportu z wszystkimi danymi dotyczącymi wybranego użytkownika/podmiotu danych.
18. Możliwość obsługi mechanizmów retencji danych osobowych oraz informacji wrażliwych (usunięcie po określonym, zadanym przez Zamawiającego w systemie okresie czasu).
19. Możliwość ograniczenia przetwarzania danych np. tylko do podglądu, tylko do wydruku itp.
20. Możliwość zastosowania architektury wysokiej dostępności (HA – High Availability).
21. Możliwość integracji z systemem klasy SIEM (Security Information and Event Management) Zamawiającego.
22. Możliwość integracji z systemami „backupu” Zamawiającego (celem szybkiego przywrócenia danych po awarii).
23. Możliwość przechowywania logów systemowych od dnia ich zapisu, przez wskazany przez Zamawiającego okres, a w przypadku braku odrębnych wskazań przez dwa lata.
24. Możliwość integracji z usługami AD (Active Directory) lub innymi umożliwiającymi implementację SSO (Single Sign-On) na bazie AD. Preferowanym rozwiązaniem jest integracja z usługą Active Directory Federation Services (ADFS).
25. Możliwość obsługi pola/flagi "odnotowano zgodę na przetwarzanie danych osobowych" / "odnotowano sprzeciw wobec przetwarzania danych osobowych".
26. Zarządzanie grupami dostępu:
 - 1) Grupy dostępu powinny łączyć czytniki z harmonogramami działania, z możliwością przypisania czytnika do wielu grup;

- 2) Dostęp posiadacza karty musi być uzależniony od harmonogramu (dzień i czas).
27. System powinien obsługiwać następujące rodzaje przepustek: jednorazowe, stałe, okresowe, alarmowe oraz zapasowe, zapewniając ich właściwe zarządzanie oraz kontrolę dostępu zgodnie z obowiązującymi procedurami.
28. System powinien zapewniać mechanizm blokady edycji numeru ewidencyjnego podczas wystawiania przepustek jednorazowych przez obsługę biur przepustek, aby zapobiec nieautoryzowanym zmianom. W przypadku przepustek stałych i okresowych przeznaczonych dla pracowników, pole numeru ewidencyjnego na stanowiskach bramkowych musi być zablokowane, a wszelkie modyfikacje w tym zakresie mogą być dokonywane wyłącznie przez uprawnionego administratora systemu.
29. Monitorowanie i pre-alarm:
- 1) System musi monitorować pozycję drzwi i generować pre-alarmy w przypadku otwarcia drzwi przez określony czas;
 - 2) Możliwość konfiguracji pre-alarmów.
30. Bezpieczeństwo PIN i karty:
- 1) Obsługa zdarzeń dotyczących nieprawidłowego PIN-u z możliwością konfiguracji liczby prób i resetu liczników;
 - 2) Alarmowanie i blokada czytnika po przekroczeniu progu błędnych prób.
31. Interfejs użytkownika:
- 1) GUI musi zapewniać dostęp do danych drzwi, statusów, trybów działania, z możliwością filtrowania i maskowania zdarzeń zgodnie z harmonogramem;
 - 2) Obsługa harmonogramów dla różnych pięter oraz raportowanie ruchu użytkowników.
32. Wejścia/wyjścia i makra:
- 1) Możliwość lokalnego wyzwalania zdarzeń przez I/O, tworzenia makr z minimum 20 krokami, oraz powiązania zdarzeń z makrami.
33. Implementacja polityki haseł (wymuszanie minimalnej długości, jakości, częstotliwości zmian, ukrywania wprowadzanych znaków) dla kont nie będących zintegrowanymi w ramach SSO.
34. Szyfrowanie komunikacji przekazywanych danych z wykorzystaniem technik kryptograficznych i długości kluczy uzgodniony na etapie projektowania z Zamawiającym.
35. Poziomy dostęp i funkcjonalności aplikacji:
- 1) Trzy poziomy dostęp: administrator, rozszerzony użytkownik, ograniczony użytkownik;
 - 2) Administrator ma dostęp do modułu zarządzania alarmami, procedur alarmowych, integracji z kamerami.
36. Wymagane jest, aby Wykonawca wykorzystał najnowszą wersję stabilną (produkcyjną) danego komponentu oraz dopasował system do udostępnianych przez producenta aktualnych wersji lub poprawek dla danej wersji w terminie maksymalnie 12 miesięcy od udostępniania nowej wersji oraz w terminie maksymalnie 1 tygodnia od udostępnienia aktualizacji bezpieczeństwa, w okresie gwarancji.
37. Wszystkie stosowane przez Wykonawcę w Systemie komponenty muszą być w wersji oficjalnie wspieranej i rozwijanej przez producenta danego komponentu.
38. Certyfikat SSL (https) musi być ważny w wymaganym okresie (ważność od/ważność do) oraz wartości „CommonName” lub „subjectAltName” muszą być zgodne z nazwą hosta serwera – nie dopuszcza się rozwiązań opartych na zabudowanych certyfikatach producenta.

39. Wymagane jest, aby wszystkie wykorzystane przez Wykonawcę komponenty firm trzecich dostarczone i wykorzystane były w oficjalnej wersji udostępnianej przez Producenta danego komponentu oficjalnym kanałem dystrybucji jego oprogramowania.
40. System kontroli dostępu ma być odporny na awarię serwera.
41. Funkcje antypassback, zasada czworga oczu czy podwójna weryfikacja, mają być realizowane bezpośrednio na poziomie kontrolerów.
42. System powinien zapewnić stale rozwijaną bibliotekę modułów, które obejmują szeroki zakres komponentów dostosowanych do różnych potrzeb. Wśród nich znaleźć się mają zarówno rozwiązania do kontroli pojedynczych drzwi, jak i bardziej zaawansowane elementy, takie jak służby powietrzne, które umożliwiają precyzyjną kontrolę przepływu osób.
43. System musi wspierać realizację skomplikowanych reguł bezpieczeństwa, takich jak zasada „czworga oczu”, która wymaga jednoczesnej autoryzacji kilku osób do uzyskania dostępu.
44. Monitorowanie stanu kontaktronów, pozwalające na natychmiastowe wykrywanie nieautoryzowanych prób otwarcia drzwi.
45. System powinien integrować funkcję kompleksowego wykrywania włamań.
46. System powinien mieć możliwość definiowania czasu otwarcia drzwi dla konkretnej karty i czytnika.
47. Elastyczne zarządzanie logiką sterowania i automatyzacją procesów bezpieczeństwa zarządzane przez wirtualny sterownik PLC.
48. System SKD powinien umożliwiać korzystanie z interfejsów webowych dedykowanych użytkownikom – rozbudowanego interfejsu pełnego przeznaczonego do realizacji zadań na biurze przepustek (m.in. zarządzanie użytkownikami, wydawanie kart dostępu, definiowanie grup przejść, konfigurowanie harmonogramów czasowych, generowanie raportów, obsługę alarmów, integrację z modułem telewizji dozorowej oraz monitorowanie zdarzeń).
49. Interfejs pełny ma być wyposażony w unikalną funkcję tworzenia indywidualnie konfigurowalnych paneli (tzw. paneli face), które będzie można dostosować do specyficznych potrzeb operacyjnych (np. na takim panelu dla wybranego przejścia dwustronnego, w momencie przyłożenia przepustki zbliżeniowej do czytnika, na ekranie operatora ma pojawić się zdjęcie właściciela przepustki zapisane w bazie danych, widok na żywo z kamer monitorujących obie strony drzwi, monitor zdarzeń tekstowych oraz wirtualne przyciski do otwarcia drzwi lub wywołania alarmu).

3.8. Bezpieczeństwo i redundancja systemu

Architektura systemu SKD powinna być pozbawiona tzw. pojedynczego punktu podatności na awarię. Należy zastosować rozwiązanie z serwerem redundantnym.

3.9. Wymagania dla SKD w zakresie ochrony danych

1) Wymagania w zakresie RODO:

Z uwagi na przetwarzanie w projektowanych/implementowanych systemach zwykłych danych osobowych, w systemie wdrożone mają być rozwiązania zapewniające bezpieczeństwo danych osobowych zgodnie z zasadami, określonymi w RODO - Rozporządzeniu 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). Na etapie analizy przedwdrożeniowej, tworzenia i uzgodnienia z Zamawiającym projekt powinien zawierać:

- a) Opis planowanych/projektowanych do implementacji rozwiązań w obszarze bezpieczeństwa teleinformatycznego, w postaci listy zabezpieczeń w warstwie architektury sieci, danych i ich szczegółowych opisów;

- b) Analizę ryzyka wystąpienia naruszenia praw wolności osób fizycznych oraz wykaz zastosowanych zabezpieczeń minimalizujących ryzyko zgodnie z art. 25 RODO wraz z oceną skutków dla ochrony danych zgodnie z art. 35 RODO. Jeżeli operacje przetwarzania danych osobowych w systemie mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych - przeprowadzenie dodatkowej szczegółowej analizy systemu zaproponowanie zabezpieczeń pozwalających zredukować zidentyfikowane ryzyko do poziomu akceptowalnego.

2) Zgodność z Dyrektywą UE:

Wszystkie zaprojektowane urządzenia i systemy muszą być zgodne z Dyrektywą w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej- NIS2 (Network and Information Systems Directive), a w szczególności obejmować one muszą mechanizmy i procedury zapewniające spełnienie obowiązków Zamawiającego w zakresie:

- a) analizy ryzyka i polityki bezpieczeństwa systemów informatycznych;
- b) obsługi incydentów (zapobieganie, wykrywanie i reagowanie na incydenty);
- c) ciągłości działania i zarządzania kryzysowego;
- d) bezpieczeństwa łańcucha dostaw;
- e) procedur (testowanie i audyt) służących ocenie skuteczności środków zarządzania ryzykiem cyberbezpieczeństwa;
- f) wykorzystywania kryptografii i szyfrowania.

3) Zgodność z CER:

Wszystkie zaprojektowane urządzenia i systemy muszą być zgodne z CER (Cyber Policy) – w sprawie odporności podmiotów krytycznych, a w szczególności obejmować one muszą mechanizmy i procedury zapewniające spełnienie obowiązków Zamawiającego w zakresie:

- a) Zapobieganie incydentom, w tym środki zmniejszania ryzyka związanego z katastrofami i przystosowania się do zmiany klimatu;
- b) Zapewnienie odpowiedniej fizycznej ochrony budynków i terenów oraz infrastruktury krytycznej;
- c) Odpowiedź na incydenty, stawianie im oporu i łagodzenie ich skutków, w tym procedury i protokoły zarządzania ryzykiem i zarządzania kryzysowego, a także procedury ostrzegawcze;
- d) Odtworzenie po incydentach, w tym środki na rzecz ciągłości działania oraz identyfikacji alternatywnych łańcuchów dostaw;
- e) Zapewnienie odpowiedniego zarządzania bezpieczeństwem pracowników;
- f) Zwiększanie świadomości odpowiedniego personelu na temat środków wzmacniania odporności.

4) Zgodność z Dyrektywą NDAA:

Producent urządzeń kontroli dostępu nie może być ani współpracować z firmami, które objęte są sankcjami dyrektywy NDAA.

4. INTEGRACJA SYSTEMU KONTROLI DOSTĘPU Z INNYMI SYSTEMAMI

4.1. Integracja z systemami SSWiN, CCTV, SSP, depozytorem kluczy

1. System SKD ma zapewnić pełną kompatybilność i sprawną integrację z systemami depozytora kluczy, takimi jak np. Traka, Deister, SAIK oraz SafeKey. Integracja tych systemów z SKD ma umożliwić wykorzystanie jednej karty dostępu lub synchronizację baz danych użytkowników pomiędzy systemami, co uprości zarządzanie kluczami i dostępem. Ponadto system ma pozwalać na aktywne blokowanie wyjścia osób z obiektu w sytuacji, gdy nie zostaną zwrócone odpowiednie klucze.

2. W zakresie monitoringu i nadzoru system SKD ma współpracować z szerokim spektrum wiodących platform telewizji dozorowej (CCTV), zapewniając integrację z systemami takimi jak IndigoVision, Cortrol Ganz, HIKCentral, Guetenbruck, AnyVision, Milestone oraz HIKVISION. Integracja ma pozwalać na centralne zarządzanie obrazem z kamer, rejestrowanie zdarzeń związanych z kontrolą dostępu oraz umożliwi szybkie reagowanie na incydenty bezpieczeństwa. Wykonawca zobowiąże się dostosować system ochrony przeciwpożarowej budynku w taki sposób, żeby wystąpiło automatyczne zwalnianie kontroli dostępu w przypadku wystąpienia alarmu pożarowego. Dotyczy przejść opisanych w tabeli: Wykaz przejść (punkt 2.1) pod numerami 3, 4, 5, 6, 11, 13, 17, 18, 19, 20, 22, 26.

4.2. Integracja w Lokalnym Centrum Nadzoru

System kontroli dostępu powinien zostać zintegrowany z lokalnym centrum nadzoru, co umożliwi centralne zarządzanie dostępem do wszystkich przejść i wjazdów na terenie obiektu. W ramach takiej integracji urządzenia kontrolujące dostęp, takie jak czytniki kart, zamki elektroniczne oraz kamery, będą połączone z centralnym punktem nadzoru, który będzie odpowiedzialny za monitorowanie oraz autoryzację dostępu. Lokalne centrum nadzoru ma pełnić funkcję centralnego ośrodka zbierającego i przetwarzającego dane z urządzeń kontrolujących dostęp.

4.3. Integracja SKD z bazą pośrednią systemów z danymi pracowników i studentów

1. Projektowany system kontroli dostępu w Akademii powinien być zintegrowany z bazą pośrednią systemów zawierających dane pracowników i studentów z bezwzględnym uwzględnieniem:

- 1) automatycznej aktualizacji danych pracowników i studentów

Integracja z bazą pośrednią umożliwia automatyczne i cykliczne aktualizowanie danych personalnych w Systemie Kontroli Dostępu, w przypadku pracowników: imię, nazwisko, stanowisko, dział, uprawnienia, status zatrudnienia, zdjęcie a w przypadku studentów imię, nazwisko, PESEL, nr albumu, wydział, status (student, doktorant), data ważności uprawnień, zdjęcie;

- 2) spójności i centralizacji danych

Dane pracowników i studentów są przetwarzane w systemach ERP i USOS. Baza pośrednia pełni rolę warstwy integracyjnej, zapewniając unifikację formatów danych, standaryzację identyfikatorów pracowników, filtrowanie i selekcję danych istotnych z punktu widzenia kontroli dostępu (np. tylko aktywni pracownicy);

- 3) reagowania w czasie zbliżonym do rzeczywistego

Dzięki integracji, zmiany statusu pracownika i studenta (np. zakończenie współpracy, zmiana działu, urlop bezpłatny, zakończenie studiów) mogą być niemal natychmiastowo odzwierciedlone w systemie kontroli dostępu. Minimalizuje to ryzyko nieautoryzowanego wejścia osób, które nie powinny mieć już uprawnień;

- 4) zgodności z polityką bezpieczeństwa informacji

Funkcjonowanie SKD musi być zgodne z wymogami polityki bezpieczeństwa informacji poprzez m.in. rejestrowanie historii zmian danych i uprawnień, możliwość śledzenia źródła danych i czasu ich aktualizacji. Integracja z bazą pośrednią ma zapewnić łatwiejsze raportowanie i kontrolę dostępu na podstawie aktualnych informacji kadrowych;

- 5) skalowalności i łatwości zarządzania

Integracja z bazą pośrednią zapewni skalowalność SKD wraz ze zmianami w organizacji (np. otwarcie nowego oddziału, zatrudnienie większej liczby pracowników) i nie będzie wymagane ręczne wprowadzanie nowych danych do systemu dostępowego. Integracja z bazą pośrednią automatyzuje zasilanie systemu niezbędnymi danymi.

5. ZAKRES DOKUMENTACJI

1. Projekt wykonawczy

- 1) Wykonawca w ciągu 2 miesięcy od daty podpisania umowy wykona i przedstawi Zamawiającemu do zatwierdzenia projekt wykonawczy (projekt podzielony na występujące branże w zakresie uwzględniającym specyfikę robót w podziale na branże:
 - a) Architektoniczno – budowlana;
 - b) Elektryczna;
 - c) Ochrony przeciwpożarowej;
 - d) Teletechniczna.
- 2) Dokumentacja projektowa do akceptacji musi być dostarczona w formie elektronicznej w wersji edytowalnej i nieedytowalnej (pliki dwg, MS Word Excel i PDF).
- 3) Zaakceptowany projekt należy dostarczyć w formie papierowej 3 komplety dokumentacji i jeden komplet na nośniku elektronicznym (pliki dwg, doc, xls i pdf).
- 4) Cały proces uzyskania niezbędnych zgód i pozwoleń spoczywa na Wykonawcy przy czynnym wsparciu Zamawiającego.
- 5) Prace realizacyjne rozpoczną się po protokolarnej akceptacji ww. projektu przez Zamawiającego oraz po uzyskaniu przez Wykonawcę w imieniu Zamawiającego wszelkich wymaganych prawem uzgodnień, pozwoleń i decyzji.

2. Projekt wykonawczy powinien zawierać:

- 1) Zakres informacji ogólnych
 - a) Podstawa opracowania (przywołanie podstawy realizacji projektu - umowa, spis kluczowych uzgodnień z Zamawiającym i podmiotami opiniującymi poczynionych w trakcie realizacji dokumentacji projektowych, dokumentacje istniejących systemów i instalacji, które wejdą w skład realizowanych prac);
 - b) Przedmiot, zakres opracowania (określenie co jest przedmiotem opracowania, jaki obiekt, jakie prace należy wykonać);
 - c) Przywołanie stosownych Norm i przepisów związanych.
- 2) W projekcie należy zawrzeć zapis:

„Dopuszcza się zastosowanie urządzeń, materiałów o parametrach równoważnych bądź lepszych od tych zawartych w niniejszym opracowaniu, przy czym Wykonawca jest zobowiązany zapewnić prawidłowe działanie poszczególnych systemów technicznych i technologicznych oraz osiągnięcie założeń funkcjonalnych dla poszczególnych elementów, wbudowanych systemów”.
- 3) Opis techniczny z częścią rysunkową:
 - a) Przedstawienie charakterystyki systemu i jego funkcjonowania;
 - b) Opis szczegółowych rozwiązań projektowych wraz ze schematami blokowymi i ideowymi;
 - c) Opis projektowanych urządzeń, oprogramowania i w odniesieniu do nich spis wymagań funkcjonalno-użytkowych;
 - d) Opis integracji i powiązań pomiędzy instalacjami i systemami z uwzględnieniem instalacji bezpieczeństwa PPOŻ, LCN oraz wymagań BHP;
 - e) schematy okablowania oraz tras kablowych;
 - f) Projekt zasilania urządzeń;
 - g) Karty katalogowe, atesty, certyfikaty urządzeń wraz ze spisem;
 - h) Oświadczenie Wykonawcy o zgodności wykonanego systemu z normami, wytycznymi i wiedzą techniczną.

3. Dokumentacja powykonawcza

- 1) Dokumentacja powykonawcza powinna zawierać:
 - a) spis treści;
 - b) oświadczenie kierownika robót;
 - c) zatwierdzone karty materiałowe wraz z załącznikami;
 - d) instrukcję konserwacji i utrzymania;
 - e) dokumentację techniczno – ruchową systemu;
 - f) protokoły pomiarowe z certyfikatem wzorcowania miernika oraz uprawnieniami osoby wykonującej pomiary i osoby sprawdzającej (uprawnienia - o ile są wymagane);
 - g) protokoły odbiorów częściowych lub robót zanikających;
 - h) protokoły rozruchów instalacji, systemów;
 - i) protokoły odbiorów;
 - j) gwarancję na urządzenia;
 - k) opis i oznaczenie przebieg przez ściany, stropy i przejść pożarowych;
 - l) potwierdzenie przeprowadzenia szkoleń.
- 2) Zamawiający nie dopuszcza dostarczenia dokumentacji projektowej jako dokumentacji powykonawczej.
- 3) Dokumentację powykonawczą należy dostarczyć Zamawiającemu w formie elektronicznej do akceptacji. Zaakceptowaną dokumentację należy dostarczyć w formie papierowej: trzy komplety dokumentacji i jeden komplet na nośniku elektronicznym (pliki edytowalne dwg, doc, xls i nieedytowalne pdf).

6. RÓWNOWAŻNOŚĆ

Zamawiający dopuszcza inne rozwiązania o parametrach nie gorszych niż dla wyspecyfikowanych urządzeń (kryteriami równoważności). Wykonawca musi zapewnić pełne wdrożenie oferowanego rozwiązania wraz z wymaganymi licencjami, przeszkoleniem użytkowników i administratorów systemu oraz zapewnić pełną współpracę z używanym obecnie środowiskiem informatycznym i systemami działającymi na terenie WAT.

7. WIZJA LOKALNA

Zamawiający przewiduje zorganizowanie obowiązkowej wizji lokalnej. (Zgodnie z art. 266 ust. 1 pkt. 18 Ustawy prawo zamówień publicznych Zamawiający może nie przyjąć oferty od firmy, która nie uczestniczyła w wizji lokalnej).

8. TERMIN REALIZACJI PRAC

Termin realizacji prac: 10 miesięcy liczone od dnia podpisania umowy.

9. WARUNKI GWARANCJI I SERWISU

Wykonawca zapewni Zamawiającemu gwarancję na dostarczony sprzęt i urządzenia na okres minimum 60 miesięcy (5 lat), która obejmie również wykonywanie autoryzowanych przez producenta przeglądów okresowych w tym czasie. W trakcie obowiązywania gwarancji Wykonawca będzie zobowiązany do regularnego podnoszenia wersji oprogramowania zainstalowanego w ramach realizacji zamówienia, bez naliczania dodatkowych kosztów dla Zamawiającego.

Zamawiający oczekuje od Wykonawcy przedstawienia harmonogramu przeglądów wraz z dokładnym określeniem wykonywanych czynności.