

## Załącznik nr 6

### Usługi Serwisowe

Zamawiający wymaga, aby począwszy od dnia podpisania Protokołu Odbioru Systemu do dnia 31.07.2012 Wykonawca świadczył Usługi Serwisowe (usługi diagnostyczne, konfiguracyjne i obsługowe) szczegółowo opisane w umowie. Wykonywanie tych zadań musi być realizowane przez dedykowany zespół (min. 2 inżynierów obecnych jednocześnie na Stadionie Narodowym, zapewniających wsparcie obsługi Systemu w poszczególnych trybach pracy obiektu tj:

- a) Tryb administracyjny (praca biurowa, obsługa najemców) – 8:00 do 20:00,
- b) Tryb specjalny (na żądanie) – w trybie specjalnym Wykonawca zapewni obsługę serwisową na Stadionie Narodowym 24h na dobę. Powiadomienie o trybie specjalnym i czasie jego trwania nastąpi 7 dni przed planowanym terminem rozpoczęcia pracy w trybie specjalnym. Praca w trybie specjalnym zastępuje w danym dniu pracę w trybie administracyjnym. Zamawiający przewiduje prace w trybie specjalnym minimalnie przez 12 dni i nie więcej niż 20 dni.
- c) Tryb nocny w godz. 20:00- 08:00 - Podjęcie działań serwisowych w czasie 2 h od wystąpienia nieprawidłowości pracy Systemu zasygnalizowanej w trybie nadzoru zdalnego, generowanego przez System administratorowi.

Wskazane tryby dotyczą również dni ustawowo wolnych od pracy.

Ponadto w ramach usług serwisowych Wykonawca jest zobowiązany do:

1. Przygotowania raportów :

Na bieżąco:

Alarmy bezpieczeństwa

Jeżeli producenci oferowanych rozwiązań publikują na stronach WWW lub poprzez inny dostępny publicznie serwis informacje o błędach w oprogramowaniu, które mają wpływ na bezpieczeństwo proponowanego rozwiązania to Zamawiający wymaga, aby Wykonawca zainstalował poprawki nie później niż jeden dzień przed ich opublikowaniem na w/w serwisach.

Codziennie:

Raport zawierający informacje o zdarzeniach w sieci. Minimalny zestaw informacji powinien obejmować analizę informacji zawartych w syslogach wszystkich urządzeń oraz wprowadzonych zmian do sieci, restartów urządzeń w sieci, błędów w dostępie do urządzeń i zmian informacji objętych raportem inwentaryzacyjnym. Raport musi zawierać analizę i wskazanie, które z informacji w nim zawartych mogą identyfikować ewentualne problemy w sieci oraz sposoby ich rozwiązania.

Raz na miesiąc:

Profil sieci- raport wysokiego poziomu zawierający ogólne informacje o stanie sieci (minimalny zakres to raport o stanie alarmów, oprogramowania, sprzętu, topologii, technologii użytych w sieci).

Analiza syslogu - raport identyfikujący źle pracujące urządzenia i oprogramowanie. Raport musi umożliwić rozwiązywanie problemów zanim wystąpi problem ograniczający funkcjonalności sieci. Raport musi zawierać dyspozycje wykonania określonych działań przez Wykonawcę wybranego w wyniku rozstrzygnięcia przedmiotowego przetargu.

Raport o konfiguracji – szczegółowy raport zawierający analizę konfiguracji pod kątem szczegółowych zaleceń Zamawiającego (szablonów). Zamawiający musi mieć możliwość definiowania zestawu szablonów konfiguracyjnych, które mają być weryfikowane.

2. Zapewnienie stałej komunikacji z systemem Stadionu Narodowego w okresie wykonania umowy.

Wykonawca musi zapewnić Zamawiającemu stałą łączność on-line z systemem analizy danych i zdarzeń sieci. Łączność musi być zapewniona przez dedykowany system. System musi zebrać niezbędne dane z urządzeń zainstalowanych w sieci lub odebrać komunikaty o zaistniałych zdarzeniach a następnie w bezpieczny sposób przesłać do analizy.

System ten musi zapewnić wysoki poziom bezpieczeństwa. Minimalne wymagania dla systemu przedstawia poniższa tabela.

Kluczowa cecha	Minimalne wymagania
Bezpieczny transfer danych poza sieć Zamawiającego	Szyfrowanie danych algorytmem AES-128 i 2048 bitowe szyfrowanie klucza PKI dla sesji.
Dostęp	Zainstalowany wewnętrzny system system firewall. Brak widoczności sieci z zewnątrz, OS fingerprinting i skanowanie portów Zabronione: FIN Scans, fragmentacja pakietów, ping, return-rsts oraz port unreachable
Sposoby dostępu do urządzeń sieciowych Zamawiającego	Dostęp SNMP RO Wykorzystywany do rozpoznawania urządzeń, zbierania danych inwentaryzacyjnych i wydajnościowych, zbieranie danych dla audytów. Dostęp SNMP RW Nie wymagany Dostęp za pomocą Telnet Wymagane korzystanie z usługi RADIUS lub TACACS+ lub równoważnej w celu ograniczenia dopuszczalnej listy komend

	Dostęp za pomocą SSH Wykorzystywany jako dostęp do CLI.
Bezpieczeństwo wysyłanych danych	Dane są wysyłane poza sieć Zamawiającego w ustalonym czasie w postaci zaszyfrowanej Szczególnie chronione dane, jak łańcuchy SNMP oraz zakodowane hasła muszą być usuwane z konfiguracji przed ich wysłaniem. Musi istnieć możliwość tworzenia własnych reguł decydujących, które komendy lub fragmenty konfiguracji powinny zostać zamaskowane Tylko wybrane rodzaje danych sieciowych są uprawnione do wysyłania. Domyślnie nic nie jest wysyłane.

3. Zamawiający wymaga ponadto, aby w okresie świadczenia usług serwisowych Wykonawca prowadził aktywne wsparcie dostawców innych systemów Stadionu Narodowego które zapewni wszystkie funkcjonalności aplikacji teleinformatycznych korzystających ze standardu Ethernet .