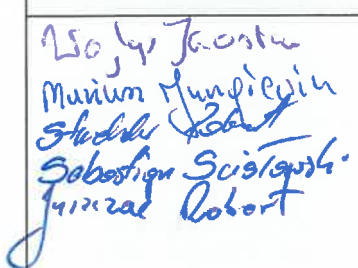






„Zaprojektowanie, dostarczenie oraz wdrożenie platformy integrującej Systemu Kontroli Dostępu, Systemu Monitoringu Wizyjnego, Systemu Awizacji w Enea Elektrownia Połaniec S.A.”

Wspólny Słownik Zamówień CPV:

50320000-4	usługi w zakresie napraw i konserwacji komputerów osobistych
50340000-0	usługi w zakresie napraw i konserwacji urządzeń audiowizualnych i optycznych
72300000- 8	usługi w zakresie danych
32333200-8 -	Kamery wideo
31350000-4 -	Przewodniki elektryczne do celów przetwarzania danych i sterowania

sporządził:	sprawił pod względem merytorycznym:	sprawił pod względem formalno-prawnym:
	<p>Kierownik Biura Bezpieczeństwa</p>  <p>Marcin Dulowski</p>	<p>Piotr Radziłowski</p>  <p>RADCA PRAWNY WA 5185</p>

Wprowadzenie

Celem niniejszego opracowania jest określenie minimalnych parametrów technicznych dla modernizowanych systemów bezpieczeństwa w elektrowni Połaniec, wraz z wyspecyfikowaniem podstawowych materiałów niezbędnych do zaprojektowania, wdrożenia i uruchomienia systemów:

- System Kontroli Dostępu (dalej „SKD”),
- System Monitoringu Wizyjnego CCTV (dalej „CCTV”),
- Zintegrowanego Systemu Bezpieczeństwa (ZSB),
- System Awizacji (dalej „SA”),\
- Książki telefonicznej

Mając na uwadze rozległą strukturalną zabezpieczanego obiektu, proponuje się systemy bezpieczeństwa oparte o sieć strukturalną TCP/IP, która będzie wspólna dla systemów zabezpieczeń technicznych i dla systemu CCTV technologicznego.

Wykonawca zadania winien przewidzieć wszystkie niezbędne materiały i urządzenia do prawidłowego wykonania modernizacji instalacji CCTV, SKD, integracji i Awizacji np: urządzenia aktywne, wybudowanie sieci LAN światłowodowej, wybudowanie sieci LAN miedzianej, przebudowy instalacji zasilającej, budowy punktów dystrybucyjnych wyposażonych w odpowiednie switche dostępowe, agregacyjne, monitory, stacje klienckie, licencje, patchcordy itp.

Nowoprojektowane i zainstalowane urządzenia/kamery powinny być oparte o istniejącą i funkcjonującą platformę VMS Mirasys, którą należy rozbudować o dodatkowe 216 kanałów wizyjnych i wykupienie licencji VCA na 100 kanałów, oraz przewidzieć odpowiednie dedykowane do platformy VMS Mirasys serwery rejestrujące, lub inny system oparty na podobnej architekturze. Przy innym proponowanym systemie i jego akceptacji należy uwzględnić już obecne wykupione 90 licencji (kanałów), czyli razem 306 licencje.

Współczesne systemy kontroli dostępu bazują na sieciach komputerowych zapewniając łatwe łączenie podsystemów, elastyczną rozbudowę oraz nieograniczoną możliwość interakcji z innymi systemami bezpieczeństwa bazującymi na tym samym medium. Wykonawca ma zaprojektować, dostarczyć oraz wdrożyć kompletny System Kontroli Dostępu, mający możliwość nadzoru, zarządzania, konfigurowania, kodowania, dodawania przepustek z jednego miejsca, zgodnie z normą EN60839-11 grade/klasa4. Wykonawca powinien w tym zakresie posiadać certyfikat wydany przez zewnętrzną jednostkę certyfikującą a nie przez producenta SKD. Wykonawca winien przewidzieć, że niektóre drzwi należy zmodernizować i przystosować do zabudowy systemu kontroli dostępu.

Minimalne wymagania dla projektowanych i implementowanych w EEP systemów w zakresie wypełnienia wymagań RODO.

Z uwagi na przetwarzanie w projektowanych/implementowanych Systemach (SKD, CCTV, Platforma Integrująca, System Awizacji, Książka Telefoniczna) zwykłych danych osobowych, w Systemach 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). W ramach wdrożenia wymaga się dostarczenia funkcjonalności wynikających z przepisów RODO oraz dobrych praktyk z zakresu bezpieczeństwa informacji, w tym:

- Zarządzanie uprawnieniami użytkowników poprzez odpowiednią strukturę ról z wyróżnieniem poziomów uprawnień przynajmniej dla administratora i użytkownika.
- Możliwość integracji z usługami AD lub innymi umożliwiającymi implementację SSO.
- Implementację polityki haseł (wymuszanie minimalnej długości, jakości, częstotliwości zmian, ukrywania wprowadzanych znaków).
- Szyfrowanie komunikacji przekazywanych danych z wykorzystaniem technik kryptograficznych i długości kluczy uważanych aktualnie za bezpieczne.
- 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.
- Logowanie zdarzeń na poziomie umożliwiającym dokładną analizę w przypadku kompromitacji systemu.
- Możliwość edycji, usuwania, anonimizacji i pseudonimizacji przetwarzanych danych osobowych oraz wygenerowanie raportu z wszystkimi danymi dotyczącymi wybranego użytkownika/podmiotu danych.
- Możliwość obsługi mechanizmów retencji danych osobowych oraz informacji wrażliwych (usunięcie po określonym, zadanym przez Zamawiającego w systemie okresie czasu).
- Możliwość ograniczenia przetwarzania danych np. tylko do podglądu, tylko do wydruku itp.
- Możliwość obsługi pola/flagi "odnotowano zgodę na przetwarzanie danych osobowych".
- Możliwość obsługi pola/flagi "odnotowano sprzeciw wobec przetwarzania danych osobowych".
- Możliwość zastosowania architektury wysokiej dostępności (HA),
- Możliwość integracji z systemem klasy SIEM Zamawiającego,
- Możliwość integracji z systemami backupu Zamawiającego (celem szybkiego przywrócenia danych po awarii),
- Logi powinny być przechowywane od dnia ich zapisu, przez wskazany przez Zamawiającego okres, a w przypadku braku odrębnych wskazań przez dwa lata.
- 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.
- 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 lub w terminie maksymalnie 1 tygodnia od udostępnienia aktualizacji bezpieczeństwa,
- Wszystkie stosowane przez Wykonawcę w Systemie komponenty muszą być w wersji oficjalnie wspieranej i rozwijanej przez producenta danego komponentu.

- Przeprowadzenie testów penetracyjnych wdrażanego rozwiązania wraz z ich wynikiem przez niezależny zewnętrzny podmiot (przedstawienie wyników Zamawiającemu).
- Systemy mają umożliwiać wyświetlanie okienek typu pop-up z komunikatami (np. informacja o RODO/klauzula informacyjna). Treść komunikatu powinna być możliwa do edycji przez Zamawiającego, powinna być też możliwość ustawienia okresu wyświetlania komunikatu. Użytkownik musi mieć możliwość potwierdzenia zapoznania się z komunikatem i jego odrzucenia. W przypadku zatwierdzenia, kolejne wejście na stronę nie będzie powodować wyświetlania komunikatu (informacja przechowywana w „cookies”). W systemie może być ustawiony więcej niż jeden pop-up.
- System powinien posiadać możliwość zarządzania plikami „cookies” przez użytkownika systemu oraz informować użytkownika o celach ich przechowywania i kategoriach (umożliwienie użytkownikowi wyrażenia zgody na stosowanie plików cookies przed rozpoczęciem korzystania z witryny – zgodnie z obowiązującymi przepisami prawa w tym unijną dyrektywą ePrivacy).
- Na etapie analizy przedwdrożeniowej (tworzenia i uzgodnienia z Zamawiającym opracowanego projektu), koncepcja powinna zawierać dla projektowanych Systemów:
 - Opis planowanych/projektowanych do implementacji rozwiązań w obszarze bezpieczeństwa teleinformatycznego, w postaci listy zabezpieczeń w warstwie architektury sieci/danych i ich szczegółowych opisów.
 - Analizę ryzyka wystąpienia naruszenia praw i 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 i zaproponowanie zabezpieczeń pozwalających zredukować zidentyfikowane ryzyko do poziomu akceptowalnego.

System Kontroli Dostępu

Dostarczony system zapewnia funkcjonalnie nieograniczoną rozbudowę w zakresie:

- 1) Liczby przejść kontrolowanych przez system.
- 2) Liczby identyfikatorów w systemie.

- 3) Liczby rekordów bazy danych.
- 4) Liczby filii zarządzanych z poziomu serwera centralnego.
- 5) Liczby zdarzeń w systemie.
- 6) Liczby użytkowników w systemie.

Dostarczony system będzie cechował się bardzo dużym stopniem stabilności i redundancji. Warunkiem koniecznym jest zapewnienie w systemie autonomicznego działania kontrolerów, dyspozycyjności 24h, 365 dni/rok oraz spełniać wymogi GRADE 4.

Oznacza to, że:

- 1) Kontrolery muszą być standardowymi urządzeniami sieciowymi (posiadającymi możliwość komunikacji z innymi urządzeniami w sieci TCP/IP, bez konieczności stosowania jakiegokolwiek formy konwersji sygnału.
- 2) Kontrolery będą komunikować się z innymi kontrolerami na zasadzie „peer to peer” (bez pośrednictwa serwera),
- 3) Kontrolery powinny posiadać dużą moc obliczeniową (CPU minimum 800MHz) i duże zasoby pamięci (min. 256 MB SDRAM, 2 GB pamięci typu Flash).
Komunikacja w systemie musi odbywać się z wykorzystaniem protokołu TCP/IP w sposób szyfrowany i zabezpieczony protokołem SSL/TLS i szyfrem co najmniej 128 bitowym. Wszystkie kontrolery sieciowe muszą wspierać model uwierzytelniania 802.1x, celem wyeliminowania niebezpieczeństwa polegającego na nieautoryzowanym dostępie do sieci już na poziomie warstwy dostępu do sieci.
- 4) Monitorowanie urządzeń powinno zostać zrealizowane poprzez protokół SNMP v3 z użyciem wszelkich dostępnych mechanizmów bezpieczeństwa lub równoważny.
- 5) Logowanie do systemu musi być zabezpieczone indywidualnym loginem i hasłem, przy czym system musi pozwalać na wymuszenie przez administratora stosowania haseł o określonej sile oraz ich zmianę po określonym interwale czasowym.
- 6) Logowanie do aplikacji systemu kontroli dostępu musi wspierać mechanizm podwójnej autentykacji tzw. Two-factor authentication (2FA)
- 7) System musi zapewniać swobodne programowanie funkcjonalności (na poziomie kontrolera) z poziomu prostej aplikacji graficznej za pomocą metod „drag and drop”.

Minimalne wymagania dla projektowanego środowiska serwerowego:

- 1) Serwer produkcyjny powinien działać w klastrze HA (w razie uszkodzenia 1 węzła zostaje uruchomiony drugi).
- 2) Środowisko serwerowe musi składać się z:
 - a) Serwera aplikacji umożliwiającego pracę w dowolnym systemie wspomagany przez rodzinę produktów firmy Microsoft.
 - b) Relacyjnej bazy danych (serwera bazodanowego) wykorzystującego język zapytań SQL.
- 3) Projektowane środowisko serwerowe powinno spełniać następujące minimalne wymagania sprzętowe:
 - a) Nowoczesna 64 bitowa maszyna serwerowa (zastosowane serwery będą serwerami wirtualnymi w środowisku VMWare.).
 - b) Jeden z poniższych systemów operacyjnych:

- Microsoft Windows Server 2016R2 lub aktualnie będący w sprzedaży.
- c) Jedna z poniższych baz danych:
 - Oracle® 19c Enterprise edition lub wyższa.
 - MS SQL Server 2016, wersja Standard lub wyższa lub Enterprise (nie akceptowalna wersja Express) - MySQL Enterprise Edition
 - PostgreSQL wersja 9.x/10.x

Aplikacja Klientka/Operatorska musi:

- 1) Umożliwiać dostęp do systemu dla Użytkownika (role typu: Administrator, Operator, Biuro Przepustek, Recepcja) z poziomu przeglądarki internetowej – brak konieczności instalowania dodatkowego, dedykowanego oprogramowania na stacjach roboczych.
- 2) Wspierać minimum poniżej wskazane przeglądarki w najnowszych oficjalnych obowiązujących wersjach:
 - a) Microsoft Edge.
 - b) Firefox.
 - c) Chrome.

Wymagania dotyczące projektowanych kontrolerów:

- 1) Kontrolery muszą zapewniać możliwość autonomicznego podejmowania decyzji o autoryzacji bez udziału serwera (informacje niezbędne do autoryzacji opcjonalnie muszą być przechowywane w pamięci kontrolerów, i na serwerze SKD).
- 2) Kontrolery muszą buforować co najmniej 1 000 000 zdarzeń pracując w trybie autonomicznym, dodatkowo musi nadpisywać najstarsze w przypadku wypełnienia bufora zdarzeń.
- 3) Buforowane zdarzenia muszą być automatycznie przesyłane, po odzyskaniu łączności z serwerem.
- 4) Kontrolery muszą mieć możliwość bieżącego przekazywania informacji o stanach czujników (np. kontaktronów drzwiowych) również podczas braku dostępu do serwera.
- 5) Kontrolery systemu muszą posiadać możliwość pracy w trybie autonomicznym. Oznacza to, że w sytuacji braku dostępu do serwera z jednej strony będą one w stanie przejąć na siebie rolę bezpośredniej komunikacji między sobą i będą przysyłać na bieżąco informacje o stanach przejść (drzwi otwarte/drzwi zamknięte, drzwi otwarte zbyt długo, drzwi sforsowane itp.) do własnego systemu monitorującego lub do zewnętrznych zintegrowanych systemów monitorujących.
- 6) Jeden kontroler powinien umożliwiać podłączenie minimum 31 modułów kontroli dostępu co pozwala na obsłużenie 32 przejść pojedynczych lub podwójnych.
- 7) Jeden kontroler wraz z modułami dostępu umożliwia obsłużenie minimum 64 czytników kart.
- 8) Zmiana oprogramowania czy konfiguracji systemu musi być możliwa dla administratora w całości systemu z jednego centralnego punktu lub dla wybranych elementów/modułów lokalnie bezpośrednio w kontrolerze (nowa konfiguracja przesyłana jest do serwera) lub centralnie poprzez serwer.

Możliwe musi być zdalne sprawdzenie pełnej konfiguracji zapisanej w pamięci wybranego kontrolera (poprzez graficzne narzędzie pozwalające na monitorowanie działania systemu w

trybie na żywo – np. przyłożenie identyfikatora do czytnika spowoduje zaznaczenie całej ścieżki sygnału w systemie od czytnika, poprzez moduł czytnika aż do kontrolera).

9) System musi być zaprojektowany w oparciu o architekturę gwiazdy przy użyciu tylko kontrolerów, połączonych bezpośrednio do przełączników sieciowych. W architekturze systemu mogą być użyte kontrolery na osobnej magistrali do obsługi modułów rozszerzających ilości wejść i wyjść. Magistrala musi być szyfrowana i w pełni zarządzana.

10) Dostarczony system musi posiadać integrację z systemem platformy integrującej potwierdzoną przez producenta tego systemu w zakresie:

a) Wizualizacji stanów pracy: otwarcie przejścia za pomocą karty, udzielenia dostępu do KD przez administratora, zakluczenia drzwi których zamki wysyłają takie stany oraz stan awarii.

b) Sterowania przejściami: otwarcie, zamknięcia drzwi,

11) Kontrolery muszą posiadać według normy PN-EN 60839-11-1 własny zasilacz z własnym akumulatorem Aby spełnić wymogi Grade 4 kontroler musi monitorować dodatkowo zasilanie 230 VAC i stan akumulatora.

Wymagania dotyczące oprogramowania aplikacyjnego:

1) System musi posiadać, co najmniej trzy rodzaje oprogramowania aplikacyjnego lub zapewniać, w zależności od uprawnień osoby zalogowanej do aplikacji uzyskanie co najmniej trzech poziomów zarządzania systemem:

a) Poziom administratora.

b) Poziom rozszerzony użytkownika (możliwość zarządzania alarmami, drzwiami, możliwość dodania komentarza dla poszczególnych alarmów).

c) Poziom ograniczony użytkownika (informacja o stanie autoryzacji wraz z prezentacją miejsc w których autoryzacja bądź jej brak miała miejsce).

2) Oprogramowanie najwyższego poziomu musi zawierać wbudowany moduł obsługi i monitorowania alarmów i stanów czujników Systemu Kontroli Dostępu. W module tym musi być możliwość przypisywania do konkretnych alarmów/zdarzeń określonych procedur. W ramach procedur alarmowych wyświetlane muszą być przygotowane wcześniej instrukcje alarmowe, a w określonych przypadkach, system musi wymuszać opatrzenie alarmu komentarzem i zestawem komentarzy pracownika ochrony pełniącego służbę na stanowisku monitoringu obiektowego. System musi umożliwiać również automatyczne pokazanie podglądu z kamery wideo, która jest skojarzana z punktem alarmowym np. główne wejście do budynku, lub wyświetlane na mapie synoptycznej.

3) Oprogramowanie niższego poziomu musi wykorzystywać do komunikacji pomiędzy systemem a użytkownikiem przede wszystkim elementy graficzne takie jak ikony, okna i przyciski. System musi pozwalać na podłączanie urządzeń do automatycznego zaczytywania niezbędnych danych z dokumentów co najmniej kilku różnych producentów, dzięki którym możliwe będzie wprowadzanie danych osobowych poprzez zaczytywanie dokumentów potwierdzających tożsamość. Oprogramowanie musi posiadać możliwość obsługi czytników kart dla biur przepustek. Oprogramowanie musi zapewniać możliwość wprowadzania tzw. pól dowolnych (np. PESEL itp.) Oprogramowanie musi pozwalać na ograniczanie dostępnych funkcjonalności w zależności od uprawnień i obowiązków użytkownika logującego się do systemu.

4) Wszelkie informacje wyświetlane w oprogramowaniu muszą być dostępne w języku polskim i zawierać polskie znaki diakrytyczne.

5) Poza standardowymi funkcjami oprogramowania systemu KD dotyczącymi nadawania posiadaczom identyfikatorów i uprawnień dla poszczególnych przejść zgodnie z określonymi harmonogramami czasowymi, system musi pozwalać na realizację poniższych funkcjonalności:

- Kontrola obchodu strażników (z możliwością swobodnego kształtowania tras obchodu i okien czasowych dla poszczególnych punktów kontrolnych – czytników).
- Automatyczne blokowanie identyfikatorów po określonym czasie nieużywania.
- Tworzenie profili tymczasowych tzn. zmiana profilu na określony czas, po którym automatycznie zostanie przywrócony poprzedni profil.
- Blokowanie identyfikatorów w wyniku określonych naruszeń instrukcji ruchu osobowego np. złamanie zasady ANTI-PASSBACK.
- System musi pozwalać na automatyczne usuwanie danych odwiedzających po definiowalnym okresie czasu.
- Tekstowy monitor zdarzeń – bieżące wyświetlanie wszystkich zdarzeń w systemie w formie tekstowej.
- Rozbudowany monitor zdarzeń – bieżące wyświetlanie zdarzeń w systemie z towarzyszącymi im zdjęciami (zdjęcia osób wyświetlane w tym samym momencie co zbliżenie identyfikatora do czytnika).
- Tworzenie tzw. czarnych list.
- Awizowanie wizyt gości/firm zewnętrznych przez pracowników posiadających dostęp do systemu.
- Zliczanie osób w określonej strefie i wprowadzanie ograniczeń liczby osób uprawnionych do przebywania w strefie.
- Tworzenie wydzielonych wirtualnie części systemu dla poszczególnych oddziałów, dzięki czemu użytkownicy w poszczególnych oddziałach będą mieli możliwość nadawania uprawnień jedynie osobom przypisanym do swojego oddziału. Wybrani użytkownicy systemu będą mogli kształtować uprawnienia wszystkich osób.
- Stosowanie filtrów przejść, dzięki czemu użytkownicy systemu w poszczególnych oddziałach będą mieli dostęp do przejść przypisanych jedynie do ich oddziału.
- Ograniczenie liczby zbliżeń identyfikatora do czytników, dzięki czemu możliwe musi być wymuszenie właściwej ścieżki poruszania się po obiekcie – jeżeli na drodze od wejścia głównego do pomieszczenia, które jest celem wizyty znajdują się 4 czytniki możliwe musi być ograniczenie tej liczby do 4, co wyeliminuje ryzyko nieuprawnionego poruszania się osoby po obiekcie.
- System KD musi mieć możliwość łączenia zdarzeń tekstowych (np. autoryzacja, otwarcie drzwi itp.) wraz ze zdjęciami poszczególnych użytkowników oraz ujęciem na żywo z kamery, aby móc w trybie rzeczywistym porównać prezentowane dane.

Możliwość importu danych osobowych z innego zewnętrznego źródła (np. baza danych działu personalnego) w minimum standardzie pliku xlsx.

System musi umożliwiać integrację z LDAP.

- System KD musi umożliwiać zastosowanie funkcjonalności ANTI-PASSBACK – uniemożliwia to dwukrotne wejście posiadacza karty do danej strefy bez jej opuszczenia albo użycia niedozwolonego przejścia. APB zapobiega autoryzowanemu wejściu do budynku, strefy lub obszaru przez osobę korzystającą z identyfikatora należącego do osoby już będącej w środku.
- System SKD musi umożliwiać zastosowanie następujących trybów ANTI-PASSBACK - Miękki APB (ANTI PASSBACK)– generuje zdarzenie alarmowe po naruszeniu w/w zasady.

- Twardy APB (ANTYPASSBACK – nie wpuszcza karty z wewnątrz strefy do tej samej strefy - - Czasowy APB (ANTYPASSBACK) – możliwy reset osoby po określonym czasie od wejścia. Infrastruktura IT Zamawiającego oparta jest o platformę wirtualizacją VMware vSphere.
- Serwery systemu KD będą również zwirtualizowane na tej platformie, zarówno środowisko testowe i produkcyjne.
- System ma być zbudowany o klastry HA tak aby wyeliminować pojedyncze punkty awarii.
- System musi posiadać możliwości architektury rozproszonej.
- Pod instalację systemu SKD zostanie udostępniona licencja Windows Server 2016 lub aktualnie będący w sprzedaży.
- System musi być oparty o czytniki obsługujące karty w standardzie Desfire EV1.
- System musi umożliwiać podłączenie dowolnych czytników kart obsługujących inne standardy, ale za pomocą bezpiecznego interfejsu (szyfrowanego) np.: OSPD w wersji 2.
- W ramach projektu zostaną wymienione dwa kołowroty na bramie wejściowej nr 1 o przepustowości nie mniejszej niż 40 osób na minutę w pracy ciągłej oraz furtki sterowane przez służby ochrony w celu całkowitego zabezpieczenia wejścia na obiekt.
- W ramach dostawy zostaną wymienione urządzenia do zczytywania potrzebnych danych z dowodów osobistych oraz drukarki do wydawania przepustek w formie naklejek oraz nadruku na kartach stałych na zgodne z obowiązującymi przepisami prawa (w tym przepisami z zakresu ochrony danych osobowych) lub zostanie zaproponowane inne rozwiązanie przez Wykonawcę w zakresie pozyskiwania niezbędnych danych.
- Klamki od wewnątrz pozostają w związku z przepisami pożarowymi. (wymagania BHP oraz P – poż w Enea Elektrownia Połaniec S. A.).
- System musi obsługiwać :
- <20 tysięcy użytkowników, 24h, 365 dni/rok.
- nadzorować < 1500 przejść, 24h, 365 dni/rok.
- umożliwiać pracę kontrolerów on line lub autonomiczną.
- pojemność zapisu zdarzeń w trybie ON-LINE min. dla kontrolera 500 tys. zdarzeń.
- możliwość określenia 120 dni wolnych, bez ograniczeń.
- funkcja Anti-pass-back.
- zakres temperatur pracy czytników – do -20 oC +50 oC.
- monitorowane wejścia czujników drzwi, przycisków wyjścia, itd.
- współpraca z czytnikami biometrycznymi różnych firm.
- Współpraca z rozwiązaniami biometrycznymi różnych firm, umożliwiającymi rozpoznawanie twarzy.
- Czas na kontrolerach ma być uregulowany i zsynchronizowany z wewnętrznym serwerem NTP obowiązującym u Zamawiającego.
- System musi posiadać przejrzysty interfejs nadawania uprawnień do stref z poziomu widoku użytkownika.
- System powinien mieć możliwość blokowania wejścia dla wybranych osób zgodnie z harmonogramem lub całkowitego zablokowania możliwości wejścia na obiekt.
- System musi posiadać możliwość rozróżnienia użytkowników z dostępem do obiektu dla firm realizujących jako wykonawcy i podwykonawcy prac na rzecz elektrowni.

- Umożliwienie zmiany karty Tymczasowej na Gościa (Tymczasowa powinna stracić uprawnienia analogicznie jak przy przepustkach stałych).
- Po zabranie uprawnień danej karcie należy dawać możliwość zmiany statusu użytkownika na nieobecny w obiekcie – bez konieczności używania karty tego użytkownika na czytniku wyjściowym z obiektu.
- Generowanie się sygnału alarmowego na stanowisku dowodzenia ochroną po odbiciu karty nieuprawnionej.
- Po wymianie czytnika i wysłaniu uprawnień, informowanie o zakończeniu przesyłania uprawnień i jego statusie.
- Umożliwienie zarządzania kontami użytkowników i operatorów całego systemu z poziomu serwera.
- System musi umożliwiać nadawanie uprawnień dla operatorów do wybranej części logicznej/fizycznej systemu.
- Dysponowanie modulem typu wartownik – wyświetlanie zdjęć osób właśnie przechodzących przez dane przejście – w celu dodatkowej weryfikacji wzrokowej – porównywania przechodzącej osoby z jej zdjęciem zapisanym w bazie danych.
- System musi posiadać możliwość integracji z Active Directory.
- Autentykacja do aplikacji będzie następowała poprzez konto domenowe.
- Firma wdrażająca system powinna udostępnić wszystkie potrzebne aplikacje i sterowniki potrzebne do ewentualnego ponownego zainstalowania systemu na stacji roboczej lub serwerze (również sterowniki do drukarek, skanerów itp.)
- Przy zerwaniu etykiety z przepustki tymczasowej brak możliwości na podstawie kodu wewnętrznego ustalenia ostatniego użytkownika, kto miał wydaną przepustkę - chodzi o dołożenie czytnika USB na bramie gdzie wydawane są przepustki tymczasowe.
- Na formularzu przepustki tymczasowej w zakładce dane użytkownika należy usunąć dane pojazdu. Pole zablokować ma być dostępne dla przepustki typu Gość oraz Kontrahent. Na przepustkach tymczasowych pole ma być zablokowane.
- Zablokować edycję numeru ewidencyjnego dla obsługi biur przepustek, podczas wystawiania przepustek rezerwowych. Nr ewidencyjny wprowadzony przy przepustkach stałych. Zablokować pole nr ewidencyjnego przy przepustkach stałych dla Pracowników na bramach, zmiany wprowadza tylko administrator systemu.
- System nie może pozwalać na wydanie równocześnie więcej niż jednej przepustki na użytkownika.
- System ma zapewnić obsłużenie minimalnej przepustowości 2 co 5 minut wjeżdżających i wyjeżdżających samochodów na bramie samochodowej nr 3. Wyjeżdżające samochody będą opuszczać teren elektrowni tą samą bramą. Istnieje możliwość że do czasu wdrożenia Systemu, powstanie 4 brama, która będzie obsługiwała tylko i wyłącznie wyjazdy dostaw biomasy, co zredukuje ilość wyjazdów bramą nr 3 ale nie zlikwiduje ich zupełnie. Sprawna i szybka obsługa pozostałych bram nr 1 i 2. Stanowiska na bramach nie ulegną zmianie. Ww. system musi posiadać możliwość tworzenia dedykowanych grup np. po nazwie firmy i pozwalać na nadawanie określonych uprawnień dla kart tych grup (grupy nie tylko mogłyby być tworzone przy wprowadzeniu do systemu użytkowników ale też wyodrębniane z istniejących już w systemie użytkowników kart.)
- System SKD musi zapewniać dedykowane zabezpieczenia chroniące przed atakami sieciowymi, polegające na wyposażeniu kontrolera drzwiowego w moduł, który umożliwia

przechowywanie certyfikatów uwierzytelniających komunikację między serwerem zarządzającym Systemem Kontroli Dostępu a kontrolerami drzwiowymi. Takie rozwiązanie wymusza autentykację nowych kontrolerów przez administratora zanim zostaną dodane do Systemu Kontroli Dostępu, a tym samym zabezpiecza przed nieautoryzowanym zmodyfikowaniem oprogramowania zarządzającego kontrolerem.

- Klucze szyfrujące Mifare DESSFire odpowiadające za odczyt danych autoryzacyjnych z karty RFID, mają posiadać opcję przechowywania w tym samym dedykowanym module kontrolera drzwiowego co certyfikaty autentykacyjne. W takim scenariuszu czytnik staje się dla karty transparentny i deszyfracja następuje po stronie kontrolera.
- Zarządzanie certyfikatami autentykacyjnymi jak i kluczami DESFire ma być możliwe z centralnego poziomu, jednej stacji roboczej. Certyfikaty i klucze mają posiadać możliwość automatycznego dystrybuowania do kontrolerów drzwiowych z jednego punktu zarządzania do wszystkich elementów systemu KD.
- Zamawiający ma mieć możliwość zarządzania i wymiany certyfikatów autentykacyjnych w każdym momencie bez ingerencji dostawcy systemów.
- Wszystkie stany alarmowe przejść muszą być zobrazowane graficznie na rzutach pomieszczeń w systemie wizualizacji zdarzeń. Ponadto należy przygotować instrukcję/zestaw instrukcji dla niżej omówionych zdarzeń (otwarcie przy pomocy przycisku, otwarcie przy pomocy karty, otwarcie przy pomocy przycisku ewakuacyjnego, zbyt długo otwarte przejście, sforsowane przejście, przejście otwarte trwale, przejście zamknięte trwale, przejście otwarte z harmonogramu, przejście uszkodzone, sabotaż krańcówki przejścia, sabotaż przycisku wyjścia, brak stanu przejścia).
- W projekcie należy zaprojektować automatyczne otwieranie się przejść objętych Systemem Kontroli Dostępu na drogach ewakuacyjnych podczas wystąpienia alarmu II stopnia instalacji sygnalizacji pożaru. Ta funkcjonalność powinna być realizowana za pomocą central sterowniczych systemu platformy integrującej i w nim zwizualizowana.
- Dodatkowo operator systemu ma mieć możliwość otwarcia wybranych przejść lub zdefiniowanych grup przejść na wypadek zdarzeń typu napad, ewakuacja.
- Dostarczony System Kontroli Dostępu musi mieć możliwość użycia systemu certyfikatów dla wszystkich urządzeń cyfrowych systemu KD, autoryzujący urządzenia i komunikację wewnątrz systemu KD (czytnik - kontroler - serwer - stacja operatorska). Dystrybucja certyfikatów na urządzenia systemu musi być w wyłącznym posiadaniu i z pełną możliwością zarządzania przez Zamawiającego i odbywać się z centralnego punktu do wszystkich urządzeń systemu KD (PKI Zamawiającego). Zastosowanie takiej architektury bezpieczeństwa spowoduje iż wszystkie wrażliwe klucze (w tym klucz odczytu numeru karty, ulokowany w standardowych rozwiązaniach na czytniku) znajdować się będą na kontrolerze w bezpiecznym module po chronionej stronie dostępu. Każdy projektowany element: czytnik, kontroler i karta muszą być gotowe do implementacji reguł end to end security w formule opisanej powyżej. Efektem implementacji mechanizmów end to end security ma być możliwość zmiany używanego klucza szyfrującego zapisanego na karcie bez rekonfiguracji każdego czytnika kart dostarczonej infrastruktury z osobna. Ma to na celu umożliwienie prewencyjnej lub reaktywnej (w chwili podwyższonego zagrożenia) wymiany używanych kluczy oraz zmianę kluczy jeśli jest podejrzenie, że zostały skopiowane.
- Uzyskanie niezbędnych raportów w zakresie ruchu pojazdów i osobowego pracowników przedstawiać wzory:
 - Możliwość wszelkiego rodzaju raportowania po wszelkich znamionach identyfikacji np. numer karty+ czasookres+ marka pojazdu +rodzaj ładunku+ Nazwisko+ imię+ nr

rejestracyjny. Samochodu i naczepy +data zdarzenia,+ określone godziny, + rodzaj zdarzenia np. wjazd wyjazd wejście wyjście z terenu lub ze strefy, rodzaj ładunku, nazwa firmy.

- Możliwość identyfikacji który z operatorów wydał daną przepustkę i kiedy.
- Umożliwienie tworzenia kombinacji filtra przejść - tak, aby można stworzyć filtr przejść dla poszczególnych rodzajów kart.
- Umożliwienie dodania firmy, marki pojazdu przez administratora, bez dodania karty.
- Umożliwienie wykonywania raportów po oznaczniku obecny na terenie zakładu tj. ile osób i pojazdów znajduje się w danej chwili na terenie zakładu.
- Umożliwienie automatycznego generowania i wysyłania raportów na e-maila zgodnie z zadaniem harmonogramem.
- Umożliwienie sortowania zdarzeń po każdym parametrze zdarzenia.
- Umożliwienie przeglądu zdarzeń oraz raportowanie przy pomocy przeglądarki www.
- Dostęp do raportów powinien być potwierdzany przy pomocy indywidualnych kont użytkowników.
- Umożliwienie generowanie raportów przy pomocy przeglądarki www, tworzonych na podstawie ruchu osób na danym przejściu oraz ruchu danego użytkownika na wielu przejściach. - Umożliwienie generowania raportów dla grup pracowników np. firma.
- Umożliwienie generowania list z przepustkami będącymi w dyspozycji użytkowników i datą ich ważności. Umożliwienie zmiany daty ważności przepustki w sposób uproszczony bez konieczności usuwania i nadawania uprawnień z nową datą.
- Umożliwienie zaznaczenia w karcie użytkownika zdania przepustki po terminie ważności oraz generowania raportów z wykazem przepustek, które utraciły ważność i nie zostały zdane. Możliwość wykonania raportu, jeżeli firma XX miała wydane 10 przepustek tymczasowych. Na koniec umowy zdała 8 przepustek. Chcemy wygenerować raport, kto z firmy XX nie oddał przepustki.
- Możliwość wykonania raportu z poziomu przeglądarki www dostępu do konkretnego pomieszczenia np. Serwerownia F12 itp., Możliwość wykonania raportu z poziomu przeglądarki www mówiący o tym gdzie dany użytkownik wchodził.
- Autentykacji dostępu do raportów przy pomocy przeglądarki www.
- Przy wykonywaniu raportów za pomocą przeglądarki www powinny działać wszystkie filtry - System musi przechowywać wszystkie dane gości z informacjami o datach wizyt, osobach odwiedzanych oraz historii przejść z wszystkich wizyt z okresu 5 lat.
- Na formularzu przepustki tymczasowej w zakładce dane użytkownika należy usunąć dane pojazdu.
- Możliwość filtrowania i sortowania w zakładce „Karty stałe”.
- Powinien umożliwiać generowanie automatycznych raportów z wybranych stref dostępu w określonym czasookresie i przysyłać te raporty drogą elektroniczną z automatu do określonych odbiorców.
- W systemie muszą być obsługiwane następujące rodzaje przepustek :
 - ✓ Stałe
 - ✓ Jednorazowe
 - ✓ Gość
 - ✓ Rezerwowe

- ✓ Serwisowe/Kontrahent • Tymczasowe
- ✓ Alarmowe.

- Przepustki stałe karty plastikowe z chipem zgodnie z Instrukcją ruchu osobowego i pojazdów obowiązującą u Zamawiającego.
- Tymczasowe muszą być wykonane w wersji plastikowej jednokrotnego użytku ze zdjęciem, również z chipem umożliwiającym zapisanie na nim danych z zacytanego przez urządzenia dokumentu tożsamości, tzn. że po upływie określonego przez operatora czasu przepustka staje się nieaktywna i nie może być przydzielona ponownie innemu nowemu użytkownikowi (ale wszystkie dane użytkownika pozostają w bazie zbioru). Zdjęcie do przepustki ma być wykorzystane (z pobranych danych z czytnika dokumentów) z dokumentu lub danych przekazanych na elektronicznym nośniku informacji, tak aby dane każdego kto wchodzi na teren zakładu znajdowały się w zbiorze systemu i w razie konieczności późniejszego wydania przepustki stałej lub tymczasowej nie będzie trzeba po raz wtóry wprowadzać danych i zdjęć do systemu.
- Przepustki stałe wydawane przez uprawnionych pracowników Zamawiającego, w wersji plastikowej wielokrotnego użytku ze zdjęciem, z chipem umożliwiającym zapisanie na nim danych z pobranych informacji z czytnika dokumentu tożsamości lub danych przekazanych na elektronicznym nośniku informacji mają mieć możliwość dodania uprawnień do stref zamkniętych jak również uprawnienia do wjazdu pojazdem na teren elektrowni.
- Przepustki Jednorazowe wydawana na pracę w firmach zewnętrznych z chipem umożliwiającym zapisanie na nim danych z pobranych informacji z czytnika dokumentu tożsamości lub danych przekazanych na elektronicznym nośniku informacji. Wykonane ze zdjęciem w wersji plastikowej jednokrotnego użytku tzn. że po odbiciu przepustki przy wychodzeniu po upływie ustalonego czasu ważności staje się nieaktywna i nie może być przydzielona ponownie innemu nowemu użytkownikowi. Przy przepustkach jednorazowych do pracy po 4 dniach ma być generowany sygnał dźwiękowy przy czytniku, ponieważ tyle pracownik dostaje czasu na załatwienie spraw związanych z wydaniem dla niego przepustki.
- Przepustka GOŚĆ, GOŚĆ z POJAZDEM w wersji plastikowej wydawana jest bez wydruku zdjęcia również z chipem umożliwiającym zapisanie na nim zdjęcia i danych z pobranych informacji z czytnika dokumentu tożsamości, maksymalnie ważna na 24h jeżeli nie została odbita przy wychodzeniu, system samodzielnie musi odebrać uprawnienia takiej karcie. Anulowana przepustka będzie powodować alarm w postaci sygnału dźwiękowego na bramach przy próbie użycia karty. - Przewidzieć możliwość wprowadzenia GOŚCIA do bazy ale bez wydawania przepustki np. PIP, NIK, UDT, ABW itp. służby te nie obowiązują odbijanie przepustek ale dane w bazie mają być zapisane.
- Przepustka rezerwowa wydawana w wersji plastikowej bez wydruku zdjęcia również z chipem umożliwiającym zapisanie na nim zdjęcia i danych z pobranych informacji z czytnika dokumentu tożsamości na bramach w przypadku gdy pracownik uprawniony do wejścia na teren Zamawiającego zapomni swojej stałej lub tymczasowej przepustki. Okres aktywności to maksymalnie 24h po upływie tego czasu, jeżeli nie została odbita przy wychodzeniu, system musi samodzielnie odebrać uprawnienia takiej karcie i będzie powodować alarm w postaci sygnału dźwiękowego na bramach przy próbie użycia karty.
- Przepustka serwisant wydawana w wersji plastikowej jednokrotnego użytku bez zdjęcia lub wielokrotnego użytku ze zdjęciem, również z chipem umożliwiającym zapisanie na nim danych z pobranych informacji z czytnika dokumentu tożsamości, na bramach w przypadku konieczności wjazdu na teren elektrowni serwisu do urządzeń, maszyn, pojazdów itp. celem

wykonania prac remontowych, przeglądu itp. Jest ważna maksymalnie na 24h z możliwością przedłużenia do 96 godzin, w przypadku nie opuszczenia zakładu po 13 godzinach włącza się alarm wyświetla kolorem na ekranie monitora i podaje sygnał dźwiękowy. Jeżeli przy wyjeździe przepustka nie została odbita system samodzielnie po upływie oznaczonego czasu musi odebrać uprawnienia takiej karcie i będzie powodować alarm w postaci sygnału dźwiękowego na bramach przy próbie użycia karty. Przepustki te mają mieć możliwość dodania uprawnień do stref zamkniętych.

- Przepustka Tymczasowa wydawana w wersji plastikowej jednokrotnego lub wielokrotnego użytku ze zdjęciem, również z chipem umożliwiającym zapisanie na nim danych z pobranych informacji z czytnika dokumentu tożsamości lub danych przekazanych na elektronicznym nośniku informacji. Przeznaczona na wykonanie prac krótkookresowych. Przepustki te mają mieć możliwość dodania uprawnień do stref zamkniętych jak również uprawnienia do wjazdu pojazdem na teren Elektrowni. Czasookres ważności Przepustek tymczasowych powinien być ustawiany dowolnie natomiast system samoczynnie powinien zabrać ważność dla przepustki której czasookres ustawiony przez operatora upłynął i powodować alarm w postaci sygnału dźwiękowego na bramach przy próbie użycia karty.
- Przepustka Alarmowa wydawana przez Pełnomocnika w sytuacjach zagrożenia uprawnionym osobom, wykonana w wersji plastikowej wielokrotnego użytku bez zdjęcia , również z chipem umożliwiającym zapisanie na nim danych z pobranych informacji z czytnika dokumentu tożsamości.
- Przepustka Samochodowa nadawana jako uprawnienie do wjazdu na teren elektrowni przez uprawnionych pracowników Zamawiającego na dowolny okres, natomiast dla firm zewnętrznych nie mających stałej siedziby na terenie elektrowni - nie dłuższy niż rok. System ma informować pracownika ochrony 5 dni przed utratą ważności pozwolenia – komunikatem na monitorze o upływie terminu jej ważności. Po upływie okresu ważności system sam powinien odebrać uprawnienia i powodować alarm w postaci sygnału dźwiękowego na bramach przy próbie użycia karty. Podczas wprowadzania numerów rejestracyjnych pojazdów należy wykluczyć możliwość używania spacji i jakichkolwiek znaków. Przy poszukiwaniu pojazdu nie trzeba zabierać ważności karcie żeby pobudziła alarm na bramach podczas próby użycia. System powinien pozwalać na przypisanie uprawnień karty do danej bramy oraz w dni powszednie po godzinie 18:00, w święta i dni wolne od pracy kierować uprawnienia dla wszystkich kart samochodowych na bramę numer 3

Brama nr 1

Obsługuje ruch osobowy i pojazdów osobowych, obciążenie 90% ruch osobowy oraz 10% ruch pojazdów wyłącznie osobowych. Wydaje przepustki typu, GOŚĆ, GOŚĆ z POJAZDEM, REZERWOWA, SERWIS.

Wprowadzenie danych interesantów, poprzez pobranie niezbędnych informacji z czytnika dokumentów tożsamości typu:

Dowód Osobisty, Prawo Jazdy, Paszport.

Brama nr 2

Obsługuje ruch osobowy i pojazdów do 3,5 tony, obciążenie osobowy 50% oraz 50% ruch pojazdów. Wprowadzenie danych poprzez pobranie niezbędnych informacji z czytnika dokumentów typu Dowód Osobisty, Prawo Jazdy, Paszport. Obsługa samochodów wjeżdżających - kierowcy posiadający stałe przepustki kierowcy i na samochód podjeżdżają do bramy, odbija przepustkę, pracownik ochrony identyfikuje kierowcę na monitorze na którym wyświetlają się info oraz zdjęcie kierowcy . (zgodność samochodu , osoby dokumentów),

przeprowadza kontrolę i wpisuje z czym wjeżdża. Po czynnościach sprawdzających pracownik ochrony podnosi szlaban i umożliwia wjazd na teren. Kierowca przejeżdża. Sytuacja wyjeżdżającego samochodu jest taka sama. Kierowca odbija przepustkę – strażnik sprawdza zgodność i czynności kontrolne pojazdów następnie pracownik ochrony podnosi szlaban i umożliwia wjazd na teren.

Brama nr 3

Obsługuje ruch głównie pojazdów o dużym tonażu typu TIR. Ruch osobowy 30% oraz ruch pojazdów 70% w tym 100% ruchu samochodów ciężarowych . Wprowadzenie danych poprzez pobranie niezbędnych informacji z czytnika dokumentów typu Dowód Osobisty, Prawo Jazdy, Paszport oraz dowodu rejestracyjnego (jeżeli to możliwe). Należy obsłużyć kombinację kiedy wjeżdża:

- Kierowca + 1 Samochód + naczepa
- 2 Kierowców +1 Samochód +naczepa
- Pojazdy samobieżne typu dźwig, ładowarka itp. + operator.

Obsługa samochodów wjeżdżających - kierowcy posiadający stałe przepustki na kierowcę i na samochód podjeżdżają do bramy, odbija przepustkę, pracownik ochrony identyfikuje kierowcę na monitorze na którym wyświetla się info. oraz zdjęcie kierowcy . (zgodność samochodu , osoby dokumentów), przeprowadza kontrolę i wpisuje z czym wjeżdża. Po czynnościach sprawdzających pracownik ochrony podnosi szlaban i umożliwia wjazd na teren. Kierowca przejeżdża. Sytuacja wyjeżdżającego samochodu jest taka sama. Kierowca odbija przepustkę – pracownik ochrony sprawdza zgodność i czynności kontrolne pojazdów następnie pracownik ochrony podnosi szlaban i umożliwia wjazd na teren.

Pracownik biura przepustek ma wpisać tylko deklarowany towar co w wozi i do kogo jedzie wybierając z listy odbiorców. System powinien posiadać funkcję możliwości wyznaczania trasy przejazdu do wybranego kontrahenta na terenie chronionym, oraz możliwość wydrukowania trasy przejazdu, wydawaną kierowcy pojazdu.

30% kierowców posiada przepustki stałe, 70% to dostawcy jednorazowi.

W bazie ma być zdefiniowany rodzaj dostaw.

System musi obsługiwać listy przewozowe, które pracownik ochrony pobiera od kierowcy. Strażnik ma wpisać dane do bazy : nr listu przewozowego + datę oraz do kogo dostawa przychodzi. W bazie ma być Lista materiałów niebezpiecznych oraz lista osób uprawnionych do wystawiania przepustek materiałowych (z wzorem podpisu) na wwóz i wywóz materiałów niebezpiecznych. Niezbędna jest funkcja możliwości aktualizacji list przez osobę do tego uprawnioną w komórce NS.

Ponadto w bazie powinna znaleźć się również lista osób upoważnionych do podpisywania pozostałych przepustek materiałowych na wywożone materiały (z wzorem podpisu). Specyfikacja w wersji papierowej co wwozi jakie narzędzia – potem przy wyjeździe co wywozi- w referencji do przepustki wywozowej. Przy wyjeździe kierowca oddaje przepustkę pracownikowi ochrony.

System ma obsługiwać samochody wywożące popiół lub gips, biomasę nie spełniającą wymaganych parametrów oraz inne materiały produkowane przez firmy mające swe siedziby na terenie Elektrowni, pośredniczące w obrocie itp.

W związku z dynamicznymi zmianami organizacyjnymi u Zamawiającego, procedury mogą ulec zmianie i zostaną przedstawiane w ramach realizacji projektu.

System ma współpracować z system SAP HR obowiązującym u Zamawiającego, Książką telefoniczną opartą na www (PHP), Awizacją biomasy.

Ze względu na modernizację Systemu Kontroli Dostępu, należy bezsprzecznie uwzględnić wymianę wyeksploatowanych istniejących tripodów na bramie wejściowej 1,(przejście nr 2) na nowe.

W ramach modernizacji Systemu SKD, należy również przewidzieć dostarczenie 10 drukarek i 15 czytników do kart dostępowych wraz z niezbędnymi materiałami eksploatacyjnymi do wydrukowania ok. 18 000 przepustek.

Wymiana i zaimplantowanie wszystkich przepustek do nowego systemu na karty disfire jest po stronie wykonawcy.

Przepustki typu Stała i Tymczasowa muszą być kompatybilne z systemem depozytorowym kluczy.

Wymagania dla tripodów wejściowych podlegających wymianie:

Parametry techniczne

- zasilanie prądem: 28 VDC
- maksymalny pobór mocy: 200Wp
- temperatura składowania: od -40°C do +50°C
- temperatura pracy: od -30°C do +50°C
- szerokość urządzenia: 236 mm
- szerokość przejścia: 525 mm
- długość: 1087 mm
- wysokość: 1010mm
- wykonanie standardowe: stal nierdzewna

(możliwość wykonania obudowy bramki ze stali nierdzewnej z dodatkiem molibdenu („316”) lub stali malowanej proszkowo)

- mechanizm wyposażony w minimum 2 ramiona

4. Książka telefoniczna

Zamawiający wymaga aby moduł książki telefonicznej był wdrożony w architekturze klient serwer z zachowaniem zasad bezpieczeństwa wymienionych w zasadach ogólnych dla systemów wdrażanych w ramach SIWZ. Funkcjonalności modułu mają zostać określone w drodze analizy obecnie wykorzystywanej Książki Telefonicznej u Zamawiającego, ponadto na etapie tworzenia dokumentu SIWE określono poniższe funkcjonalności.

- 4.1 W zakresie Administratora książka musi posiadać możliwość tworzenia kont aplikacyjnych z uprawnieniami administracyjnymi do kont danej spółki, dla przedstawicieli spółek którzy będą administrowali Użytkownikami spółek. Przykładowo spółka 'A', której pracownicy są zarejestrowani w bazie danych kontroli dostępu, ma utworzone konto aplikacyjne dla swojego administratora, który może manipulować danymi pracowników spółki 'A' wyświetlanymi w książce telefonicznej, ale bez możliwości usuwania użytkownika z bazy danych systemu kontroli dostępu oraz bez możliwości usuwania związanych z nim zdarzeń wejścia/wyjścia. Uprawnienia administracyjne mają być tylko do dodatkowych metadanych konta użytkownika spółki 'A': Telefon st.; Telefon kom.; Zakład; Dział; Stanowisko.
- 4.2 Mechanizm importu słowników metadanych podstawowych spółek wraz z strukturą Zakład; Dział; Stanowisko.
- 4.3 Mechanizm integracji z systemem HR wykorzystywanym u Zamawiającego
- 4.4 Moduł Użytkownika – przeszukiwanie po wszystkich kolumnach po wyborze tak jak jest obecnie z kolumn Zakład, Dział, Stanowisko, oraz wpisaniu z palca dla pozostałych. Zakładany czas odpowiedzi systemu zapytanie użytkownika nie będzie przekraczał 5 sekund. Wykonawca zoptymalizuje zapytania SQL pod kątem prędkości oraz określi wymagania sprzętowe dla serwerów wirtualnych hostujących aplikację jak i bazę danych. System będzie wyświetlał status Obecny/Nieobecny w interfejsie Książki Telefonicznej.
- 4.5 Szata graficzna – zgodnie z wytycznymi Biura PR i Komunikacji Zamawiającego.

System Monitoringu Wizyjnego CCTV

Mając na uwadze ogólnoswiatowe problemy związane z zagrożeniami w zakresie cyberbezpieczeństwa, zarówno tego realnego jak i tego przeczuwanego, oraz wynikającymi z tego konsekwencjami dla systemów bezpieczeństwa i nadzoru, wymaga się żeby użyte przy modernizacji kamery były zgodne z obowiązującymi standardami bezpieczeństwa. Dodatkowo wymaga się aby kamery były zgodne z protokołem ONVIF - potwierdzone na stronie onvif.org. Wymaga się zapewnienia dostępności części serwisowych do naprawy urządzeń. Instalacja powinna zostać wykonana przez autoryzowanego / certyfikowanego partnera producenta rozwiązań. Kamery objęte 2 letnią gwarancją producenta. Wszystkie kamery muszą być kompatybilne z systemem VMS, lub innym wybranym system i zastosowanym na obiekcie.

Wymaga się również aby projekt i wykonanie ujmował zakup/modernizację/wymianę urządzeń wizyjnych takich jak monitory, stacje robocze, serwery, rejestratory, kamery i inne materiały niezbędne do wybudowania, uruchomienia i wdrożenia systemu CCTV.

Platforma monitoringu musi być dedykowanym rozwiązaniem będąc niezawodnym elementem, który można integrować z innymi systemami. Równocześnie można ją szeroko rozbudowywać i skalować dostosowując funkcjonalność do wymagań. Oprogramowanie specjalnie zaprojektowane dla średnich i dużych instalacji sieciowych, od kilku serwerów po rozległy system z setkami lokalizacji.

Oprogramowanie rejestrujące powinno działać w architekturze klient serwer oraz umożliwiać funkcjonalnie obsługę nielimitowanej liczby serwerów rejestrujących (master/slave) – w tym do 250 kamer na jednym serwerze, lub 500 kamer na serwerze wirtualnym posiadającym 2 karty sieciowe. Serwer master zarządza główną bazą danych, zawierającą wszystkie informacje

o systemie, użytkownikach i konfiguracji komponentów platformy oraz serwerach podrzędnych. Serwery podrzędne zarządzają przydzielonymi kamerami i koderami oraz archiwizują wideo/audio, a także przesyłają wideo i audio ze źródła do aplikacji klienckiej. Platforma musi mieć możliwość zaimplementowania kamer różnych producentów co najmniej 8000 modeli poprzez wbudowane pełne aktywne sterowniki kamer (pełna kontrola wejść/wyjść alarmowych, audio, sterowanie PTZ, itd.). Oprogramowanie musi obsługiwać także protokół ONVIF Profile M. Producent powinien umożliwiać darmową aktualizację sterowników kamer wraz z protokołem ONVIF w okresie realizacji umowy oraz w okresie gwarancyjnym – aktualizacja ma być wykonywana obowiązkowo w trakcie corocznych przyjazdów do EEP. Interfejs użytkownika dostępny w wielu językach w tym również w języku polskim. Licencjonowanie systemu bezterminowe w oparciu o ilość kanałów wizyjnych. Licencje nie są przypisane do konkretnej kamery co pozwala w dowolnej chwili wymianę na inny model. Obsługa nielimitowanej liczby użytkowników. Każdy użytkownik po zalogowaniu otrzymuje swój własny interfejs, który może indywidualnie konfigurować i zapisać. Oprogramowanie musi być platformą otwartą umożliwiającą integrację z innymi systemami dostępnymi na obiekcie w celu otrzymania dodatkowych korzyści jak np. scentralizowanego zarządzania różnymi systemami z poziomu jednej aplikacji. System musi posiadać zaimplementowaną funkcję tzw. watchdog. Obsługa dwu stopniowej autentykacji (podwójne hasło) oraz szyfrowana komunikacja między aplikacją kliencką, a serwerem gwarantuje najwyższy poziom bezpieczeństwa. Możliwość integracji i zarządzania użytkownikami z Active Directory.

System nie może być ograniczony maksymalną obsługiwaną pojemnością przestrzeni dyskowej. Powinien obsługiwać dyski o różnej pojemności w ramach jednego serwera. Konfiguracja nagrywania i czasu przechowywania nagrań może być zmieniona dla każdej kamery indywidualnie co pozwoli na zadeklarowanie minimalnego i maksymalnego czasu przechowywania dla każdej kamery z osobna. Oznacza to, że materiał nie zostanie nadpisany do momentu zakończenia minimalnego czasu oraz będzie usuwany po przekroczeniu maksymalnego czasu przechowywania. Możliwość konfiguracji harmonogramu nagrywania: tryb ciągły, detekcja ruchu, brak ruchu, przekroczenie zadanego progu głośności, zdarzenie alarmowe. Wbudowany moduł detekcji ruchu pracujący w 3 trybach: detekcja porównawcza, detekcja adaptacyjna, detekcja hermeneutyczna. Możliwość wygenerowania akcji: wyjścia cyfrowego, nagrywania, wysłania maila, wygenerowania funkcji kamery PTZ - przejście do określonej pozycji bądź wygenerowanie patrolu. System musi umożliwić przypisanie wielu akcji do jednego alarmu. Nagrywanie obrazu do 60kl/s oraz brak ograniczenia co do maksymalnej rozdzielczości. Wsparcie dla kodowania MJPEG, MPEG-4, H.264, H.265/HEVC. Platforma musi posiadać możliwość tworzenia automatycznego archiwum na nośnikach zdalnych np.: macierzach dyskowych NAS/SAN z wybranych lub wszystkich kamer. System pozwoli na wykorzystanie serwera redundantnego typu failover, którego zadaniem jest przejęcie nagrywania kamer w momencie uszkodzenia jednego z serwerów nagrywających. Architektura systemu pozwoli na wykorzystanie więcej niż jednego serwera zapasowego. Możemy zadeklarować czas po którym takie przełączenie nastąpi. Obsługa wielostrumieniowości dla każdej kamery z osobna: strumień dla nagrywania, strumień do podglądu lokalnego oraz strumień do podglądu zdalnego. Dowolna konfiguracja dla każdego strumienia osobno jakości nagrywania w rozumieniu rozdzielczości, kompresji, odświeżania. Wbudowana obsługa inteligentnej analizy obrazu i możliwość jej uruchomienia na każdej kamerze znajdującej się w systemie (możliwość przenoszenia funkcji analizy między kamerami). Obsługiwane analizy: wejście w strefę, wyjście ze strefy, pojawienie się,

zniknięcie, zatrzymanie, przebywanie w strefie, filtr kierunkowy, przekroczenie prędkości, pojawienie się przedmiotu, zniknięcie przedmiotu, zliczanie, wykrywanie sabotażu. Na podstawie kilku analiz na jednym obrazie możemy stworzyć scenariusz generujący np. alarm w systemie (tworzenie funkcji logicznych z VCA). Dodatkowo wsparcie obsługi funkcji analitycznych oraz rozpoznawania tablic rejestracyjnych ANPR bezpośrednio w wybranych modelach kamer. Kamery takie będą zamontowane na bramie nr 3, dwie sztuki. W przypadku uruchomienia nowej bramy wyjazdowej też należy tam zamontować dwie takie kamery. Możliwość tworzenia nowego, własnego interfejsu użytkownika przez operatora aby zapewnić intuicyjną pracę oraz ekspresowy czas reakcji. Oprogramowanie klienckie nie wymaga żadnych dodatkowych płatnych licencji i jest dostępne w ramach zakupu licencji na kanały nagrywające. W pełni skalowalny interfejs oprogramowania klienckiego pozwala dostosować wielkość obszaru roboczego oraz siatki kamer, osi czasu i drzewa urządzeń. Obsługa podglądu na żywo/odtwarzanie za pomocą konfigurowalnej osi czasu z możliwością rozróżnienia: nagrania/zakładki/alarmy. Operator będzie mógł zapisać rozłożenie kamer na obrazie i w dowolnej chwili powrócić do tego schematu. Oprogramowanie pozwoli na definiowanie widoków (wyświetlanie na pojedynczym monitorze) oraz multi-widoków (wyświetlanie na wielu monitorach) o różnej zawartości poszczególnych kart (np. obraz na żywo, odtwarzanie, lista zdarzeń, mapa obiektu, wyskakujące okna alarmowe). Rozmieszczenie oraz liczba pól na danym monitorze może być dowolnie konfigurowalna przez użytkownika. Istnieje również możliwość definiowania własnych niestandardowych podziałów. Możliwość sterowania aplikacją oraz funkcjami za pomocą skrótów klawiaturowych. Generowanie podglądu w 3 trybach: strumień zawsze z rejestratora, strumień zawsze z kamery, strumień z rejestratora, a w przypadku rozłączenia bezpośrednio z kamery. Takie rozwiązanie wspiera bezpieczeństwo oraz niweluje sytuacje braku podglądu na żywo. System umożliwi obsługę do 8 monitorów. Obrazy z kamer mogą być odświeżane w sposób ciągły, z detekcji ruchu lub co zadeklarowany czas w przypadku braku aktywności w polu widzenia kamery. Podgląd odbywać się może poprzez dedykowane oprogramowanie bądź przeglądarkę internetową. Obsługa stref prywatności konfigurowanych dla poszczególnych lub wszystkich użytkowników poza administratorem. Funkcja ochrony prywatności czyli maskowanie twarzy w czasie rzeczywistym tzw. facial blurring lub maskowanie wszystkich ruchomych obiektów. Oprogramowanie musi wspierać zdarzenia przychodzące z inteligentnej analizy obrazu wraz z możliwością wyszukania danej analizy wraz z wizualizacją stref z tych funkcjonalności na żywo. System musi posiadać wyszukiwanie ruchu na już nagrany materiał. Powinna istnieć funkcja tworzenia wirtualnych kamer (wiele widoków z jednej kamery). Funkcja pozwoli przy szerokim kadrze sceny wyciąć interesujący fragment i pozostawić jako podgląd na żywo bądź podgląd z archiwum wraz z obrazem pełnego kadru kamery. System powinien wspierać kamery tzw. 360 stopni, czyli umożliwiać programowe prostowanie (dewarping) obrazu bezpośrednio z oprogramowania nadzorującego. Pozwoli to na stworzenie 4 niezależnych widoków, 2 widoków 180 stopni (panorama) oraz pojedynczego widoku (cyfrowy PTZ). Widoki te można zapisać i wrócić do danego ustawienia w przypadku gdy zajdzie taka potrzeba. Obsługa wielopoziomowych map zawierających plan wraz z naniesionymi kamerami, we/wy alarmowymi oraz urządzeniami audio. Obsługa okna alarmowego w którym pojawiają się informacje o zdarzeniach wraz z widokiem kamery lub kamer powiązanych w tym zdarzeniu. W trybie odtwarzania będzie możliwość podglądu obrazu archiwalnego z 32 kamer jednocześnie na jednej stacji operatorskiej z prędkością 1 fps, 0.1x, 1/8x, 1/4x, 1/2x, 1x, 2x, 4x, 8x, 16x, 32x, 64x. Aplikacja umożliwi tworzenie zakładek na materiale wideo indywidualnie dla każdej kamery. Tworzenie archiwum ze zdarzenia powinno mieć do wyboru formaty ASF, .AVI, .MATROSKA, .SEF. Dostępny format wewnętrzny pozostawiający znak wodny - potwierdzenie autentyczności oraz

możliwość ustawienia hasła dla nagrania jak i format ogólnodostępny, który można odtwarzać w ogólnodostępnym oprogramowaniu odtwarzającym wideo. Możliwość zapisania do jednego pliku z materiałem archiwalnym kopii zapasowej z kilku kamer. Zapis pojedynczej klatki z kamery w formatach .JPF, .BMP, .GIF, .TIFF, .PNG poprzez kliknięcie przycisku eksportowania. Oprogramowanie umożliwi tworzenie tzw. storyboard czyli połączonego wideo z wielu kamer z różnych przedziałów czasowych do jednego pliku. Pozwoli to na zmontowanie i wyeksportowanie takiego klipu na poziomie aplikacji CMS. Funkcja używana w momencie kiedy zachodzi potrzeba wyeksportowania nagrania z przemieszczającego się obiektu widzianego na różnych kamerach w różnym czasie. Aplikacja kliencka musi pozwalać na programowanie i aktywowanie presetów, tur kamer PTZ. Wsparcie dla dowolnego kontrolera USB z joystickiem do kontrolowania funkcji PTZ ruchomych punktów kamerowych oraz możliwość kontrolowanie kamer PTZ z poziomu panelu w oprogramowaniu. Obsługa cyfrowych modułów I/O aktywowanych z poziomu dedykowanych przycisków ekranowych. W przypadku potrzeby wyświetlania wielu kamer z różnych lokalizacji np. duże centra monitoringu istnieje możliwość wykorzystania funkcjonalności wirtualnej krosownicy. Funkcjonalność pozwala na łatwe zarządzanie dużymi ścianami wizyjnymi złożonymi z wielu monitorów z poziomu jednej stacji roboczej. Daje to możliwość swobodnej konfiguracji dla widoków obrazów z kamer. Możliwość szyfrowanego zdalnego dostępu za pomocą klienta www w oparciu o HTML 5.

Minimalne wymagania dla kamer PTZ:

- rozdzielczość 2MP (1920x1080)
- przetwornik 1/2.8" CMOS lub większy
- zoom optyczny min. 31x -zoom cyfrowy min. 12x -jasność obiektywu min. F1.6
- obsługiwane rozdzielczości: 1920x1080, 1280x1024, 1280x720, 640x480
- WDR min. 120dB
- obsługa kompresji H.264, M-JPEG
- wielostrumieniowość
- odświeżanie 60kl/s dla pełnej rozdzielczości H.264
- 32 maski prywatności
- wsparcie HTTPS, SSL, 802.1x, TLS
- network security: HTTPS(SSL) Login Authentication, Digest Login Authentication, IP Address Filtering, User access log, 802.1X Authentication(EAP-TLS, EAP-LEAP)
- analiza obrazu: pojawianie, znikanie, wirtualna linia, wykrywanie sabotażu, klasyfikacja obiektu człowiek/pojazd
- min. zasięg promiennika IR 200m
- wbudowana wycieraczka lub system osuszania kopuły poprzez wibrację
- obsługa karty pamięci micro SD/SDHC/SDXC
- certyfikaty IP66, IK10 (obudowa), NEMA4X
- kamery zgodne NDAA
- temperatura pracy -40°C~+55°C
- zasilanie PoE (IEEE802.3bt, typ 3)

Minimalne wymagania dla kamer typu bullet:

- rozdzielczość min. 4MP
- przetwornik 1/2.9" CMOS lub większy
- obiektyw 2.8 – 8.5mm lub większy
- jasność obiektywu min. F1.4
- WDR 120dB
- obsługa kompresji H.264, M-JPEG
- wielostrumieniowość: min. 3 strumienie
- odświeżanie min. 25kl/s dla pełnej rozdzielczości (H.264)
- wsparcie HTTPS, 802.1x, TLS
- detekcja ruchu, detekcja audio, wykrywanie sabotażu, wykrywanie wstrząsów
- możliwość instalowania dodatkowych aplikacji bezpośrednio w kamerze
- zasięg promiennika IR 30m
- obsługa karty pamięci micro SD/SDHC/SDXC -ONVIF Profile S/G/T
- certyfikaty IP66, IP67, NEMA4X, IK10
- kamery zgodne NDAA
- temperatura pracy -40°C~+55°C
- zasilanie PoE (IEEE802.3af)

Minimalne wymagania dla kamer wandaloodpornych kopułowych:

- rozdzielczość min. 4MP
- przetwornik 1/2.8" progressive CMOS lub większy
- obiektyw 4.5 – 8.5 mm lub większy
- jasność obiektywu min. F1.5 -WDR 120dB
- obsługa kompresji H.264, M-JPEG
- wielostrumieniowość: min. 3 strumienie
- odświeżanie min. 25kl/s dla pełnej rozdzielczości (H.264)
- wsparcie HTTPS, 802.1x, TLS
- detekcja ruchu, detekcja audio, wykrywanie sabotażu, wykrywanie wstrząsów
- możliwość instalowania dodatkowych aplikacji bezpośrednio w kamerze
- zasięg promiennika IR 40m
- obsługa karty pamięci micro SD/SDHC/SDXC -ONVIF Profile S/G/T
- certyfikaty IP66, IP67, NEMA4X, IK10
- kamery zgodne NDAA
- temperatura pracy -40°C~+55°C
- zasilanie PoE / 12V DC

Minimalne wymagania dla kamer ANPR:

- rozdzielczość min. 2MP
- przetwornik 1/2.8" CMOS lub większy
- obiektyw 12 - 48mm lub większy
- jasność obiektywu min. F1.7 -WDR
- 120dB
- obsługa kompresji H.264, M-JPEG -wielostrumieniowość:
min. 3 strumienie
- odświeżanie min. 25kl/s
- wsparcie HTTPS, 802.1x, TLS
- detekcja ruchu, detekcja audio, wykrywanie sabotażu, wykrywanie wstrząsów
- możliwość instalowania dodatkowych aplikacji bezpośrednio w kamerze
- kamera z zainstalowaną aplikacją do sczytywania tablic rejestracyjnych
- zasięg promiennika IR 50m lub więcej
- obsługa karty pamięci micro SD/SDHC/SDXC -ONVIF
Profile S/G/T
- certyfikaty IP66, IP67, NEMA4X, IK10
- kamery zgodne NDAA
- temperatura pracy -40°C~+60°C
- zasilanie PoE (IEEE802.3at)

Minimalne wymagania dla stacji roboczych:

- obudowa Tower
- Intel Core 9th Gen i7 8 Cores 8 Threads
- 16GB DDR4 ECC Server Memory
- fabrycznie zainstalowany system operacyjny
- dysk systemowy 240GB SSD
- 6 x USB 3.0, 1 x Audio line out, 1 x Audio Mic
- 2 x Nvidia GTX 1050Ti GPU 1 x DP 1.4, 1 x DVI-D, 1 x HDMI 2.0
- zasilacz 750W 80 Plus Certified Bronze
- 2-letnia gwarancja w następnym dniu roboczym

Wymagania stawiane monitorom

Wielkość i rodzaj ekranu	55" IPS – podświetlenie krawędziowe LED
Rozdzielczość natywna panelu (min)	3840 x 2160 px
Jasność	700 cd/m2
Poziom kontrastowości statycznej	8 000:1 (włączone lokalne gaszenie podświetlenia)
Poziom refleksyjności panelu	minimum 28% (panel matowy)

Gamut barwowy	86% DCi-P3
Możliwość pracy 24h/7	TAK
Programowalna tablica LUT:	TAK, minimalnie 30bit
Tryby PiP i PbP	TAK
Obsługiwana orientacja	Poziom, Pion, Ekranem w dół i do góry
Wejścia wideo	2x DisplayPort (RGB) (obsługa do 7680 x 4320 30Hz) 1x HDMI (YUV, RGB) (obsługa do 4096 x 2160 60Hz) 1x HDMI (ARC)
Wyjście wideo	1x DisplayPort (pętla z DisplayPort i slotu komputera) 1x HDMi (pętla z HDMi i slotu komputera)
Slot na minikomputer	TAK – typu OPS lub SDM z możliwością zamontowania modułu mikrokomputera o zużyciu energii max 15W
Zasilany port USB	TAK – 5V / 2A
Wzmacniacz audio	TAK - wbudowany
Wbudowane czujniki	3 czujniki temperatury z możliwością programowania działań, oraz czujnik natężenia oświetlenia w otoczeniu
Zgodność elektromagnetyczna	EMC Class B
<ul style="list-style-type: none"> • Kalibracja kolorymetryczna, polegająca na możliwości zapisania wewnętrznej tablicy LUT monitora za pomocą oprogramowania tego samego producenta co monitor. • Kalibracja sprzętowa zawierająca, możliwość kalibracji koordynatów chromatycznych bieli, krzywej transferu elektro optycznego, barwy niebieskiej, zielonej i czerwonej w zakresie zgodności kolorymetrycznej. • Obudowa wykonana z metalu, włącznie z ramką frontową ekranu • Aktywny system chłodzenia awaryjnego za pomocą wentylatorów • Możliwość sklonowania ustawień monitora do pamięci USB • Możliwość aktualizacji oprogramowania układowego przez port USB • Sterowanie monitorem za pomocą przeglądarki www, lub przez oprogramowanie producenta 	

Typ i rozmiar ekranu	Matryca aktywna na tranzystorach cienkowarstwowych TFT podświetlenie W-LED - 24"
Natywna rozdzielczość panelu	1920 x 1080 / 60 Hz
Rozmiar Gamutu Barwowego	72% NTSC / 100% pokrycia sRGB
Jasność	250 cd/m2
Czas reakcji	6 ms (g-g)

Wejścia wideo	1x DisplayPort (RGB) (HDCP) 1x DVI-D (RGB) (HDCP) 1x HDMI (YUV, RGB) (HDCP) 1x D-sub (Analog RGB)
Wyjścia wideo	1x DisplayPort (RGB) (HDCP)
Pozostałe złącza	4x USB (minimum ver. 3.0) (0,9A na port USB) 1x minijack / 1x wyjście słuchawkowe
Możliwości regulacyjne ekranu	- Pochylenie w zakresie -5 do 30 stopni - Wysokość, w zakresie do 100mm - Obrót poziomy od -170 do +170 stopni - Funkcja PIVOT
Monitor bez ramkowy	grubość ramki - 0,8mm (z każdej z 4 stron)
Zintegrowane głośniki	2x 1W
<ul style="list-style-type: none"> • Sprzętowa kalibracja kolorymetryczna, za pomocą zintegrowanej tablicy LUT monitora, w zakresie skorelowanej temperatury barwowej (podawanej za pomocą koordynatów chromatycznych), jasności bieli, jasności czerni oraz krzywej EOTF. Kalibracja powinna umożliwiać precyzyjne ustawienie temperatury barwowej 6500K, 4000K zgodnej z krzywą Plancka o odchyleniu +/- x:0.002, y:0,=0.002 • Technologia chroniąca oczy przed nadmiernym wysiłkiem, eliminująca migotanie, oraz emisję światła niebieskiego. • Funkcja poprawiająca jednorodność obrazu, dostępna z poziomu OSD monitora • Technologia pozwalająca na synchronizację ustawień na 6 monitorach przy obsłudze tylko jednego (głównego) • Zdalne sterowanie monitorem, za pomocą dedykowanego oprogramowania producenta, poprzez dwukierunkową komunikację, realizowaną interfejsem video □ Fabryczny preset DICOM 	

Rejestracja obrazu w systemie VMS.

System nie powinien być ograniczony maksymalną obsługiwaną pojemnością przestrzeni dyskowej. Powinien obsługiwać dyski o różnej pojemności w ramach jednego serwera. Konfiguracja nagrywania i czasu przechowywania nagrań może być zmieniona dla każdej kamery indywidualnie co pozwoli na zadeklarowanie minimalnego i maksymalnego czasu przechowywania dla każdej kamery z osobna. Oznacza to, że materiał nie zostanie nadpisany do momentu zakończenia minimalnego czasu oraz będzie usuwany po przekroczeniu maksymalnego czasu przechowywania. Możliwość konfiguracji harmonogramu nagrywania: tryb ciągły, detekcja ruchu, brak ruchu, zdarzenie alarmowe. Wbudowany moduł detekcji ruchu pracujący w 3 trybach: detekcja porównawcza, detekcja adaptacyjna, detekcja hermeneutyczna. Możliwość wygenerowania akcji: wyjścia cyfrowego, nagrywania, wysłania maila, wygenerowania funkcji kamery PTZ - przejście do określonej pozycji bądź wygenerowanie patrolu. System musi umożliwić przypisanie wielu akcji do jednego alarmu. Nagrywanie obrazu

do 60kl/s oraz brak ograniczenia co do maksymalnej rozdzielczości. Wsparcie dla kodowania MJPEG, MPEG-4, H.264, H.265/HEVC. Platforma musi posiadać możliwość tworzenia automatycznego archiwum na nośnikach zdalnych np.: macierzach dyskowych NAS/SAN z wybranych lub wszystkich kamer. System pozwoli na wykorzystanie serwera redundantnego typu failover, którego zadaniem jest przejęcie nagrywania kamer w momencie uszkodzenia jednego z serwerów nagrywających. Architektura systemu pozwoli na wykorzystanie więcej niż jednego serwera zapasowego. Możemy zadeklarować czas po którym takie przełączenie nastąpi. Obsługa wielostrumieniowości dla każdej kamery z osobna: strumień dla nagrywania, strumień do podglądu lokalnego oraz strumień do podglądu zdalnego. Dowolna konfiguracja dla każdego strumienia osobno jakości nagrywania w rozumieniu rozdzielczości, kompresji, odświeżania. Wbudowana obsługa inteligentnej analizy obrazu i możliwość jej uruchomienia na każdej kamerze znajdującej się w systemie (możliwość przenoszenia funkcji analizy między kamerami). Obsługiwane analizy: wejście w strefę, wyjście ze strefy, pojawienie się, zniknięcie, zatrzymanie, przebywanie w strefie, filtr kierunkowy, przekroczenie prędkości, pojawienie się przedmiotu, zniknięcie przedmiotu, zliczanie, wykrywanie sabotażu. Na podstawie kilku analiz na jednym obrazie możemy stworzyć scenariusz generujący np. alarm w systemie (tworzenie funkcji logicznych z VCA). Dodatkowo wsparcie obsługi funkcji analitycznych oraz rozpoznawania tablic rejestracyjnych ANPR bezpośrednio w wybranych modelach kamer.

Oprogramowanie VMS umożliwia i powinno umożliwiać tworzenie elastycznego interfejsu użytkownika z polskim menu zapewnia intuicyjną pracę oraz ekspresowy czas reakcji. Oprogramowanie klienckie nie wymaga żadnych dodatkowych płatnych licencji i jest dostępne w ramach zakupu licencji na kanały nagrywające. W pełni skalowalny interfejs oprogramowania klienckiego pozwala dostosować wielkość obszaru roboczego oraz siatki kamer, osi czasu i drzewa urządzeń. Obsługa podglądu na żywo/odtwarzanie za pomocą konfigurowalnej osi czasu z możliwością rozróżnienia: nagrania/zakładki/alarmy. Operator będzie mógł zapisać rozłożenie kamer na obrazie i w dowolnej chwili powrócić do tego schematu. Oprogramowanie pozwoli na definiowanie widoków (wyświetlanie na pojedynczym monitorze) oraz multi-widoków (wyświetlanie na wielu monitorach) o różnej zawartości poszczególnych kart (np. obraz na żywo, odtwarzanie, lista zdarzeń, mapa obiektu, wyskakujące okna alarmowe). Rozmieszczenie oraz liczba pól na danym monitorze może być dowolnie konfigurowalna przez użytkownika. Istnieje również możliwość definiowania własnych niestandardowych podziałów. Możliwość sterowanie aplikacją oraz funkcjami za pomocą skrótów klawiaturowych. Generowanie podglądu w 3 trybach: strumień zawsze z rejestratora, strumień zawsze z kamery, strumień z rejestratora, a w przypadku rozłączenia bezpośrednio z kamery. Takie rozwiązanie wspiera bezpieczeństwo oraz niweluje sytuacje braku podglądu na żywo. System umożliwi obsługę do 4 monitorów. Obrazy z kamer mogą być odświeżane w sposób ciągły, z detekcji ruchu lub co zadeklarowany czas w przypadku braku aktywności w polu widzenia kamery. Podgląd odbywać się może poprzez dedykowane oprogramowanie bądź przeglądarkę internetową. Obsługa stref prywatności konfigurowanych dla poszczególnych lub wszystkich użytkowników poza administratorem. Funkcja ochrony prywatności czyli maskowanie twarzy w czasie rzeczywistym tzw. facial blurring lub maskowanie wszystkich ruchomych obiektów. Oprogramowanie musi wspierać zdarzenia przychodzące z inteligentnej analizy obrazu wraz z możliwością wyszukania danej analizy wraz z wizualizacją stref z tych funkcjonalności na żywo. System musi posiadać wyszukiwanie ruchu na już nagranych materiale. Powinna istnieć funkcja tworzenia wirtualnych kamer (wiele widoków z jednej kamery). Funkcja pozwoli przy szerokim kadrze sceny wyciąć interesujący fragment i pozostawić jako podgląd na żywo bądź podgląd z archiwum wraz z obrazem pełnego

kadru kamery. System powinien wspierać kamery tzw. 360 stopni. czyli umożliwiać programowe prostowanie (dewarping) obrazu bezpośrednio z oprogramowania nadzorującego. Pozwoli to na stworzenie 4 niezależnych widoków, 2 widoków 180 stopni (panorama) oraz pojedynczego widoku (cyfrowy PTZ). Widoki te można zapisać i wrócić do danego ustawienia w przypadku gdy zajdzie taka potrzeba. Obsługa wielopoziomowych map zawierających plan wraz z naniesionymi kamerami, we/wy alarmowymi oraz urządzeniami audio. Obsługa okna alarmowego w którym pojawiają się informacje o zdarzeniach wraz z widokiem kamery lub kamer powiązanych w tym zdarzeniu. W trybie odtwarzania będzie możliwość podglądu obrazu archiwalnego z 32 kamer jednocześnie na jednej stacji operatorskiej z prędkością 1 fps, 0.1x, 1/8x, 1/4x, 1/2x, 1x, 2x, 4x, 8x, 16x, 32x, 64x. Aplikacja umożliwi tworzenie zakładki na materiale wideo indywidualnie dla każdej kamery. Tworzenie archiwum ze zdarzenia powinno mieć do wyboru formaty ASF, .AVI, .MATROSKA, .SEF. Dostępny format wewnątrz pozostawiający znak wodny - potwierdzenie autentyczności oraz możliwość ustawienia hasła dla nagrania jak i format ogólnodostępny, który można odtwarzać w ogólnodostępnym oprogramowaniu odtwarzającym wideo. Możliwość zapisania do jednego pliku z materiałem archiwalnym kopii zapasowej z kilku kamer. Zapis pojedynczej klatki z kamery w formatach .JPF, .BMP, .GIF, .TIFF, .PNG poprzez kliknięcie przycisku eksportowania. Oprogramowanie umożliwi tworzenie tzw. storyboard czyli połączonego wideo z wielu kamer z różnych przedziałów czasowych do jednego pliku. Pozwoli to na zmontowanie i wyeksportowanie takiego klipu na poziomie aplikacji CMS. Funkcja używana w momencie kiedy zachodzi potrzeba wyeksportowania nagrania z przemieszczającego się obiektu widzianego na różnych kamerach w różnym czasie. Aplikacja kliencka musi pozwalać na programowanie i aktywowanie presetów, tur kamer PTZ. Wsparcie dla dowolnego kontrolera USB z joystickiem do kontrolowania funkcji PTZ ruchomych punktów kamerowych oraz możliwość kontrolowania kamer PTZ z poziomu panelu w oprogramowaniu. Obsługa cyfrowych modułów I/O aktywowanych z poziomu dedykowanych przycisków ekranowych. W przypadku potrzeby wyświetlania wielu kamer z różnych lokalizacji np. duże centra monitoringu istnieje możliwość wykorzystania funkcjonalności wirtualnej krosownicy. Funkcjonalność pozwala na łatwe zarządzanie dużymi ścianami wizyjnymi złożonymi z wielu monitorów z poziomu jednej stacji roboczej. Daje to możliwość swobodnej konfiguracji dla widoków obrazów z kamer. Możliwość szyfrowanego zdalnego dostępu za pomocą klienta www w oparciu o HTML 5.

System okablowania warstwy aktywnej sieci LAN

Ze względu na brak sieci światłowodowej w miejscach gdzie należy zmodernizować instalacje monitoringu, należy zaprojektować wybudowanie sieci światłowodowej SM, zakończonej w standardzie LC/PC o odpowiedniej ilości włókien (8J wyłącznie do pojedynczych kamer, 12J, 24J do Punktów Dystrybucyjnych i Pośrednich Punktów Dystrybucyjnych.

Switch 24 port.

- Typ przełącznika - Zarządzany
- Obsługa jakości serwisu (QoS) – Tak
- Zarządzanie przez stronę www - Tak
- Podstawowe przełączanie RJ-45 Liczba portów Ethernet - 24
- Podstawowe przełączania Ethernet RJ-45 porty typ - Gigabit Ethernet (10/100/1000)

- Liczba zainstalowanych modułów SFP - 2
- Liczba zainstalowanych modułów SFP+ - 2
- Liczba portów USB 2.0 - 3
- Standardy komunikacyjne - IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3at, IEEE 802.3bz, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z
- Obsługa 10G - Tak
- Technologia okablowania Copper Ethernet - 100BASE-FX, 1000BASE-LX, 1000BASE-SX, 1000BASE-T
- Przekierowywanie IP - Tak
- Pozycja routingu - 3000
- Protokół drzewa rozpinającego - Tak
- Technologie wirtualizacji sieci - Virtual Extensible LAN (VXLAN)
- Trasy IPv4 - 3000
- Trasy IPv6 - 1500
- Liczba VLANs - 1024
- Przepustowość rutowania/przełączania - 176 Gbit/s
- Prędkość przekazywania - 130,95 Mpps
- Wielkość tabeli adresów - 16000 wejścia
- Zgodny z Jumbo Frames - Tak
- Rozszerzenie Jumbo Frames - 9198
- Pamięci bufora pakietów - 6 MB
- Lista kontrolna dostępu (ACL) - Tak
- Szyfrowanie / bezpieczeństwo - 128-bit AES
- Obsługa Multicast - Tak
- Protokoły zarządzające - SNMPv1/v2c/v3
- Protokół wybierania drogi - CDP, EIGRP, OSPF, RIP, VRRP
- Produkt stackowalny - Tak
- Kolor produktu - Szary
- Bezpieczeństwo - IEC 60950-1, UL 60950-1, CAN/CSA C22.2 No. 60950-1, EN 60950-1, AS/NZS 60950.1, Class I Equipment
- Standardy EMC - 47 CFR Part 15, CISPR 22 Class A, CISPR 32 Class A, CNS 13438, EN 300 386, EN 55022 Class A, EN 55032 Class A, EN61000-3-2, EN61000-3-3, ICES-003 Class A, KN 32, TCVN 7189 Class A, V-3 Class A, CISPR 24, EN 300 386, EN 55024, KN 35, TCVN 7317
- Typ pamięci - DRAM
- Pojemność pamięci wewnętrznej - 2048 MB
- Wielkość pamięci flash - 4096 MB
- Poziom hałasu - 42 dB
- Obsługa funkcji Plug & Play - Tak
- MTBF (Średni okres międzyawaryjny) - 346270 h
- Zasilacz dołączony - Tak
- Obsługa zasilania zapasowego (RPS) - Tak
- Napięcie wejściowe AC - 100 - 240 V

- Częstotliwość wejściowa AC - 50 - 60 Hz
- Prąd wejściowy - 6 - 12 A
- Obsługa PoE - Tak
- Power over Ethernet Plus (PoE+) ilość portów - 48
- Zasilanie przez Ethernet (PoE) zasilanie na port - 30 W
- Całkowita Power over Ethernet (PoE) budżetu - 740 W
- Zakres temperatur (eksploatacja) - -5 - 45 °C
- Zakres temperatur (przechowywanie) - -40 - 70 °C
- Zakres wilgotności względnej - 5 - 90%

Switch przemysłowy 8 port RJ45, 2xSFP.

- Typ przełącznika - Zarządzany
- Przełącznik wielowarstwowy - L2
- Obsługa jakości serwisu (QoS) - Tak
- Zarządzanie przez stronę www - Tak
- Kształtowanie ruchu - Tak
- Podstawowe przełączanie RJ-45 Liczba portów Ethernet - 8
- Podstawowe przełączanie Ethernet RJ-45 porty typ - Fast Ethernet (10/100)
- Ilość portów Fast Ethernet (copper) - 8
- Liczba portów SFP Combo - 2
- Liczba portów USB 2.0 - 1
- Złącze zasilania - DC-in jack
- Standardy komunikacyjne - IEEE 802.3ab, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z
- Obsługa 10G - Nie
- Pełny duplex - Tak
- Przekierowywanie IP - Tak
- Agregator połączenia - Tak
- Kontrola wzrostu natężenia ruchu - Tak
- Protokół drzewa rozpinającego - Tak
- Obsługa sieci VLAN - Tak
- Liczba VLANs - 255
- Przepustowość - 6,5 Mpps
- Wielkość tabeli adresów - 8000 wejścia
- Pamięci bufora pakietów - 2 MB
- Funkcje DHCP - DHCP server
- Lista kontrolna dostępu (ACL) - Tak
- Szyfrowanie / bezpieczeństwo - FIPS 140-2, SSH-2
- Filtrowanie adresów MAC - Tak
- Obsługuje SSH/SSL - Tak
- Filtrowanie BPDU / Ochrona - Tak
- Obsługa Multicast - Tak

- Liczba grup multiemisji filtrowanych - 255
- Protokoły zarządzające - SNMPv3
- Bezpieczeństwo - UL 60950-1, CSA C22.2 No. 60950-1, EN 60950-1, CB IEC 60950-1, NOM NOM-019-SCF1
- Certyfikaty - FCC, IEC/EN 55022A, VCCI, AS/NZS CISPR 22, CISPR 11, CISPR 22, IEC 60068-2-27, IEC 60068-2-6, IEC 60068-2-64, EN 61373, UL/CSA, CE, AS/NZ RCM, BSMI, KCC, ANATEL, RoHS
- Pojemność pamięci wewnętrznej - 256 MB
- Wielkość pamięci flash - 64 MB
- MTBF (Średni okres międzyawaryjny) - 374052 h
- Napięcie wejściowe AC - 110 - 220 V
- Pobór mocy - 15 W
- Obsługa PoE - Nie
- Zakres temperatur (eksploatacja) - -40 - 70 °C
- Zakres temperatur (przechowywanie) - -40 - 85 °C
- Dopuszczalna wilgotność względna - 5 - 95%

Wymagania odnośnie zasilania Punktów Dystrybucyjnych i kamer

Realizacja powinna przewidywać zasilanie wszystkich Punktów Dystrybucyjnych i wszystkich Pośrednich Punktów Dystrybucyjnych. Zasilanie należy przewidzieć z rozdzielni napięć gwarantowanych, a w przypadku braku rozdzielni w której występuje zasilanie gwarantowane przewidzieć zasilanie z najbliższej tablicy rozdzielczej.

Do zasilania elektrycznego kamer używamy istniejących sprawnych kabli typu YnKY, które są doprowadzone w miejsce instalacji kamery. W przypadku kiedy instalacja wygląda na wysłużoną, zaprojektować i wymienić okablowanie. Miejsca wpiąć instalacji elektrycznych w rozdzielnie należy przy projektowaniu uzgodnić ze służbami technicznymi Zamawiającego.

SPECYFIKACJA

I. System CCTV

1. Dwa stanowiska dla stacji roboczej (*workstation*),
 - a. Dwanaście monitorów do pracy ciągłej minimum 55",
 - b. Stelaż do montażu monitorów,
 - c. Sterownik-klawiatura do kamer szybkoobrotowych PTZ IP, 2 sztuki,
2. Wymiana kamer na IP

- a. 70 szt. kamer obrotowych analogowych na IP, minimum 2 Mpix z doświetleniem powyżej 100 metrów,
- b. kamery w obudowie przeciwwybuchowej.
- c. 129 szt. kamer stałych analogowych na IP, minimum 4 Mpix z doświetleniem powyżej 30 metrów,
- d. 10 szt. kamer IP, minimum 4 Mpix stacjonarne, z doświetleniem powyżej 50 metrów,
- e. 4 szt. kamer do rozpoznawania tablic rejestracyjnych ANPR
- f. kamery wielokierunkowe z 4 obiektywami korzystająca z jednego adresu IP
- g. rejestratory czterokanałowe IP, bez dysku.

Zintegrowany System Bezpieczeństwa

System integrujący ZSB ma być systemem spójnym, którego zadaniem jest integracja czyli zbieranie, analizowanie, przetwarzanie, archiwizowanie i zaprezentowanie w formie graficznej i opisowej sygnałów, informacji pozyskanych za pośrednictwem odpowiednich interfejsów komunikacyjnych z następujących systemów bezpieczeństwa (SB) zainstalowanych w Elektrowni Połaniec :

- telewizyjnego nadzoru obiektów CCTV,
- systemu kontroli dostępu SKD,

Zintegrowany System Bezpieczeństwa („ZSB”) ma być wykonany w technologii przeglądarki internetowej bez konieczności instalacji aplikacji klienckiej oprogramowania z opcją wyświetlania planu graficznego poszczególnych budynków. Funkcją ZSB jest pomoc i ułatwienie w zarządzaniu ww. systemami bezpieczeństwa przez pracowników obsługi oraz rozszerzenie możliwości współdziałania SB pomiędzy sobą a także podniesienie poziomu bezpieczeństwa. ZSB ma być zbudowany w architekturze klient-serwer zaimplementowanej w modularnej sieci PC. Serwer powinien być zainstalowany w środowisku wirtualnym i spełnia funkcje serwera redundantnego. Serwer ma umożliwiać podłączenie i integrację budynkowych systemów technicznych, systemów bezpieczeństwa oraz zapewnia dostęp dla stacji operatorskich do wszystkich zdefiniowanych w bazie danych rekordów i zmiennych.

W wykonaniu ZSB należy przewidzieć następujące elementy:

- Stacje operatorskie złożone z komputera stacjonarnego oraz dwóch monitorów minimum 27” dedykowanych dla instalacji technicznych, oparte o komputer klasy PC wraz z oprogramowaniem graficznym umożliwiające operatorom dostęp za pomocą przeglądarki internetowej do wszystkich sterowanych i monitorowanych punktów oraz funkcjonujące jako podstawowy interfejs systemu zarządzania bezpieczeństwem.

- Połączenie serwera ze stacjami operatorskimi z wykorzystaniem sieci Ethernet LAN/WAN wykorzystującej odpowiednie protokoły komunikacyjne (np. TCP/IP).
- Interfejsy zewnętrzne, zapewniające komunikacje po protokole cyfrowym pomiędzy KD oraz ZSB.

Projekt powinien zawierać informację dotyczącą możliwości zwizualizowania kamer oraz wejścia/wyjścia alarmowe kamer w miejscach ich instalacji na planach sytuacyjnych oraz na planszach zbiorczych. System ZSB ma mieć możliwość utworzenia wirtualnego powiązania kamer z pozostałymi systemami budynkowymi między innymi KD, których zadziałanie spowoduje (jeśli rozmieszczenie kamer CCTV na to pozwoli) przełączenie kamery na wybrany monitor alarmowy, wykonanie zdjęcia z danej kamery. Zakres opracowania koncepcji nie dotyczy integracji systemu KD.

Operator ma mieć możliwość przełączenia obrazu z kamer poprzez kliknięcie np. na piktogramy kamer umieszczone na planach sytuacyjnych (architektonicznych).

W ZSB mają zostać zwizualizowane kamery, oraz wejścia/wyjścia alarmowe kamer w miejscach ich instalacji na planach sytuacyjnych oraz na planszach zbiorczych.

W przypadku zastosowania dedykowanego modułu sterowania video, system ma pozwolić na przełączanie kamer i monitorów, sterowanie kamerami obrotowymi, zmianę ostrości obrazu i przybliżenia, komponowaniem oraz zapisywaniem układów na monitorach oraz ustawianiem presetów na kamerach obrotowych. W ZSB mają zostać utworzone wirtualne powiązania kamer z pozostałymi systemami budynkowymi między innymi KD, których zadziałanie spowoduje (jeśli rozmieszczenie kamer CCTV na to pozwoli) przełączenie kamery na wybrany monitor alarmowy, wykonanie zdjęcia z danej kamery. W ZSB ma zostać zdefiniowane okno alarmowe, które będzie dedykowane do wyświetlania obrazów z kamer, gdy elementy wykonawcze zintegrowanych systemów zgłoszą meldunek (alarm, zakłócenie, uszkodzenie itd.). Operator ma mieć również możliwość przełączenia obrazu z kamer poprzez kliknięcie np. na piktogramy kamer umieszczone na planach sytuacyjnych (architektonicznych).

Interfejs VMS ma być oparty na protokole IP - oba systemy muszą działać w tym samym segmencie sieciowym (dwa odrębne VLAN). Centralny serwer VMS ma działać, jako proxy pomiędzy ZSB a systemem BVMS. Dlatego serwer VMS musi być obecny, aby wszystkie funkcje interfejsu były dostępne. Integracja z systemem CCTV ma zapewnić nadzorowanie następujących stanów systemu CCTV:

- stanu wejść (włączony, wyłączony, awaria, praca)
- stanu wyjść (aktywne, nie aktywne, włączony, wyłączony, awaria, praca)
- stanu kamer (zazbrojony, rozbrojony, awaria, praca, wymagana konserwacja, aktywna, nie aktywna, stan oświetlenia kamery, włączona, wyłączona, nagrywanie)

Integracja z systemem CCTV ma umożliwić następujące sterowanie systemem

CCTV : • wyjścia (włącz, wyłącz)

- stanu kamer (praca, alarm testowy, zazbrojenie czujnika kamery, włączenie, wyłączenie, włączenie oświetlenia kamery, sterownie kamerą obrotową, ustawianie presetów, wybór presetu, zoom +/-),
- monitory (aktywny, nie aktywny, praca)
- rejestratory/ serwer (przełączenie kamery, uruchomienie nagrania ze stemplem czasu, uruchomienie nagrania ze stemplem zdarzenie, awaria, praca)

- odtwarzacz (sterownie odtwarzaniem (stop, pause, wstecz, przewijanie wstecz, w przód, odtworzenie nagrania ze stempla czasu lub zdarzenia) W przypadku akcji ratowniczo-gaśniczej, ZSB ma:
- Umożliwiać przełączanie obrazu z kamer, poprzez kliknięcie np. na piktogramy kamer umieszczone na planach sytuacyjnych

Integracja z systemem SKD ma umożliwić następujące sterowanie systemem SKD:

- System zarządzania bezpieczeństwem musi zapewniać dwukierunkową wymianę i edytowanie współdzielonych danych w pełnym zakresie, w czasie rzeczywistym, z zastosowanym systemem kontroli dostępu.
- W systemie zarządzania bezpieczeństwem muszą być prezentowane stany drzwi, czujników zamknięcia drzwi, czytników i przycisków w miejscach ich lokalizacji na planach sytuacyjnych (architektonicznych) oraz na schematach zbiorczych.
- W systemie zarządzania bezpieczeństwem operator otrzymywać powinien nie tylko informacje o stanie urządzeń systemu kontroli dostępu, ale także informacje o numerze identyfikatora osobistego użytego do operacji związanych z używaniem systemu kontroli dostępu.
- W systemie zarządzania bezpieczeństwem musi zapewniać możliwość powiązania zdarzeń z systemu KD z systemem CCTV.
- Z poziomu stacji roboczej systemu bezpieczeństwa operator musi mieć możliwość sterować drzwiami kontroli dostępu, np. otworzyć na chwilę, otworzyć na stałe i zablokować drzwi. Dla każdego drzwi z czytnikami i przyciskami zdefiniowana powinna zostać procedura działania oraz plan sytuacyjny.
- Wymaga się, aby z poziomu panelu obsługi punktu danych systemu KD w systemie zarządzania bezpieczeństwem (np. drzwi), w czasie rzeczywistym, możliwy był podgląd bieżącej historii zdarzeń w celu identyfikacji osób odpowiedzialnych za zdarzenia alarmowe, np. w przypadku alarmu drzwi za długo otwarte, ostanie przyłożenie karty na drzwiach, wraz z informacją o danych personalnych danej osoby możliwością przejścia do pełnej historii działań danej osoby.

5. System Awizacji

Awizacja Ruchu Towarowego 2(ART2) będzie głównym narzędziem operacyjnym i platformą integrującą w zakresie procesów dostaw i wywozu transportem kołowym i kolejowym z Elektrowni Połaniec. ART2 będzie zbiorem systemów i modułów realizujących funkcjonalności z obszaru dostaw i wywozu transportem kołowym i kolejowym z Elektrowni Połaniec.

System będzie realizował usługi integracyjne back office w zakresie zasilania i odczytu danych podstawowych, dotyczących dostaw i wywozów, systemów użytkowanych przez Elektrownię, a w szczególności z systemy wagowe MicroWAG, GSW i SCALEX DSRS, systemem poboru prób LabSys, systemem zarządzania zasobami przedsiębiorstwa SAP, systemem Kontroli Dostępu oraz umożliwi w przyszłości integrację z innymi systemami

System będzie gotowy do obsługi Ecmr(elektroniczny list przewozowy) zgodnie z protokołem dodatkowym do Konwencji o umowie międzynarodowego przewozu drogowego towarów

(eCMR) dotyczący elektronicznego listu przewozowego w 2019, oraz do wymiany informacji regulacyjnych z właściwymi organami publicznymi w zakresie transportu drogowego i kolejowego zgodnie z Rozporządzeniem (UE) 2020/1056

System będzie umożliwiał tworzenie harmonogramu dostaw i wywozu wszystkich asortymentów dla Enea Elektrownia Połaniec i spółek zależnych. System umożliwi wprowadzanie planów produkcyjnych Elektrowni Połaniec w ramach których będzie realizowane planowanie dostaw. Umożliwi wymianę informacji z kontrahentami na temat planów i harmonogramów.

System będzie umożliwiał awizację dostaw przez kontrahentów. Dostawca będzie mógł uzyskać dostęp do listy zamówień z SAP możliwych do zaawizowania, które będą pobierane do systemu ART2 automatycznie oraz na żądanie użytkownika.

Wszyscy przedstawiciele kontrahenta oraz uprawnieni użytkownicy ART2 mogą uzyskać wgląd do zaplanowanych awizacji dzięki specjalnie zaprojektowanym interfejsom w postaci planu awizacji oraz tablicy awizacji. Nadawanie uprawnień do ART2 będzie realizowane zarówno w aplikacji ART2 jak i przy pomocy grup domenowych z kontrolera domeny zamawiającego.

System ART2 będzie umożliwiał wielopoziomowe planowanie czasu podstawienia środka transportu na wywóz lub czasu dostawy przez kontrahentów.

System umożliwi określanie elastycznych harmonogramów pracy magazynów i węzłów oraz ich przepustowości. Dla każdego zlecenia transportowego będzie istniała możliwość określenia wymaganych ram czasowych dla załadunku/rozładunku w każdym węźle.

Kontrahent będzie mógł wskazać konkretne, niezajęte jeszcze okienko czasowe, w którym planuje podstawić samochód w ramach czasu wyznaczonego w dwóch poprzednich punktach.

Algorytm wyliczania okna czasowego będzie możliwy do wydruku z systemu. Zapis algorytmu będzie w postaci umożliwiającej dołączenie go do umowy zawieranej z Kontrahentami na dowóz lub wywóz asortymentów.

System będzie umożliwiał awizowanie dostaw i wywozu przez kontrahentów zewnętrznych w definiowanych horyzontach czasowych.

Dostawca system będzie posiadał w ofercie moduł w oferowanym systemie do zestawu funkcjonalności z zakresu YMS(Yard Management System), które będą wdrażane u Zamawiającego w przyszłości.

W zakresie transportu kolejowego system będzie oferował moduły Administracji, Ekspedycji, Dyspozytora, Manewrów oraz Listu Kolejowego. Moduły będą wykonywały operacje na danych podstawowych zintegrowanych z systemami Enea Elektrownia Połaniec oraz systemem wag kolejowych w Enea Elektrownia Połaniec jakim jest SCALEX DSRS.

W zakresie Administracji system będzie umożliwiał wprowadzanie ustawień ogólnych, z których korzystają pozostałe moduły systemu.

W module Ekspedycji system umożliwi gromadzenie informacji o wagonach i przesyłkach przybyłych i wysłanych z bocznic, stanie przesyłek i wagonów, dodatkowych informacji. Gromadzenie danych z ważeń importowanych z wagi kolejowej lub wprowadzonych przez operatora, drukowania protokołów ważeń i archiwizacji raportów z ważeń. Ustalania czasu pobytu wagonów na bocznicach i rozliczania na poszczególnych użytkownikach bocznic oraz

rozliczania kosztów dyspozycji na poszczególne rodzaje działalności. Sporządzanie dokumentacji wysyłanej z wagonami i innych wymaganych dokumentów przewozowych i pociągowych.

W module Dyspozytor będzie zarządzanie nadzorem i organizacją pracy wagonów na bocznicach.

W module Tabor zawarte będą informacje o wagonach prywatnych, wydierżawionych, sprzęcie i lokomotywach. Będzie służył do ewidencji własnych lub wydierżawianych wagonów włączonych do taboru kolejowego jak i przeznaczonych do potrzeb technologicznych firmy. W ramach technicznej eksploatacji w programie przewidziana jest kontrola czasu dla rewizji - badań technicznych oraz rejestrowanie i rozliczanie przeprowadzonych napraw taboru. Na podstawie zapisów w module Ekspedycji program pozwala na ustalenie miejsca pobytu wagonu własnego poza bocznicą, obliczenie jego przebiegu [km] i wykonanej pracy [tkm] przy założeniu, że obrót dla wykonanej pracy jest rejestrowany w programie.

W zakresie Listu Kolejowego system umożliwi wydruk w trybie tekstowym na dowolnej drukarce igłowej na składance komputerowej albo formularzach użytkownika, wydruk na czystych kartkach rubryk z wypełnieniem, możliwość wypełniania dokumentów w wielu językach europejskich (w tym alfabety łacińskie, cyrylica, grecki), uproszczone wpisywanie znaków z języków obcych, możliwość pracy z wieloma plikami i dokumentami równocześnie; program będzie tworzył pliki o strukturze zgodnej z formatem XML(Extensible Markup Language). Umożliwi zapis wprowadzonych danych i ich późniejszą edycję, funkcje notatników stacji, klientów, oświadczeń, szablony całych dokumentów. Umożliwi generowanie dokumentów R-27/28, R7 i R-16 na podstawie dokumentów przewozowych.

Przedmiotem zamówienia Systemu Awizacji będzie:

- opracowanie harmonogramu prac, których celem będzie wytworzenie i wdrożenie Systemu Awizacji u Zamawiającego, obejmującego poniższe etapy
- przeprowadzenie analizy procesów biznesowych z obszaru planowania, realizowania oraz raportowania dostaw i wywozów w Enea Elektrownia Połaniec
- opracowanie i dostarczenie dokumentacji w standardzie BPMN/BPEL/UML(Business Process Model and Notation)/BPEL(Business Process Execution Language)/UML(Unified Modeling Language) z analizy procesów biznesowych w Enea Elektrownia Połaniec z obszaru planowania, realizowania oraz raportowania dostaw i wywozów
- zaprojektowanie Systemu Awizacji wspierającego procesy biznesowe z obszaru planowania, realizowania oraz raportowania dostaw i wywozów w Enea Elektrownia Połaniec
- zaprojektowanie integracji Systemu Awizacji z istniejącymi systemami informatycznymi w Enea Elektrownia Połaniec
- zaprojektowanie uniwersalnych interfejsów do wymiany danych pomiędzy Systemu Awizacji, a systemami informatycznymi które będą wdrożone w przyszłości w Enea Elektrownia Połaniec, w taki sposób by skorzystanie z interfejsu nie wymagało zmian programistycznych po stronie Systemu Awizacji
- opracowanie i dostarczenie dokumentacji technicznej Systemu Awizacji

- wytworzenie wersji testowej Systemu Awizacji i wdrożenie jej na infrastrukturze Zamawiającego
- opracowanie i dostarczenie dokumentacji użytkowej, w wersji testowej , Systemu Awizacji
- przygotowanie scenariuszy testowych dla wersji testowej Systemu Awizacji wdrożonego u Zamawiającego, które będą podstawą do odbioru systemu testowego
- wytworzenie wersji produkcyjnej Systemu Awizacji i wdrożenie jej na infrastrukturze Zamawiającego
- opracowanie i dostarczenie dokumentacji użytkowej, w wersji produkcyjnej , Systemu Awizacji
- przygotowanie scenariuszy testowych dla wersji produkcyjnej Systemu Awizacji wdrożonej u Zamawiającego, które będą podstawą do odbioru systemu produkcyjnego
- opracowanie i dostarczenie dokumentacji powykonawczej Systemu Awizacji zawierającej zaktualizowane na stan wdrożenia systemu w wersji produkcyjnej dokumenty: Architektoniczny Model Systemu, Podręcznik Użytkownika Zewnętrznego, Podręcznik Użytkownika Wewnętrznego, Podręcznik Administratora Systemu, Podręcznik eksploatacji Systemu

Ponadto system ma spełniać:

5.1 Wymagane warunki wdrożenia

- 5.1.1. Zamawiający wymaga wdrożenia rozwiązania w architekturze klient serwer, w które hostowane będzie na serwerach dostarczonych przez Zamawiającego, przy zachowaniu określonych przez Zamawiającego wymagań bezpieczeństwa oraz w zgodzie z standardami obowiązującymi u Zamawiającego. Wymagania co do zasobów dostarczy Wykonawca w porozumieniu z Zamawiającym.
- 5.1.2. Zamawiający wymaga analizy obszaru dziedzinowego logistyki w Enea Elektrownia Połaniec w zakresie planowania, realizowania oraz raportowania dostaw i wywozów środkami transportu kołowego i kolejowego
- 5.1.3. Zamawiający wymaga wdrożenia równoległego do obecnie użytkowanego systemu Awizacji
- 5.1.4. Zamawiający wymaga opracowania dokumentacji etapu analizy – modelu biznesowego opisującego przepływ danych, użytkowników zaangażowanych w przepływ, role i zakresy odpowiedzialności użytkowników i systemów. Diagramy w dokumentacji mają zostać przygotowane w notacjach BPMN(Business Process Model and Notation)/BPEL(Business Process Execution Language)/UML(Unified Modeling Language). Opisy procesów, ról, zakresów w uporządkowanej postaci tabelarycznej.
- 5.1.5. Zamawiający wymaga skonfigurowania Systemu pod wymagania Zamawiającego zgodnie z wynikiem analizy 5.1.4.wraz z integracją z istniejącymi systemami, aplikacjami, w szczególności: SAP, GSW, microWAG, LabSys, SCALEX DSRS, Qdata, KD oraz wskazanie możliwości integracji przez dostarczenie wraz z dokumentacją opisującą (opis metod) - specjalistycznego API umożliwiającego integrację bez zmian programistycznych w dostarczonym oprogramowaniu umożliwiającemu zasilanie danymi wprowadzanymi automatycznie lub ręcznie.

- 5.1.6. Zamawiający wymaga opracowania harmonogramu wdrożeniowego uwzględniającego scenariusze testowe wraz z ich realizacją dla kolejnych wersji przedmiotu zamówienia
- 5.1.7. Zamawiający wymaga opracowania scenariuszy testowych dla wszystkich etapów harmonogramu w których powstaje System.
- 5.1.8. Zamawiający wymaga przygotowania wersji testowej Systemu, a po testach akceptacyjnych wersji produkcyjnej Systemu, na środowisku wykorzystującym infrastrukturę Zamawiającego w terminach wskazanym przez Zamawiającego w czasie trwania umowy.
- 5.1.9. Zamawiający wymaga oszacowania kosztów utrzymania systemu po upływie okresu gwarancji w ramach umowy serwisowej/licencyjnej oraz okresu na jaki może być ona zawarta. Parametry umowy serwisowej - możliwość całodobowego zgłaszania awarii i szybką reakcją na zgłoszenie serwisowe, w tym doradztwo i pomoc telefoniczną oraz przez połączenie VPN. Dostępność służb technicznych Wykonawcy (24 godzinny, 7 dni w tygodniu) do usuwania zgłoszonych awarii i usterek instalacji.
- 5.1.10. Zamawiający wymaga objęcia systemu usługą asysty technicznej i konserwacji (ATiK).
- 5.1.11. Zamawiający wymaga licencjonowania systemu bez ograniczeń na liczbę użytkowników, komputerów, serwerów, transakcji, ilości danych itp.
- 5.1.12. Okna dialogowe systemu powinny być dostępne w 3 wariantach językowych: polski, angielski, rosyjski . Jeżeli aplikacja będzie wykonana w technologii WWW to pliki z literałami powinny mieć postać zbliżoną do resx by bez zmian programistycznych była możliwość zmian literałów.

5.2 Wymagania dotyczące dokumentacji

- 5.2.1. Wykonawca w ramach przedmiotu zamówienia przygotuje i dostarczy koncepcję techniczną i biznesową rozwiązania oraz instrukcje eksploatacyjne administratora, użytkowników zarówno wewnętrznych jak i zewnętrznych (Kontrahenci) oraz eksploatacji zgodnie z poniższymi wymaganiami
- 5.2.2. Podręcznik Eksploatacji Systemu(PES)

Wymagania

- a. Podręcznik PES pokrywa pełny zakres procedur eksploatacyjnych Systemu.
- b. Podręcznik, poprzez wprowadzane zasady eksploatacji, optymalizuje wykorzystanie zasobów (organizacyjnych i technologicznych) pod kątem spełnienia wymagań eksploatacyjnych systemu.
- c. Opis działań dotyczących eksploatacji systemu umożliwia Zamawiającemu ich realizację bez udziału Wykonawcy.

Minimalny zakres informacyjny

Element zakresu informacyjnego (np. rozdział)	Opis elementu zakresu informacyjnego
Role i ich zakresy odpowiedzialności	Wykaz ról pełnionych przez osoby w realizacji zadań eksploatacyjnych.
Cykliczne zadania eksploatacyjne	<p>Szczegółowy wykaz cyklicznych zadań eksploatacyjnych wraz z pełnym opisem:</p> <ul style="list-style-type: none"> Nazwa zadania. Wykaz ról uczestniczących w realizacji zadania, również jeśli rola występuje wyłącznie w czynnościach opcjonalnych. Określenie kiedy zadanie jest wykonywane. Określenie momentu zakończenia zadania - np. poprzez określenie czasu trwania lub czasu zakończenia. Czynności wykonywane w ramach zadania, z określeniem: o roli, która wykonuje daną czynność, o wykorzystywanych komponentów oprogramowania, o opisu czynności
Jednorazowe zadania eksploatacyjne	Określenie zasad zlecania jednorazowych zadań eksploatacyjnych oraz szablonu zlecenia zadania jednorazowego.
Opis stanowisk pracy	<p>Pełna charakterystyka stanowiska pracy Użytkownika Systemu:</p> <ul style="list-style-type: none"> Opis przeznaczenia danego stanowiska pracy. Wymagany sprzęt stanowiska pracy, np. minimalna konfiguracja komputera dla stanowiska pracy. Wymagane oprogramowanie stanowiska pracy wspierające pracę systemu np. system operacyjny, przeglądarka, oprogramowanie biurowe, etc. Wymagane wsparcie telekomunikacyjne (sieć telefoniczna, LAN, karta GPRS, etc). Wymagane materiały eksploatacyjne. Wymagania charakteryzujące bezpieczne użytkowanie systemu informatycznego, np. umiejscowienie stanowiska, prace w pomieszczeniu o ograniczonym dostępie. Wymagane doświadczenie/umiejętności administratora Systemu. Inne wymagania specyficzne dla Systemu.

5.2.3 Podręcznik Administratora Systemu(PAS)

Wymagania

- a. Podręcznik PAS obejmuje wszystkie czynności administracyjne związane z Systemem.

- b. W szczególności PAS zawiera opis zadań administratora Systemu, w sposób umożliwiający Zamawiającemu ich realizację bez udziału Wykonawcy:
- i. instrukcje konfiguracji i administracji dostarczonych Systemu,
 - ii. instrukcje postępowania w Przypadkach Szczególnych oraz Awarii, w tym odtworzenia Systemu,
 - iii. opisy komunikatów o błędach w Systemie i procedury rozwiązania takich sytuacji,
 - iv. dokumenty wymagane przez ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych i przepisy wykonawcze do tej ustawy oraz Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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.
- c. Podręcznik jest zgodny z elementami Systemu, które opisuje.

Minimalny zakres informacyjny

Element zakresu informacyjnego (np. rozdział)	Opis elementu zakresu informacyjnego
Wykaz instrukcji i odpowiedzialności	Pełna lista instrukcji wraz z określeniem zespołu odpowiedzialnego za wykonywanie i przestrzeganie danej instrukcji w zakresie administrowania Systemem.
Określenie wersji	Określenie wersji Systemu/Produktów, których dotyczy wraz z wersjami systemu operacyjnego/bazy danych/serwerów itp.
Wytyczne do planu eksploatacji	Wytyczne do Planu Eksploatacji Systemu sugerujące np. harmonogram wykonywanych okresowo instrukcji.
Instrukcje administratorskie	Opis instrukcji obsługi wszystkich elementów Systemu (w tym uwzględniające mechanizmy bezpieczeństwa przetwarzania danych) niezbędnych dla eksploatacji i utrzymania Systemu. Instrukcje administracyjne powinny dotyczyć co najmniej: <ul style="list-style-type: none"> • oprogramowania (wraz z obsługą danych), • wymaganej konfiguracji infrastruktury programowo - sprzętowej. Opis powinien zawierać szczegółowe scenariusze postępowania przypadku wystąpienia awarii i konieczności odtworzenia Systemu.
Komunikaty systemu	Opis komunikatów systemu (np. występujących w logach czy wyświetlanych na ekranie), w tym komunikatów o błędach - wraz ze szczegółowym wyjaśnieniem ich znaczenia.
Wymogi prawne	Opis dokumentów wymaganych przez ustawę o ochronie danych osobowych - w kontekście administrowania Systemem.

5.2.4 Podręcznik Użytkownika Wewnętrznego

Wymagania

- a) Dokumentacja powinna zostać uzupełniona o elementy identyfikujące dokument.
- b) Dokumentacja powinna zostać uzupełniona o zasady świadczenia wsparcia technicznego dla tej grupy użytkowników.
- c) Dokumentacja powinna zawierać kompletny opis sposobu realizacji wszystkich scenariuszy użycia systemu możliwych do realizacji przez użytkowników nie będących administratorami systemu. Opis powinien zawierać zrzuty ekranów ilustrujące wykonywanie określonych czynności
- d) Elementy Dokumentacji odpowiedzialne za wykonywanie konkretnych czynności w systemie powinny być udostępnione użytkownikom zarówno w postaci ogólnego dokumentu, jak też powinny zostać dostarczone w postaci wbudowanego w system mechanizmu pomocy kontekstowej.

Minimalny zakres informacyjny

Element zakresu informacyjnego (np. rozdział)	Opis elementu zakresu informacyjnego
Identyfikator dokumentu	Informacje na temat: wersji dokumentu, historii zmian, nazwy i wersja Systemu, do którego się odnosi.
Opis ogólny	Ogólnie opis do czego służy System, zasady nawigacji pomiędzy poszczególnymi komponentami Systemu oraz generalne zasady współpracy z Systemem oraz zasady świadczenia wsparcia technicznego.
Opis funkcji	Opis ról i ich uprawnień dla tej klasy użytkowników, opis funkcjonalności oraz interfejsu użytkownika dla tej klasy użytkowników, zasady walidacji pól, opis raportów i zestawień.

5.2.5 Podręcznik Użytkownika Zewnętrznego

Wymagania

- e) Dokumentacja powinna zostać uzupełniona o elementy identyfikujące dokument.
- f) Dokumentacja powinna zostać uzupełniona o zasady świadczenia wsparcia technicznego dla tej grupy użytkowników.
- g) Dokumentacja powinna zawierać kompletny opis sposobu realizacji wszystkich scenariuszy użycia systemu możliwych do realizacji przez użytkowników nie będących administratorami systemu. Opis powinien zawierać zrzuty ekranów ilustrujące wykonywanie określonych czynności
- h) Elementy Dokumentacji odpowiedzialne za wykonywanie konkretnych czynności w systemie powinny być udostępnione użytkownikom zarówno w postaci ogólnego dokumentu, jak też powinny zostać dostarczone w postaci wbudowanego w system mechanizmu pomocy kontekstowej.

Minimalny zakres informacyjny

Element zakresu informacyjnego (np. rozdział)	Opis elementu zakresu informacyjnego
Identyfikator dokumentu	Informacje na temat: wersji dokumentu, historii zmian, nazwy i wersja Systemu, do którego się odnosi.
Opis ogólny	Ogólnie opis do czego służy System, zasady nawigacji pomiędzy poszczególnymi komponentami Systemu oraz generalne zasady współpracy z Systemem oraz zasady świadczenia wsparcia technicznego.
Opis funkcji	Opis ról i ich uprawnień dla tej klasy użytkowników, opis funkcjonalności oraz interfejsu użytkownika dla tej klasy użytkowników, zasady walidacji pól, opis raportów i zestawień.

5.2.3. Dokumentacja będzie dostarczana Zamawiającemu przez Wykonawcę w trakcie realizacji Umowy, w terminach określonych Harmonogramem Wdrożenia, odpowiednio do postępu prac i będzie podlegała opiniowaniu i akceptacji. Nie później jednak niż 2 tygodnie przed terminem odbioru etapu prac, którego dotyczy dokumentacja.

5.2.4. Zamawiający wymaga dokumentacji sporządzonej w języku polskim.

5.2.5. Zamawiający wymaga dokumentacji w formie edytowalnej w formacie bpmn, bpmn.di , .docx , .xls, .vsdx itp.

5.3 Techniczne warunki wdrożenia

5.3.1. Wszystkie strony wykorzystywane w ramach Systemu muszą zostać zabezpieczone certyfikatem bezpieczeństwa SSL.

5.3.2. System musi zabezpieczać integralność przetwarzanych informacji.

5.3.3. System musi wspierać integrację z AD/IdM w ramach SSO.

5.3.4. System musi zapewnić możliwość zarządzania prawami dostępu do Systemu w oparciu o mechanizm ról (RBAC), obsługę ograniczeń dla kont użytkowników uprawnionych.

5.3.5. System musi gromadzić i archiwizować logi operacji mających na celu zapewnienia rozliczalności Użytkowników Uprawnionych:

- Logi związane ze zmianą uprawnień (kto, kiedy, kogo dotyczy, jakie uprawnienia).
- Logi związane ze zmianą konfiguracji Systemu (kto, kiedy, co, opcjonalnie wartość).
- Logi związane z obsługą Systemu przez Użytkowników Uprawnionych (kto, kiedy, id procesu, rodzaj operacji, opcjonalnie wartości).

5.3.6. Wykonawca wskaże miejsce i sposób przechowywania/gromadzenia logów, udostępni do wglądu Zamawiającego i opíše w dokumentacji sposób ich odczytu (weryfikacji).

- 5.3.7. Dostęp do Systemu musi być możliwy we wszystkich wymienionych przeglądarkach internetowych: MS Edge, Firefox, Chrome, Opera ze wsparciem wstecznym dwóch wersji.
- 5.3.8. Dostęp do System dla użytkowników zewnętrznych (Kontrahenci) musi umożliwiać uwierzytelnianie dwuskładnikowe

5.4 Infrastruktura Zamawiającego

- 5.4.1. Na potrzeby wdrożenia w środowisku Zamawiającego, Zamawiający zapewni własną infrastrukturę informatyczną obejmującą cały obszar wdrożenia Systemu. Środowisko serwerowe i bazodanowe Zamawiającego jest zlokalizowane w Centrach Przetwarzania Danych i jest otwarte pod względem skalowalności zasobów (mocy obliczeniowej, pamięci operacyjnej, przestrzeni dyskowej). Instalacja i konfiguracja serwerów, systemów operacyjnych i instancji baz danych zostaną przeprowadzone przez Zamawiającego w uzgodnieniu z Wykonawcą oraz w oparciu o Koncepcję Techniczną dostarczoną przez Wykonawcę.
- 5.4.2. Zamawiający udostępni platformę sprzętową z oprogramowaniem wirtualizacyjnym w środowisku VMware vSphere na serwerach z procesorami INTEL.
- 5.4.3. Dopuszczalne systemy operacyjne serwerów dla tego środowiska :
- system operacyjny Windows Server 2016 64-bit
 - system operacyjny Linux:
 - Red Hat 64-bit
 - SLES 64-bit
 - Oracle Entrprice Linux
 - Centos
- 5.4.4. Zamawiający wymaga aby System działał na najnowszych wersjach systemów operacyjnych wymienionych powyżej. Zastosowanie innych wersji wymaga uzgodnienia z Zamawiającym.
- 5.4.5. Wykonawca w ramach Koncepcji Technicznej dostarczy zestawienie serwerów, które będą wykorzystane przez System. Wykaz będzie zawierał informacje o wydajności (moc obliczeniowa, pamięć operacyjna, obszar dyskowy) i wymaganiach konfiguracji ze wskazanym systemem operacyjnym, na podstawie którego Zamawiający przygotuje i skonfiguruje serwery dla Systemu.
- 5.4.6. Licencje niezbędne do uruchomienia i udostępnienia środowiska serwerowego (systemy operacyjne, wirtualizator, bazy danych) na potrzeby Systemu zostaną dostarczone przez Zamawiającego. Wykonawca dostarczy pozostałe licencje, które będą wymagane do prawidłowego działania Systemu.
- 5.4.7. Zamawiający udostępni bazy danych:
- ORACLE w wersji 19c Enterprise Edition
 - Microsoft MSSQL wersja 2016 Standard lub wyższa
 - MySQL
- 5.4.8. Zamawiający dysponuje systemem backupu obejmującym swoim działaniem posiadaną infrastrukturę serwerową i bazodanową, w tym zasoby które będą udostępnione dla Systemu.

5.4.9. Zamawiający wymaga, by każdy istotny element oprogramowania wchodzącego w skład Systemu objętego umowami licencyjnymi innymi, niż Open Source lub freeware:

- pochodził od uznanych wytwórców, o światowym zasięgu,
- był realizowany w nowoczesnej i rozwojowej technologii,
- był wspierany przez możliwie licznych liczących się integratorów i innych usługodawców działających na terenie Polski i Unii Europejskiej,
- nie był objęty prawami wyłącznymi Wykonawcy ani żadnej spółki powiązanej kapitałowo z Wykonawcą (w tym z konsorcjantem).

5.4.10. Zamawiający wymaga, by każdy istotny element oprogramowania wchodzącego w skład Systemu objętego umowami licencyjnymi Open Source lub freeware:

- był realizowany w nowoczesnej i rozwojowej technologii,
- nie był wskazany przez wytwórcę, jako produkt, którego dalszy rozwój lub wsparcie będą wstrzymane w terminie krótszym niż 5 lat od daty oferowanego zakończenia realizacji umowy.

5.4.11. Na potrzebę dostępu Wykonawcy do prowadzenia prac zdalnie zostanie zestawiony tunel VPN site-to-site pomiędzy Wykonawcą, a Zamawiającym. W tym celu Wykonawca musi zapewnić w swojej lokalizacji i na swój koszt urządzenie pozwalające na skonfigurowanie tunelu VPN w technologii IPSec według parametrów podanych przez Zamawiającego po podpisaniu Umowy.

5.5 Wymagania bezpieczeństwa

5.5.1. System i wszystkie jego komponenty oraz mechanizmy zabezpieczeń zapewniają monitorowane parametrów związanych z bezpieczeństwem poprzez wysyłanie logów systemowych do systemu SIEM Zamawiającego.

5.5.2. Kontrola i eliminacja błędów programistycznych

- na etapie opracowywania kolejnych wersji oprogramowania dokonywana jest automatyczna kontrola kodu przez Wykonawcę,
- Zamawiający jest uprawniony do dowolnego przeprowadzania testów bezpieczeństwa aplikacji/systemu oraz infrastruktury technicznej utrzymywanej na potrzeby systemu.. W przypadku zidentyfikowania błędów bezpieczeństwa, w oprogramowaniu i konfiguracji dostarczonej przez Wykonawcę, Wykonawca niezwłocznie je poprawi bez pobierania dodatkowych opłat.

5.5.3. Komunikacja pomiędzy wszelkimi elementami Systemu powinna być zabezpieczona kryptograficznie.

5.5.4. Wykonawca zapewnia uprawnienia na najniższym wymaganym do utrzymania i rozwoju systemu poziomie i tylko dla wykwalifikowanego personelu Wykonawcy. Pozostali pracownicy Wykonawcy nie mają dostępu do sieci i infrastruktury IT dedykowanej dla ENEA Elektrownia Połaniec S.A.. Praca serwisów zewnętrznych (dostawców sprzętu i rozwiązań IT) możliwa tylko pod stałą kontrolą uprawnionego personelu Zamawiającego. Wykonawca prowadzi rejestr takich prac i na wniosek Zamawiającego umożliwi wgląd w ten rejestr.

5.5.5. Wszelkie komponenty sprzętowe i software'owe stosowane przez Wykonawcę na potrzeby świadczenia usługi posiadają Wsparcie producenta i mają na bieżąco instalowane poprawki bezpieczeństwa.

- 5.5.6. System zapewnia granulację uprawnień (podział na Grupy), zgodnie z potrzebami biznesowymi ENEA Elektrownia Połaniec S.A. przy zachowaniu zasady przydzielania minimalnych potrzebnych uprawnień.
- 5.5.7. System będzie zintegrowany z systemem AD obowiązującym u Zamawiającego.
- 5.5.8. Wykonawca musi zapewnić rozwój systemu zgodnie z wymaganiami Zamawiającego uwarunkowanymi zmianami prawnymi.
- 5.5.9. Wykonawca musi zapewnić rozwój systemu zgodnie z powstającymi wymaganiami Zamawiającego uwarunkowanymi powstawaniem nowych zagrożeń cybernetycznych oraz nowych wymagań bezpieczeństwa Zamawiającego.

5.6 Wymagania funkcjonalne

- 5.6.1. awizacja dostaw i wywozów wszystkich asortymentów realizowanych w Elektrowni transportem samochodowym i kolejowym
- 5.6.2. dodawanie i parametryzacja bram(przepustowość, kierunek ruchu, obsługiwane asortymenty)
- 5.6.3. algorytm podziału doby na sloty czasowe(awizacje) spełniający wszystkie twarde ograniczenia
- 5.6.4. dokumentacja algorytmu(opis działania) w systemie
- 5.6.5. GUI(formatki) do ręcznego wprowadzania ograniczeń
- 5.6.6. moduł do tworzenia raportów z możliwością eksportu do Excel
- 5.6.7. wyświetlanie zbiorczej informacji o zbliżających się dostawach/wywozach (awizacje) oraz poruszających się po terenie elektrowni dostawach/wywozach (informacje z systemów zintegrowanych)
- 5.6.8. filtrowanie wyświetlanych awizacji wedle parametrów określonych przez użytkownika
- 5.6.9. import/export harmonogramów asortymentów spoza SAP
- 5.6.10. panel podglądu wszystkich dostaw i wywozów w bieżącej dekadzie wraz z możliwością zwiększania zakresu dat
- 5.6.11. import zamówień z SAP
- 5.6.12. planowanie i harmonogramowanie dostaw w ramach zamówień
- 5.6.13. obsługa współczynnika tolerancji z zamówień SAP

5.7 Funkcjonalności dla użytkowników wewnętrznych

- 5.7.1. tworzenie i usuwanie zapotrzebowań na asortymenty
- 5.7.2. wyświetlanie zapotrzebowań wraz z filtrowaniem
- 5.7.3. tworzenie i usuwanie dyspozycji dobowych
- 5.7.4. wyświetlanie dyspozycji dobowych wraz z filtrowaniem
- 5.7.5. dodawanie i usuwanie awizacji
- 5.7.6. powielanie awizacji
- 5.7.7. wyświetlanie awizacji w formie tabelarycznej wraz z filtrowaniem
- 5.7.8. wyświetlanie awizacji w formie kalendarza (dobowy/tygodniowy) z granulacją wynikającą z podziału doby na sloty wraz z filtrowaniem oraz wolnymi slotami
- 5.7.9. tworzenie harmonogramów dostaw i wywozów z podziałem na asortymenty i kontrahentów
- 5.7.10. awaryjne sloty awizacyjne widoczne tylko dla Biura Awizacji
- 5.7.11. informacja o odbyciu szkolenia (do weryfikacji czy nie powinno to być w KD)

- 5.7.12. komunikacja z kontrahentami w zakresie planowania i harmonogramowania zapotrzebowań na dostawy w ramach umów zaimportowanych z SAP

5.8 Funkcjonalności dla użytkowników zewnętrznych

- 5.8.1. wprowadzanie, edycja i wyświetlanie danych podstawowych kierowców (poprzez wywołanie metody do systemu KD)
- 5.8.2. wprowadzanie, edycja i wyświetlanie danych podstawowych pojazdów (poprzez wywołanie metody do systemu KD)
- 5.8.3. dodawanie i usuwanie awizacji
- 5.8.4. powielanie awizacji
- 5.8.5. wyświetlanie awizacji w formie tabelarycznej wraz z filtrowaniem
- 5.8.6. wyświetlanie awizacji w formie kalendarza (dobowy/tygodniowy) z granulacją wynikającą z podziału doby na sloty wraz z filtrowaniem oraz wolnymi slotami
- 5.8.7. panel nawigacyjny wyświetlający informację o aktualnie zaawizowanym wolumenie z zamówienia, aktualnie dostarczonym, itp.: w celu ułatwienia planowania awizacji
- 5.8.8. udostępnianie i workflow akceptacji harmonogramów
- 5.8.9. informacja o czasie obsługi na bramie/ilości aut w kolejce/przybyłych transportach

5.9 Ograniczenia do algorytmu 5.6.3. (Parametry zmienne):

- 5.9.1. Przepustowość bram
- 5.9.2. Przepustowość asortymentów
- 5.9.3. Wolumen asortymentu z zamówień
- 5.9.4. Pula awizacji dla kontrahenta wynikająca z wolumenu umowy
- 5.9.5. Zapotrzebowanie na asortyment (10 dni)
- 5.9.6. Dyspozycja dobową na asortyment (1 doba)
- 5.9.7. Równomierne obciążenie pór dnia
- 5.9.8. Sloty czasowe dla dostawców równomiernie na dobę, np. dostawca 'x' w godzinowym przedziale czasowym może mieć tylko 1 slot
- 5.9.9. Informacja zwrotna z systemów wagowych o rzeczywistym wolumenie zrealizowanej dostawy zmniejsza dostępny do awizowania wolumen z zamówienia
- 5.9.10. Anulowanie awizacji w przypadku braku wolumenu na skutek nadmiarowych dostaw rzeczywistych w ramach poprzednich awizacji z zamówienia wraz z powiadamianiem email kontrahenta
- 5.9.11. Strefy w ramach doby w ramach których kontrahent może mieć określoną liczbę awizacji

Wskazania Zamawiającego należy traktować, jako priorytetowe. System CCTV, system SKD, awizacja oraz platformy integrującej musi posiadać 3 letnie wsparcie serwisowe.

SLA

- 1. Wykonawca zobowiązany jest do dostarczenia zamawiającemu zestaw serwisowy do wdrożenia systemu SKD.
 - 3 szt. rezerwowych czytników każdego rodzaju jakie będą występować w systemie,

- 5 szt. zasilaczy,
 - 3 szt. kontrolerów,
2. Szkolenie administratorów i operatorów systemu z obsługi urządzeń.
 3. Wykonanie dokumentacji projektowej, powykonawczej dla elementów systemu objętych modernizacją i rozbudową i przekazanie jej Zamawiającemu.
 4. Wykonawca zapewnia aktualizację (upgrade) dla całości oprogramowania wskazanego w ofercie/wskazanego w niniejszym opisie przedmiotu zamówienia, w całym okresie realizacji zamówienia oraz w okresie gwarancji. Aktualizacja ma zapewniać funkcjonalności oprogramowania na poziomie tożsamym lub wyższym z oprogramowaniem wskazanym w ofercie/wskazanym w niniejszym opisie przedmiotu zamówienia. Aktualizacja będzie wykonywana przynajmniej 1 raz na koniec każdego roku obowiązywania gwarancji.
 5. Wykonawca zapewnia w okresie gwarancji serwis gwarancyjny. W ramach serwisu Wykonawca zapewnia:
 - Obsługę procesu zgłaszania problemów, tj. przyjmowanie, ewidencjonowanie, monitorowanie oraz dokumentowanie zamykanie zgłoszeń,
 - Analiza problemów i identyfikacja miejsc oraz komponentów Systemów najprawdopodobniej odpowiedzialnych za problemy,
 - Uruchamianie i realizowanie procedur serwisowych.
 6. Na etapie wdrożenia przedstawiciele Zamawiającego oraz Wykonawcy dokonają wspólnie analizy i podziału elementów podsystemów na kategorie awarii oraz związane z nimi czasy naprawy zgodnie z poniższą tabelą:

Rodzaj awarii	Dni powszednie, godz. 07:00 – 22:00	Dni świąteczne oraz dni powszednie, godz. 22:00 - 07:00
Lekka	Reakcja 2h/ naprawa 72h	Reakcja 4h/ naprawa 96h
Średnia	Reakcja 2h/ naprawa 48h	Reakcja 4h/ naprawa 72h
Krytyczna	Reakcja 2h/ naprawa 24h	Reakcja 2h/ naprawa 36h

Czasy indywidualnej naprawy mogą zostać skorygowane w oparciu o uzgodnienia poczynione przez przedstawicieli Zamawiającego oraz Wykonawcy.

Reakcja serwisowa to rozpoznanie powodu awarii, określenie sposobu jej usunięcia, określenie zakresu naprawy oraz terminu wizyty serwisowej. Naprawa serwisowa to całkowite usunięcie awarii i przywrócenie pełnej sprawności urządzeń/oprogramowania. Za termin przyjęcia zgłoszenia przez Wykonawcę, Strony przyjmują moment dokonania przez Zamawiającego zgłoszenia za pośrednictwem poczty elektronicznej lub telefonicznie.

7. Udzielenie gwarancji na zakres zadań objęty przedmiotem zamówienia na okres zadeklarowany w formularzu ofertowym jednak nie mniejszy niż 36 miesięcy.
8. Świadczenie usługi serwisowej dla zakresu objętego przedmiotem zamówienia na okres udzielenia gwarancji.
9. Wykonawca obejmuje, w ramach niniejszego zamówienia, serwisem zamontowane urządzenia przez okres udzielonej przez Wykonawcę gwarancji 36 miesięcy. Serwis winien obejmować wszelkie wytyczne producenta w tym m.in. częstotliwość serwisowania urządzeń, wymianę elementów objętych serwisem, w celu zapewnienia prawidłowej eksploatacji zamontowanych urządzeń oraz zapewniania utrzymania warunków gwarancji.

10. Serwis hardwarowy i softwarowy systemu SKD w trakcie trwania gwarancji jest po stronie wykonawcy.
11. System CCTV oraz platformy integrującej, a także System SA są objęte serwisem softwarowym Wykonawcy (nie wyłączając gwarancji urządzeń).
 - Harmonogram wdrożenia po wyłonieniu Wykonawcy i podpisaniu umowy:
 - ✓ Trzy miesiące na wykonanie i dostarczenie Zamawiającemu projektu,
 - ✓ Osiem miesięcy na wykonanie pozostałego zakresu.
12. Wdrożenie nowego systemu musi odbyć się z zachowaniem ciągłości pracy (działania) istniejącego systemu.
13. Wymagane jest, aby Wykonawca dokonał wizji lokalnej miejsca dostawy, aby uzyskać informacje, które mogą być konieczne do przygotowania oferty oraz zawarcia umowy i wykonania zamówienia. Koszty dokonania wizji lokalnej ponosi Wykonawca.
14. Zapewnienie dla każdego systemu odpowiedniej retencji danych, zgodnie z powszechnie obowiązującymi przepisami prawa.

Ogólna zasada równoważności rozwiązań.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań, materiałów i urządzeń służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne.
5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może proponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. W zakresie SKD rozstrzygające będzie to, czy oprogramowanie/sprzęt spełnia wymagania normy EN60839-11 grade/klasa4.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te

są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

9. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

Ogólne wymogi prawne.

Oferowane przez Wykonawcę rozwiązania muszą być na dzień odbioru zgodne z aktami prawnymi regulującymi pracę Zamawiającego. Oferowane rozwiązania muszą być zgodne w szczególności z następującymi przepisami (z ich późniejszymi zmianami):

Wymagania ogólne dostawy sprzętu.

1. Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt musi być fabrycznie nowy (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą się znajdować na liście „end-of-sale” oraz „end-of-support” producenta.

4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzeń pozwalających na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
11. Dla dostaw sprzętu informatycznego z systemem operacyjnym Zamawiający wymaga fabrycznie nowego systemu operacyjnego (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego systemu operacyjnego nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku systemu operacyjnego naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

Wymogi licencjonowania oprogramowania.

1. Licencjobiorcą wszystkich licencji będzie EEP.
2. Licencje muszą zostać wystawione na czas nieoznaczony (bezterminowy).
3. Oferowane licencje muszą pozwalać na użytkowanie Oprogramowania zgodnie z przepisami prawa.
4. Licencja Oprogramowania nie może ograniczać prawa licencjobiorcy do rozbudowy, zwiększenia ilości serwerów obsługujących oprogramowanie, przeniesienia oprogramowania na inny serwer, rozdzielenia funkcji serwera (osobny serwer bazy danych, osobny serwer aplikacji, osobny serwer plików).
5. Licencja Oprogramowania musi umożliwiać działanie systemu lokalnie na serwerach Zamawiającego.
6. Licencja Oprogramowania musi być licencją bez ograniczenia ilości komputerów, serwerów, na których można zainstalować i używać Oprogramowanie.
7. Licencja na Oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet).
8. Licencja Oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.

9. Licencja Oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji i użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.

10. Licencja Oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z Oprogramowania na dowolnym komputerze klienckim (licencja nie może być przypisana do komputera/urządzenia).

11. Licencja Oprogramowania musi pozwalać na modyfikację, zmianę, rozbudowę Oprogramowania w celu przystosowania go do potrzeb Zamawiającego w zakresie, w którym Oprogramowanie to umożliwia przez istniejące w Oprogramowaniu mechanizmy konfiguracyjne.

