Załącznik nr 1 do SIWP nr GAPR-DPRJ/695/22/W

OPIS PRZEDMIOTU ZAMÓWIENIA

dot. wyboru wykonawcy prac projektowych i robót modernizacyjnych w trybie „zaprojektuj i wybuduj" dla zadania pn. *„Modernizacja systemu kontroli dostępu i systemu sprzedażowego"* na obiekcie Stadionu Miejskiego im. Piotra Wieczorka zlokalizowanego na działce nr 842 obręb Podlesie, ul. Okrzei 20, 44-100 Gliwice

1. Słownik pojęć

- **Stadion** – modernizowany obiekt sportowy – Stadion Miejski im. Piotra Wieczorka w Gliwicach przy ulicy Stefana Okrzei 20 44-100 Gliwice.
- **System, System biletowy, System sprzedaży i kontroli biletów** – stadionowy system sprzedaży biletów i kontroli biletów.
- **Baza Danych** – serwer bazodanowy Systemu typu SQL.
- **LAN (Local Area Network)** – komputerowa sieć lokalna.
- **Lokalny Punkt Dystrybucyjny (LDP)** – miejsce instalacji urządzeń sieciowych w ramach fizycznej sieci strukturalnej (okablowania), obsługującym najczęściej dany obszar roboczy lub piętro.
- **Główny Punkt Dystrybucyjny (GPD)** – miejsce stanowiące centrum okablowania w topologii gwiazdy. Umiejscowiony w budynku głównym w pomieszczeniu serwerowni.
- **Punkt Kasowy (PK)** – pomieszczenia kasowe, w których usytuowano wyposażenie stanowisk kasowych.
- **Punkt Sprzedaży** – Punkt Kasowy.
- **Przełącznik sieci LAN (Switch)** – urządzenie łączące segmenty sieci komputerowej pracujące w drugiej warstwie modelu ISO/OSI (łącza danych), jego zadaniem jest przekazywanie ramek między segmentami; najczęściej wykorzystywane do komunikacji w sieci Ethernet.
- **ETH, Ethernet** – technologia, w której zawarte są standardy wykorzystywane w budowie sieci komputerowych. Obejmuje ona specyfikację kabli oraz przesyłanych nimi sygnałów. Ethernet opisuje również format ramek (dane z nagłówkami warstwy drugiej) i protokoły z dwóch najniższych warstw modelu ISO/OSI. Jego specyfikacja została podana w standardzie IEEE 802.
- **IP (Internet Protocol)** – protokół warstwy trzeciej modelu ISO/OSI, powszechnie stosowany w sieciach komputerowych lokalnych i publicznych (Internet) do adresowania i transmitowania pakietów (ramki z nagłówkami warstwy trzeciej). W koncepcji określenie sieci IP oznacza sieć komputerową ogólnie dostępną dla transmisji nie tylko danych ale również wideo i głosu.
- **Zapora ogniowa (Firewall)** – urządzenie zabezpieczające sieć komputerową przed zagrożeniami zarówno w sieci Internet jak również w sieci LAN; termin ten może odnosić się zarówno do dedykowanego sprzętu komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego niepowołany dostęp do komputera; pełni rolę połączenia ochrony sprzętowej i programowej sieci wewnętrznej LAN przed dostępem z zewnątrz, chroni też przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz.
- **Dokument Wejściowy** – bilety wejściowe na obiekt (papierowe, elektroniczne).
- **Punkt Kontrolny** - kołowroty wejściowe wyposażone w elektroniczne czytniki biletów.

2. System biletowy

2.1. Wymagania ogólne

System musi zapewniać kompleksową obsługę Klientów/Kibiców w zakresie wszystkich procesów związanych z wejściem na obiekt, na którym organizowane jest przedsięwzięcie, zwane dalej imprezą. Wejście na obiekt będzie uzależnione jest od posiadanego Dokumentu Wejściowego (biletu) lub innego dokumentu upoważniającego do wejścia.

System przez okres 60 miesięcy musi być bezpłatnie aktualizowany do najnowszej wersji oferowanej przez Wykonawcę, być zgodny z przepisami prawa powszechnego, przepisami organizatorów rozgrywek, a także dostosowywany do wymagań Zamawiającego (w tym Użytkownika). Wykonawca zapewnia przez ten okres bezawaryjne, ciągłe działanie systemu i udziela zdalnego wsparcia technicznego lub w przypadku awarii krytycznej (przez co rozumie się brak możliwości zdalnej naprawy systemu) osobistej naprawy systemu przez techników Wykonawcy w terminie ustalonym z Zamawiającym, lecz nie dłuższym niż 24 godziny od zgłoszenia awarii. Wykonawca zapewnia bezpłatne wdrożenie i szkolenie wstępne dla wskazanych pracowników przez Zamawiającego po zakończeniu prac zawiązanych z systemem biletowym.

Architektura Systemu musi być zbudowana z następujących warstw:

- Warstwa kontroli mechanicznej, na którą składać się będą istniejące stadionowe kołowroty wysokie (bramofurty stadionowe),
- Warstwa kontroli elektronicznej, odpowiedzialna za odczyt Dokumentów Wejściowych (biletu z kodem 1D, 2D lub elektronicznej karty zbliżeniowej – Karty Kibica), podjęcie decyzji o dostępie, bądź jego odmowie oraz odpowiednie wysterowanie kołowrotem wejściowym, na którą składać się będą czytniki biletów oraz terminale mobilne,
- Warstwa informatyczna odpowiadająca za proces sprzedaży i dystrybucji biletów, weryfikację uprawnień wejściowych, kontrolę dostępu do obiektu i stref, przetwarzanie danych osobowych i zarządzanie całym systemem, za którą odpowiadać będzie System biletowy,
- Instalacja zasilająca wszystkie elementy systemu,
- Stanowiska kasowe,
- System kontroli dostępu do strefy VIP w budynku za pomocą urządzeń mobilnych (palmtopów).

Zgodnie z wymaganiami ustawy o bezpieczeństwie imprez masowych z dnia 20 marca 2009 r. (t.j. Dz.U. z 2019 r. poz. 2171 ze zm.), zwanej dalej w skrócie ustawą o BIM, System biletowy musi umożliwiać zakup Dokumentów Wejściowych w wewnętrznych, zewnętrznych i wyniesionych punktach sprzedaży w obiekcie (lokalne i zdalne stanowiska kasowe), za pomocą zewnętrznych systemów sprzedaży biletów oraz na portalu - Aplikacji WWW.

System musi gwarantować sprzedaż w czasie rzeczywistym z jednoczesnym dostępem do wszystkich wolnych miejsc przez wszystkich sprzedawców, użytkowników Aplikacji WWW.

Dokument Wejściowy musi umożliwiać przekroczenie określonego Punktu Kontrolnego prowadzącego do obiektu i zajęcie miejsca w określonym sektorze, rzędzie i miejscu lub na wydzielonym sektorze na płycie stadionu.

Punktami Kontrolnymi będą istniejące wejściowe stadionowe kołowroty wysokie (bramofurty), które będą wyposażone w nowe czytniki biletów.

Wszystkie wejścia dla kibiców muszą zostać przypisane do stref wejścia w zależności od tego, na jakie sektory prowadzą.

Wejściowe kołowroty wysokie (bramofurty) muszą zostać wyposażone w zintegrowane Czytniki biletów odczytujące kody kreskowe 1D i 2D oraz chipy RFID w standardzie MIFARE. Czytniki musza posiadać kolorowe wyświetlacze graficzne o wielkości min 7" oraz rozdzielczości min. 1024x600 px. Czytniki muszą posiadać dwa interfejsy sieciowe do komunikacji oraz kontroler środowiskowy. Czytniki biletów muszą porównać dane zawarte na Dokumencie Wejściowym z danymi zawartymi w serwerze (Bazie Danych Systemu) lub pamięci wewnętrznej czytnika biletów i umożliwić wejście Klienta/Kibica na obiekt.

Zwolnienie blokady bramofurty musi odbywać się automatycznie. Jednak ze względów bezpieczeństwa musi zostać zapewnione również ręczne sterowanie kołowrotami. W tym zarówno zablokowanie bramofurty dla kolejnego kibica jak i zwolnienie blokady. Sterowanie ręczne musi posiadać wyższy priorytet niż elektroniczne, tzn. że zablokowana ręcznie bramofurta po przyłożeniu uprawnionego biletu musi pozostać zablokowana.

Wszelkie nieprawidłowości w odczycie danych muszą spowodować zablokowanie wejścia, odesłanie Klienta/Kibica do stewarda lub Punktu Sprzedaży, pełniącego również funkcję kasy reklamacyjnej celem wyjaśnienia przyczyn nieprawidłowości. Po sprawdzeniu danych zawartych na Dokumencie Wejściowym z danymi zapisanymi w pamięci serwera obsługa kasy reklamacyjnej podejmie decyzję o wpuszczeniu Klienta/Kibica do obiektu poprzez wydanie biletu zastępczego lub niewpuszczeniu Klienta/Kibica do obiektu.

System biletowy musi składać się z modułów funkcjonalnych:

- Moduł Budowania i Zarządzania Bazą Klientów,
- Moduł Sprzedaży Dokumentów Wejściowych,
- Bazy kibiców,
- Moduł Aplikacji WWW,
- Moduł Administracyjny,
- Moduł Kontroli Biletów,

System biletowy realizować musi następujące zadania:

- budowanie i zarządzanie bazą Klientów/Kibiców,
- sprzedaż karnetów, biletów jednorazowych oraz Kart Kibica/Klienta zarówno w punktach kasowych na stadionie, wyniesionych punktach obsługi klienta a także za pomocą Internetu w portalu obsługi klienta z dowolnego miejsca w Polsce,
- sprzedaż voucherów, generowanie kodów rabatowych, darmowych biletów,
- kontrolę osób wchodzących na stadion,
- prezentację zapełnienia stadionu, wraz z innymi raportami niezbędnymi administratorowi i pracownikom odpowiedzialnymi za bezpieczeństwo imprez,
- wprowadzanie i egzekwowanie sądowych i klubowych zakazów wejść na imprezy,
- obsługę kibiców nieletnich zgodnie z ustawą o BIM,
- obsługę Kibiców Gości,
- sporządzanie w Systemie raportów i statystyk z danych zawartych w Systemie,
- administrowanie Systemem przez Użytkownika Końcowego bez udziału Wykonawcy.
- posiadać system sprzedaży z możliwością sprzedaży grupowej związanej z importowaniem odpowiednik plików CSV lub XLS oraz hurtowym drukowaniem biletów.

- zbierać dane takie jak numer telefonu, adres e-mail i adres zamieszkania.
- być kompatybilny z aplikacją kibica Piasta Gliwice wydaną na urządzenia mobilne przez PRIMO Partner lub innym wskazanymi przez Zamawiającego.
- uwzględniać promocję związane z nowymi kibicami.
- udostępniać API dla zewnętrznych systemów sprzedaży.

System nie może wpuścić do obiektu Klienta/Kibica z zakazem stadionowym, klubowym lub indywidualnie stworzoną listą zakazów, a także Klienta/Kibica posługującego się fałszywym Dokumentem Wejściowym lub Dokumentem, który już raz został użyty.

Moduł Kontroli Biletów musi umożliwiać identyfikację Klientów/Kibiców na etapie sprzedaży Dokumentu Wejściowego, składania wniosku o elektroniczną Kartę Klienta/Kibica, kontroli Dokumentów Wejściowych w Punktach Kontrolnych, a także w dowolnym momencie trwania imprezy masowej.

System musi umożliwiać kompleksową obsługę Klientów/Kibiców poprzez Aplikację WWW w zakresie rejestracji profilu, złożenia i opłacenia wniosku o wydanie Karty Klienta/Kibica, zakupu Dokumentów Wejściowych oraz uzyskania wszechstronnych informacji dotyczących imprez organizowanych na obiekcie.

Moduł Aplikacji WWW Systemu biletowego musi zapewniać responsywność strony pod kątem urządzeń mobilnych.

System musi umożliwiać nadawanie uprawnień Użytkownikom Oprogramowania poprzez ograniczenie dostępności do jego zasobów i funkcji.

Oprogramowanie musi zapewniać szczelność Systemu przed wtargnięciem do Bazy Danych przez osoby nieupoważnione w następujący sposób. System biletowy oraz jego architektura (klient-serwer) muszą zapewniać standardy bezpieczeństwa określone w Ustawie o Ochronie Danych Osobowych z dnia 14 grudnia 2018 roku wraz z późniejszym zmianami (Dz. U. z 2019, poz. 125)".

Wszystkie operacje systemowe jak: wejście, przejście przez strefę, próba przejścia z użyciem wykorzystanego biletu, próba przejścia przez osobę z zakazem stadionowym muszą być rejestrowane w bazie danych systemu i być kojarzone z rekordem identyfikacji kibica celem dalszego ich przetwarzania na potrzeby wydruków, raportów i innych zestawień potrzebnych do prawidłowej pracy służb stadionowych.

System biletowy musi umożliwiać:

- identyfikację kibica na etapie kontroli biletu, a także w dowolnym momencie trwania imprezy masowej,
- blokowanie dostępu dla osób nieuprawnionych oraz z zakazami stadionowymi,
- nadawanie uprawnień użytkownikom oprogramowania poprzez ograniczanie dostępności do jego zasobów i funkcji,
- zabezpieczenie przed wtargnięciem do bazy danych przez osoby nieupoważnione,
- przechowywanie wszystkich informacji w bazie danych,
- kontrolowanie sprawność funkcjonowania poszczególnych czytników kołowrotów.
- Kompatybilność z systemem monitoringu i rejestracją wejść kibiców na stadion.

Serwery systemu i klaster bezpieczeństwa:

System biletowy musi zostać skonfigurowany na maszynach wirtualnych, które będą działały w oparciu o wirtualizator w systemie Windows Server. Logicznie muszą zostać wydzielone 2 węzły klastra (dwa serwery fizyczne), które będą pracowały w klastrze wysokiej dostępności HA w ramach usługi systemowej np. FailoverCluster.

Taka konfiguracja musi zapewniać zabezpieczenie działania systemu w przypadku awarii jednego z fizycznych serwerów.

Dodatkowo lokalnie na dyskach serwerów muszą być przechowywane maszyny wirtualne pełniące funkcje kontrolerów domeny podstawowy i zapasowy (wymagane w konfiguracji klastrowej). W przypadku niedostępności jednego z serwerów fizycznych musi być dostępny jeden z kontrolerów domeny.

Macierz:

Kluczowym elementem zabezpieczającym dane systemu musi być macierz dyskowa. Musi ona udostępniać zasoby dyskowe dla dwóch fizycznych serwerów oraz stanowić wspólny udział dla klastra niezawodnościowego HA. Maszyny wirtualne Systemu biletowego tj. serwer aplikacyjny i bazy danych oraz serwer www muszą być przechowywane na macierzy dyskowej.

Na serwerze bazodanowym musi być zainstalowana baza danych, która musi być chroniona hasłem. Dodatkowo wszystkie maszyny muszą znajdować się w domenie z wdrożoną podstawową polityką bezpieczeństwa. Systemy i serwery muszą pracować w wydzielonej sieci wewnętrznej, specjalnie dla Systemu biletowego.

Dostęp do serwerów musi być realizowany za pomocą tunelu VPN, skonfigurowany na dedykowanym urządzeniu typu firewall.

Oprogramowanie Systemu musi umożliwiać przechowywanie wszystkich informacji w Bazie Danych Systemu. Oprogramowanie musi zbierało informacje o wszystkich transakcjach sprzedaży, musi umożliwiać tworzenie raportów i sprawozdań z funkcjonowania obiektu i Systemu, a także umożliwiać sprawdzenie i raportowanie poprawność funkcjonowania poszczególnych Punktów Kontrolnych i urządzeń końcowych.

System musi pozwalać na wyłączenie platformy serwerowej (w całości lub częściowo), w trakcie wpuszczania osób na obiekt, bez zatrzymywania ruchu osobowego przez Punkty Kontrolne i bez utraty informacji zbieranych w trakcie wpuszczania kibiców na obiekt. Funkcjonalność ta musi pozwalać na prace systemu w trybie off-line. Chwilowe wstrzymanie pracy systemu komputerowego (w tym aplikacji w Punktach Sprzedaży) nie może spowodować zatrzymania ruchu osobowego na obiekcie w trakcie wpuszczania osób przez Punkty Kontrolne. W tym celu czytniki biletów muszą posiadać pamięć wewnętrzną na min. 100 tys. rekordów uprawnionych Dokumentów Wejściowych, które zapewnią ciągłość ruchu osobowego.

System musi umożliwiać stacjonarną sprzedaż biletów na stanowiskach kasowych (zainstalowanych w punktach kasowych) oraz sprzedaż on-line-ową poprzez Aplikację WWW, zewnętrzne punkty sprzedaży, punkty wyniesione. Sprzedaż przez zewnętrzne punkty sprzedaży musi odbywać się on-line. Systemy zewnętrzne muszą łączyć się z Systemem biletowym za pośrednictwem dedykowanego i udostępnionego API.

Moduł Kontroli Biletów musi umożliwiać:

- weryfikację aktualnych zakazów stadionowych i klubowych na etapie kontroli biletów,
- identyfikację kibiców przy wejściu na obiekt oraz w dowolnym momencie podczas trwania imprezy,

- monitorowanie liczby osób będących na imprezie (w systemie on-line) oraz stopnia zapełnienia poszczególnych trybun,
- prezentować statystyki kibiców z podziałem na wiek, płeć, miejsce zakupu biletu, ilością imprez, w których kibic uczestniczył,
- bieżącą prezentację zapełnienia obiektu w rozbiciu na poszczególne sektory, poszczególne wejścia oraz wszystkie wejścia razem,
- określenie dostępu do wyznaczonych sektorów obiektu dla zdefiniowanych posiadaczy biletów,
- zapisanie w pamięci serwera daty i godziny otwarcia bramki wejściowej dla określonego biletu,
- pełną dokumentację ruchu osobowego na obiekcie (z datą i czasem wejścia i wyjścia klienta),
- weryfikację poprawności biletu w czasie nie dłuższym niż 1 sekunda,
- eliminowanie ponownego użycia biletu oraz biletu nienależącego do puli danej imprezy,
- skierowanie ruchu osobowego do dedykowanych wejść i wyjść (wybrane grupy biletów do wybranych grup kołowrotów) oraz całkowite blokowanie przejść przez kołowroty (lub dla wybranych grup biletów),
- obsługi chwilowych wyjść z sektorów,
- chwilowe wyłączenie systemu kołowrotów bez wstrzymywania sprzedaży biletów,
- obsługę reklamacji z nieudanych wejść na obiekt w punktach kasowych.

2.2. Wymagania systemowe i serwerowe

1.1.1. Platforma serwerowa

System musi pracować w oparciu o platformę serwerową składającej się z 2 serwerów fizycznych (maszyny serwerowe o parametrach opisanych poniżej) i wyodrębnionych na niej funkcjonalnych serwerach wirtualnych oraz macierzy dyskowej.

Wszystkie komponenty muszą posiadać zsynchronizowany czas rzeczywisty oraz procesy warunkujące poprawną, nieprzerwaną i niezakłóconą pod względem wydajności i dyspozycyjności pracę platformy. Zasoby dyskowe serwera muszą umożliwiać przechowywanie danych z imprez masowych przez okres min. 90 dni.

System musi pracować na serwerze relacyjnej Bazy Danych typu SQL. System musi pracować w oparciu o jedną Bazę Danych.

Serwery i macierz systemu muszą zostać umieszczone w istniejącej 19" szafie teleinformatycznej w pomieszczeniu GPD.

1.1.1.1. Serwery fizyczne systemu biletowego

System musi pracować w oparciu o dwa fizyczne serwery o następujących minimalnych parametrach technicznych:

- procesor: minimum 8 rdzeniowy (min. 16 wątkowy), minimum 2.0 GHZ/rdzeń,
- pamięć RAM: minimum 32GB DDR4,
- dyski twarde: 4 x SSD minimum 240GB, kieszenie „hot-swap”,

- kontroler RAID: z opcją RAID 0,1,5,6,10 z minimum 512 MB pamięci cache z zabezpieczeniem bateryjnym,
- napęd: DVD-RW SATA,
- karta sieciowa: zintegrowana minimum 2x RJ-45 1GBit,
- karta sieciowa dodatkowa minimum 2xRJ-45 1GBit,
- dedykowany interfejs RJ45 z oprogramowaniem do zarządzania serwerem z opcjami (restart, power up, power down oraz zdalnym podglądem ekranu konsoli),
- 2 zasilacze redundantne pracujące w trybie „hot-swap".

Dostarczone serwery muszą posiadać co najmniej 5 letnią gwarancję producenta świadczoną w miejscu instalacji „on-site".

Na serwerach musi zostać zainstalowane oprogramowanie systemowe oraz oprogramowanie do wirtualizacji oraz muszą zostać wydzielone komponenty funkcyjne (serwery wirtualne).

Specyfikacja funkcjonalna serwerów wirtualnych została opisana w dalszej części (Serwery funkcjonalne systemu).

1.1.1.2. System operacyjny dla serwerów Systemu biletowego

Serwerowy system operacyjny musi posiadać następujące, wbudowane minimalne cechy:

- Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
- Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64 TB przez każdy wirtualny serwerowy system operacyjny.
- Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
- Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy miedzy fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
- Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
- Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
- Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
- Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    - pozwalają na zmianę rozmiaru w czasie pracy systemu,
    - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,

    - umożliwiają zdefiniowanie list kontroli dostępu (ACL).
- Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FiPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
- Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
- Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
- Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    - Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    - Dotykowy, umożliwiający sterowanie dotykiem na monitorach dotykowych.
- Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
- Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
- Mechanizmy logowania w oparciu o:
    - Login i hasło,
    - Karty z certyfikatami (smartcard),
    - Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
- Możliwość wymuszania wieloelementowej kontroli dostępu dla określonych grup użytkowników.
- Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB Plug&Play).
- Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
- Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
- Wsparcie dla środowisk Java i .NET Framework 4.x - możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
- Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
    - Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

- Podłączenie do domeny w trybie offline - bez dostępnego połączenia sieciowego z domeną,
- Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika - na przykład typu certyfikatu użytego do logowania,
- Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
- Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o i0S i Windows 10.
- Zdalna dystrybucja oprogramowania na stacje robocze.
- Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
- Szyfrowanie plików i folderów.
- Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
- Serwis udostępniania stron WWW.
- Wsparcie dla protokołu IP w wersji 6 (IPv6),
- Wsparcie dla algorytmów Suite B (RFC 4869),
- Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
  - dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
  - obsługi ramek typu jumbo frames dla maszyn wirtualnych,
  - obsługi 4-KB sektorów dysków,
  - nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
  - możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,
  - możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode),
  - możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,

- wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath),
- możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,
- mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,
- możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF,

- Oprogramowanie systemowe dla serwerów fizycznych musi być wspierane przez producenta tego oprogramowania oraz na bieżąco udostępniać poprawki systemowe producenta,
- W przypadku wykorzystania systemu operacyjnego bez wsparcia producenta odpowiedzialność za ewentualne naruszenie bezpieczeństwa systemu spoczywa w całości na dostawcy (wykonawcy), przez cały okres gwarancji. Licencje musza mieć bezterminową ważność.

1.1.1.3. Macierz dyskowa

Platforma serwerowa musi składować dane z backupów systemu na jednej macierzy dyskowej o minimalnych parametrach technicznych:

- procesor: o częstotliwości zegara min. 1,4 GHz,
- pamięć RAM: min. 4 GB DDR3,
- ilość dysków: min. 4 x 3.5" lub 2.5" SATA 3Gb/s typ HDD (4 x NLSAS 1TB 7.2 2.5),
- pojemność dysków: min. 1 TB GB (każdy dysk),
- interfejsy sieciowe: min. 4 x Gigabit RJ-45 Ethernet,
- interfejsy zarządzające: min 2xRJ-45 Ethernet, umożliwiające zarządzanie z opcjami (restart, power up, power down oraz zdalnym podglądem ekranu konsoli),
- dostępne tryby RAID: 0, 1, 1+0, 5, 5+0, 6,
- Interfejs napędu: Serial Attached SCSI (6 Gbit/s),
- Obsługiwane systemy zarządzające:
  - Microsoft Windows Server 2019,
  - Microsoft Windows Server 2016,
  - Microsoft Windows Server 2012, 2012 R2,
  - Microsoft Windows Server 2008, 2008 R2,
  - Solaris11 (11/11 or later),
  - Red Hat Enterprise Linux 7,
  - Microsoft Windows Server 2016 Hyper-V,
  - Microsoft Windows Server 2012, 2012 R2,
  - Hyper-V 2.0,
- Dostarczona macierz musi posiadać co najmniej 5 letnią gwarancję producenta, świadczoną w miejscu instalacji „on-site", a licencje muszą mieć bezterminową ważność.

1.1.1.4. Przełączniki sieciowe (switche)

W ramach wdrożenia przewiduje się dostarczenie 1 zarządzanego przełącznika sieciowego o następujących minimalnych parametrach technicznych:

- 24 porty miedziane UTP 10/100/1000 Base-T (Gigabit Ethernet RJ-45),
- 4 porty światłowodowe 10 GBit (SFP+),
- Temperatura pracy: od 0° do 45° C,
- Możliwość przekierowania IP,
- Przepustowość routowania min 125 Gbit/s,
- Minimum 5 lat gwarancji.

1.1.1.5. Firewall

W ramach wdrożenia przewiduje się dostarczenie nowego 1 systemu bezpieczeństwa realizujący funkcję firewall.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Musi istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Minimalne wymagania dla systemu bezpieczeństwa (Firewall):

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum: 10 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Minimalne parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 690 tys. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 6 Gbps dla pakietów 64 B.
4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1800 Mbps.
5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 6.5 Gbps.
6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.

Minimalne funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Kontrola Antywirusowa

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Ochrona przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do nieograniczonego, bezterminowego korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres co najmniej 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24h 7 dni w tygodniu.

1.1.2. Serwery funkcjonalne systemu

Na platformie serwerowej Systemu muszą zostać wyodrębnione następujące serwery funkcjonalne:

Serwer bazodanowy i aplikacyjny – musi przechowywać całość informacji o bazie danych Klientów/Kibiców, imprezach, cennikach, widowni, udostępniać informacje z bazy dla serwera sklepu www, aplikacji kasjerskiej i serwera kontroli. Serwer musi umożliwiać tworzenie kopii zapasowych i replikację bazy danych oraz cykliczne archiwizowanie danych. Serwer ten również musi: udostępniać aplikacje dla kasjerów i pośredników w Punktach Sprzedaży, umożliwiać gromadzenie i budowanie bazy danych Klientów/Kibiców w Punktach Sprzedaży oraz poprzez Zewnętrzne Systemy Dystrybucji Biletów, obsługiwać proces rezerwacji i sprzedaży dokumentów wejściowych, produktów i usług a także składania elektronicznych wniosków o Karty Klienta/Kibica w Punktach Sprzedaży oraz poprzez Zewnętrzne Systemy Dystrybucji Biletów (wstępna rezerwacja miejsc, produktów i usług, zwalnianie biletów, usług, obiektów i stref bez potwierdzenia wpłaty, itp.), pozwalać na sprawdzanie dostępności stref/obiektów. System musi posiadać zewnętrze API do integracji z zewnętrznymi systemami sprzedaży.

Serwer www – musi umożliwiać gromadzenie i budowanie bazy danych Klientów/Kibiców poprzez portal - Aplikację WWW, kontrolować i uzupełniać informacje w bazie internetowej (wystawianie imprez, produktów i usług do sprzedaży w Aplikacji WWW), obsługiwać proces rezerwacji i sprzedaży biletów, produktów i usług przez Internet oraz składania elektronicznych wniosków o Karty Klienta/Kibica (wstępna rezerwacja miejsc, produktów i usług dla klientów internetowych, zwalnianie biletów, usług, obiektów i stref bez potwierdzenia wpłaty, zakup dokumentu wejściowego z płatnością definiowaną, itp.).

Z powodów bezpieczeństwa serwer bazodanowy musi być odseparowany od części portalowej (Internet). Dostęp do zasobów serwera musi być możliwy jedynie z poziomu sieci lokalnej, z zachowaniem niezbędnych restrykcji związanych z dostępem do danych osobowych i informacji o charakterze strategicznym. Dostęp do Internetu musi być możliwy dla serwera www.

System serwerowy musi być odporny na stany awaryjne, tj. powinien umożliwiać ciągłą pracę systemu biletowego bez utraty danych (redundancja) w pełnym zakresie, w przypadku:

- całkowitego lub częściowego uszkodzenia jednego z serwerów fizycznych – wyłączenie serwera fizycznego,
- całkowitego lub częściowego uszkodzenia dysku serwera fizycznego – wyłączenie dysku fizycznego,
- całkowitego lub częściowego uszkodzenia 2 dysków w macierzy dyskowej – wyłączenie dysków,
- uszkodzenia kontrolera sieci Ethernet serwera – wyłączenie kontrolera,
- uszkodzenie przełącznika sieciowego – wyłączenie jednego przełącznika sieci,
- uszkodzenie zasilacza serwera fizycznego – wyłączenie zasilacza,
- uszkodzenie zasilacza macierzy dyskowej – wyłączenie zasilacza.

Oba fizyczne serwery muszą pracować w klastrze HA (HA – High Availability - zespół serwerów działających na rzecz wspólnego dobra, jakim jest ciągłe działanie wirtualnych maszyn uruchomionych na wszystkich hostach należących do klastra HA). Wyznaczone serwery w klastrze HA muszą posiadać wszystkie informacje o uruchomionych maszynach wirtualnych (na którym hoście dana maszyna jest uruchomiona, jakie ma przydzielone zasoby i priorytety, jaka jest ścieżka do katalogu z plikami konfiguracyjnymi danej maszyny itp.). Licencje systemowe muszą umożliwić obsługę klastra oraz obsługę dwóch serwerów wirtualnych. System musi pracować poprawnie po całkowitej awarii jednej z dwóch fizycznych maszyn.

Wszelkie nieprawidłowości pracy całego systemu powinny być raportowane w sposób automatyczny.

1.1.3. Backup systemu

System musi być wyposażony w mechanizm tworzenia kopii zapasowej umożliwiający jego konfigurację w momencie instalacji Systemu wg wytycznych Zamawiającego ustalonych w czasie analizy przedwdrożeniowej oraz na podstawie Polityki Bezpieczeństwa Danych Osobowych Zamawiającego. System musi umożliwiać wykonywanie kopii Bazy Danych wraz z całym Systemem oraz jego ustawieniami konfiguracyjnymi raz dziennie w godzinach nocnych. Utworzona kopia musi być automatycznie zapisywana na platformie serwerowej Systemu.

W momencie instalacji Systemu należy zdefiniować okres przechowywania codziennych backupów, który musi zostać ustalony w trakcie analizy przedwdrożeniowej z Zamawiającym. Backup'y muszą być przechowywanie przez okres minimum jednego miesiąca od ich wykonania.

2.3. Strefy wejścia

W zakres modernizacji strefy wejścia i wyjścia na potrzeby Systemu biletowego, wchodzi konserwacja istniejących bramofurt (łącznie 32 sztuki – 15 typu GASTOP BR3-2-S, 1 typu GASTOP BR3-1-S, 1 typu GASTOP BR3-1-I [dla niepełnosprawnych]) oraz montaż i podłączenie 25 zestawów składających się z nowych czytników biletów wraz z wymaganym uzbrojeniem w elementy systemu biletowego (wymagane okablowanie, kolumny sygnalizacyjne, głośniki akustyczne).

Każdy tor wejściowy kołowrotu wysokiego musi zostać wyposażony w zestaw składający się z 1 czytnika biletów, spełniającego wymagania opisane w pkt. 1.1.4 Czytniki biletów, 1 kolumny sygnalizacyjnej oraz 1 głośnika akustycznego.

Każdy tor wejściowy (łącznie 26 [25 wymienionych powyżej oraz 1 bramofurta dla niepełnosprawnych]) musi zostać poddany serwisowi z pełną konserwacją i wymianą zużytych elementów, na które składają się przede wszystkim:

- regulacja i konserwacja sprzęgieł oraz urządzeń sterujących zwolnieniem rygla i elektromagnesu, by czas pomiędzy fizycznym odbiciem biletu wstępu (zaakceptowanym przez system) a umożliwieniem wejścia przez kibica przez kołowrót (przez co rozumie się zwolnienie elektromagnesu) nie był dłuższy niż 2 sekundy,

- wymiana łożysk stóp rotora na nowe (w przypadku konieczności),

- wymiana sterownika elektronicznego (w przypadku konieczności),

- demontaż dwumonitorowych wyświetlaczy do zastosowania zewnętrznych aktualnie zainstalowanych przy wejściach,

- demontaż starych czytników biletów w ilości 31 sztuk,

- w przypadku pozostałych 6 bramofurt wyjściowych: regulacja i konserwacja sprzęgieł oraz urządzeń sterujących zwolnieniem rygla i elektromagnesu, by czas pomiędzy fizycznym użyciem przycisku zwalniającego a umożliwieniem wyjścia kibicowi na zewnątrz obiektu przez kołowrót (przez co rozumie się zwolnienie elektromagnesu) nie był dłuższy niż 2 sekundy.

Wykonawca po demontażu wszystkich starych urządzeń, których dotyczy wymiana na nowe (zainstalowanych na obiekcie przed pracami) podzieli je na uszkodzone (niemożliwe do poddania naprawie), możliwe do poddania regeneracji (celem doprowadzenia ich do stanu używalności w przyszłości) oraz do ponownego użycia (które będą stanowiły części zapasowe w razie awarii). Posegregowane urządzenia Wykonawca złoży w magazynie wskazanym przez Zamawiającego (na terenie modernizowanego obiektu).

1.1.4. Czytniki biletów

Czytniki biletów (łącznie 25 sztuk) muszą być zintegrowane z Systemem biletowym. Komunikacja pomiędzy czytnikiem biletowym a Systemem musi się odbywać poprzez interfejs ETH oraz protokół komunikacyjny.

Czytniki należy zamontować na panelu bocznym istniejących kołowrotów firmy GASTOP, aby uniemożliwić wejście przez kołowrót osobom postronnym w momencie odczytu biletu przez Klienta/Kibica.

Czytniki biletów muszą weryfikować poprawność biletu, rozpoznawać bilety zniżkowe oraz sterować kołowrotem oraz kolumną sygnalizacyjną i odbierać sygnał zwrotny z kołowrotu umożliwiający zaliczenie biletu na podstawie faktycznego przejścia osoby.

Czytniki biletów muszą umożliwiać co najmniej następujących rodzajów dokumentów wejściowych i znaczników elektronicznych:

- kart zbliżeniowych RFID w standardzie MIFARE: ISO14443 A,
- biletów papierowych i plastikowych z kodem kreskowym 1D i 2D,
- biletów papierowych z elementem RFID (MIFARE),
- biletów w systemie print@Home,
- urządzeń mobilnych na podstawie odczytu kodu QR Code.

Czytniki biletów muszą posiadać pamięć wewnętrzną. Wymagana wielkość bufora dla min. 100 000 rekordów uprawnionych Dokumentów Wejściowych.

Czytnik biletów musi mieć możliwość pracy w trybie off-line – sterowanie kołowrotem na podstawie odpowiedzi z Systemu zarządzającego lub po porównaniu z wewnętrzną bazą danych.

Po przywróceniu pracy Systemu do trybu on-line, czytniki muszą umożliwiać uaktualnienie w serwerze zarządzającym Systemu danych zbuforowanych w czytniku podczas pracy w trybie off-line.

Wszystkie czytniki biletów muszą być wyposażone w kolorowy wyświetlacz graficzny odporny na warunki atmosferyczne na którym będą wyświetlane informacje tekstowe i graficzne dla Kibiców/Odwiedzających.

Czytniki muszą odczytywać i sygnalizować wszystkie rodzaje biletów oraz sterować kołowrotem i odbierać sygnał zwrotny z kołowrotu umożliwiając zaliczenie biletu na podstawie faktycznego przejścia osoby.

Czytniki muszą być przystosowane do pracy całorocznej na wolnym powietrzu. Muszą być odporne na akty wandalizmu (wytrzymała obudowa).

1.1.5. Kolumny sygnalizacyjne

Kolumny sygnalizacyjne (łącznie 25 sztuk) powinny być wykonane jako trójkolorowe sygnalizatory świetlne i montowane po stronie wewnętrznej stadionu. Kolumny muszą sygnalizować status biletu kibica, np. kolor czerwony – odmowa dostępu, kolor zielony – wstęp, kolor pomarańczowy – gotowość, kolor zielono-pomarańczowy – bilet zniżkowy.

1.1.6. Głośniki akustyczne

Głośniki akustyczne należy montować w obrębie kołowrotu wysokiego w ilości 25 sztuk.

2.3.1. Terminale mobilne

System musi umożliwiać kontrolę biletów przy Punktach Kontrolnych za pomocą 6 sztuk terminali mobilnych.

Terminale mobilne będą mogły pracować przy wszystkich strefach wejściowych. Terminale mobilne muszą być wyposażone minimum w czytnik kodów 1D, 2D i chipów RFID w standardzie MIFARE, skaner dokumentów tożsamości (OCR) .

2.4. Stanowiska kasowe

Na obiekcie sprzedaż Dokumentów Wejściowych jest prowadzona na 12 Stanowiskach Kasowych. W ramach modernizacji Zamawiający zmodernizuje następujące wyposażenie:

- 11 szt. laptopów wraz z myszką przewodową,
- 2 szt. stołowych czytników kart RFID,
- 10 szt. drukarek fiskalnych z kopią elektroniczną wraz z szufladą kasową.

Wykonawca zainstaluje i skonfiguruje sprzęt w miejscach wskazanych przez Zamawiającego.

Pojedyncze Stanowisko Kasowe będzie umożliwiać co najmniej:

- zbieranie danych osobowych Klientów/Kibiców i weryfikowanie tożsamości,
- przyjmowanie elektronicznych wniosków o Imienną Kartę Klienta/Kibica i płatności za nie,
- sprzedaż dokumentów wejściowych (biletów jednorazowych i karnetów),
- fiskalizację transakcji,
- drukowanie biletów wstępu z rezerwacji internetowych,
- drukowanie i wydawanie Imiennych Kart Klienta/Kibica,
- rozpatrywanie reklamacji z nieudanego wejścia kibica na obiekt.

- przyjmowanie elektronicznych wniosków i płatności za wydanie Karty Kibica,
- wyrabianie i drukowanie Kart Kibica,
- wydawanie lub wysyłanie Kart Kibica,
- sprzedaż biletów jednorazowych i karnetów,
- pobieranie danych osobowych kibiców, VIP-ów, obsługi technicznej,
- wydawanie kart VIP-owskich, zaproszeń, wejściówek technicznych,
- automatyczna wymiana voucherów na właściwe bilety wstępu,
- drukowanie biletów wstępu z rezerwacji internetowych,
- fiskalizacja transakcji,
- udostępnianie informacji o obiekcie, imprezach, kalendarzu imprez,
- rozpatrywanie reklamacji z nieudanego wejścia kibica na obiekt.

Laptop powinien posiadać następujące parametry minimalne:

- monitor: ekran minimum 15" jakości co najmniej HD, matowy, LED, TN,
- system operacyjny min. Windows 10 lub nowszy, w wersji PROFESSIONAL,
- pamięć RAM minimum. 8 GB DDR4,
- pojemność dysku min. 500 GB,
- procesor minimum Intel Core i5 lub AMD Ryzen 5,
- wbudowane porty: minimum 7 x USB (dopuszcza się możliwość zainstalowania rozgałęźników [koncentratorów sieciowych], minimum 1 x HDMI,
- minimum karta sieciowa i karta graficzna wbudowane,
- karta bezprzewodowa IEEE 802.11a/b/g/n,
- przewodowa mysz USB z dwoma klawiszami oraz rolką (scroll),
- dołączone nośniki ze sterownikami,
- dźwięk: zintegrowana karta dźwiękowa, wbudowane głośniki, wbudowany mikrofon,
- wbudowana kamera internetowa,
- zasilacz.

Stołowy czytnik kart RFID o następujących parametrach minimalnych:

- czytnik nabiurkowy, przeznaczony do zastosowań w punkcie kasowym, odczyt dokumentów wejściowych z chipem RFID w standardzie MIFARE (ISO14443 A+B),
- wyposażony w interfejs USB (zasilanie i transmisja),
- zasięg odczytu do 7 cm,
- częstotliwość pracy 13,56 MHz,
- musi umożliwiać programowanie mediów identyfikujących z elementami RFID.

Drukarka fiskalna z kopią elektroniczną o następujących parametrach minimalnych:

- bardzo szybki wydruk (ponad 20 linii na sekundę),

- wyświetlacz LCD,
- możliwość wprowadzania różnych stawek podatkowych,
- możliwość wprowadzenia towarów zawierających dużą liczbę znaków,
- możliwość sterowania szufladą,
- wyposażona w zasilanie awaryjne,
- kopia elektroniczna.

2.5. Organizacja wejścia na obiekt

System musi wspierać procesy wejścia na obiekt wg następujących reguł:

- **Obsługa kibiców**

Posiadacz konkretnego Dokumentu Wejściowego (biletu, Karty Klienta/Kibica) tylko raz w ciągu całej imprezy będzie mógł przekroczyć kołowrót wejściowy. Próba kolejnego wejścia do obiektu z wejściówką o tym samym numerze musi być zarejestrowana jako próba nieuprawnionego wejścia, zasygnalizowana odpowiednimi komunikatami świetlnymi i tekstowymi na wyświetlaczu czytnika biletów.

- **Obsługa nieletnich**

System musi wspierać wszystkie procesy związane z zakupem i kontrolą dostępu osób nieletnich, zgodnie ustawą o BIM.

- **Obsługa kibiców gości**

System musi pozwalać na obsługę wejścia kibiców gości z wykorzystaniem zarówno czytników stacjonarnych jak i terminali mobilnych (czytników mobilnych z zainstalowaną Aplikacją Mobilną Systemu). Terminale mobilne muszą pozwalać na automatyczną weryfikację uprawnień wejściowych kibiców gości na podstawie ich dokumentów tożsamości.

- **Obsługa obcokrajowców oraz innych osób nieposiadających numeru PESEL**

System musi umożliwiać wydawanie karty lub sprzedaż biletów na podstawie innego dokumentu tożsamości przedstawionego przez osobę nieposiadającą numer PESEL.

W tym celu osoba taka musi przedłożyć ważny dokument jednoznacznie określający jego tożsamość, posiadający unikatowy numer seryjny.

- **Obsługa kibiców niepełnosprawnych oraz VIP**

W celu obsługi kibiców niepełnosprawnych oraz klientów VIP System musi oferować możliwość kontroli biletów z użyciem terminali mobilnych (palmtopów) z czytnikiem kodów kreskowych (1D i 2D) oraz kart zbliżeniowych MIFARE. Na terminalach mobilnych musi zostać zainstalowana Aplikacja Mobilna Systemu. Pracownik ochrony odpowiedzialny za obsługę ruchu osobowego będzie weryfikował bilety tych kibiców przykładając bilet lub kartę do terminala.

Poprawna weryfikacja musi wyświetlić danych kibica na ekranie terminala, wraz z odpowiednim komunikatem wskazującym ważność biletu oraz sektor i miejsce na obiekcie.

Terminal Mobilny terminal (palmtop) musi łączyć z Systemem za pośrednictwem WiFi lub sieci GSM (LTE).

- **Zakazy stadionowe i klubowe**

System musi umożliwiać wprowadzanie przez administratora zakazów stadionowych i klubowych oraz zarządzanie nimi, wprowadzanie terminów obowiązywania zakazów dla poszczególnych kibiców, blokadę sprzedaży biletu osobie z aktualnym zakazem stadionowym.

2.6. Prawa autorskie

1. W ramach określonego wynagrodzenia Wykonawca przenosi na Zamawiającego majątkowe prawa autorskie powstałe w związku z wykonywaniem przez niego przedmiotu umowy (w tym zwłaszcza wykonane przez Wykonawcę zdjęcia, schematy oraz inne opracowania), bez ograniczania co do miejsca i czasu korzystania w szczególności na następujących polach eksploatacji:
   - w zakresie utrwalania i powielania dzieła, jego części albo fragmentów wszelkimi znanymi technikami, w tym cyfrowymi, elektronicznymi, wszelkimi technikami video, technikami poligraficznymi,
   - rozpowszechniania poprzez udostępnianie publiczne egzemplarzy całości lub części dzieła, w tym w postaci papierowej, jak i poprzez wprowadzenie do sieci teleinformatycznej, telekomunikacyjnej, komputerowej, w tym do sieci Internet, oraz do innych sieci,
   - wprowadzania do pamięci komputera lub innego urządzenia elektronicznego,
   - udostępnienie dzieła w całości lub w części na stronie internetowej Zamawiającego w sposób umożliwiający dowolne wykorzystywanie i nieograniczone zwielokrotnianie wyników przedmiotu zamówienia przez każdego z użytkowników sieci publicznej w miejscu i czasie przez niego wybranym,
   - w zakresie przekazywania dzieła przez Zamawiającego podmiotom trzecim, korzystającym z jego usług w zakresie wskazanym przez Zamawiającego,
2. Przeniesienie autorskich praw majątkowych nie dotyczy systemu informatycznego (biletowego). System biletowy będzie udostępniony Zamawiającemu na zasadzie bezterminowej licencji do oprogramowania.
3. Wykonawca wyraża zgodę na dokonanie zmian lub opracowań dzieła polegających na przystosowaniu, przetworzeniu, tłumaczeniu, zmianie układu lub jakichkolwiek innych zmian w dziele z zachowaniem przez Zamawiającego praw do tych zmian.
4. Wykonawca wyraża zgodę na przeniesienie lub udzielenie licencji na oprogramowanie przez Zamawiającego na rzecz podmiotów trzecich w zakresie jaki przysługuje Zamawiającemu, z prawem dalszego przenoszenia lub udzielania licencji.
5. Wykonawca zobowiązuje się nie rejestrować w szczególności jako znaków towarowych, w imieniu własnym lub na rzecz innych podmiotów, dzieła lub elementów stanowiących elementy przedmiotu umowy.
6. W przypadku wystąpienia przez osobę trzecią przeciwko Zamawiającemu, jego następcom prawnym lub kontrahentom, w tym także przeciwko licencjobiorcom lub innym podmiotom korzystającym z dzieła, z roszczeniami wynikającymi lub związanymi z naruszeniem jakichkolwiek przysługujących mu praw własności intelektualnej do dzieła lub związanych z jego wykorzystaniem, Wykonawca zobowiązuje się do ich zaspokojenia i zwolnienia Zamawiającego, jego następców prawnych lub kontrahentów od obowiązku wszelkich świadczeń z tego tytułu.
7. W przypadku dochodzenia na drodze sądowej przez osoby trzecie roszczeń w zakresie praw przysługujących Zamawiającemu na podstawie niniejszej umowy przeciwko Zamawiającemu, jego następcom prawnym lub kontrahentom, w tym także licencjobiorcom lub innym podmiotom korzystającym z dzieła, Wykonawca zobowiązuje się do przystąpienia w procesie obok Zamawiającego, jego następców prawnych lub kontrahentów i podjęcia wszelkich czynności w celu ich zwolnienia od udziału w sprawie. Wykonawca zobowiązuje się w szczególności do dostarczenia Zamawiającemu, jego następcom prawnym lub kontrahentom informacji, dokumentów, nośników i innych środków umożliwiających obronę.

8. W przypadku określonym w pkt 6 lub 7 powyżej, Wykonawca zobowiązuje się do poniesienia kosztów postępowań, w szczególności kosztów sądowych, kosztów związanych z mediacją, arbitrażem, negocjacjami lub innymi pozasądowymi sposobami rozwiązania sporu i kosztów udzielenia pomocy prawnej Zamawiającemu lub innym podmiotom wskazanym w pkt 5 lub 6 powyżej.
9. Wraz z przeniesieniem praw do dzieła, Wykonawca udziela Zamawiającemu, jego następcom prawnym i kontrahentom, w tym także licencjobiorcom lub innym podmiotom korzystającym z utworu, zgody na dokonywanie, rozporządzanie i korzystanie z wszelkich opracowań dzieła, a także przenosi na Zamawiającego prawo do zezwalania na korzystanie z zależnych praw autorskich do opracowań dzieła, przy czym Zamawiający będzie uprawniony do przeniesienia tej zgody na inne osoby, w tym dalszych nabywców praw do dzieła.
10. Zamawiający oraz podmioty wymienione w pkt 6 będą uprawnione do dalszego rozporządzania wszystkimi prawami autorskimi, o których mowa w niniejszej umowie i które na jej podstawie zostały nabyte.
11. Wykonawca zobowiązuje się do niewykonywania autorskich praw osobistych w zakresie utrudniającym lub uniemożliwiającym Zamawiającemu, jego następcom prawnym lub kontrahentom, w tym także licencjobiorcom lub innym podmiotom korzystającym z dzieła, wykorzystanie dzieła w całości lub części.
12. Wykonawca potwierdza, że z chwilą otrzymania wynagrodzenia, skutecznie i nieodwołalnie zobowiązuje się do niewykonywania wobec Zamawiającego, jego następców prawnych i kontrahentów autorskich praw osobistych do dzieła, w szczególności w zakresie nienaruszalności formy i treści, decydowania o udostępnieniu dzieła, nadzoru nad sposobem korzystania z dzieła itp.