Numer sprawy: DZ.8.24.PP **Załącznik nr 2B do zaproszenia (cz.2)**

OPIS PRZEDMIOTU ZAMÓWIENIA NA ŚWIADCZENIE USŁUGI SERWISU I KONSERWACJI ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ W LABORATORIUM OCENY BEZPIECZEŃSTWA PRODUKTÓW TELEINFORMATYCZNYCH ITSEF

Przedmiotem zamówienia jest konserwacja ESZ w Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych ITSEF wymienionych w załączniku nr 1do OPZ, oraz serwis polegający na bieżącym usuwaniu wszelkich awarii i uszkodzeń w ESZ, poprzez naprawę lub wymianę uszkodzonych Urządzeń ESZ w Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych w Instytucie Łączności - PIB Warszawa, ul. Szachowa 1. Wykonawca w trakcie trwania umowy tj. w ciągu 36 miesięcy musi wykonać 3 przeglądy w odstępach 12-miesięcznych, w tym pierwszy niezwłocznie po podpisaniu umowy. Zakres czynności konserwacyjnych określa załącznik nr 2 do OPZ.

Wszystkie systemy elektronicznych zabezpieczeń w Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych ITSEF zaprojektowane i wykonane zostały zgodnie z normą PN-EN- 60839-11-1 w stopniu 3 (Grade 3).

Ogólne wymagania dla Wykonawcy usługi serwisu i konserwacji systemów SSWIN, CCTV i SKD w laboratorium ITSEF:

1. Dokumentacja ESZ Laboratorium ITSEF opatrzona jest klauzulą „zastrzeżone" zgodnie z Ustawą o ochronie informacji niejawnych (Dz.U. 2023 poz. 756).
2. W celu dostępu do dokumentacji ESZ, Wykonawca oraz pracownicy Wykonawcy, wykonujący prace konserwacyjne i naprawcze muszą spełniać wymagania zawarte w Ustawie o ochronie informacji niejawnych odpowiednie do przetwarzania tych informacji o klauzuli „Zastrzeżone"
3. Wykonawca musi oświadczyć, a na żądanie Zamawiającego każdorazowo przedstawić odpowiednie dokumenty świadczące o tym, ze zatrudnia przeszkolonych techników wyspecjalizowanych w obsłudze instalacji słaboprądowych (posiadających certyfikaty spełniające stopień zabezpieczenia (Grade 3) zgodnie z normą EN50131-1) z zakresu zintegrowanego systemu zabezpieczeń ATS Master, Zintegrowanego systemu zarządzania bezpieczeństwem ATS 8300 ALLIANCE,ATS 8600 Advisor management software do klasy Business Edition oraz Systemy CCTV IP - TruVision Navigator.
4. Wykonawca musi oświadczyć, a na żądanie Zamawiającego każdorazowo przedstawić odpowiednie dokumenty świadczące o tym, ze zatrudnia przeszkolonych techników wyspecjalizowanych w obsłudze następujących systemów i oprogramowania:
   a. System kontroli dostępu zbudowany w oparciu o urządzenia i oprogramowanie firmy Lenel.
   b. Oprogramowanie Lenel OnGuard 8.0,
   c. System sygnalizacji włamania i napadu ATS Advisor Advanced w którym rolę głównego sterownika SSWiN pełni centrala ATS4500A-IP-LM.
   d. System CCTV IP - TruVision Navigator,
   e. System operacyjny Linux,
5. Wykonawca musi oświadczyć, a na żądanie Zamawiającego każdorazowo przedstawić odpowiednie dokumenty świadczące o tym, ze zatrudnia przeszkolonych techników wyspecjalizowanych w obsłudze zintegrowanych systemów Lenel, ATS i TruVision zgodnie z licencją SWG-1450-1.
6. Wykonawca skieruje do realizacji zamówienia co najmniej jednego pracownika wpisanego na listę kwalifikowanych pracowników zabezpieczenia technicznego oraz posiadającego kurs pracownika zabezpieczenia technicznego w zakresie projektowania, instalowania i konserwacji technicznych systemów zabezpieczeń do stopni 1-4.
7. Wykonawca – w razie potrzeby zmian w systemach zabezpieczenia technicznego, na żądanie zlecającego, wystawi poświadczenia zgodności poszczególnych systemów z Rozporządzeniem

Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz.U. 2012 poz. 683).

Uwaga: Elektroniczne systemy zabezpieczeń Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych ITSEF są zintegrowane sprzętowo z istniejącym systemem sygnalizacji pożarowej (SSP) w Instytucie.

Załącznik nr 1 do OPZ

Wykaz elektronicznych systemów zabezpieczeń w Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych (ITSEF):

1. System kontroli dostępu (SKD)

System kontroli dostępu (SKD) zbudowany jest w oparciu o urządzenia i oprogramowanie firmy Lenel. Głównymi składnikami części sprzętowej systemu są:

- 13 programowalnych wejść,
- inteligentny kontroler systemowy (ISC), szyfrowana komunikacja z modułami DRI i I/O oraz serwer w standardzie AES256 (Advanced Encryption Standard) kluczem o długości 256 bitów, - 1 szt.
- czytnik kart zbliżeniowych z gniazdem dla kart SAM (Secure Access Module), komunikacja z kontrolerem przez protokół OSDP (Open Supervised Device Protocol) w wersji v2 (Secure Channel Protocol), szyfrowanie symetryczne AES128 kluczem o długości 128 bitów, - 17 szt.
- czytnik kart zbliżeniowych z gniazdem dla kart SAM wyposażony w klawiaturę, komunikacja z kontrolerem przez protokół OSDP w wersji v2, szyfrowanie symetryczne AES128 – 5 szt.
- Serwer systemu SDK - 1 szt.
- Stacja operatorska - 1 szt.

2. System SSWiN

System SSWiN typu Advisor Advanced firmy UTC F&S jest zbudowany w oparciu o centralę typu ATS4500A-IP-LM. System SSWiN spełnia wymagania stopnia zabezpieczenia Grade 3, wszystkie zastosowane urządzenia także spełniają wymagania Grade 3.

Linie alarmowe z:

- czujek przestrzennych,
- czujek magnetycznych kontaktronowych,
- przycisku napadowego,
- obwodów sabotażowych (sygnalizacja otwarcia obudowy),

Głównymi składnikami części sprzętowej systemu są:

- Centrala typu ATS4500A-IP-LM – 1 szt.,
- Manipulator LCD 2*16 znaków/16 LED – 3 szt.,
- Przycisk napadowy podwójny - 1 szt.,
- Wewnętrzny sygnalizator akustyczno-optyczny – 2 szt.,
- Zewnętrzny sygnalizator akustyczno-optyczny – 1 szt.,
- Czujka kontaktronowa – 26 szt.,
- Czujka pasywna – 14 szt.,
- Czujka dualna – 9 szt.,
- Czujka wibracyjna – 7 szt.,
- Czujka stłuczeniowa – 5 szt.
- Przycisk ewakuacyjny – 12 szt.
- Nadajnik GSM – 1 szt.

3. System wizyjny CCTV

System VSS spełnia wymagania rodziny norm PN-EN 62676 w stopniu Grade 3 dla wysokiego stopnia ryzyka. Do tych wymagań są dostosowane parametry wszystkich urządzeń. System VSS

zapewnia wizualną kontrolę nad działaniami osób przebywających na terenie laboratorium i dostarcza materiał dowodowy w przypadku zaistnienia niebezpiecznych incydentów. Kamery są rozmieszczone w taki sposób, by możliwa była dokładna obserwacja wejść i wyjść do/z pomieszczeń laboratorium oraz korytarza wewnątrz laboratorium.

Głównymi składnikami części sprzętowej systemu są:

- Rejestrator – 1 szt.,
- Kamery – 16 szt.

4. System wideo-domofonowy

Instalacja wideo-domofonowa przewidziana została jako system wspomagający komunikację z osobami nie mającymi uprawnień dostępu do laboratorium, nie posiadającymi ważnej karty dostępu.

Głównymi składnikami części sprzętowej systemu są:

- Stacja bramowa "Villa" 1.3 M, Rozdzielczość kamery: HD720P, 4 wej. i 1 wyj. alarmowe,dwa przyciski wzywowe – 2 szt.
- Stacja wewnetrzna, wielkość ekranu 7 cali, ekran dotykowy, rozdzielczość 800*480, 10/100Mbps, 8 wej. alarmowych, HIKVISION – 2 szt.
- Wideo/Audio Distributor, w zestawie zasilacz 24V DC, 8x RJ45 10M/100M LAN, HIKVISION – 1 szt.

Załącznik nr 2 do OPZ

RZECZOWY ZAKRES CZYNNOŚCI KONSERWACYJNYCH.

System	Zakres czynności konserwacyjnych
(SSWiN)- System Sygnalizacji Włamania i Napadu	Wysłuchanie uwag użytkownika dotyczących wewnętrznego systemu alarmowego. Uwzględnienie próśb i uwag użytkownika systemu, o ile są zasadne i nie wiążą się z jego modernizacją.
	Elementy wykrywające - czujki
	Sprawdzenie, czy w dozorowanym pomieszczeniu nie występują czynniki mogące wywołać fałszywe alarmy
	Sprawdzenie zasięgu działania, wykonanie próby działania, a także ewentualna korekta ustawienia kąta obserwacji czujki
	Przycisk napadowy przewodowy, bezprzewodowy i kontrolny
	Sprawdzenie skuteczności działania wszystkich przycisków poprzez kolejne naciśnięcie ich i stwierdzenie, czy jest odzwierciedlenie tej czynności w postaci alarmu dźwiękowego (akustycznego) lub optycznego w alarmowym centrum nadzoru
	Element decyzyjny - centrala alarmowa
	Sprawdzenie stabilności zamontowania centrali alarmowej oraz jej wszystkich przyłączy
	Sprawdzenie zegara centrali i porównanie z czasem rzeczywistym, w przypadku rozbieżności dokonać korekty czasu
	Wykonanie wydruku historii zdarzeń systemu, np. próby działania dla wszystkich czujek lub kopia na USB
	Urządzenia sygnalizacyjne - sygnalizatory
	Sprawdzenie poprawności działania każdego sygnalizatora akustycznego, optycznego, akustyczno-optycznego pod względem: czasu działania, źródła pobudzenia, natężenia dźwięku
	Sprawdzenie stabilności zamocowania sygnalizatora i jego podłączeń
	Urządzenia rejestrujące - mechaniczne, elektroniczne
	Sprawdzenie, czy rejestrowane są wszystkie zdarzenia zaistniałe w systemie (alarmowe, techniczne - awarie, testy}
	Sprawdzenie i ustawienie rzeczywistego czasu i daty
	Sprawdzenie stabilności podłączeń
	Zasilanie
	Pomiar napięcia zasilania pochodzącego ze źródła podstawowego (z sieci)
	Pomiar napięcia pochodzącego ze źródła rezerwowego (UPS, agregaty prądotwórcze, akumulatory
	Sprawdzenie, czy po zaniku napięcia sieciowego następuje automatyczne przełączenie na zasilanie rezerwowe
	Sprawdzenie stanu baterii akumulatorowych
	Sprawdzenie stabilności połączeń kabli zasilających
(VSS)- Video Surveillance System – Wizyjny System Dozorowy	Wysłuchanie uwag użytkownika dotyczących wewnętrznego VSS. Uwzględnienie próśb i uwag użytkownika systemu, o ile są zasadne i nie wiążą się z jego modernizacją
	Punkty kamerowe
	Sprawdzenie stabilności montażu wysięgnika oraz stabilności przymocowania do niego kamery
	Sprawdzenie ustawienia pola widzenia punktu kamerowego
	Sprawdzenie ustawienia ostrości punktu kamerowego

	Czyszczenie obiektywu kamery
	Czyszczenie obudowy kamery i wysięgnika
	Stanowiska obserwacyjne osób nadzorujących pracę systemu
	Sprawdzenie jakości obrazu przesyłanego z kamer i zobrazowanego na monitorach
	Czyszczenie monitora
	Sprawdzenie wartości napięcia zasilającego ze źródła podstawowego i rezerwowego
	Sprawdzenie poprawności zaprogramowania rejestratorów cyfrowych, przełączników
	Sprawdzenie i ustawienie poprawnego czasu i daty
	Po przeprowadzonej konserwacji wykonanie kompleksowej kontroli poprawności działania całego systemu
(SKD) – System Kontroli Dostępu	Wysłuchanie uwag użytkownika dotyczących wewnętrznego systemu SKD. Uwzględnienie próśb i uwag użytkownika systemu, o ile są zasadne i nie wiążą się z jego modernizacją.
	Sprawdzenie skuteczności obwodu antysabotażowego czytników oraz jego sygnalizacji poprzez zdjęcie obudowy
	Sprawdzenie właściwego działania czytnika
	Sprawdzenie poprawności działania mechanicznych i elektromechanicznych elementów blokujących systemu kontroli dostępu (bramki obrotowe, śluzy, szlabany elektryczne, blokady drogowe, rygle elektryczne, elektrozaczepy oraz zwory elektromagnetyczne)
	Sprawdzenie poprawności działania przycisków wyjścia awaryjnego.
	Sprawdzenie odblokowania wszystkich przejść na wypadek alarmu, pożaru itp.
	Sprawdzenie zegara systemu kontroli dostępu z czasem rzeczywistym, w przypadku rozbieżności dokonać korekty tego czasu
	Sprawdzenie automatycznego przełączania zasilania sieciowego na zasilanie awaryjne
	Sprawdzenie stabilności połączeń kabli zasilających
	Przeprowadzenie kontroli poprawności działania systemu kontroli dostępu

Do zadań oferenta należy również sprawdzenie poprawności działania integracji pomiędzy systemami SKD , SSWiN oraz VSS. (alarmowe / napadowe wygaszane systemu, blokada czytników przy zazbrajaniu strefy, rejestracja video przy odczycie karty).

W przypadku konieczności wymiany wewnętrznego, uszkodzonego elementu/modułu centrali SSWiN, SSV lub SKD Wykonawca zobowiązany jest do aktualizacji dokumentacji powykonawczej systemu.

Zakończeniem przeglądu jest raport zawierający wykaz wykonanych testów kontrolnych wraz z ewentualnymi uwagami eksploatacyjnymi.