

## B. OPIS CZĘŚCI 2 ZAMÓWIENIA

### 1. Zakres Zamówienia

Wykonawca w ramach realizacji części 2 zamówienia:

- 1) obejmie gwarancją producenta wskazane przez Zamawiającego urządzenia, licencje i oprogramowanie obecnie eksploatowane przez Straż Graniczną, przy czym gwarancja ta będzie obowiązywać od dnia przekazania Zamawiającemu zaświadczenia o wykupieniu przez Wykonawcę gwarancji producenta na ww. urządzenia. Wykonawca jest zobowiązany do dostarczenia ww. zaświadczenia producenta w terminie do 14 dni od daty zawarcia umowy w sprawie realizacji części 2 zamówienia.  
Wykaz sprzętu, który zostanie objęty gwarancją producenta zawarto w Załączniku nr 3 do niniejszego OPZ.
- 2) zapewni zaawansowane wsparcie techniczne dla Zamawiającego przy rozwiązywaniu problemów i administrowaniu systemem telekomunikacyjnym Straży Granicznej i będzie ono realizowane przez inżynierów sieciowych producenta urządzeń od dnia przekazania przez Wykonawcę zaświadczenia o wykupieniu gwarancji producenta na urządzenia, o których mowa w punkcie 1);
- 3) przeprowadzi szkolenia opisane w punkcie 4 niniejszego rozdziału OPZ (zgodnie z harmonogramem określonym w §5 ust. 6 umowy – załącznik nr 3a do SIWZ)

### 2. Gwarancja i serwis

Wykonawca jest zobowiązany objąć gwarancją producenta dostarczone urządzenia i oprogramowanie, przy czym:

- a) Wykonawca obejmie gwarancją sprzęt, oprogramowanie i licencje określone w załączniku nr 3 do niniejszego OPZ pn. „Lista urządzeń i oprogramowania, które zostaną objęte gwarancją producenta”. Zamawiający informuje, że dane o numerach seryjnych urządzeń wskazanych w załączniku nr 3 zostaną udostępnione w terminie do 3 dni od podpisania umowy.
- b) Wykonawca jest zobowiązany objąć gwarancją producenta wskazany przez Zamawiającego sprzęt przez okres 36 miesięcy licząc od dnia przekazania Zamawiającemu zaświadczenia o wykupieniu przez Wykonawcę gwarancji producenta na ww. urządzenia.
- c) Gwarancja będzie obejmować:
  - wymianę uszkodzonego sprzętu najpóźniej do końca następnego dnia roboczego licząc od dnia zgłoszenia awarii, jeżeli zgłoszenie awarii wpłynęło w dniu roboczym do godziny 12:00; wymianę uszkodzonego sprzętu najpóźniej w ciągu dwóch dni roboczych licząc od dnia zgłoszenia awarii, jeżeli zgłoszenie wpłynęło w dniu roboczym po godzinie 12:00
  - możliwość pobierania poprawek i aktualizacji oprogramowania (zarówno update jak i upgrade) oraz sygnatur dla systemów IPS przez 7 dni w tygodniu i 24 godziny na dobę, przez wszystkie dni w roku.
- d) Przez pojęcie dnia roboczego należy rozumieć dni od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy.
- e) Dla umożliwienia Zamawiającemu dokonywania zgłoszeń o awarii, Wykonawca przekaże adres poczty elektronicznej oraz numer telefonu dostępny dla Zamawiającego całodobowo. O każdej zmianie adresu poczty elektronicznej Wykonawca zobowiązany jest niezwłocznie powiadomić Zamawiającego w formie pisemnej. Powiadomienie o powyższych zmianach nie stanowi zmiany umowy wymagającej sporządzenia aneksu
- f) Wykonawca zobowiązuje się do przyjmowania od Zamawiającego awarii/zgłoszeń serwisowych przez 7 dni w tygodniu i 24 godziny na dobę, przez wszystkie dni w



roku. Reakcja na zgłoszenie i rozpoczęcie naprawy nie może być dłuższa niż 2 godziny od momentu zgłoszenia przez Zamawiającego. W ramach czasu reakcji Zamawiający wymaga potwierdzenia (telefonicznie lub pocztą elektroniczną) otrzymanego zgłoszenia na adres poczty elektronicznej z podaniem w potwierdzeniu daty i godziny przystąpienia do naprawy.

- g) Gwarancja musi być świadczona w miejscu użytkowania systemu i sprzętu.
- h) Gwarancja nie może ograniczać praw Zamawiającego do zmiany miejsca instalacji sprzętu w obrębie siedziby Zamawiającego, instalowania i wymiany w dostarczonym sprzęcie standardowych podzespołów i urządzeń, zgodnie z zasadami sztuki, przez wykwalifikowany personel Zamawiającego lub przez autoryzowanego przez producenta sprzętu inżyniera innego Wykonawcy.
- i) Wykonawca zobowiązuje się do usunięcia powstałych awarii. Wykonawca będzie pośredniczył w zgłaszaniu wszelkich problemów do Centrum Serwisowego Producenta dostarczonego sprzętu.
- j) Wykonawca zobowiązuje się przenieść na Zamawiającego wszelkie uprawnienia z tytułu gwarancji udzielonych przez producentów urządzeń będących przedmiotem umowy.
- k) W przypadku, gdy wadą objęte będą urządzenia, sprzęt teleinformatyczny posiadający nośnik pamięci (np. dysk twardy), nośnik ten zostanie wymontowany przed przekazaniem wadliwego urządzenia, sprzętu teleinformatycznego Wykonawcy do naprawy. Uszkodzone nośniki danych, w tym dyski twarde pozostają własnością Zamawiającego.
- l) Zamawiający wymaga, aby świadczenie usługi serwisowej było objęte jednym centrum obsługi zgłoszeń serwisowych. Wymagane formy zgłaszania awarii to telefon, e-mail.

### 3. Zaawansowane wsparcie techniczne

System telekomunikacyjny Straży Granicznej jest całodobowo nadzorowany przez wykwalifikowaną kadrę inżynierską Zamawiającego, która monitoruje stan pracy systemu, dokonuje planowych rekonfiguracji, nadzoruje rozbudowę oraz reaguje na awarie.

Ze względu na wielkość, duży stopień skomplikowania oraz krytyczne znaczenie systemu telekomunikacyjnego Straży Granicznej dla bezprzerwowej obsługi podróżnych przekraczających granicę oraz ochronę zewnętrznego odcinka granicy UE, niezbędne jest zaawansowane wsparcie techniczne przez okres 36 miesięcy podnoszące poziom niezawodności systemu.

W związku z powyższym, Zamawiający wymaga, aby Wykonawca zapewnił zaawansowane wsparcie techniczne w usuwaniu awarii i diagnostyce sieci Zamawiającego zbudowanej na bazie sprzętu oraz oprogramowania Cisco Systems. Dla zapewnienia powyższego wykonawca będzie dysponował co najmniej 3 inżynierami Network Consulting Engineer Cisco Advanced Services, w tym:

- 1) jednym Inżynierem producenta z certyfikatem co najmniej Cisco Certified Internetwork Expert – CCIE Routing&Switching lub równoważnym
- 2) jednym Inżynierem producenta ze stopniem certyfikacji dla bezpieczeństwa co najmniej Cisco Certified Internetwork Expert - CCIE Security lub równoważnym
- 3) jednym Inżynierem producenta z certyfikatem co najmniej Cisco Certified Internetwork Expert - CCIE Voice lub równoważnym



Zamawiający wymaga, aby inżynierowie mieli bezpośredni dostęp do wewnętrznych baz danych producenta oraz do ekspertów technicznych w celu skutecznej diagnostyki sieci oraz szybkiej reakcji na awarie, a w szczególności muszą posiadać:

- 1) bezpośredni dostęp do zasobów stanowiących własność intelektualną producenta. Zakres dostępu musi obejmować, co najmniej wewnętrzną bazę wiedzy producenta na temat konfiguracji, wewnętrzną bazę danych na temat błędów w oprogramowaniu, bazę wiedzy producenta Technical Knowledge Library;
- 2) możliwość bezpośredniej zmiany priorytetów i kolejkwania zgłoszeń serwisowych;
- 3) dostęp pozwalający na uzupełnianie i zmianę numerów seryjnych urządzeń w bazach danych producenta.

Zadaniem inżynierów wsparcia technicznego będzie między innymi:

- 1) szczegółowa analiza i pomoc w rozwiązywaniu zgłoszeń serwisowych dotyczących awarii oraz włamań do systemu;
- 2) analiza trendów zgłoszeń serwisowych w oparciu o dane zawarte w systemie producenta;
- 3) analiza błędów oraz wartości parametrów obciążenia poszczególnych elementów sieci;
- 4) przygotowywanie zaleceń konfiguracyjnych dla administratorów Straży Granicznej w celu optymalizacji pracy sieci pod względem wydajności i niezawodności;
- 5) analiza sieci pod kątem bezpieczeństwa oraz przygotowywanie zaleceń konfiguracyjnych dla administratorów Straży Granicznej w celu poprawy bezpieczeństwa sieciowego;
- 6) przeprowadzanie wewnętrznych szkoleń dla administratorów Straży Granicznej o tematyce związanej z rozwiązaniami stosowanymi w sieci Straży Granicznej. Szkolenia będą prowadzone w CWT dla wskazanej grupy inżynierów Zamawiającego;
- 7) realizacja innych zleconych przez Zamawiającego bieżących zadań projektowych i diagnostycznych systemu telekomunikacyjnego Straży Granicznej w ramach ustalonego czasu pracy.

Zamawiający wymaga by wsparcie techniczne udzielane przez inżynierów CCIE producenta odbywało się w Centralnym Węźle Telekomunikacyjnym SG (Warszawa ul. 17 Stycznia 23). Zamawiający zapewni dostęp do systemu oraz miejsce do pracy. Wsparcie prowadzone będzie od poniedziałku do piątku w godzinach od 7.00 do 18.00, z tym że Zamawiający zastrzega sobie możliwość w uzasadnionych przypadkach (np. poważna awaria lub rekonfiguracja systemu wpływająca na dostępność systemu) zmianę godzin pracy (dotyczy również weekend'ów oraz dni ustawowo wolnych od pracy).

Wsparcie będzie realizowane w wymiarze czasu łącznie 150 godzin kwartalnie, ale nie więcej niż 100 godzin miesięcznie. Zamawiający zastrzega sobie możliwość w uzasadnionych przypadkach (np. poważna awaria lub rekonfiguracja systemu wpływająca na dostępność systemu) przesunięcia części godzin miesięcznego wsparcia technicznego na miesiąc kolejny, jednak z zachowaniem zasady wymiaru czasu łącznie 150 godzin kwartalnie. Rozkład godzin w miesiącu pomiędzy poszczególnymi inżynierami wsparcia technicznego winien być dostosowany do aktualnych potrzeb Zamawiającego.

Harmonogram i zakres wsparcia określany będzie co miesiąc przed rozpoczęciem okresu rozliczeniowego przez wyznaczonego przez Zamawiającego przedstawiciela. Harmonogram może ulegać modyfikacji w ramach potrzeb Zamawiającego.

Ponadto Zamawiający zastrzega sobie prawo zmiany wyznaczonego przez Wykonawcę inżyniera w uzasadnionych przypadkach niewywiązywania się z wyznaczonych zadań.

Inżynierowie kierowani do realizacji usług wsparcia muszą:

- 1) biegle posługiwać się językiem polskim w mowie i w piśmie;
- 2) spełniać warunki Instrukcji Bezpieczeństwa Przemysłowego;

## 4. Szkolenia

W ramach realizacji części 2 zamówienia Wykonawca przeprowadzi następujące szkolenia dla pracowników Zamawiającego:

- 1) **Szkolenie dla 26 osób z zakresu Troubleshooting and Maintaining Cisco IP Networks v2.0 (TSHOOT) lub 5 dniowe szkolenie równoważne**, na którym kursanci poznają narzędzia i metodologię rozwiązywania problemów z uwzględnieniem aspektów technologicznych, jak również proceduralnych i organizacyjnych.
- 2) **Szkolenie dla 6 osób z zakresu Cisco Collaboration Solution Release 10.0 Bootcamp (CSR10BC) lub 5 dniowe szkolenie równoważne**, na którym zostaną omówione tematy:
  - omówienie serwerów Cisco z rodziny UCS C-Series na poziomie administratora rozwiązania Unified Communications
  - omówienie produktu VMware vSphere ESXi i jego instalacji w środowisku Cisco UCS pod rozwiązania Unified Communications
  - omówienie i implementacja Cisco Unified Communications Manager'a i jego funkcjonalności
  - omówienie i implementacja Cisco Unity Connection i jego funkcjonalności
  - omówienie i implementacja Cisco Unified IM and Presence i jego funkcjonalności
  - omówienie i implementacja Cisco Prime Collaboration i jego funkcjonalności
- 3) **Szkolenie dla 2 osób z zakresu Securing Networks with Cisco Firepower Next-Generation Intrusion Prevention System 3.0 (SSFIPS) lub 5 dniowe szkolenie równoważne**, na którym zostaną omówione tematy:
  - komponenty i cechy Cisco Firepower System
  - Zarządzanie Cisco Firepower Management Center
  - wdrożenie Cisco Firepower Managed Devices
  - moduł Cisco Firepower Discovery
  - moduł Access Control Policy Prerequisites
  - implementacja Access Control Policies
  - moduł File Control oraz Advanced Malware Protection
  - system nowej generacji Intrusion Prevention Systems
  - moduł Network Analysis Policies
- 4) **Szkolenie dla 3 osób w zakresie ISE Bootcamp (ISE Boot) lub 5 dniowe szkolenie równoważne**, na którym zostaną omówione tematy:
  - a. Graficzny interfejs użytkownika
  - b. Nowości w ISE 2.x
  - c. Omówienie polityk AuthC i AuthZ
  - d. Protokół 802.1x oraz EAP
  - e. Mac Authentication Bypass (MAB)
  - f. Metody wdrożenia ISE
  - g. Zasady profilowania urządzeń
  - h. Konfiguracja profilowania
  - i. Sprawdzanie stacji przed dostępem do sieci Konfiguracja modułu AnyConnect Posture Scenariusze Posture dla połączeń Wired, Wireless oraz VPN Client Provisioning
  - j. Guest Internet Access with Hotspot



- k. Self-Registered Guest Access with Sponsor Approval Sponsored Guest Access
- l. Omówienie technologii TrustSec
- m. Użycie SGT do segmentacji sieci
- n. Konfiguracja Cisco ASA z SGT
- o. Nowości w ISE 2.x
- p. Omówienie scenariuszy BYOD
- q. Device Onboarding
- r. Device Management
- s. Konfiguracja TACACS+
- t. Użycie TACACS+ do administracji urządzeniami Cisco Role-based access control  
Autoryzacja komend
- u. Integracja za pomocą pxGRID
- v. Integracja z Firepower

5) **Szkolenie dla 20 osób w zakresie Advanced Routing&Switching Bootcamp lub 5 dniowe szkolenie równoważne**, na którym zostaną omówione tematy:

- 1) Transmisja sieciowe, dane pakietowe, unicast, multicast, anycast, broadcast, usługi połączeniowe i bezpołączeniowe, topologie
- 2) Modele ISO/OSI/Internet/warstwowe, enkapsulacja, PDU, SDU
- 3) Używanie poprawnej terminologii: bity, pakiety, ramki, datagramy, segmenty
- 4) Organizacje standaryzacyjne i inne: IETF, IEEE, IANA, RIPE, dokumenty RFC
- 5) Stosy IP Windows i Linux
- 6) Wgląd w pakiety: sniffery, analizatory, tcpdump, Wireshark
- 7) Dostęp do urządzeń Cisco poprzez IPv4 oraz IPv6
- 8) Podstawy protokołów IPv4/IPv6. Wymiana informacji, routing, przełączanie.
- 9) Protokoły TCP/UDP/inne
- 10) Metody dostępu do urządzeń Cisco, CLI/GUI/inne
- 11) Kontrola lokalna i zdalna dostępu Telnet/SSH, linie terminalowe i ich parametry
- 12) Zarządzanie użytkownikami lokalnymi, no aaa new-model, lokalne AAA
- 13) Praca z urządzeniami Cisco
- 14) Protokoły AAA: RADIUS i Tacacs
- 15) Efektywne CLI: filtry, aliasy, ranges, itp.
- 16) Systemy plików IOS, protokoły wymiany TFTP/FTP/SCP. Zarządzanie oprogramowaniem.
- 17) Zarządzanie konfiguracjami, config replace, funkcjonalność archive
- 18) Podstawy kryptografii: hashe MD5/SHA, szyfrowanie, klucze symetryczne i asymetryczne
- 19) Bezpieczeństwo konfiguracji, plain text, ochrona haseł
- 20) Opisywanie interfejsów
- 21) Właściwe logowanie: ustawienia syslog, NTP, Embedded Syslog Manager (ESM)
- 22) Bezpieczniki errdisable
- 23) Wprowadzenie do architektur urządzeń sieciowych
- 24) Control / Data / Management plane, dane tranzytowe i lokalne
- 25) Ethernet i jego standardy: miedziane i optyczne, 10/100G, monitorowanie i diagnostyka, TDR
- 26) Struktura i adresacja ramek, unicast i multicast, bit U/L
- 27) Internet Protocol, adresy IPv4, IPv6, planowanie adresacji
- 28) Multicasty w L3, IPv4 i IPv6



- 29) IPv4 ARP kontra IPv6 Neighbor Discovery, funkcje ICMPv4 oraz ICMPv6
- 30) Bezstanowa konfiguracja IPv6 (SLAAC)
- 31) DHCP w IPv4 oraz IPv6
- 32) Opcje IPv4, nagłówki rozszerzeń IPv6
- 33) Praca protokołów TCP oraz UDP
- 34) Praca hosta w sieci IP, wiele interfejsów, interfejs źródłowy ruchu
- 35) Brama domyślna, redundancja bramy domyślnej, potrzeba FHRP(HSRP/GLBP/VRPP) w IPv4 and IPv6
- 36) Wpływ MTU na ruch, fragmentacja w IPv4 i IPv6, PMTUD
- 37) Znaczniki QoS w ramkach i pakietach
- 38) Podstawy troubleshootingu i diagnostyki, metodologia
- 39) Narzędzia diagnostyczne IOS oraz Open Source
- 40) Przełączanie L2 i L3
- 41) Praca przełącznika Ethernet, tablica przełączania, implementacja, skalowalność
- 42) Praca routera, tablica routingu, metryka, admin distance, AD255, routing a przełączanie L3
- 43) Wiele podsieci IP: IPv4 secondary, kilka podsieci IPv6
- 44) Tablica przełączania: podział na RIB i FIB, przełączanie CEF (Cisco Express Forwarding)
- 45) Wirtualizacja przełączania L2 i L3, co to jest VPN, taksonomia VPN
- 46) Wirtualizacja przełączania L2 (VLANy, VLAN database, zarządzanie VLANami, VTP)
- 47) Wirtualizacja przełączania L3, VRF
- 48) Łączenie L2 i L3, trunki 802.1q
- 49) Praca współczesnych przełączników: multilayer i L3, porty switched, routed, subinterfejsy
- 50) Najprostsza wymiana informacji między tablicami urządzeń, VRF-Lite
- 51) Klasyczne brydżowanie na routerze
- 52) Sztuka rysunkowej dokumentacji sieci
- 53) Brama domyślna kontra trasa domyślna
- 54) Powiązanie między L2 i L3, timery ARP / ND / MAC
- 55) Interfejsy wirtualne: null, loopback, tunnel, SVI, virtual-template, NVI
- 56) Zarządzania VRF-aware, VRF i interfejs źródłowy ruchu wysyłanego przez urządzenie
- 57) Przeskakiwanie między urządzeniami
- 58) Networkers Nightmare
- 59) Podstawy IP multicast
- 60) Filozofia przełączania multicast
- 61) Kontrola dołączania do sieci multicast: IGMP/MLD. IGMP snooping.
- 62) Routing PIM
- 63) Zarządzanie topologiami Ethernet/IP,
- 64) Topologie L1, L2, L3, inne
- 65) Zarządzanie topologią L2 poprzez STP: PVSTP, PVRSTP, MST, narzędzia STP
- 66) Architektura sieci kampusowej
- 67) Interakcja między L2 i L3 oraz FHRP
- 68) Topologie wirtualne L2, połączenia fizyczne, logiczne, kanały (PVC, SVC), NBMA
- 69) Technologie starożytne: Frame Relay, ATM
- 70) NBMA w Ethernet: private VLANs
- 71) Ścieżki równoległe: ECMP (Equal-Cost MultiPath), ECMP CEF load-sharing
- 72) Ścieżki równoległe: L2/L3 portchannel, 802.3ad/PAGP/LACP



- 73) Wykrywanie topologii poprzez MAC/ARP/CDP/LLDP, ping, traceroute, STP, itp.
- 74) Tunelowanie L2: ukrywanie tagów, QinQ, 802.1ad
- 75) Globalna i lokalna pula VLANów
- 76) Tunelowanie MAC: Provider Backbone Bridging, 802.1ah
- 77) Infrastruktura Carrier Ethernet
- 78) Tunelowanie L3: GRE, non-IP, multipoint GRE, konieczność NHRP, tunele IPv6
- 79) Ukrywanie adresacji poprzez NATv4, NATv6, ALG, kontrola routingu poprzez NAT
- 80) Generyczny mechanizm tunelowania: labelki, wprowadzenie do filozofii i aplikacji MPLS
- 81) Wirtualizacja urządzeń, urządzenia logiczne, VDC, stakowanie, VSS, extenders, moduły wyniesione
- 82) Wpływ wirtualizacji na zagadnienia projektowe
- 83) Walidacja ruchu wchodzącego: statyczna, anti-spoofing
- 84) ACLki na przełączniku L3: PACL, RAACL, VACL, implementacja
- 85) Storm control
- 86) Prosta kontrola MAC: ACLki MAC, port-security
- 87) Dynamiczna kontrola, anti-spoofing, DHCP snooping, uRPF, source guard
- 88) Walidacja ARP
- 89) Zaawansowana kontrola: 802.1x / EAP / MAB
- 90) Podstawy QoS: klasyfikacja, oznaczanie, policing, wygładzanie, WRED, QoS na routerze i przełączniku
- 91) Monitorowanie ruchu tranzytowego
- 92) Statystyki, liczniki, NetFlow
- 93) Przechwytywanie ruchu, SPAN/RSPAN/ERSPAN, VLAN filters, Embedded Packet Capture
- 94) Budowa konfiguracji Data Plane, makra, wzorce, AutoConf
- 95) Tworzenie rekomendowanego wzorca konfiguracji Data Plane
- 96) Networkers Nightmare
- 97) Podstawy technologii szyfrowania, IPSec (S2S, RA), GETVPN, SSL, Flex, MACSec, 802.3ae
- 98) Funkcje firewalli, IOS firewall
- 99) PoE i wsparcie dla telefonii IP, Voice VLAN
- 100) Bardziej zaawansowane zarządzanie, SNMP
- 101) Automatyka: KRON, EEM (Embedded Event Manager)
- 102) Bezpieczeństwo infrastruktury, kontrola otwartych usług
- 103) Control Plane Policing (CoPP)
- 104) Budowa rekomendowanej konfiguracji Control i Management plane
- 105) Narzędzia dynamiki: IP SLA, Enhanced Object Tracking (EOT)
- 106) Omijanie tablicy routingu poprzez Policy-Based Routing (PBR)
- 107) Routing statyczny nie taki statyczny: opcje 'ip route' + EOT + IP SLA + EEM
- 108) Podstawy routingu dynamicznego, trzy źródła informacji routingowej
- 109) Osiągalność (reachability) kontra topologia (topology)
- 110) Klasy protokołów routingu: Distance-Vector / Link State / Path Vector
- 111) System Autonomiczny (AS), routing wewnątrz i pomiędzy AS
- 112) Co jest złego w RIPie?
- 113) Uruchamianie routingu EIGRP, OSPF, IS-IS, BGP
- 114) Użycie komendy 'network' i jej dwie funkcje, konfiguracje AF w OSPF i EIGRP
- 115) Uwierzytelnianie sąsiadów i informacji routingowej
- 116) Głębiej w protokoły, rozgłaszanie sieci, natywne i redystrybucja





- 117) Równoległe procesy routingu, ships in the night, IPv4/IPv6 dual stack, tablice protokołów
  - 118) Kontrolowanie metryki, mechanizmy unikania pętli w protokołach routingu
  - 119) Rozgłaszanie trasy domyślnej
  - 120) Kontrolowanie topologii - segmentacja sieci, podział na regiony, obszary i systemy autonomiczne
  - 121) Znakowanie informacji routingowej, tagi, community
  - 122) Narzędzia kontroli routingu: prefix-listy, route-mapy, RPL (Route Policy Language)
  - 123) Redystrybucja informacji między protokołami. Seed metric.
  - 124) Redukcja prefiksów: sumaryzacja, agregacja, filtrowanie, routing stub (EIGRP, OSPF)
  - 125) Anycast i jego usługi
  - 126) Networkers Nightmare
  - 127) Więcej skalowalności: czego nie lubi EIGRP, BGP route-reflectors i peery dynamiczne
  - 128) Który protokół routingu jest lepszy? Potrzeba stosowania inżynierii ruchowej.
  - 129) Proces konwergencji: składowe, analiza procesu
  - 130) Przyspieszanie konwergencji, tuning protokołów, BFD (Bidirectional Forwarding Detection)
  - 131) Zarządzanie FIB: priorytetyzacja prefiksów, Prefix Independent Convergence (PIC)
  - 132) Stabilizacja informacji: dampening
  - 133) Budowa rekomendowanej konfiguracji routingu
  - 134) Fałszywe ścieżki: blackholing
  - 135) Pułapki FHRP: suboptymalny routing, pułapki agregacji prefiksów
  - 136) Celowy blackholing: RTBH (Remote Triggered BlackHoling)
  - 137) Pętle w sieci: informacji, danych, mikropętle, pętle sąsiedztwa, nieskończona rekurencja
  - 138) Budowa ścieżek z wykorzystaniem MPLS: L2VPN, L3VPN, MPLS over GRE
  - 139) Dobrze mieć ścieżkę zapasową: EIGRP feasible successor, IP LFA, BGP AddPath
  - 140) Dodatkowe narzędzia do kontroli ścieżki w BGP: AS\_PATH ACL, community lists
  - 141) Kontrola ruchu wchodzącego i wychodzącego
  - 142) Asymetria routingu, routing nieoptymalny
  - 143) Wzajemna redystrybucja, migracja protokołów routingu
  - 144) Automatyczna kontrola ścieżki z wykorzystaniem PfR (Performance Routing)
  - 145) Wiarygodne przełączanie: Stateful SwitchOver (SSO), NSF/GR, NSR
  - 146) Nie tylko Ethernet
  - 147) Topologie zaawansowane i sieci nakładkowe
  - 148) VRF a VPN, złożone VPN, wymiana informacji między VPN
  - 149) Proste sieci nakładkowe, L2TPv3, MPLS AToM
  - 150) Sieci nakładkowe NVGRE, OTV, VxLAN
  - 151) Matryce L2; FabricPath, TRILL
  - 152) Aktualne trendy: converged access, Network Function Virtualization (NFV), IoT
  - 153) Programowalność: SDN, REST API, OnePK, Cisco One, REST API
- 6) **Szkolenie dla 10 osób z zakresu Advanced Security Bootcamp lub 5 dniowe szkolenie równoważne** dla 10 osób, na którym zostaną omówione tematy:

#### **Next Generation Firewall**

- 1) architecture and overview
- 2) deployment scenarios

- 3) Clustering
- 4) failover
- 5) NAT and ACL
- 6) PBR, VRF
- 7) virtualization

### **Threat Defense**

- 1) IPS architecture
- 2) deployment scenarios
- 3) virtualization
- 4) intrusion policy
- 5) anti-malware protection
- 6) file policy
- 7) event analysis
- 8) correlation policy and compliance
- 9) endpoint protection

### **Identity Management**

- 1) 802.1x theory
- 2) trustsec framework
- 3) AAA services deployment
- 4) BYOD
- 5) MDM
- 6) guest access
- 7) administrative access
- 8) posture assessment

### **Remote access**

- 1) Virtual Private Networks
- 2) SSL VPNs
- 3) IKEv1/IKEv2
- 4) Overlay VPNs
- 5) DMVPN vs. GETVPN
- 6) FlexVPN

### **Enterprise Security**

- 1) secure proxy services
- 2) user authentication
- 3) secure mobile users
- 4) cloud proxy
- 5) security events correlation
- 6) behavioral network analysis

Wszystkie szkolenia zamówienia muszą odbyć się w Warszawie. Wykonawca zapewni materiały szkoleniowe, zakwaterowanie oraz całodobowe wyżywienie w czasie trwania szkolenia. Typ szkoleń: 4-5 dniowe, otwarte, grupa szkoleniowa nie może jednak liczyć więcej niż 8 osób. Szkolenia będą zrealizowane w autoryzowanych centrach szkoleniowych.

Terminy szkoleń muszą zostać uzgodnione z Przedstawicielem Zamawiającego i zrealizowane do końca trwania umowy.



## 5. Procedury odbioru prac

1. Każdorazowo po zakończeniu miesiąca świadczenie usługi gwarancyjnej dla posiadanego sprzętu i oprogramowania będzie potwierdzane podpisaniem przez Strony Protokołu Odbioru dla części 2 zamówienia za dany miesiąc.
2. Każdorazowo po zakończeniu miesiąca świadczenie zaawansowanego wsparcia technicznego będzie potwierdzane podpisaniem przez Strony Raportu Miesięcznego Inżyniera stanowiącego załącznik do Protokołu Odbioru dla części 2 zamówienia za dany miesiąc.
3. Każdorazowo odbiór szkolenia prowadzonego dla Zamawiającego zgodnie z zapotrzebowaniem na dany miesiąc będzie potwierdzany podpisaniem przez Strony Protokołu Odbioru Szkolenia.

## 6. Wzory formularzy

### PROTOKÓŁ ODBIORU

ZA MIESIĄC .../

na podstawie umowy nr        zawartej w  
pomiędzy Komendantem Głównym Straży Granicznej  
a firmą

Miejsce i data wystawienia protokołu:

1. (Nazwa firmy       ) oświadcza, iż Część Druga /za miesiąc        umowy

została zrealizowana. W związku z powyższym przedstawiamy do akceptacji niniejszy Protokół.

Rozliczenie godzin inżynierów sieciowych:

Lp.	Inżynier sieciowy	Ilość godzin zgodnie z umową	Ilość wykorzystanych	Pozostało godzin do
1.	Inżynier sieciowy CCIE Routing&Switching			
2.	Inżynier sieciowy CCIE Security			
3.	Inżynier sieciowy CCIE - Voice			
	Razem			

Zamawiający potwierdza wykorzystanie wsparcia technicznego zgodnie z umową.

2. Do niniejszego protokołu załączono:

Raporty Miesięczne Inżyniera ; szt. , stron

Inne załączniki

3. Zamawiający nie wnosi zastrzeżeń do realizacji umowy.

Uwagi Zamawiającego:

Podpis osoba upoważniana Zamawiającego (data, pieczęć, czytelny podpis)	Podpis osoba upoważniona Wykonawcy (data, pieczęć, czytelny podpis)



## RAPORT MIESIĘCZNY INŻYNIERA

na podstawie umowy nr        zawartej w  
 pomiędzy Komendantem Głównym Straży Granicznej  
 a firmą

Miejsce, data i czas realizacji:	CWT		
----------------------------------	-----	--	--

NR TYGODNI			
Sporządził:	Imię i nazwisko inżyniera	czytelny podpis inżyniera	

1. Podsumowanie Prac wykonanych w okresie miesiąca:
2. Kamienie milowe zrealizowane w raportowanych tygodniach:
3. Lista zadań opóźnionych w stosunku do zaplanowanych w poprzednich tygodniach (wraz z przyczynami opóźnień):
4. Lista zadań do wykonania w następnych tygodniach:

PRIORYTET	LP	ZADANIE	ODPOWIEDZIALNOŚĆ	DATA

PRIORYTET - Ważność zadania (WYSOKI, ŚREDNI, NISKI)

5. Ryzyka związane z pracami w następnych tygodniach:
6. Zasoby Straży Granicznej niezbędne do prac w następnych tygodniach:
7. Otwarte kwestie i zaległe decyzje:
8. Załączniki

Na tym raport zakończono.

Podpis osoba upoważniona Zamawiającego	Podpis osoba upoważniona Wykonawcy (data,



PROTOKÓŁ NAPRAWY URZĄDZENIA NR.....

na podstawie umowy nr ..... zawartej w .....

pomiędzy Komendantem Głównym Straży Granicznej

a firmą .....

Miejsce i czasookres naprawy urządzenia:		Od	Do
Typ urządzenia, Nr seryjny, Nr Ewidencyjny Straży Granicznej			

Rodzaj gwarancji

Sporządził:

Opis Awarii:

.....  
.....

Podjęte czynności:

.....  
.....

Opis stanu urządzenia po usunięciu awarii:

.....  
.....

Przedłużenie okresu gwarancji zgodnie z umową:

Naliczone dodatkowe dni gwarancji	(wyliczenia zgodnie z umową)
Sprawdził:	



	(czytelny podpis osoby upoważnionej SG)
--	---

Dodatkowe uwagi:

.....  
.....  
.....

Na tym raport zakończono.

Podpis osoba upoważniona Zamawiającego (data, pieczęć, czytelny podpis)	Podpis osoba upoważniona Wykonawcy (data, pieczęć, czytelny podpis)



## PROTOKÓŁ ODBIORU SZKOLENIA

na podstawie umowy nr ..... zawartej w dniu .....

pomiędzy Komendą Główną Straży Granicznej

a firmą .....

Lp.	Szkolenie	Ilość
1.		

1. .... oświadcza, iż wymienione powyżej szkolenie zostało zrealizowane w terminie:..... W związku z powyższym przedstawiamy do akceptacji niniejszy Protokół Odbioru Szkolenia.

2. Do niniejszego protokołu załączono:

- lista obecności osób ze strony Zamawiającego: szt. ...., stron .....

- skany certyfikatów osób ze strony Zamawiającego: szt..... stron .....

Uwagi Zamawiającego:

.....

.....

.....

.....

Podpis osoba upoważniona Zamawiającego (data, pieczęć, czytelny podpis)	Podpis osoba upoważniona Wykonawcy (data, pieczęć, czytelny podpis)



Załącznik nr 1 do OPZ  
(dotyczy części 1 zamówienia)

1. Wykaz urządzeń, które będą dostarczone w ramach części 1 zamówienia etap 1

Jednostka Organizacyjna	10G-SR	1000BASE-LX SM	1000BASE-SX MM	10G-LR	10G-LRM	GLC-T
Nadodrzański Oddział Straży Granicznej	0	110	0	0	0	0
Bieszczadzki Oddział Straży Granicznej	0	63	7	20	25	41
Karpacki Oddział Straży Granicznej	0	18	38	0	1	2
Komenda Główna Straży Granicznej	0	0	0	0	0	0
Suma	0	112	192	3	8	22
Przełącznik 8 portowy z uplink 2xSFP	0	0	0	0	0	0
Przełącznik 24 portowy z uplink 4xSFP	0	0	0	0	0	0
Przełącznik 48 portowy z uplink 4xSFP	0	0	0	0	0	0
Przełącznik modularny 3	0	0	0	0	0	0
Przełącznik modularny 6	0	0	0	0	0	0
Zasilacz do przełącznika modularnego	0	0	0	0	0	0
karta RJ-45 do przełącznika modularnego	0	0	0	0	0	0
Karta SFP do przełącznika modularnego	0	0	0	0	0	0
Przełącznik 12 portowy z uplink 2xSFP	0	0	0	0	0	0
Przełącznik 24 portowy z uplink 2xSFP+	0	0	0	0	0	0
Przełącznik 48 portowy z uplink 2xSFP+	0	0	0	0	0	0
Przełącznik agregacyjny 32 portowy SFP+	0	0	0	0	0	0
Przełącznik agregacyjny 12 portowy SFP	0	0	0	0	0	0
Przełącznik agregacyjny 48 SFP+ 6xQSFP+	0	0	0	0	0	0
Przełącznik agregacyjny 48 RJ-45 6xQSFP+	0	0	0	0	0	0
Serwer PROXY	0	0	0	0	0	0
Firewall dla bloku CPSI	0	0	0	0	0	0
Firewall do Extranetu	0	0	0	0	0	0
Firewall do Internetu	0	0	0	0	0	0
Router do Internetu	0	0	0	0	0	0
Router do PSTN	0	0	0	0	0	0
Router dla dostępu zdalnego	0	0	0	0	0	0
Firewall do bloku APN	0	0	0	0	0	0
Firewall do MGMT	0	0	0	0	0	0
Licencje do Centralnego Systemu Uwierzytelniania Stacji Końcowych	0	0	0	0	0	0
Oprogramowanie do balansowania ruchu	0	0	0	0	0	0
Urządzenie do balansowania ruchu	0	0	0	0	0	0
Router do sieci MetroEthernet	0	0	0	0	0	0
Router do OST112	0	0	0	0	0	0
Karty do NEXUS 24 portowa 40Gbps	0	0	0	0	0	0
Centralny system zarządzania IPS	0	0	0	0	0	0

Jednostka organizacyjna	10G-SR	1000BASE-LX SM	1000BASE-SX MM	10G-LR	10G-LRM	GLC-T
Nadodrzański Oddział Straży Granicznej	0	30	220	0	0	0
Bieszczadzki Oddział Straży Granicznej	33	135	399	0	0	0
Karpacki Oddział Straży Granicznej	0	2	232	0	0	0
Komenda Główna Straży Granicznej	102	0	0	4	0	0
SUMA	135	167	851	4	0	0

2. Wykaz urządzeń które będą dostarczone w ramach części 1 zamówienia etap 2

Jednostka Organizacyjna	Przełącznik 8 portowy z uplink 2xSFP	Przełącznik 24 portowy z uplink 4xSFP	Przełącznik 48 portowy z uplink 4xSFP	Przełącznik modułarny 3	Przełącznik modułarny 6	Zasilacz do przełącznika modułarnego	karta RJ-45 do przełącznika modułarnego	Karta SFP do przełącznika modułarnego	Przełącznik 12 portowy z uplink 2xSFP	Przełącznik 24 portowy z uplink 2xSFP+	Przełącznik 48 portowy z uplink 2xSFP+	Przełącznik agregacyjny 32 portowy SFP+	Przełącznik agregacyjny 12 portowy SFP	Firewall	Przełącznik agregacyjny 48 SFP+ 6xQSFP+	Przełącznik agregacyjny 48 RJ-45 6xQSFP+	Serwer PROXY	Firewall dla bloku CPSI	Firewall do Extranetu	Firewall do Internetu	Router do Internetu	Router do PSTN	Firewall dla dostępu zdalnego	Firewall do bloku APN	Firewall do MGMT	Licencje do Centralnego Systemu Uwierzytelniania Stacji Końcowych	Oprogramowanie do balansowania ruchu	Urządzenie do balansowania ruchu	Router do sieci MetroEthernet	Router do OST112	Karty do NEXUS 24 portowa 40Gbps	Centralny system zarządzania IPS
Śląski Oddział Straży Granicznej	6	22	37	0	0	0	0	0	0	0	0	2	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Podlaski Oddział Straży Granicznej	33	21	60	3	8	22	21	16	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Ośrodek Szkoleń Specjalistycznych w Lubaniu	0	12	26	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Nadwiślański Oddział Straży Granicznej	6	21	25	0	0	0	0	0	0	5	25	4	2	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Centralny Wzrost Teleinformatyczny	4	2	2	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Centralny Ośrodek Szkolenia Straży Granicznej w Koszalinie	0	14	24	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Suma	49	92	174	3	8	22	21	16	0	5	30	12	12	4	6	6	3	1	2	2	2	2	2	2	2	1	2	2	2	2	2	2

Jednostka Organizacyjna	10G-SR	1000BASE-LX 5M	1000BASE-SX MM	10G-LR	10G-LRM	GLC-T
Śląski Oddział Straży Granicznej	0	14	232	0	0	0
Podlaski Oddział Straży Granicznej	0	164	246	0	0	0
Ośrodek Szkoleń Specjalistycznych w Lubaniu	0	4	50	0	0	0
Nadwiślański Oddział Straży Granicznej	2	182	77	38	0	0
Centralny Wzrost Teleinformatyczny	96	0	0	0	0	90
Centralny Ośrodek Szkolenia Straży Granicznej w Koszalinie	0	12	78	0	0	0
SUMA	98	376	683	38	0	90



3. Wykaz urządzeń, które będą dostarczone w ramach zamówienia objętego prawem opcji (w przypadku skorzystania przez Zamawiającego z prawa opcji)

Jednostka Organizacyjna	10G-SR	1000BASE-LX SM	1000BASE-SX MM	10G-LR	10G-LRM	GLC-T
Warmińsko-Mazurski Oddział Straży Granicznej	36	39	27	10	0	0
Morski Oddział Straży Granicznej	15	32	0	0	0	0
Nadbużański Oddział Straży Granicznej	0	48	60	33	0	0
<b>Suma</b>	<b>51</b>	<b>113</b>	<b>87</b>	<b>43</b>	<b>0</b>	<b>0</b>
Centralny system zarządzania IPS	0	0	0	0	0	0
Karty do NEXUS 24 portowa 40Gbps	0	0	0	0	0	0
Router do OST112	0	0	0	0	0	0
Router do sieci MetroEthernet	0	0	0	0	0	0
Urządzenie do balansowania ruchu	0	0	0	0	0	0
Oprogramowanie do balansowania ruchu	0	0	0	0	0	0
Licencje do Centralnego Systemu Uwierzytelniania Stacji Końcowych	0	0	0	0	0	0
Firewall do MGMT	0	0	0	0	0	0
Firewall do bloku APN	0	0	0	0	0	0
Firewall dla dostępu zdalnego	0	0	0	0	0	0
Router do PSTN	0	0	0	0	0	0
Router do Internetu	0	0	0	0	0	0
Firewall do Internetu	0	0	0	0	0	0
Firewall do Extranetu	0	0	0	0	0	0
Firewall dla bloku CPSI	0	0	0	0	0	0
Serwer PROXY	0	0	0	0	0	0
Przełącznik agregacyjny 48 RJ-45 6xQSFP+	0	0	0	0	0	0
Przełącznik agregacyjny 48 SFP+ 6xQSFP+	0	0	0	0	0	0
Firewall	0	0	0	0	0	0
Przełącznik agregacyjny 12 portowy SFP	0	0	0	0	0	0
Przełącznik agregacyjny 32 portowy SFP+	2	2	2	0	0	0
Przełącznik 48 portowy z uplink 2xSFP+	49	0	0	0	34	83
Przełącznik 24 portowy z uplink 2xSFP+	0	0	0	0	0	0
Przełącznik 12 portowy z uplink 2xSFP	0	0	0	136	0	136
Karta SFP do przełącznika modularnego	10	33	43	0	0	0
karta RJ-45 do przełącznika modularnego	27	60	87	0	0	0
Zasilacz do przełącznika modularnego	20	40	60	0	0	0
Przełącznik modularny 6	9	20	29	0	0	0
Przełącznik modularny 3	1	0	1	0	0	0
Przełącznik 48 portowy z uplink 4xSFP	39	45	78	0	162	0
Przełącznik 24 portowy z uplink 4xSFP	33	32	48	0	113	0
Przełącznik 8 portowy z uplink 2xSFP	36	15	0	0	51	0

Jednostka Organizacyjna	10G-SR	1000BASE-LX SM	1000BASE-SX MM	10G-LR	10G-LRM	GLC-T
Warmińsko – Mazurski Oddział Straży Granicznej	12	291	92	22	14	0
Morski Oddział Straży Granicznej	0	0	64	0	0	0
Nadbużański Oddział Straży Granicznej	13	64	1166	9	0	0
<b>SUMA</b>	<b>25</b>	<b>355</b>	<b>1322</b>	<b>31</b>	<b>14</b>	<b>0</b>

Adresy jednostek organizacyjnych Zamawiającego do których będą realizowane dostawy

Nazwa jednostki organizacyjnej SG	Adres
Komenda Główna Straży Granicznej w Warszawie	ul. 17 Stycznia 23, 02-148 Warszawa
Nadwiślański Oddział Straży Granicznej w Warszawie	ul. 17 Stycznia 23, 02-148 Warszawa
Centralny Ośrodek Szkolenia Straży Granicznej w Koszalinie	ul. Piłsudskiego 92, 75-902 Koszalin
Morski Oddział Straży Granicznej w Gdańsku	ul. Oliwska 35, 80-917 Gdańsk
Warmińsko-Mazurski Oddział Straży Granicznej w Kętrzynie	ul. Sikorskiego 78, 11-400 Kętrzyn
Podlaski Oddział Straży Granicznej w Białymstoku	ul. Bema 100, 15-370 Białystok
Nadbużański Oddział Straży Granicznej w Chełmie	ul. Tubakowska 2, 22-100 Chełm
Bieszczadzki Oddział Straży Granicznej w Przemyślu	ul. Mickiewicza 34, 37-700 Przemyśl
Ośrodek Szkoleń Specjalistycznych w Lubaniu	ul. Wojska Polskiego 2, 59-800 Lubań
Nadodrzański Oddział Straży Granicznej w Krośnie Odrzańskim	ul. Poprzeczna 1, 66-600 Krosno Odrzańskie
Karpacki Oddział Straży Granicznej w Nowym Sączu	ul. I Pułku Strzelców Podhalańskich 5, 33-301 Nowy Sącz
Śląski Oddział Straży Granicznej w Raciborzu	ul. Dąbrowskiego 2, 47-400 Racibórz

Dostawa nastąpi w dwóch etapach:

**etap 1** w poniższych lokalizacjach:

Nazwa jednostki organizacyjnej SG	Adres
Nadodrzański Oddział Straży Granicznej	ul. Poprzeczna 1, 66-600 Krosno Odrzańskie
Bieszczadzki Oddział Straży Granicznej	ul. Mickiewicza 34, 37-700 Przemyśl
Karpacki Oddział Straży Granicznej	ul. I Pułku Strzelców Podhalańskich 5, 33-301 Nowy Sącz
Komenda Główna Straży Granicznej w Warszawie	ul. 17 Stycznia 23, 02-148 Warszawa

**etap 2** w poniższych lokalizacjach:

Nazwa jednostki organizacyjnej SG	Adres
Śląski Oddział Straży Granicznej	ul. Dąbrowskiego 2, 47-400 Racibórz
Podlaski Oddział Straży Granicznej	ul. Bema 100, 15-370 Białystok
Ośrodek Szkoleń Specjalistycznych w Lubaniu	ul. Wojska Polskiego 2, 59-800 Lubań
Nadwiślański Oddział Straży Granicznej	ul. 17 Stycznia 23, 02-148 Warszawa
Komenda Główna Straży Granicznej w Warszawie (CWT)	ul. 17 Stycznia 23, 02-148 Warszawa
Centralny Ośrodek Szkolenia Straży Granicznej w Koszalinie	ul. Piłsudskiego 92, 75-902 Koszalin

Zamówienie objęte prawem opcji (w przypadku skorzystania przez Zamawiającego z tego prawa) będzie realizowane do poniższych lokalizacji:

Nazwa jednostki organizacyjnej SG	Adres
Warmińsko- Mazurski Oddział Straży Granicznej	ul. Sikorskiego 78, 11-400 Kętrzyn
Morski Oddział Straży Granicznej	ul. Oliwska 35, 80-917 Gdańsk
Nadbużański Oddział Straży Granicznej	ul. Trubakowska 2, 22-100 Chełm





Lista urządzeń i oprogramowania, które zostaną objęte gwarancją producenta

Nazwa	ilość	aktywne wsparcie	Wymagane wsparcie
CON-ECMU-LPPIF1KU	1	brak	36 miesięcy od odbioru
CON-ECMU-LPPIF100	5	Brak	36 miesięcy od odbioru
L-CSMR50-U-4.2-K9	1	brak	36 miesięcy od odbioru
N10-S6100	2	brak	36 miesięcy od odbioru
DS-C9148-16P-K9	2	brak	36 miesięcy od odbioru
VG224	50	brak	36 miesięcy od odbioru
DS-C9506	2	brak	36 miesięcy od odbioru
N20-B6625-1	12	brak	36 miesięcy od odbioru
N20-C6508	4	brak	36 miesięcy od odbioru
DS-C9513	2	brak	36 miesięcy od odbioru
DS-HP-8GFC-K9	4	brak	36 miesięcy od odbioru
C3945E-VSEC/K9	5	2019-06-09	36 miesięcy od odbioru
C3945-AX/K9	1	2019-06-09	36 miesięcy od odbioru
C2921-AX/K9	107	2019-06-09	36 miesięcy od odbioru
C3925-AX/K9	18	2019-06-09	36 miesięcy od odbioru
WS-C2960S-24PS-L	12	2019-06-09	36 miesięcy od odbioru
ASA5515-IPS-K9	5	2019-06-09	36 miesięcy od odbioru
N77-C7706-B23S2E	2	2019-06-09	36 miesięcy od odbioru
CISCO3945-SEC/K9	2	2019-06-09	36 miesięcy od odbioru
ASR1002X-5G-SECK9	2	2019-06-09	36 miesięcy od odbioru
ASA5585-S40P40-K9	2	2019-06-09	36 miesięcy od odbioru
WS-C3750X-12S-S	4	2019-06-09	36 miesięcy od odbioru
ISE-VM-K9=	2	2019-06-09	36 miesięcy od odbioru
L-NS-1KV-1KE=	2	2019-06-09	36 miesięcy od odbioru
CSACS-5.5-VM-K9	2	2019-06-09	36 miesięcy od odbioru
UCS-FI-6248UP-UPG	2	2019-06-09	36 miesięcy od odbioru
SMA-WMGT-3Y-S9 + SMA-WMGT-LIC=	12000	2017-12-23	36 miesięcy od odbioru
WSA-WSP-3Y-S9 + WSA-WSP-LIC + CON-TSSWP-AWSPLIC	12000	2017-12-23	36 miesięcy od odbioru
UPG-UCM1011-ENHP-A	1505	brak	36 miesięcy od odbioru
CON-ECMU-UPGUCMAP	1505	brak	36 miesięcy od odbioru
UPG-UCM1011-ENH-A	10519	brak	36 miesięcy od odbioru
CON-ECMU-UPGUCMHN	10519	brak	36 miesięcy od odbioru
UPG-UCM1011-ESS-A	2002	brak	36 miesięcy od odbioru
CON-ECMU-UPGUCMEA	2002	brak	36 miesięcy od odbioru
UPG-TP-10TO11-ROOM	7	brak	36 miesięcy od odbioru
CON-ECMU-LICTP1RO	7	brak	36 miesięcy od odbioru
UPG-UWL-11X-PRO	75	brak	36 miesięcy od odbioru
CON-ECMU-UWL11XPR	75	brak	36 miesięcy od odbioru
WBXMTSVR2-USR-K9	75	2018-07-06	36 miesięcy od odbioru
CON-ECMU-WBXMUSR9	75	2018-07-07	36 miesięcy od odbioru

.....  
(nazwa, adres, numer telefonu, nr faksu Wykonawcy)

### OFERTA NA CZĘŚĆ 1 ZAMÓWIENIA

Ja (My), niżej podpisany (i).....  
działając w imieniu i na rzecz .....

.....  
(pełna nazwa i adres siedziby Wykonawcy)

w odpowiedzi na ogłoszenie o przetargu nieograniczonym na realizację zadania pn: „**Rozbudowa systemu telekomunikacyjnego Straży Granicznej**” – numer sprawy 14/BF/BŁil/17 – składam(y) niniejszą ofertę.

- Oświadczamy, że zapoznaliśmy się z dokumentacją przetargową udostępnioną przez Zamawiającego i akceptujemy w całości jej treść (w tym wymagania Instrukcji Bezpieczeństwa Przemysłowego) oraz potwierdzamy, że zamówienie będzie zrealizowane przez nas zgodnie ze wszystkimi wymaganiami Zamawiającego określonymi w Specyfikacji Istotnych Warunków Zamówienia, zwanej dalej SIWZ.
- Oferujemy realizację zamówienia w sposób zgodny z wymaganiami Zamawiającego za łączną cenę brutto <sup>1),4)</sup> ..... zł, słownie: .....

..... zł

w tym obowiązujący podatek VAT, zgodnie z poniższą kalkulacją:

Lp.	Nazwa przedmiotu zamówienia	Zamówienie podstawowe	Zamówienie objęte prawem opcji	Cena jednostkowa brutto <sup>1),2),3)</sup> (zł)	Zamówienie podstawowe	Zamówienie objęte prawem opcji
		liczba zamawianych sztuk urządzeń	liczba zamawianych sztuk urządzeń		Cena brutto <sup>1),2)</sup> (zł) [kol. 03 x kol. 05]	Cena brutto <sup>1),2)</sup> (zł) [kol. 04 x kol. 05]
01	02	03	04	05	06	07
1.	przełącznik 8 portowy z uplink 2xSFP	49	51			
2.	przełącznik 24 portowy z uplink 4xSFP	204	113			
3.	przełącznik 48 portowy z uplink 4xSFP	366	162			
4.	przełącznik modułarny 3	6	1			
5.	przełącznik modułarny 6	16	29			
6.	zasilacz do przełącznika modułarnego	44	60			
7.	karta RJ-45 do przełącznika modułarnego	48	87			
8.	karta SFP do przełącznika modułarnego	32	43			
9.	przełącznik 12 portowy z uplink 2xSFP	15	136			
10.	przełącznik 24 portowy z uplink 2xSFP+	8	-			
11.	przełącznik 48 portowy z uplink 2xSFP+	110	83			

- Cenę brutto wpisują wyłącznie Wykonawcy krajowi. Wykonawcy spoza terytorium RP zamiast ceny brutto wpisują cenę netto potwierdzając ten fakt pisemnie w niniejszym formularzu ofertowym. W przypadku Wykonawców spoza wspólnego obszaru UE cena netto musi zawierać należne opłaty celne na warunkach DDP miejsca realizacji zamówienia, jak również inne opłaty związane z wprowadzeniem oferowanych produktów na terytorium RP. Wybór oferty Wykonawcy spoza terytorium RP będzie prowadził do powstania obowiązku podatkowego u Zamawiającego zgodnie z ustawą o podatku od towarów i usług (Dz.U. z 2011r. Nr 177 poz. 1054 z późn. zm.).
- Ceny jednostkowe podane w tabeli muszą uwzględniać wszystkie koszty realizacji zamówienia (w tym m. in. koszt oprogramowania, licencji, gwarancji, szkoleń i inne).
- Cena każdego z urządzeń objętych zamówieniem podstawowym i zamówieniem objętym prawem opcji musi być taka sama.
- Łączna cena brutto podana w punkcie 2 niniejszego formularza ofertowego musi być równa łącznej cenie brutto podanej w tabeli w wierszu 40



Lp.	Nazwa przedmiotu zamówienia	Zamówienie podstawowe	Zamówienie objęte prawem opcji	Cena jednostkowa brutto <sup>1),2),3)</sup> (zł)	Zamówienie podstawowe	Zamówienie objęte prawem opcji
		liczba zamawianych sztuk urzędzeń	liczba zamawianych sztuk urzędzeń		Cena brutto <sup>1),2)</sup> (zł) [kol. 03 x kol. 05]	Cena brutto <sup>1),2)</sup> (zł) [kol. 04 x kol. 05]
01	02	03	04	05	06	07
12.	przełącznik agregacyjny 32 portowy SFP+	23	6			
13.	przełącznik agregacyjny 12 portowy z SFP	16	-			
14.	Firewall	8	-			
15.	przełącznik agregacyjny 48 SFP+ 6xQSFP+	6	-			
16.	przełącznik agregacyjny 48 RJ-45 6xQSFP+	2	-			
17.	serwer PROXY	3	-			
18.	Firewall dla bloku CPSI	1	-			
19.	Firewall dla Extranetu	2	-			
20.	Firewall dla Internetu	2	-			
21.	Router do Internetu	2	-			
22.	Router do PSTN	2	-			
23.	Firewall dla dostępu zdalnego	2	-			
24.	Firewall dla bloku APN	2	-			
25.	Firewall dla MGMT	2	-			
26.	Licencje do Centralnego Sytemu Uwierzytelniania Stacji Końcowych	1	-			
27.	Oprogramowanie do balansowania ruchu	2	-			
28.	Urządzenie do balansowania ruchu	2	-			
29.	Router do sieci MetroEthernet	2	-			
30.	Router do OST112	2	-			
31.	Karty do NEXUS 24 portowe 40Gbps	2	-			
32.	Centralny System Zarządzania IPS	2	-			
33.	10G-SR	233	25			
34.	1000BASE-LX SM	543	355			
35.	1000BASE-SX MM	1534	1322			
36.	10G-LR	42	31			
37.	10G-LRM	-	14			
38.	GLC-T	90	0			
39.	Cena brutto <sup>1),2)</sup> (zł)				za zamówienie podstawowe	za zamówienie objęte prawem opcji
40.	Łączna cena brutto <sup>1),2),4)</sup> (zł) (łącznie za zamówienie podstawowe i opcję)					

- 1) **Cene brutto wpisują wyłącznie Wykonawcy krajowi. Wykonawcy spoza terytorium RP zamiast ceny brutto wpisują cenę netto potwierdzając ten fakt pisemnie w niniejszym formularzu ofertowym. W przypadku Wykonawców spoza wspólnego obszaru UE cena netto musi zawierać należne opłaty celne na warunkach DDP miejsca realizacji zamówienia, jak również inne opłaty związane z wprowadzeniem oferowanych produktów na terytorium RP. Wybór oferty Wykonawcy spoza terytorium RP będzie prowadził do powstania obowiązku podatkowego u Zamawiającego zgodnie z ustawą o podatku od towarów i usług (Dz.U. z 2011r. Nr 177 poz. 1054 z późn. zm.).**
- 2) Ceny jednostkowe podane w tabeli muszą uwzględniać wszystkie koszty realizacji zamówienia (w tym m. in. koszt oprogramowania, licencji, gwarancji, szkoleń i inne).
- 3) Cena każdego z urzędzeń objętych zamówieniem podstawowym i opcją musi być taka sama.
- 4) Łączna cena brutto podana w tabeli w wierszu 40 tabeli musi być równa łącznej cenie brutto podanej w punkcie 2 niniejszego formularza ofertowego;



3. Oświadczamy, że łączna cena za realizację zamówienia obejmuje wszystkie koszty związane z jego realizacją.
4. Potwierdzamy, że zamówienie zostanie przez nas zrealizowane w następujących terminach:
- 1) **zamówienie w zakresie podstawowym**
    - a) **Etap pierwszy** – w terminie do dnia **11.12.2017r.**
    - b) **Etap drugi** – w terminie do **28.09.2018r.**
  - 2) **zamówienia objęte prawem opcji** – w terminie do dnia **28.09.2018r.**
5. Potwierdzamy, że dostarczone przez nas urządzenia, oprogramowanie i licencje będą objęte przez nas ..... **miesięczną gwarancją<sup>5)</sup>**, przy czym
- gwarancja na urządzenia (oprogramowanie, licencje) dostarczone do danej jednostki organizacyjnej Straży Granicznej w ramach realizacji Etapu pierwszego zamówienia rozpocznie swój bieg od dnia podpisania przez Strony Protokołu Odbioru urządzeń (oprogramowania, licencji) dostarczonych do tej jednostki organizacyjnej;
  - gwarancja na urządzenia (oprogramowanie, licencje) dostarczone do danej jednostki organizacyjnej Straży Granicznej w ramach realizacji Etapu drugiego zamówienia rozpocznie swój bieg od dnia podpisania przez Strony Protokołu Odbioru urządzeń (oprogramowania licencji) dostarczonych do tej jednostki organizacyjnej;
  - gwarancja na urządzenia (oprogramowanie, licencje) dostarczone do danej jednostki organizacyjnej Straży Granicznej (lokalizacji) w ramach zamówienia objętego prawem opcji rozpocznie swój bieg od dnia podpisania przez Strony Protokołu Odbioru urządzeń (oprogramowania licencji) dostarczonych do tej jednostki organizacyjnej.

<sup>5)</sup> Minimalny wymagany okres gwarancji na przedmiot zamówienia wynosi 48 miesięcy licząc od daty podpisania Protokołu Odbioru urządzeń (oprogramowania, licencji) dla danej jednostki organizacyjnej

6. Zobowiązujemy się do wymiany uszkodzonego sprzętu w czasie określonym poniżej<sup>6)</sup>:

<input type="checkbox"/>	zgłoszenie awarii w dniu roboczym do godz. 12:00 – wymiana uszkodzonego sprzętu najpóźniej do końca następnego dnia roboczego licząc od dnia zgłoszenia awarii; zgłoszenie awarii w dniu roboczym po godz. 12:00 – wymiana uszkodzonego sprzętu najpóźniej w ciągu dwóch dni roboczych licząc od dnia zgłoszenia awarii
<input type="checkbox"/>	zgłoszenie awarii w dniu roboczym o dowolnej godzinie – wymiana uszkodzonego sprzętu najpóźniej do końca następnego dnia roboczego licząc od dnia zgłoszenia awarii

<sup>6)</sup> **należy wpisać znak X we właściwy kwadrat** - należy wskazać oferowany termin wymiany uszkodzonego sprzętu, wybierając **wyłącznie jedną** z pozycji wymienionych w tabeli powyżej.  
Czas wymiany uszkodzonego sprzętu dostawy stanowi jedno z kryteriów oceny ofert, o którym mowa w Rozdziale XVI pkt 1 ppkt 3) SIWZ.

7. Oświadczamy, że całość dostarczanego sprzętu, oprogramowania i licencji dostarczonych w ramach realizacji zamówienia będzie pochodzić z autoryzowanego kanału sprzedaży producentów i będzie fabrycznie nowa (nieużywana wcześniej), wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą.

8. Potwierdzamy również, że wraz z dostawą dostarczymy oświadczenie producenta o:
- wykupieniu przez Wykonawcę wymaganych przez Zamawiającego gwarancji na dostarczone urządzenia, oprogramowanie, licencje;
  - o dacie produkcji urządzeń
  - pochodzeniu całości dostarczonych urządzeń, oprogramowania, licencji
9. Oświadczamy, że powierzmy<sup>7)</sup>/nie powierzmy<sup>7)</sup> niżej wymienionym podwykonawcom wykonanie niżej wskazanych części zamówienia:

Lp.	Firma (nazwa) podwykonawcy <sup>8)</sup>	Część (zakres) zamówienia <sup>8)</sup>
1.		
2.		

<sup>7)</sup> niepotrzebne skreślić

<sup>8)</sup> naależy wypełnić wyłącznie w sytuacji, gdy Wykonawca zamierza powierzyć podwykonawcy(om/) do realizacji określoną część (zakres) zamówienia.

10. Wskazujemy poniżej numer, nazwę, zakres informacji do wykorzystania oraz datę wszczęcia odrębnego postępowania prowadzonego przez Zamawiającego, w którym złożyliśmy „JEDZ” zawierający nadal aktualne informacje do wykorzystania w niniejszym postępowaniu.<sup>9)</sup>

Numer postępowania	Nazwa postępowania	Data wszczęcia postępowania	Informacje do wykorzystania

<sup>9)</sup> naależy wypełnić wyłącznie w sytuacji, gdy Wykonawca przewiduje wykorzystanie przez Zamawiającego informacji zawartych w „JEDZ” złożonym do Zamawiającego w odrębnym postępowaniu

11. Potwierdzamy również, że wybór naszej oferty nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego<sup>10)</sup>.

<sup>10)</sup> dotyczy wyłącznie Wykonawców krajowych

12. Przyjmujemy zasady płatności określone w projekcie umowy stanowiącym Załącznik nr 3 do SIWZ.

13. Oświadczamy, że oferta zawiera<sup>7),11)</sup>/nie zawiera<sup>11)</sup> informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Informacje takie zawarte są w następujących dokumentach: .....

.....  
znajdujących się na stronach ..... oferty.

<sup>7)</sup> niepotrzebne skreślić

<sup>11)</sup> Wykonawca, który zastrzegł informacje jako stanowiące tajemnicę przedsiębiorstwa zobowiązany jest wykazać, że zastrzeżone przez niego informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji



14. Uważamy się za związanych niniejszą ofertą przez okres 60 dni licząc od dnia, w którym upływa termin składania ofert.
15. Na potwierdzenie powyższego wnieśliśmy wadium w wysokości **340.000, 00 zł** (słownie: **trzysta czterdzieści tysięcy złotych**) i jesteśmy świadomi zasad jego zwrotu lub zatrzymania przez Zamawiającego.
16. W razie wybrania naszej oferty zobowiązujemy się do podpisania umowy w miejscu i w terminie określonym przez Zamawiającego.
17. Ofertę składamy na ..... kolejno ponumerowanych stronach.
18. Załącznikami do niniejszego formularza stanowiącymi integralną część oferty są:
  - 1) .....
  - 2) .....
  - 3) .....
  - 4) .....
  - 5) .....
  - 6) .....

....., dn. ....

.....  
(podpis(y) osób uprawnionych do reprezentacji Wykonawcy)



.....  
(nazwa, adres, numer telefonu, nr faksu Wykonawcy)

## OFERTA NA CZĘŚĆ 2 ZAMÓWIENIA

Ja (My), niżej podpisany (i).....

działając w imieniu i na rzecz .....

.....  
(pełna nazwa i adres siedziby Wykonawcy)

w odpowiedzi na ogłoszenie o przetargu nieograniczonym na realizację zadania pn: „**Rozbudowa systemu telekomunikacyjnego Straży Granicznej**” – numer sprawy 14/BF/Błil/17 – składam(y) niniejszą ofertę.

1. Oświadczamy, że zapoznaliśmy się z dokumentacją przetargową udostępnioną przez Zamawiającego i akceptujemy w całości jej treść (w tym wymagania Instrukcji Bezpieczeństwa Przemysłowego) oraz potwierdzamy, że zamówienie będzie zrealizowane przez nas zgodnie ze wszystkimi wymaganiami Zamawiającego określonymi w Specyfikacji Istotnych Warunków Zamówienia, zwanej dalej SIWZ.

2. Oferujemy realizację zamówienia w sposób zgodny z wymaganiami Zamawiającego za łączną cenę brutto<sup>1)</sup> ..... zł, słownie: .....

..... zł  
plus obowiązujący podatek VAT, zgodnie z poniższą kalkulacją:

Lp.	Zakres realizacji zamówienia	Cena brutto <sup>1)</sup> (zł)
01	02	03
1.	Wsparcie techniczne i gwarancja	
2.	Szkolenia <sup>2)</sup>	
3.	Łączna cena brutto za realizację zamówienia <sup>1),3)</sup>	

1) Cenę brutto wpisują wyłącznie Wykonawcy krajowi. Wykonawcy spoza terytorium RP zamiast ceny brutto wpisują cenę netto potwierdzając ten fakt pisemnie w niniejszym formularzu ofertowym. W przypadku Wykonawców spoza wspólnego obszaru UE cena netto musi zawierać należne opłaty celne na warunkach DDP miejsca realizacji zamówienia, jak również inne opłaty związane z wprowadzeniem oferowanych produktów na terytorium RP. Wybór oferty Wykonawcy spoza terytorium RP będzie prowadził do powstania obowiązku podatkowego u Zamawiającego zgodnie z ustawą o podatku od towarów i usług (Dz.U. z 2011r. Nr 177 poz. 1054 z późn. zm.).

2) **UWAGA!** Szkolenia prowadzone w ramach przedmiotowego postępowania są zwolnione z podatku VAT zgodnie z treścią art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11.03.2004r. o podatku od towarów i usług (Dz. U. nr 54 poz. 535 ze zm.)

3) Łączna cena brutto za realizację zamówienia wskazana w wierszu 3 tabeli powyżej musi być równa odpowiednio łącznej cenie brutto wskazanej w punkcie 2 niniejszego formularza ofertowego

3. Oświadczamy, że łączna cena za realizację zamówienia obejmuje wszystkie koszty związane z jego realizacją.
4. Potwierdzamy, że będziemy realizować wsparcie techniczne dla systemu telekomunikacyjnego i świadczyć gwarancję dla wskazanych przez Zamawiającego urządzeń (licencji, oprogramowania) obecnie eksploatowanych przez Straż Graniczną **przez okres 36 miesięcy** licząc od dnia przekazania Zamawiającemu zaświadczenia o wykupieniu przez nas gwarancji producenta na urządzenia objęte serwisem gwarancyjnym.

5. Zobowiązujemy się do wymiany uszkodzonego sprzętu w czasie określonym poniżej<sup>4)</sup>:

<input type="checkbox"/>	zgłoszenie awarii w dniu roboczym do godz. 12:00 – wymiana uszkodzonego sprzętu najpóźniej do końca następnego dnia roboczego licząc od dnia zgłoszenia awarii; zgłoszenie awarii w dniu roboczym po godz. 12:00 – wymiana uszkodzonego sprzętu najpóźniej w ciągu dwóch dni roboczych licząc od dnia zgłoszenia awarii
<input type="checkbox"/>	zgłoszenie awarii w dniu roboczym o dowolnej godzinie – wymiana uszkodzonego sprzętu najpóźniej do końca następnego dnia roboczego licząc od dnia zgłoszenia awarii

4) należy wpisać znak X we właściwy kwadrat - należy wskazać oferowany termin wymiany uszkodzonego sprzętu, wybierając wyłącznie jedną z pozycji wymienionych w tabeli powyżej.  
Czas wymiany uszkodzonego sprzętu dostawy stanowi jedno z kryteriów oceny ofert, o którym mowa w Rozdziale XVI pkt 2 ppkt 2) SIWZ.

6. Oświadczamy, że przeprowadzimy szkolenia dla Administratorów sieci TI Straży Granicznej zgodnie z harmonogramem przekazany przez nas Zamawiającemu w terminie 14 dni od daty zawarcia umowy.

7. Oświadczamy, że powierzmy<sup>5)</sup>/nie powierzmy<sup>5)</sup> niżej wymienionym podwykonawcom wykonanie niżej wskazanych części zamówienia:

Lp.	Firma (nazwa) podwykonawcy <sup>6)</sup>	Część (zakres) zamówienia <sup>6)</sup>
1.		
2.		

5) niepotrzebne skreślić

6) należy wypełnić wyłącznie w sytuacji, gdy Wykonawca zamierza powierzyć podwykonawcy(om/) do realizacji określoną część (zakres) zamówienia.

8. Wskazujemy poniżej numer, nazwę, zakres informacji do wykorzystania oraz datę wszczęcia odrębnego postępowania prowadzonego przez Zamawiającego, w którym złożyliśmy „JEDZ” zawierający nadal aktualne informacje do wykorzystania w niniejszym postępowaniu:<sup>7)</sup>

Numer postępowania	Nazwa postępowania	Data wszczęcia postępowania	Informacje do wykorzystania

7) należy wypełnić wyłącznie w sytuacji, gdy Wykonawca przewiduje wykorzystanie przez Zamawiającego informacji zawartych w „JEDZ” złożonym do Zamawiającego w odrębnym postępowaniu

9. Potwierdzamy również, że wybór naszej oferty nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego<sup>8)</sup>.

8) dotyczy wyłącznie Wykonawców krajowych



10. Przyjmujemy zasady płatności określone w projekcie umowy stanowiącym Załącznik nr 3a do SIWZ.
11. Oświadczamy, że oferta zawiera<sup>5),9)</sup>/nie zawiera<sup>9)</sup> informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Informacje takie zawarte są w następujących dokumentach: .....
- .....  
znajdujących się na stronach ..... oferty.
- 5) niepotrzebne skreślić
- 9) Wykonawca, który zastrzegł informacje jako stanowiące tajemnicę przedsiębiorstwa zobowiązany jest wykazać, że zastrzeżone przez niego informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji
12. Uważamy się za związanych niniejszą ofertą przez okres 60 dni licząc od dnia, w którym upływa termin składania ofert.
13. Na potwierdzenie powyższego wnieśliśmy wadium w wysokości **79.000, 00 zł** (słownie: **siedemdziesiąt dziewięć tysięcy złotych**) i jesteśmy świadomi zasad jego zwrotu lub zatrzymania przez Zamawiającego.
14. W razie wybrania naszej oferty zobowiązujemy się do podpisania umowy w miejscu i w terminie określonym przez Zamawiającego.
15. Ofertę składamy na ..... kolejno ponumerowanych stronach.
16. Załącznikami do niniejszego formularza stanowiącymi integralną część oferty są:
- 1) .....
- 2) .....
- 3) .....
- 4) .....
- 5) .....
- 6) .....

....., dn. ....

.....  
(podpis(y) osób uprawnionych do reprezentacji Wykonawcy)



Umowa nr ...../BF/BŁiI/2017

na realizację projektu pn.:

„Rozbudowa systemu telekomunikacyjnego SG – część 1 zamówienia”

zawarta w dniu..... w Warszawie

pomiędzy:

Komendantem Głównym Straży Granicznej, z siedzibą w Warszawie przy al. Niepodległości 100, będącym podatnikiem podatku od towarów i usług, posiadającym NIP 521-29-21-032, reprezentowanym przez:

..... - Dyrektora Biura Łączności i Informatyki Komendy Głównej Straży Granicznej

oraz przy kontrasygnacie:

..... - Głównego Księgowego Komendy Głównej Straży Granicznej

..... - Zastępcy Dyrektora Biura Finansów Komendy Głównej Straży Granicznej

zwanym dalej „Zamawiającym”,

a

.....  
reprezentowanym przez:

.....  
zwanym w dalszej treści umowy „Wykonawcą”,

zwanymi dalej łącznie „Stronami”, a każdego z osobna „Stroną”.

## § 1

### Przedmiot Umowy

1. Przedmiotem niniejszej umowy jest **wykonanie części 1 zamówienia** prowadzonego pn.: „**Rozbudowa systemu telekomunikacyjnego Straży Granicznej**” zgodnie z Opiszem Przedmiotu Zamówienia (OPZ) stanowiącym załącznik nr 1 do niniejszej umowy, a w szczególności: dostawa infrastruktury sieciowej, oprogramowania oraz licencji do jednostek organizacyjnych Straży Granicznej.
2. Przedmiot zamówienia zostanie zrealizowany zgodnie z warunkami zawartymi w **OPZ (w pkt A OPZ dotyczącym realizacji części 1 zamówienia)** stanowiącym załącznik nr 1 do niniejszej umowy oraz zgodnie z ofertą Wykonawcy stanowiącą załącznik nr 2 do niniejszej umowy.

## § 2

### Terminy oraz sposób wykonania Umowy

Strony ustalają, że wykonanie przedmiotu umowy objętego zamówieniem podstawowym będzie realizowane przez Wykonawcę zgodnie ze wskazanymi poniżej terminami:

1. **Etap pierwszy** – obejmujący dostawę urządzeń sieciowych (wraz z oprogramowaniem, licencjami i gwarancją producenta) do jednostek organizacyjnych Straży Granicznej (w tym wdrożenie niektórych z dostarczonych urządzeń w Bieszczadzkiem Oddziale Straży Granicznej) oraz przeprowadzenie szkoleń z obsługi tych urządzeń – zgodnie z pkt A OPZ (w tym z treścią załączników nr 1 i 2 do OPZ) – w **terminie do 11.12.2017 r.**;
2. **Etap drugi** – obejmujący dostawę urządzeń sieciowych (wraz z oprogramowaniem, licencjami i gwarancją producenta) do jednostek organizacyjnych Straży Granicznej oraz przeprowadzenie szkoleń z obsługi tych urządzeń – zgodnie z pkt A OPZ (w tym z treścią załączników nr 1 i 2 do OPZ) – w **terminie do 28.09.2018 r.**

## § 3

### Prawo opcji

1. Zamawiający przewiduje możliwość skorzystania z prawa opcji w zakresie dostawy urządzeń sieciowych (wraz z oprogramowaniem, licencjami i gwarancją producenta) w ilościach wskazanych w załączniku nr 1 do OPZ.
2. Dostarczone urządzenia muszą spełniać wymagania zawarte w treści OPZ.
3. **Oświadczenie o skorzystaniu z prawa opcji Zamawiający przekaże Wykonawcy w formie pisemnej nie później niż do dnia 31.01. 2018 r.**

4. Wykonawca zrealizuje przedmiot zamówienia objęty prawem opcji na warunkach ogólnych określonych w niniejszej Umowie, **przy czym zamówienie objęte prawem opcji musi zostać zrealizowane do dnia 28 września 2018 roku.**
5. W przypadku niedotrzymania terminu, o którym mowa w ust. 4 Zamawiający zastrzega prawo do rezygnacji z zamówienia, o którym mowa w ust. 1.
6. Zamawiający zastrzega sobie prawo do wielokrotnego złożenia oświadczenia o skorzystaniu z prawa opcji z tym, że całkowita liczba dostarczonych w ramach opcji urządzeń nie przekroczy ilości wskazanych w załączniku nr 1 do OPZ.
7. Oświadczenie o skorzystaniu z prawa opcji zostanie złożone zgodnie ze wzorem stanowiącym załącznik nr 5 do umowy.

#### § 4

##### Reprezentacja Stron

1. Osobą odpowiedzialną za realizację Umowy po stronie Zamawiającego jest  
p. ...., tel. ...., fax ....., adres email: .....
2. Osobą odpowiedzialną za realizację Umowy po stronie Wykonawcy jest  
p. ...., tel. ...., fax ....., adres email: .....
3. Osoby, o których mowa w ust. 1 i 2 odpowiadają za wykonanie przedmiotu Umowy zgodnie z wymaganiami określonymi w Umowie oraz załącznikach do Umowy.
4. Każda ze Stron może dokonać zmian osób wskazanych w ust. 1 - 2, informując o tym pisemnie drugą Stronę, z co najmniej dwudniowym wyprzedzeniem. Powiadomienie o powyższych zmianach nie stanowi zmiany wymagającej aneksu do Umowy.

#### § 5

##### Zobowiązania i oświadczenia Wykonawcy

1. Wykonawca zobowiązuje się do realizacji przedmiotu umowy w sposób zgodny z wymaganiami Zamawiającego określonymi w OPZ.
2. Wykonawca złoży w siedzibie Zamawiającego, najpóźniej w ciągu 14 dni od daty podpisania umowy, zbiorczy Wykaz produktów (wraz z ich numerami seryjnymi) dostarczanych w ramach realizacji zamówienia (w wersji papierowej oraz elektronicznej) zgodnie ze wzorem stanowiącym załącznik nr 3 Umowy.
3. Wykonawca gwarantuje, że dostarczony przedmiot umowy, w tym oprogramowanie nie są obciążone wadami prawnymi.





4. W przypadku wystąpienia wad prawnych, Zamawiającemu przysługuje w okresie udzielonej gwarancji prawo do odstąpienia od umowy i żądania naprawienia poniesionej w związku z tym rzeczywistej szkody.

#### § 6

#### Wykonanie i odbiór przedmiotu Umowy

1. W przypadku stwierdzenia, że dostarczony przedmiot umowy jest niezgodny z wymaganiami Zamawiającego określonymi w OPZ Zamawiający sporządzi protokół rozbieżności zawierający przyczyny odmowy odbioru przedmiotu umowy.
2. Wykonawca powiadomi pisemnie Zamawiającego o gotowości do dokonania odbioru dostawy w danej jednostce organizacyjnej SG wskazanej w treści załącznika nr 1 do OPZ.
3. Procedura odbioru przedmiotu zamówienia została szczegółowo określona w OPZ.

#### § 7

#### Wynagrodzenie

1. Strony ustalają maksymalną, całkowitą wartość przedmiotu Umowy, uwzględniając prawo opcji, na kwotę brutto: ..... złotych (słownie: ..... złotych), w tym obowiązujący podatek VAT, zgodnie z formularzem ofertowym stanowiącym załącznik nr 2 Umowy.
2. W powyższej kwocie zawarta jest wartość przedmiotu Umowy w zakresie zamówienia podstawowego, o którym mowa w § 2 Umowy wynosząca brutto: ..... zł (słownie: ..... 00/100 złotych), w tym obowiązujący podatek VAT.
3. Wynagrodzenie, obejmuje wszystkie koszty związane z wykonaniem przedmiotu Umowy przez Wykonawcę.
4. Zapłata dokonana będzie przelewem na rachunek Wykonawcy wskazany w fakturze.
5. Za termin zapłaty przyjmuje się dzień obciążenia rachunku Zamawiającego.
6. Wykonawca wystawi Zamawiającemu fakturę na adres: Komenda Główna Straży Granicznej, 02-514 Warszawa, Al. Niepodległości 100, NIP 521-29-21-032.
7. W przypadku skorzystania przez Zamawiającego z prawa opcji, ceny jednostkowe poszczególnych urządzeń nie ulegną zmianie w stosunku do cen jednostkowych tych urządzeń zaoferowanych w zamówieniu podstawowym.
8. Zapłata za wykonanie przedmiotu zamówienia w danej jednostce organizacyjnej SG zostanie dokonana w terminie 30 dni od daty dostarczenia do Zamawiającego prawidłowo wystawionej faktury. Podstawę do wystawienia faktury będzie stanowił podpisany przez

strony Protokół Odbioru Końcowego dla tej jednostki organizacyjnej SG.

## §8

### Gwarancja i serwis

1. Wykonawca udziela Zamawiającemu ... miesięcznej gwarancji na wszystkie dostarczone elementy zamówienia.
2. Warunki świadczenia gwarancji zostały określone w OPZ pkt. A ppkt 3.
3. Strony zgodnie rozszerzają odpowiedzialność z tytułu rękojmi i postanawiają, że okres rękojmi upływa 14 dni po upływie okresu gwarancji.

## § 9

### Kary umowne i roszczenia odszkodowawcze

1. W przypadku niedotrzymania terminu wykonania przedmiotu umowy, o którym mowa w § 2 ust. 1 Wykonawca zapłaci za każdy rozpoczęty dzień opóźnienia realizacji karę umowną w wysokości 0,01 % wynagrodzenia brutto określonego w § 7 ust. 2.
2. W przypadku niedotrzymania terminu wykonania przedmiotu umowy, o których mowa w § 2 ust. 2 Wykonawca zapłaci za każdy rozpoczęty dzień opóźnienia karę umowną w wysokości 0,01 % wynagrodzenia brutto określonego w § 7 ust. 2.
3. W przypadku niedotrzymania terminu wymiany uszkodzonego sprzętu, o którym mowa w ofercie Wykonawcy, Wykonawca zapłaci za każde rozpoczęte 24 godziny opóźnienia karę umowną w wysokości 1000 (słownie: jeden tysiąc) złotych.
4. W przypadku odstąpienia od umowy w części lub całości z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% wartości brutto niezrealizowanego podstawowego przedmiotu umowy.
5. Strony ustalają, iż wysokość kar umownych określonych w ust. 1 – 4 nie może przekroczyć 20% wartości wynagrodzenia brutto określonego w § 7 ust. 2.
6. Wykonawca oświadcza, że wyraża zgodę na potrącenie w rozumieniu art. 498 i 499 Kodeksu cywilnego przez Zamawiającego powstałych wierzytelności w tym z tytułu kar umownych, z jakiegokolwiek należności Wykonawcy. Jednocześnie Wykonawca oświadcza, że powyższe oświadczenie nie zostało złożone pod wpływem błędu, ani nie jest obarczone jakąkolwiek wadą oświadczenia woli skutkującą jego nieważnością.
7. W przypadku nie dokonania potrącenia, o którym mowa w ust. 6, Wykonawca dokona zapłaty powstałych wierzytelności w terminie do 7 dni od dnia otrzymania od Zamawiającego noty obciążeniowej.



8. Zamawiający oświadcza, że w przypadku zaistnienia sytuacji, o których mowa w ust. 6 wystawi Wykonawcy notę w terminie 21 dni od dnia dokonania potrącenia zawierającą szczegółowe naliczenie wierzytelności, w tym z tytułu kar umownych.
9. W przypadku nie dokonania przez Wykonawcę wymiany uszkodzonego sprzętu w okresie gwarancji lub rękojmi w terminie wskazanym w OPZ, Zamawiający jest uprawniony do wymiany uszkodzonego sprzętu na koszt Wykonawcy. W takim przypadku Zamawiający nie traci praw do gwarancji i rękojmi za wady.
10. Pobranie kar umownych nie pozbawia Zamawiającego prawa dochodzenia odszkodowania na zasadach ogólnych.

## §10

### Odstąpienie od Umowy

1. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy, lub dalsze wykonywanie umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, Zamawiający może odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach. W takim przypadku Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części Umowy.
2. Zamawiający ma także prawo odstąpić od Umowy:
  - a) w terminie do 30 dni od dnia określonego w § 2 ust. 1 - w przypadku niedotrzymania terminu realizacji Etapu pierwszego zamówienia,
  - b) w terminie do 30 dni od dnia określonego w § 2 ust. 2 - w przypadku niedotrzymania terminu realizacji Etapu drugiego zamówienia,
- 2) jeżeli łączna wysokość kar umownych z tytułu realizacji niniejszej Umowy naliczonych przez Zamawiającego osiągnie 20% wartości wynagrodzenia brutto Umowy, określonego w § 7 ust. 1;
- 3) w przypadku postawienia Wykonawcy w stan likwidacji.
3. Odstąpienie od umowy jest skuteczne pod warunkiem dokonania tej czynności w formie pisemnej.

## § 11

### Siła wyższa

1. Strona nie jest odpowiedzialna za niewykonanie lub nienależyte wykonanie swoich zobowiązań z powodu zaistnienia siły wyższej, to jest, jeżeli niewykonanie zostało spowodowane wydarzeniem będącym poza jej kontrolą oraz gdy w chwili zawarcia Umowy



niemożliwe było przewidzenie zdarzenia i jego skutków, które wpłynęły na zdolność Strony do wykonania Umowy oraz gdy niemożliwe było uniknięcie samego zdarzenia lub przynajmniej jego skutków.

2. Za siłę wyższą nie uznaje się braku środków u Wykonawcy, niedotrzymania zobowiązań przez jego kontrahentów oraz braku zezwoleń niezbędnych Wykonawcy dla wykonania Umowy, wydawanych przez uprawniony do tego organ.
3. Strony zobowiązują się do wzajemnego powiadamiania się o zaistnieniu siły wyższej i dokonania stosownych ustaleń celem wyeliminowania możliwych skutków działania siły wyższej. Powiadomienia, o którym mowa w zdaniu pierwszym, należy dokonać pisemnie lub w inny dostępny sposób, niezwłocznie po fakcie wystąpienia siły wyższej, nie później jednak niż w ciągu 3 dni od chwili jej wystąpienia. Do powiadomienia należy dołączyć dowody na poparcie zaistnienia siły wyższej.
4. Strona jest zobowiązana do powiadomienia o ustaniu siły wyższej w terminie nie później niż w ciągu 3 dni od momentu ustąpienia siły wyższej.
5. Zwolnienie od odpowiedzialności nie ma zastosowania w przypadku braku zawiadomienia zarówno o zaistnieniu jak i o ustaniu okoliczności siły wyższej, jak również nie przedstawienia powiadomień, o których mowa w ust. 3 lub 4 niniejszego paragrafu.
6. W przypadku niemożności wykonania przedmiotu Umowy z powodu zaistnienia siły wyższej przez okres dłuższy niż 14 dni, Zamawiający może odstąpić od Umowy płacąc Wykonawcy za wykonaną część przedmiotu Umowy.

## § 12

### Dostęp do informacji niejawnych

1. Wykonawca zobowiązuje się do zachowania poufności wszystkich informacji, w których posiadanie wszedł w trakcie wykonywania umowy lub w związku z wykonywaną umową oraz do nie wykorzystywania ich do innych celów niż wykonywanie czynności wynikających z niniejszej umowy zgodnie z Ustawą z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (Dz.U. z 2016r. poz. 1167 ze zm.) oraz do przestrzegania Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2016 poz. 922) wraz z przepisami wykonawczymi wydanymi na ich podstawie.
2. Przekazywanie informacji niejawnych poza terytorium RP będzie realizowane zgodnie z umowami międzynarodowymi (zawartymi pomiędzy Polską, a krajem Wykonawcy) w sprawie wzajemnej ochrony informacji niejawnych.
3. Wszystkie osoby, którym Wykonawca zleci wykonanie umowy lub jej części związanej

z dostępem do informacji niejawnych, a w szczególności osoby mające dostęp do systemów, w których przetwarzane są informacje Zamawiającego lub osoby, którym Wykonawca zleca wykonanie umowy oraz jej bezpośrednią realizację na terenie SG, muszą posiadać ważne poświadczenie bezpieczeństwa lub pisemne upoważnienie do dostępu do informacji niejawnych oznaczonych klauzulą tajności zastrzeżone oraz zaświadczenie potwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych.

4. Dostęp Wykonawcy do informacji niejawnych może nastąpić wyłącznie w zakresie niezbędnym do realizacji przez niego przedmiotu Umowy.
5. W przypadku niewykonania lub nienależytego wykonywania obowiązków wynikających z ustawy o ochronie informacji niejawnych, ustawy o ochronie danych osobowych, nieprzestrzegania wymagań określonych w Instrukcji Bezpieczeństwa Przemysłowego, Zamawiający ma prawo rozwiązać umowę, a powstałe z tego faktu skutki finansowe i prawne obciążą Wykonawcę.
6. Wykonawca zobowiązuje się do przestrzegania zasad dostępu do informacji niejawnych oraz danych osobowych określonych w „Instrukcji Bezpieczeństwa Przemysłowego”, która stanowi integralną część umowy (załącznik nr 4 do niniejszej umowy).
7. Wykonawca zobowiązuje się do bezzwłocznego dostarczenia informacji dotyczących nowych podwykonawców, w tym podania ich nazwy (firmy) i siedziby oraz danych, które umożliwiają Zamawiającemu stwierdzenie, że każdy z nich posiada kwalifikacje wymagane do zachowania poufnego charakteru informacji niejawnych, do których mają dostęp lub które zostaną wytworzone w związku z wykonywaniem umowy o podwykonawstwo.

### § 13

#### Zabezpieczenie należytego wykonania umowy

1. Wykonawca wniósł zabezpieczenie należytego wykonania Umowy oraz roszczeń z tytułu udzielonej rękojmi za wady w wysokości 2 % ceny całkowitej podanej w ofercie o której mowa w §7 ust. 1, co stanowi kwotę ..... zł (słownie: ..... ) w formie zgodnej z art. 148 ust. 1 ustawy Prawo zamówień publicznych.
2. Zamawiający dokona zwrotu zabezpieczenia należytego wykonania umowy oraz roszczeń z tytułu udzielonej rękojmi za wady w następujący sposób:
  - a) 70% wartości zabezpieczenia zostanie zwrócone w terminie 30 dni od dnia wykonania zamówienia i uznania przez Zamawiającego za należyte wykonane (tj. od dnia

- zakończenia realizacji zamówienia podstawowego – potwierdzonego kompletem protokołów odbiorowych z poszczególnych jednostek organizacyjnych SG objętych zamówieniem podstawowym, a w przypadku skorzystania przez Zamawiającego z prawa opcji – od dnia zakończenia realizacji całości zamówienia (obejmującego zamówienie podstawowe i zamówienie objęte prawem opcji z którego skorzystał Zamawiający) – potwierdzonego kompletem protokołów odbiorowych z poszczególnych jednostek organizacyjnych SG objętych zamówieniem podstawowym i zamówieniem opcjonalnym,
- b) 30% wartości zabezpieczenia, zatrzymane przez Zamawiającego na zabezpieczenie roszczeń z tytułu rękojmi za wady, zostanie zwrócone nie później niż w 15 dniu po upływie okresu rękojmi za wady dla urządzeń objętych ostatnią dostawą w ramach realizacji zamówienia.
3. Strony dopuszczają możliwość potrącenia przysługujących Zamawiającemu wierzytelności z tytułu kar umownych także z zabezpieczenia określonego w ust. 1.

#### § 14

#### Postanowienia końcowe

1. W sprawach nieuregulowanych Umową mają zastosowanie obowiązujące przepisy prawa polskiego, w szczególności przepisy ustawy - Kodeks cywilny, ustawy - Prawo zamówień oraz innych, które odnoszą się do Umowy.
2. Strony zobowiązują się do rozstrzygania polubownie wszelkich sporów, mogących wyniknąć na tle wykonania Umowy. W przypadku nieosiągnięcia porozumienia spór rozstrzygać będzie sąd powszechny, właściwy dla siedziby Zamawiającego.
3. Załączniki wymienione w Umowie stanowią jej integralną część.
4. Umowę sporządzono w 4 jednobrzmiących egzemplarzach, w tym trzy egzemplarze dla Zamawiającego i jeden egzemplarz dla Wykonawcy.

Załączniki do Umowy:

Załącznik nr 1 – Opis Przedmiotu Zamówienia;

Załącznik nr 2 – Oferta Wykonawcy;

Załącznik nr 3 – Wzór wykazu produktów/usług dostarczanych w ramach realizacji zamówienia

Załącznik nr 4 – Instrukcja Bezpieczeństwa Przemysłowego

Zamawiający

Wykonawca



.....  
 (nazwa i adres Wykonawcy)

**WZÓR WYKAZU PRODUKTÓW/USŁUG DOSTARCZANYCH W RAMACH REALIZACJI ZAMÓWIENIA**

Lp.	Nazwa/opis produktu/usługi <sup>1</sup>	Nazwa Producenta	Model/typ/symbol/nr serijny	J.m. <sup>2</sup>	Liczba dostarczanych j.m.	Cena jednostkowa netto (zł)	Cena jednostkowa brutto (zł) <sup>3</sup>	Stawka VAT <sup>4</sup>	Wartość netto (zł) <sup>5</sup>	Wartość brutto (zł) <sup>3</sup>
<b>Łączna cena</b>										

<sup>1</sup> w wykazie należy wyszczególnić wszystkie elementy (produkty/usługi) realizowanego zamówienia uwzględniając przy tym m.in. dostawę i instalację sprzętu, uruchomienie systemu oraz przeprowadzenie szkolenia.

<sup>2</sup> w przypadku kompletów, należy wykazać poszczególne składniki kompletu.

<sup>3,4</sup> wypełniają wyłącznie Wykonawcy krajowi.

<sup>5</sup> wartość netto w poszczególnych pozycjach wykazu należy przedstawić jako iloczyn ceny jednostkowej netto i liczby dostarczanych jednostek miary. W przypadku Wykonawców spoza wspólnego obszaru UE cena netto musi zawierać należne opłaty celne na warunkach DDP miejsca dostawy sprzętu i inne ewentualne opłaty związane z wprowadzeniem produktu na terytorium RP.

**UWAGA**

Łączne ceny netto/brutto, podane w niniejszych wykazach, muszą odpowiadać łącznej cenie netto/brutto określonej w formularzu ofertowym.

.....  
 (miejscowość) ..... dn. .... 2017 r.  
 (data)  
 ..... (podpis upoważnionego przedstawiciela Wykonawcy)

.....  
 (nazwa i adres Wykonawcy)



**KOMENDA GŁÓWNA STRAŻY GRANICZNEJ**

***BIURO OCHRONY INFORMACJI***

**Instrukcja**  
**Bezpieczeństwa Przemysłowego**

A handwritten signature in blue ink is located in the bottom right corner of the page. The signature is stylized and appears to be a personal name.





Instrukcja Bezpieczeństwa Przemysłowego, określa szczegółowe wymagania dotyczące ochrony informacji, a w tym informacji niejawnych, danych osobowych oraz innych informacji prawnie chronionych, do których Wykonawca będzie miał dostęp w związku z wykonywaniem umowy.

Instrukcja Bezpieczeństwa została opracowana przez Biuro Ochrony Informacji KGSG na podstawie wymagań obowiązujących przepisów, w tym wymagań zawartych w ustawie z dnia 05 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2016 r. poz. 1167 z późn. zm.), w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922.) oraz przepisów wykonawczych do nich wydanych oraz instrukcjach bezpieczeństwa obowiązujących w Straży Granicznej.

Żadne odstępstwa lub poprawki do niniejszej Instrukcji Bezpieczeństwa Przemysłowego nie są dozwolone, dopóki nie zostaną zaakceptowane przez Komendanta Głównego Straży Granicznej.

1. Wykonawca, pod rygorem zerwania umowy z winy Wykonawcy i odpowiedzialności karnej za ujawnienie informacji (w tym informacji niejawnych, danych osobowych, innych informacji prawnie chronionych) udostępnionych przez Zamawiającego i inne osoby bądź wytwarzanych w trakcie realizacji umowy, zobowiązuje się do przestrzegania i stosowania przepisów i procedur właściwych do ochrony tych informacji zgonie z:
  - a) przepisami prawa obowiązującymi na terytorium Polski
    - ustawą z dnia 05 sierpnia 2010 r. o ochronie informacji niejawnych (tekst jednolity Dz. U. z 2016r. poz. 1167 z późn. zm.) zwaną dalej Ustawą,
    - ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2016r. poz. 922),oraz przepisami wykonawczymi do nich wydanymi,
  - b) umowami międzynarodowymi (pomiędzy Polską a krajem Wykonawcy) w przedmiotowej sprawie.
2. Wszystkie osoby bezpośrednio zaangażowane w realizację umowy mające mieć dostęp do informacji niejawnych oraz kierownik projektu ze strony Wykonawcy, muszą posiadać ważne:
  - a) poświadczenia bezpieczeństwa lub pisemne upoważnienie, o którym mowa w art. 21 ust. 4 ustawy o ochronie informacji niejawnych o klauzuli tajności „zastrzeżone”, wydane przez kierownika jednostki organizacyjnej Wykonawcy, jeżeli osoba nie posiada poświadczenia bezpieczeństwa;
  - b) zaświadczenie potwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych.
3. Upoważnienie, o którym mowa w pkt. 2 lit. a) powinno zawierać:
  - oznaczenie jednostki organizacyjnej,
  - datę i miejsce wydania,
  - podstawę prawną,
  - imię (imiona), nazwisko, PESEL,
  - cel wydania (np. wykonanie określonego zadania) bądź okres na jaki upoważnienie zostaje wydane (wskazanie konkretnych dat albo wydarzenia, które spowoduje utratę ważności upoważnienia np. „na czas zatrudnienia w jednostce organizacyjnej”),
  - pieczęć i podpis kierownika jednostki organizacyjnej.
4. Wykonawca przekaże do Zamawiającego kserokopie dokumentów, o których jest mowa w pkt. 2 niezwłocznie po podpisaniu umowy. Przedmiotowe kserokopie muszą być potwierdzone za zgodność z oryginałem przez upoważnioną osobę i muszą umożliwiać łatwe odczytanie ich treści i pieczęci.
5. Do przetwarzania danych osobowych, mogą być dopuszczone wyłącznie osoby Wykonawcy:
  - posiadające upoważnienie do przetwarzania danych osobowych nadane przez Zamawiającego,
  - przeszkolone przez Wykonawcę z zakresu ochrony danych osobowych.

6. Przed dostępem do danych osobowych Wykonawca zwróci się do Zamawiającego z wnioskiem o wydanie upoważnień do przetwarzania danych osobowych dla pracowników Wykonawcy wskazanych we wniosku.
7. Dostęp przedstawicieli Wykonawcy do informacji (w tym do informacji niejawnych, danych osobowych, innych informacji prawnie chronionych) może być zrealizowany tylko w zakresie niezbędnym do wykonywania przez nich powierzonej (zleconej) pracy pod warunkiem spełnienia wymagań określonych w niniejszej Instrukcji Bezpieczeństwa Przemysłowego.
8. Wykonawca w trakcie realizacji umowy oraz każdorazowo po zmianie danych i na wniosek Zamawiającego przedstawi kompletny wykaz osób realizujących umowę w imieniu Wykonawcy. Wykaz ten musi zawierać następujące dane:
  - imię, nazwisko, PESEL,
  - pełniona funkcja w ramach realizacji umowy lub wykonywane zadanie,
  - nazwę przedsiębiorcy, u którego jest zatrudniona osoba w związku z realizacją umowy,
  - informację o odbyciu szkolenia z ochrony danych osobowych,
  - informację o odbyciu szkolenia z ochrony informacji niejawnych, o którym mowa w pkt. 2 lit. b),
  - informację o posiadaniu poświadczenia bezpieczeństwa lub upoważnienia, o którym mowa w pkt. 2 lit. a),
  - informację o zapoznaniu się z Instrukcją Bezpieczeństwa Przemysłowego.

Zamawiający ma prawo do żądania innych danych osób Wykonawcy niezbędnych w ramach realizacji umowy, a w szczególności nr telefonu kontaktowego, nr dowodu osobistego oraz adresu zamieszkania.

Prawo dostępu do informacji i materiałów podlegających ochronie, mają wyłącznie osoby, które są objęte wykazem.

9. Wykonawca ma obowiązek niezwłocznego informowania Zamawiającego o wszystkich zmianach dotyczących osób wymienionych w wykazie osób realizujących umowę, a także o:
  - ogłoszeniu upadłości, likwidacji lub rozwiązania jednostki organizacyjnej Wykonawcy albo zakończeniu przez nią działalności w innej formie,
  - potrzebie zawarcia umowy z podwykonawcą,
  - wypowiedzeniu umowy,
  - zmianach osób wykonujących umowę,
  - innych spraw mających wpływ na ochronę informacji (w tym informacji niejawnych, danych osobowych, innych informacji prawnie chronionych).
10. Realizacja czynności wykonywanych przez Wykonawcę w ramach umowy, będzie się każdorazowo odbywała w obecności przedstawiciela Zamawiającego lub innej upoważnionej przez niego osoby.
11. Merytoryczny oraz dyscyplinarny nadzór i kierownictwo nad zatrudnionymi przez siebie pracownikami sprawuje Wykonawca.
12. Zmiana pracownika do realizacji zadań związanych z realizacją umowy, może nastąpić tylko po wcześniejszym, pisemnym powiadomieniu Zamawiającego o powyższej zmianie i jego akceptacji.
13. Zamawiający wyznaczy osobę (lub zespół osób) odpowiedzialnych za nadzorowanie, kontrolę i doradztwo w zakresie wykonywania przez Wykonawcę obowiązku ochrony informacji oraz przestrzegania niniejszej Instrukcji Bezpieczeństwa Przemysłowego. Wykonawca zobowiązany jest do poddania się tym czynnościom.
14. Zamawiający powiadomi Wykonawcę o osobach, o których mowa w pkt. 13.
15. Za stały nadzór nad udostępnianymi informacjami odpowiedzialni są:

- a) kierownik projektu ze strony Zlecającego,
  - b) kierownicy jednostek organizacyjnych Straży Granicznej lub komórek organizacyjnych Komendy Głównej Straży Granicznej, które udostępniają informacje oraz osoby przez nich wskazane,
  - c) osoby wskazane do współpracy z Wykonawcą umowy.
16. Kierownik projektu ze strony Zlecającego, lub inna wyznaczona osoba do kontaktów z Wykonawcą, jest odpowiedzialny za informowanie kierowników właściwych komórek organizacyjnych Komendy Głównej Straży Granicznej oraz jednostek organizacyjnych Straży Granicznej o informacjach związanych z realizacją umowy, a mających wpływ na bezpieczeństwo przetwarzanych w Straży Granicznej informacji.
17. Jeżeli w związku z realizacją umowy, zostaną wytworzone informacje niejawne, odpowiednią klauzulę tajności nadaje osoba po stronie Zamawiającego, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału zgodnie ze wskazówkami zawartymi w niniejszej Instrukcji, a w przypadku ich braku, po uzgodnieniu z osobą, o której mowa w pkt. 13.
18. Zniesienie lub zmiana klauzuli tajności w stosunku do dokumentów niejawnych, wytworzonych w związku z realizacją umowy realizuje uprawniona osoba po stronie Zamawiającego.
- Zamawiający zastrzega sobie prawo w zakresie przyznawania, zmiany lub znoszenia klauzuli tajności oraz określania okresu, przez jaki informacja niejawna podlega ochronie wobec dokumentów niejawnych wytworzonych podczas wykonywania umowy.
19. W przypadku konieczności wykonywania migracji danych podlegających ochronie Wykonawca przedstawi Zamawiającemu procedurę wykonania migracji danych zawierającej planowane do wykonania czynności. Procedura migracji danych podlega akceptacji Zamawiającego.
20. Zabrania się wykonywania kopii dokumentów bez zgody kierownika jednostki organizacyjnej Straży Granicznej lub uprawnionego kierownika komórki organizacyjnej Komendy Głównej Straży Granicznej.
21. Wszystkie dokumenty i materiały udostępnione Wykonawcy podlegają ewidencji we właściwych kancelariach jednostek organizacyjnych i komórkach organizacyjnych Straży Granicznej przekazujących przedmiotowe dokumenty i materiały.
22. Po zakończeniu realizacji umowy wszystkie materiały i dokumenty udostępnione, zawierające informacje (w tym informacje niejawne, dane osobowe, inne informacje prawnie chronione, powstałe w wyniku realizacji umowy) muszą być zwrócone przez Wykonawcę do Zamawiającego lub zniszczone protokolarnie za zgodą Zamawiającego, chyba że przepisy prawa stanowią inaczej. Kopia protokołu powinna zostać przekazana do Zamawiającego. Dalsze przetwarzanie materiałów i dokumentów przez Wykonawcę jest dopuszczalne tylko i wyłącznie po uzyskaniu pisemnej zgody ze strony Straży Granicznej.
- Materiały i dokumenty, które zostaną udostępnione w trakcie realizacji umowy muszą być zwrócone w ciągu 14 od zakończenia realizacji umowy.
23. Zamawiający ma prawo do żądania od Wykonawcy danych osobowych osób realizujących w Straży Granicznej umowę w zakresie niezbędnym dla potrzeb zapewnienia ochrony budynków i pomieszczeń Straży Granicznej, wydania niezbędnych upoważnień oraz zapewnienia kontroli nad tym, jakie informacje, kiedy i przez kogo oraz komu zostały przekazywane.
24. Wejście pracowników Wykonawcy do obiektów Straży Granicznej i przebywanie w nich może odbywać się tylko na podstawie przepustki wydanej przez właściwy podmiot Straży Granicznej zgodnie z obowiązującymi procedurami. Przepustki terminowe będą wydawane na podstawie pisemnego wniosku Wykonawcy. W uzasadnionych wypadkach Zamawiający zastrzega sobie prawo do odmowy wydania przepustki, o czym Wykonawca zostanie powiadomiony.



25. Uprawnieni pracownicy Straży Granicznej mogą kontrolować zasadność i sposób przebywania pracowników Wykonawcy na terenie Straży Granicznej.
26. Wykonawca zastosuje się do przyjętego w obiektach Straży Granicznej systemu kontroli osób oraz wwożonych i wywożonych materiałów.
27. Zabrania się Wykonawcy umowy, bez uzyskania wcześniejszej zgody Zamawiającego:
  - a. wnoszenia do obiektów Straży Granicznej materiałów i przedmiotów niebezpiecznych,
  - b. wnoszenia do obiektów Straży Granicznej informatycznych nośników danych oraz urządzeń służących do przesyłania i rejestrowania informacji (komputerów, magnetofonów, aparatów fotograficznych itp.) bez uzyskania wcześniejszej zgody Zamawiającego,
  - c. utrwalania obrazu i dźwięku, w tym robienia zdjęć, nagrywania rozmów i wywiadów,
  - d. pozostawiania przedmiotów i materiałów bez nadzoru,
  - e. przebywania po urzędowych godzinach pracy w obiektach Straży Granicznej bez uzyskania wcześniejszej zgody Zamawiającego.
28. Wszystkie informatyczne nośniki danych wykorzystywane przez Wykonawcę mogą podlegać procedurze kontroli przez Wykonawcę i Zamawiającego na obecność oprogramowania złośliwego.
29. Wszystkie informatyczne nośniki danych wielokrotnego zapisu przekazane przez Wykonawcę i użyte w systemach informatycznych Straży Granicznej i innych, muszą pozostać u administratora systemu. Zwrot nośników może nastąpić dopiero po usunięciu wszystkich informacji zawartych na nośniku przez administratora systemu. W przypadku niemożliwości usunięcia informacji nośniki nie zostają zwrócone.
30. Jeżeli w ramach realizacji umowy wyniknie potrzeba dostępu do systemów teleinformatycznych Straży Granicznej, pracownicy Wykonawcy muszą uzyskać zgodę gestora (kierownika jednostki organizacyjnej lub osoby upoważnionej) przedmiotowego systemu. Dostęp do tych systemów będzie realizowany zgodnie z przyjętymi procedurami, politykami, oraz instrukcjami bezpieczeństwa, z którymi w niezbędnym zakresie zostanie zapoznany Wykonawca.
31. Zabrania się kopiowania jakichkolwiek informacji z systemów Straży Granicznej i wnoszenie ich poza miejsce zainstalowania systemów teleinformatycznych, bez zgody Zamawiającego.
32. Zabrania się wnoszenia wszelkich elementów wchodzących w skład systemu teleinformatycznego (zwłaszcza informatycznych nośników danych).
33. Jeżeli w ramach realizacji umowy wyniknie potrzeba przeprowadzenia kontroli poprawności działania systemu, Wykonawca zobowiązany jest przeprowadzić testy wykorzystując wprowadzone i przygotowane przez siebie dane testowe. Użycie systemów i programów przy wykorzystaniu danych rzeczywistych może odbywać się wyłącznie na terenie obiektów Straży Granicznej i za zgodą Zamawiającego.
34. Informacje (w tym informacje niejawne, dane osobowe, inne informacje prawnie chronione) mogą być udostępniane Wykonawcy i przetwarzane przez niego tylko na terenie obiektów Straży Granicznej lub w miejscach, w których są one przetwarzane przez Straży Granicznej.
35. Udostępnianie przez Wykonawcę innym podmiotom (np. podwykonawcom) informacji związanych z wykonaniem umowy i podlegających ochronie, może odbywać się wyłącznie za zgodą Zamawiającego.
36. Pracownicy Wykonawcy zobowiązani są do poinformowania Straży Granicznej o sytuacjach mogących naruszać przepisy ustawy o ochronie informacji niejawnych, danych osobowych oraz zapisy niniejszej Instrukcji Bezpieczeństwa Przemysłowego.
37. W przypadku naruszenia przepisów o ochronie informacji niejawnych, danych osobowych, innych dot. informacji prawnie chronionych oraz zapisów niniejszej Instrukcji Bezpieczeństwa Przemysłowego, Zamawiający i Wykonawca podejmą działania zmierzające do wyjaśnienia okoliczności naruszenia oraz

- spowodują właściwe zabezpieczenie materialnych śladów działania lub jego zaniechania, które były związane ze zdarzeniem.
38. W przypadku niewykonania lub nienależytego wykonania obowiązków wynikających z ustaw o ochronie informacji niejawnych, danych osobowych, nieprzestrzegania wymagań określonych niniejszą Instrukcją Bezpieczeństwa Przemysłowego, Zamawiający ma prawo rozwiązać umowę z winy Wykonawcy, a powstałe z tego faktu skutki finansowe i prawne obciążą Wykonawcę.
39. Wykonawca, pracownicy Wykonawcy, mający dostęp do informacji (w tym informacji niejawnych, danych osobowych, innych informacji prawnie chronionych) Zamawiającego, zobowiązani są zarówno podczas realizacji umowy, jak również po jej zakończeniu lub odstąpieniu od jej wykonania, do:
- zapewnienia ochrony i bezpieczeństwa wszelkich informacji uzyskanych od Zamawiającego lub wytworzonych w związku z realizacją umowy, zgodnie z obowiązującymi przepisami prawa oraz na warunkach i zasadach określonych w niniejszej Instrukcji Bezpieczeństwa Przemysłowego,
  - zachowania poufności informacji, w których posiadanie wejdzie w trakcie realizacji umowy,
  - niewykorzystywania informacji do innych celów niż wykonywanie czynności wynikających z umowy,
  - zapewnienia kontroli nad tym, jakie informacje, kiedy i przez kogo oraz komu zostały przekazywane,
  - zachowania w tajemnicy informacji i sposobów ich zabezpieczenia, również po zakończeniu umowy,
  - nie ujawniania informacji związanych z wykonaniem umowy osobom nieupoważnionym,
  - umożliwienia Zamawiającemu, przeprowadzania kontroli stanu ochrony informacji udostępnionych lub wytworzonych w związku z realizacją umowy.
40. Wszyscy pracownicy Wykonawcy mający dostęp do informacji udostępnionych w ramach realizacji umowy są zobowiązani do zapoznania się oraz przestrzegania zasad i postanowień zawartych w niniejszej Instrukcji Bezpieczeństwa Przemysłowego.
41. Ochronie podlegają także wszystkie pozostałe informacje, nieoznaczone żadną klauzulą tajności, a objęte ochroną innymi przepisami.
42. Materiały jawne i materiały niejawne podlegające ochronie nie mogą być wykorzystywane do żadnych innych celów niż te, które określono w umowie. Zabrania się wykorzystywania tych materiałów, w tym do celów propagandowych oraz prezentowania ich w mediach bez wiedzy i zgody Zamawiającego.
43. Wykaz informacji niejawnych, do których Wykonawca może mieć dostęp lub, które mogą być wytworzone przez Wykonawcę podczas realizacji umowy. Zamawiający zastrzega sobie prawo do zmiany lub rozszerzenia listy dokumentów lub spraw zawartych w wykazie. Zmiana w tym zakresie nie będzie wymagała podpisania aneksu do umowy.

L.p.	Nazwa dokumentu lub sprawy	Maksymalna klauzula tajności
1.		
2.		

3.		
----	--	--

44. Wykonawca ma obowiązek niezwłocznego informowania Zamawiającego, o naruszeniu przepisów o ochronie informacji niejawnych przez pracowników Wykonawcy, zgodnie z Art.71 ust.5 pkt.1 Ustawy.
45. Zamawiający ma prawo postawić dodatkowe warunki w zakresie ochrony informacji niejawnych, danych osobowych i innych informacji prawnie chronionych, wynikające ze zmiany obowiązujących przepisów.
46. Wykonawca zaakceptuje wymagania określone w niniejszej Instrukcji Bezpieczeństwa Przemysłowego poprzez podpisanie umowy.
47. Ustalenia zawarte w niniejszej Instrukcji Bezpieczeństwa Przemysłowego dotyczą wszystkich osób, które w imieniu Wykonawcy będą wykonywały umowę, w tym także podwykonawców – jeśli ich wykonywanie umowy wiąże się z dostępem do informacji niejawnych, danych osobowych, innych informacji prawnie chronionych Zamawiającego. Wykonawca zobowiązuje się zawrzeć analogiczne postanowienia w umowach zawieranych z podwykonawcami, zgodnie z Art.54 ust.6 Ustawy.

Wykonał: Andrzej Pindor  
tel.: +48 500 40 44  
Dnia: .....r.





### OŚWIADCZENIE O SKORZYSTANIU Z PRAWA OPCJI

Zamawiający oświadcza, że zgodnie z zapisami umowy nr .../BF/BLiI/... z dnia ..... korzysta z przysługującego mu prawa opcji w poniższym zakresie:

Zamówienie nr:

Data zamówienia:

Telefon Zamawiającego:

Fax Zamawiającego:

Pozycje zamówienia:

Lp.	Nazwa produktu	Liczba	Cena jednostkowa

.....  
Zamawiający

Umowa nr ...../BF/BŁiI/2017

na realizację projektu pn.:

„Rozbudowa systemu telekomunikacyjnego SG – część 2 zamówienia”

zawarta w dniu..... w Warszawie

pomiędzy:

Komendantem Głównym Straży Granicznej, z siedzibą w Warszawie przy al. Niepodległości 100, będącym podatnikiem podatku od towarów i usług, posiadającym NIP 521-29-21-032, reprezentowanym przez:

..... - Dyrektora Biura Łączności i Informatyki Komendy Głównej Straży Granicznej

oraz przy kontrasygnacie:

..... - Głównego Księgowego Komendy Głównej Straży Granicznej

..... - Zastępcy Dyrektora Biura Finansów Komendy Głównej Straży Granicznej

zwanym dalej „Zamawiającym”,

a

.....  
reprezentowanym przez:

.....  
zwanym w dalszej treści umowy „Wykonawcą”,

zwanymi dalej łącznie „Stronami”, a każdego z osobna „Stroną”.

## § 1

### Przedmiot Umowy

1. Przedmiotem niniejszej umowy jest:
  - a) objęcie gwarancją producenta urządzeń (licencji i oprogramowania) wskazanych przez Zamawiającego w Załączniku nr 3 do OPZ,
  - b) zapewnienie zaawansowanego wsparcia technicznego w usuwaniu awarii i diagnostyce sieci przez inżynierów sieciowych producenta urządzeń,
  - c) przeprowadzenie certyfikowanych szkoleń.
2. Przedmiot zamówienia zostanie zrealizowany zgodnie z warunkami określonymi w Opisie Przedmiotu Zamówienia (OPZ) (w pkt B OPZ dotyczącym realizacji części 2 zamówienia) stanowiącym załącznik nr 1 do niniejszej umowy oraz zgodnie z ofertą Wykonawcy stanowiącą załącznik nr 2 do niniejszej umowy.

## § 2

### Terminy oraz sposób wykonania Umowy

Strony ustalają, że wykonanie przedmiotu umowy będzie realizowane przez Wykonawcę zgodnie ze wskazanymi poniżej terminami:

1. objęcie gwarancją producenta wskazanych przez Zamawiającego urządzeń w terminie do 14 dni od daty zawarcia umowy, co zostanie potwierdzone przekazaniem przez Wykonawcę Zamawiającemu zaświadczenia Producenta o wykupieniu pakietów gwarancyjnych;
2. realizacja wsparcia technicznego w okresie 36 miesięcy, licząc od dnia przekazania Zamawiającemu zaświadczenia, o którym mowa w ust. 1.
3. przeprowadzenie certyfikowanych szkoleń, zgodnie z harmonogramem, o którym mowa w §5 ust. 5.

## § 3

### Reprezentacja Stron

1. Osobą odpowiedzialną za realizację Umowy po stronie Zamawiającego jest p....., tel....., fax ....., adres email:.....
2. Osobą odpowiedzialną za realizację Umowy po stronie Wykonawcy jest p....., tel....., fax ..... adres email: .....
3. Osoby, o których mowa w ust. 1 i 2 odpowiadają za wykonanie przedmiotu Umowy zgodnie z wymaganiami określonymi w Umowie oraz załącznikach do Umowy.

Każda ze Stron może dokonać zmian osób wskazanych w ust. 1 - 2, informując o tym pisemnie drugą Stronę z co najmniej dwudniowym wyprzedzeniem. Powiadomienie o powyższych zmianach nie stanowi zmiany wymagającej aneksu do Umowy.



#### § 4

#### Zobowiązania Wykonawcy

Wykonawca zobowiązuje się do realizacji przedmiotu umowy w sposób zgodny z wymaganiami Zamawiającego określonymi w OPZ, w tym m. in. do:

1. objęcia gwarancją producenta wskazanych przez Zamawiającego urządzeń, gwarantujących naprawę lub wymianę urządzenia w przypadku awarii,
2. zapewnienia zaawansowanego wsparcia technicznego w usuwaniu awarii i diagnostyce sieci przez inżynierów sieciowych producenta realizujących wsparcie techniczne w Centralnym Węźle Telekomunikacyjnym Straży Granicznej,
3. przeprowadzenia certyfikowanych szkoleń,
4. dostarczenia w ciągu 7 dni po podpisaniu umowy dokumentu wydanego przez polskie przedstawicielstwo producenta, poświadczające spełnienie wymagań określonych w OPZ przez inżynierów sieciowych,

#### § 5

#### Szkolenia

1. W ramach realizacji zamówienia Wykonawca przeprowadzi certyfikowane szkolenia dla Administratorów sieci TI Straży Granicznej.
2. Szczegółowy zakres szkoleń został określony w OPZ pkt. B ppkt 4.
3. Wykonawca zobowiązuje się do przeprowadzenia wszystkich szkoleń w terminie nie dłuższym niż do dnia zakończenia realizacji umowy.
4. Wszystkie szkolenia muszą zostać zrealizowane w autoryzowanych centrach szkoleniowych przez producenta posiadanych przez Zamawiającego urządzeń.
5. Wykonawca, w terminie 7 dni od dnia zawarcia umowy, przekaże Zamawiającemu wykaz szkoleń zawierający ich nazwę oraz cenę jednostkową.
6. Wykonawca, w terminie 14 dni od dnia zawarcia umowy, przedstawi do akceptacji Zamawiającego harmonogram przeprowadzenia szkoleń w kolejnych latach obowiązywania umowy.
7. Po każdym przeprowadzonym szkoleniu Strony podpiszą Protokół Odbioru Szkolenia będący podstawą wystawienia faktury.

#### § 6

#### Wynagrodzenie

1. Zamawiający zobowiązuje się zapłacić Wykonawcy za przedmiot umowy określony w §1 ust. 1 łączne wynagrodzenie ustalone na podstawie oferty w kwocie brutto ..... zł (słownie: ..... zł brutto) zawierającej obowiązujący podatek VAT w tym:
  - a) Zamawiający zobowiązuje się zapłacić Wykonawcy za przedmiot umowy określony

w § 1 ust. 1 lit. a - b wynagrodzenie ustalone na podstawie oferty w kwocie brutto:  
..... zł (słownie: ..... zł brutto)

- b) Zamawiający zobowiązuje się zapłacić Wykonawcy za przedmiot umowy określony w § 1 ust. 1 lit. c wynagrodzenie ustalone na podstawie oferty w kwocie brutto: ..... zł (słownie:..... zł brutto)
2. W kwocie, o której mowa w ust. 1 niniejszego § mieszczą się wszystkie koszty realizacji przedmiotu zamówienia.
  3. Zapłata za wykonywanie przedmiotu zamówienia określonego w ust. 1 pkt a) zostanie dokonana w formie 36 opłat miesięcznych, każda w wysokości 1/36 wartości umowy określonej w ust. 1 pkt a).
  4. Zapłata za wykonanie przedmiotu zamówienia określonego w ust. 1 pkt b) zostanie dokonana każdorazowo po zrealizowaniu zaplanowanego szkolenia.
  5. Zapłata za wykonywanie przedmiotu umowy określona w ust. 1 pkt a) nastąpi w terminie 30 dni od daty dostarczenia Zamawiającemu prawidłowo wystawionej faktury. Podstawę wystawienia faktury stanowić będzie protokół odbioru prac wykonanych przez Inżynierów Wykonawcy w ramach wsparcia technicznego i gwarancji świadczonej przez Wykonawcę - za dany miesiąc.
  6. Zapłata za wykonywanie przedmiotu umowy określona w ust. 1 pkt b) nastąpi w terminie 30 dni od daty dostarczenia Zamawiającemu prawidłowo wystawionej faktury. Podstawę wystawienia faktury stanowić będzie protokół odbioru szkolenia, o którym mowa w § 5 pkt 7.
  7. Za termin zapłaty przyjmuje się dzień obciążenia rachunku Zamawiającego.
  8. Zapłata dokonana będzie przelewem na rachunek Wykonawcy, wskazany w fakturze.
  9. Wynagrodzenie za przedmiot umowy nie ulegnie zmianie w trakcie obowiązywania umowy z zastrzeżeniem § 10.

## § 7

### Gwarancja i serwis

Warunki gwarancji i serwisowania urządzeń stanowiących przedmiot umowy określono szczegółowo w OPZ pkt. B ppkt 3.

## § 8

### Kary umowne i roszczenia odszkodowawcze

1. W przypadku nie dotrzymania terminu wykonania przedmiotu umowy, o którym mowa w § 2 ust. 1 Wykonawca zapłaci za każdy rozpoczęty dzień opóźnienia karę umowną w wysokości 0,5 % wynagrodzenia brutto wskazanego w § 6 ust. 1 pkt a) umowy.
2. W przypadku niedotrzymania terminu wymiany uszkodzonego sprzętu, o którym mowa w ofercie Wykonawcy, Wykonawca zapłaci za każde rozpoczęte 24 godziny opóźnienia



karę umowną w wysokości 1000 (słownie: jeden tysiąc) złotych.

3. W przypadku odstąpienia od Umowy z przyczyn leżących po stronie Wykonawcy, zapłaci on na rzecz Zamawiającego karę umowną w wysokości 10% wartości wynagrodzenia brutto, określonego w §6 ust. 1.
4. Strony ustalają, iż wysokość kar umownych określonych w ust. 1 – 3 nie może przekroczyć 20% wartości wynagrodzenia brutto, określonego w §6 ust. 1.
5. Wykonawca oświadcza, że wyraża zgodę na potrącenie w rozumieniu art. 498 i 499 Kodeksu cywilnego przez Zamawiającego powstałych wierzytelności w tym z tytułu kar umownych, z jakiegokolwiek należności Wykonawcy. Jednocześnie Wykonawca oświadcza, że powyższe oświadczenie nie zostało złożone pod wpływem błędu, ani nie jest obciążone jakąkolwiek wadą oświadczenia woli skutkującą jego nieważnością.
6. W przypadku nie dokonania potrącenia, o którym mowa w ust. 5, Wykonawca dokona zapłaty powstałych wierzytelności w terminie do 7 dni od dnia otrzymania od Zamawiającego noty obciążeniowej.
7. Zamawiający oświadcza, że w przypadku zaistnienia sytuacji, o których mowa w ust. 5 wystawi Wykonawcy notę w terminie 21 dni od dnia dokonania potrącenia zawierającą szczegółowe naliczenie wierzytelności w tym z tytułu kar umownych.
8. W przypadku nie dokonania przez Wykonawcę wymiany uszkodzonego sprzętu w okresie gwarancji lub rękojmi w terminie wskazanym w OPZ, Zamawiający jest uprawniony do wymiany uszkodzonego sprzętu na koszt Wykonawcy. W takim przypadku Zamawiający nie traci praw do gwarancji i rękojmi za wady.
9. Pobranie kar umownych nie pozbawia Zamawiającego prawa dochodzenia odszkodowania na zasadach ogólnych.

## §9

### Odstąpienie od Umowy

1. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy, lub dalsze wykonywanie umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, Zamawiający może odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach. W takim przypadku Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części Umowy.
2. Zamawiający ma także prawo odstąpić od Umowy w przypadku zaistnienia następujących okoliczności:



- 1) w terminie do 30 dni od terminu określonego w § 2 ust. 1 – w przypadku niedostarczenia zaświadczenia producenta o wykupieniu pakietów gwarancyjnych.
  - 2) jeżeli łączna wysokość kar umownych z tytułu realizacji niniejszej Umowy naliczonych przez Zamawiającego osiągnie 20% wartości wynagrodzenia brutto Umowy, określonego w § 6 ust. 1;
  - 3) w przypadku postawienia Wykonawcy w stan likwidacji.
3. Odstąpienie od Umowy jest skuteczne pod warunkiem dokonania tej czynności w formie pisemnej.

## § 10

### Zmiana umowy

1. Strony przewidują możliwość dokonania zmian w treści umowy w sytuacji, gdy:
  - a) nastąpi zmiana wysokości podatku od towarów i usług (VAT);
  - b) wejdą w życie zmiany przepisów dotyczących wysokości minimalnego wynagrodzenia za pracę ustalonego przez Ustawodawcę – jeżeli zmiany te będą miały wpływ na koszty wykonania przedmiotu umowy przez Wykonawcę. Wykazanie zmiany kosztów spoczywa na Wykonawcy i podlega akceptacji Zamawiającego;
  - c) wejdą w życie zmiany przepisów dotyczących zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne – jeżeli zmiany te będą miały wpływ na koszty wykonania przedmiotu Umowy.  
Wykazanie zmiany kosztów spoczywa na Wykonawcy i podlega akceptacji Zamawiającego.
2. Zmiany, o których mowa w ust. 1 wymagają zachowania formy pisemnej pod rygorem nieważności, w postaci aneksu.

## § 11

### Siła wyższa

1. Strona nie jest odpowiedzialna za niewykonanie lub nienależyte wykonanie swoich zobowiązań powodów siły wyższej, to jest, jeżeli niewykonanie zostało spowodowane wydarzeniem będącym poza jej kontrolą oraz gdy w chwili zawarcia Umowy niemożliwe było przewidzenie zdarzenia i jego skutków, które wpłynęły na zdolność Strony do wykonania Umowy oraz gdy niemożliwe było uniknięcie samego zdarzenia lub przynajmniej jego skutków.
2. Za siłę wyższą nie uznaje się braku środków u Wykonawcy, niedotrzymania zobowiązań przez jego kontrahentów oraz braku zezwoleń niezbędnych Wykonawcy dla wykonania Umowy, wydawanych przez uprawniony do tego organ.

3. Strony zobowiązują się do wzajemnego powiadamiania się o zaistnieniu siły wyższej i dokonania stosownych ustaleń celem wyeliminowania możliwych skutków działania siły wyższej. Powiadomienia, o którym mowa w zdaniu pierwszym, należy dokonać pisemnie lub w inny dostępny sposób, niezwłocznie po fakcie wystąpienia siły wyższej, nie później jednak niż w ciągu 3 dni od chwili jej wystąpienia. Do powiadomienia należy dołączyć dowody na poparcie zaistnienia siły wyższej.
4. Strona jest zobowiązana do powiadomienia o ustaniu siły wyższej w terminie nie później niż w ciągu 3 dni od momentu ustąpienia siły wyższej.
5. Zwolnienie od odpowiedzialności nie ma zastosowania w przypadku braku zawiadomienia zarówno o zaistnieniu jak i o ustaniu okoliczności siły wyższej, jak również nie przedstawienia powiadomień, o których mowa w ust. 3 lub 4 niniejszego paragrafu.
6. W przypadku niemożności wykonania przedmiotu Umowy przez Wykonawcę z powodu siły wyższej przez okres dłuższy niż 14 dni, Zamawiający może odstąpić od Umowy płacąc Wykonawcy za wykonaną część przedmiotu Umowy.

## § 12

### Dostęp do informacji niejawnych

1. Wykonawca zobowiązuje się do zachowania poufności wszystkich informacji, w których posiadanie wszedł w trakcie wykonywania umowy lub w związku z wykonywaną umową oraz do nie wykorzystywania ich do innych celów niż wykonywanie czynności wynikających z niniejszej umowy zgodnie z Ustawą z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (Dz.U. z 2016r. poz. 1167 ze zm.) oraz do przestrzegania Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2016 poz. 922) wraz z przepisami wykonawczymi wydanymi na ich podstawie.
2. Przekazywanie informacji niejawnych poza terytorium RP będzie realizowane zgodnie z umowami międzynarodowymi (zawartymi pomiędzy Polską, a krajem Wykonawcy) w sprawie wzajemnej ochrony informacji niejawnych.
3. Wszystkie osoby, którym Wykonawca zleci wykonanie umowy lub jej części związanej z dostępem do informacji niejawnych, a w szczególności osoby mające dostęp do systemów, w których przetwarzane są informacje Zamawiającego lub osoby, którym Wykonawca zleca wykonanie umowy oraz jej bezpośrednią realizację na terenie SG, muszą posiadać ważne poświadczenie bezpieczeństwa lub pisemne upoważnienie do dostępu do informacji niejawnych oznaczonych klauzulą tajności zastrzeżone oraz zaświadczenie potwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych.
4. Dostęp Wykonawcy do informacji niejawnych może nastąpić wyłącznie w zakresie

niezbędnym do realizacji przez niego przedmiotu Umowy.

5. W przypadku niewykonania lub nienależytego wykonywania obowiązków wynikających z ustawy o ochronie informacji niejawnych, ustawy o ochronie danych osobowych, nieprzestrzegania wymagań określonych w Instrukcji Bezpieczeństwa Przemysłowego, Zamawiający ma prawo rozwiązać umowę, a powstałe z tego faktu skutki finansowe i prawne obciążą Wykonawcę.
6. Wykonawca zobowiązuje się do przestrzegania zasad dostępu do informacji niejawnych oraz danych osobowych określonych w „Instrukcji Bezpieczeństwa Przemysłowego”, która stanowi integralną część umowy (załącznik nr 3 do niniejszej umowy).
7. Wykonawca zobowiązuje się do bezzwłocznego dostarczenia informacji dotyczących nowych podwykonawców, w tym podania ich nazwy (firmy) i siedziby oraz danych, które umożliwiają Zamawiającemu stwierdzenie, że każdy z nich posiada kwalifikacje wymagane do zachowania poufnego charakteru informacji niejawnych, do których mają dostęp lub które zostaną wytworzone w związku z wykonywaniem umowy o podwykonawstwo.

#### § 13

#### Postanowienia końcowe

1. W sprawach nieuregulowanych Umową mają zastosowanie obowiązujące przepisy prawa polskiego, w szczególności przepisy ustawy - Kodeks cywilny, ustawy - Prawo zamówień oraz innych, które odnoszą się do Umowy.
2. Strony zobowiązują się do rozstrzygnięcia polubownie wszelkich sporów, mogących wyniknąć na tle wykonania Umowy. W przypadku nieosiągnięcia porozumienia spór rozstrzygać będzie sąd powszechny, właściwy dla siedziby Zamawiającego.
3. Załączniki wymienione w Umowie stanowią jej integralną część.
4. Umowę sporządzono w 4 jednobrzmiących egzemplarzach, w tym trzy egzemplarze dla Zamawiającego i jeden egzemplarz dla Wykonawcy.

Załączniki do Umowy:

Załącznik nr 1 – Opis Przedmiotu Zamówienia;

Załącznik nr 2 – Oferta Wykonawcy;

Załącznik nr 3 – Instrukcja bezpieczeństwa przemysłowego

Zamawiający

Wykonawca





**KOMENDA GŁÓWNA STRAŻY GRANICZNEJ**

*BIURO OCHRONY INFORMACJI*

**Instrukcja**  
**Bezpieczeństwa Przemysłowego**

A handwritten signature in blue ink is located in the bottom right corner of the page.



Instrukcja Bezpieczeństwa Przemysłowego, określa szczegółowe wymagania dotyczące ochrony informacji, a w tym informacji niejawnych, danych osobowych oraz innych informacji prawnie chronionych, do których Wykonawca będzie miał dostęp w związku z wykonywaniem umowy.

Instrukcja Bezpieczeństwa została opracowana przez Biuro Ochrony Informacji KGSG na podstawie wymagań obowiązujących przepisów, w tym wymagań zawartych w ustawie z dnia 05 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2016 r. poz. 1167 z późn. zm.), w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922.) oraz przepisów wykonawczych do nich wydanych oraz instrukcjach bezpieczeństwa obowiązujących w Straży Granicznej.

Żadne odstępstwa lub poprawki do niniejszej Instrukcji Bezpieczeństwa Przemysłowego nie są dozwolone, dopóki nie zostaną zaakceptowane przez Komendanta Głównego Straży Granicznej.

1. Wykonawca, pod rygorem zerwania umowy z winy Wykonawcy i odpowiedzialności karnej za ujawnienie informacji (w tym informacji niejawnych, danych osobowych, innych informacji prawnie chronionych) udostępnionych przez Zamawiającego i inne osoby bądź wytwarzanych w trakcie realizacji umowy, zobowiązuje się do przestrzegania i stosowania przepisów i procedur właściwych do ochrony tych informacji zgonie z:
  - a) przepisami prawa obowiązującymi na terytorium Polski
    - ustawą z dnia 05 sierpnia 2010 r. o ochronie informacji niejawnych (tekst jednolity Dz. U. z 2016r. poz. 1167 z późn. zm.) zwaną dalej Ustawą,
    - ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2016r. poz. 922),oraz przepisami wykonawczymi do nich wydanymi,
  - b) umowami międzynarodowymi (pomiędzy Polską a krajem Wykonawcy) w przedmiotowej sprawie.
2. Wszystkie osoby bezpośrednio zaangażowane w realizację umowy mające mieć dostęp do informacji niejawnych oraz kierownik projektu ze strony Wykonawcy, muszą posiadać ważne:
  - a) poświadczenia bezpieczeństwa lub pisemne upoważnienie, o którym mowa w art. 21 ust. 4 ustawy o ochronie informacji niejawnych o klauzuli tajności „zastrzeżone”, wydane przez kierownika jednostki organizacyjnej Wykonawcy, jeżeli osoba nie posiada poświadczenia bezpieczeństwa;
  - b) zaświadczenie potwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych.
3. Upoważnienie, o którym mowa w pkt. 2 lit. a) powinno zawierać:
  - oznaczenie jednostki organizacyjnej,
  - datę i miejsce wydania,
  - podstawę prawną,
  - imię (imiona), nazwisko, PESEL,
  - cel wydania (np. wykonanie określonego zadania) bądź okres na jaki upoważnienie zostaje wydane (wskazanie konkretnych dat albo wydarzenia, które spowoduje utratę ważności upoważnienia np. „na czas zatrudnienia w jednostce organizacyjnej”),
  - pieczętkę i podpis kierownika jednostki organizacyjnej.
4. Wykonawca przekaze do Zamawiającego kserokopie dokumentów, o których jest mowa w pkt. 2 niezwłocznie po podpisaniu umowy. Przedmiotowe kserokopie muszą być potwierdzone za zgodność z oryginałem przez upoważnioną osobę i muszą umożliwiać łatwe odczytanie ich treści i pieczęci.
5. Do przetwarzania danych osobowych, mogą być dopuszczone wyłącznie osoby Wykonawcy:
  - posiadające upoważnienie do przetwarzania danych osobowych nadane przez Zamawiającego,
  - przeszkolone przez Wykonawcę z zakresu ochrony danych osobowych.



6. Przed dostępem do danych osobowych Wykonawca zwróci się do Zamawiającego z wnioskiem o wydanie upoważnień do przetwarzania danych osobowych dla pracowników Wykonawcy wskazanych we wniosku.
7. Dostęp przedstawicieli Wykonawcy do informacji (w tym do informacji niejawnych, danych osobowych, innych informacji prawnie chronionych) może być zrealizowany tylko w zakresie niezbędnym do wykonywania przez nich powierzonej (zleconej) pracy pod warunkiem spełnienia wymagań określonych w niniejszej Instrukcji Bezpieczeństwa Przemysłowego.
8. Wykonawca w trakcie realizacji umowy oraz każdorazowo po zmianie danych i na wniosek Zamawiającego przedstawi kompletny wykaz osób realizujących umowę w imieniu Wykonawcy. Wykaz ten musi zawierać następujące dane:
  - imię, nazwisko, PESEL,
  - pełniona funkcja w ramach realizacji umowy lub wykonywane zadanie,
  - nazwę przedsiębiorcy, u którego jest zatrudniona osoba w związku z realizacją umowy,
  - informację o odbyciu szkolenia z ochrony danych osobowych,
  - informację o odbyciu szkolenia z ochrony informacji niejawnych, o którym mowa w pkt. 2 lit. b),
  - informację o posiadaniu poświadczenia bezpieczeństwa lub upoważnienia, o którym mowa w pkt. 2 lit. a),
  - informację o zapoznaniu się z Instrukcją Bezpieczeństwa Przemysłowego.

Zamawiający ma prawo do żądania innych danych osób Wykonawcy niezbędnych w ramach realizacji umowy, a w szczególności nr telefonu kontaktowego, nr dowodu osobistego oraz adresu zamieszkania.

Prawo dostępu do informacji i materiałów podlegających ochronie, mają wyłącznie osoby, które są objęte wykazem.

9. Wykonawca ma obowiązek niezwłocznego informowania Zamawiającego o wszystkich zmianach dotyczących osób wymienionych w wykazie osób realizujących umowę, a także o:
  - ogłoszeniu upadłości, likwidacji lub rozwiązania jednostki organizacyjnej Wykonawcy albo zakończeniu przez nią działalności w innej formie,
  - potrzebie zawarcia umowy z podwykonawcą,
  - wypowiedzeniu umowy,
  - zmianach osób wykonujących umowę,
  - innych spraw mających wpływ na ochronę informacji (w tym informacji niejawnych, danych osobowych, innych informacji prawnie chronionych).
10. Realizacja czynności wykonywanych przez Wykonawcę w ramach umowy, będzie się każdorazowo odbywała w obecności przedstawiciela Zamawiającego lub innej upoważnionej przez niego osoby.
11. Merytoryczny oraz dyscyplinarny nadzór i kierownictwo nad zatrudnionymi przez siebie pracownikami sprawuje Wykonawca.
12. Zmiana pracownika do realizacji zadań związanych z realizacją umowy, może nastąpić tylko po wcześniejszym, pisemnym powiadomieniu Zamawiającego o powyższej zmianie i jego akceptacji.
13. Zamawiający wyznaczy osobę (lub zespół osób) odpowiedzialnych za nadzorowanie, kontrolę i doradztwo w zakresie wykonywania przez Wykonawcę obowiązku ochrony informacji oraz przestrzegania niniejszej Instrukcji Bezpieczeństwa Przemysłowego. Wykonawca zobowiązany jest do poddania się tym czynnościom.
14. Zamawiający powiadomi Wykonawcę o osobach, o których mowa w pkt. 13.
15. Za stały nadzór nad udostępnianymi informacjami odpowiedzialni są:

- a) kierownik projektu ze strony Zlecającego,
  - b) kierownicy jednostek organizacyjnych Straży Granicznej lub komórek organizacyjnych Komendy Głównej Straży Granicznej, które udostępniają informacje oraz osoby przez nich wskazane,
  - c) osoby wskazane do współpracy z Wykonawcą umowy.
16. Kierownik projektu ze strony Zlecającego, lub inna wyznaczona osoba do kontaktów z Wykonawcą, jest odpowiedzialny za informowanie kierowników właściwych komórek organizacyjnych Komendy Głównej Straży Granicznej oraz jednostek organizacyjnych Straży Granicznej o informacjach związanych z realizacją umowy, a mających wpływ na bezpieczeństwo przetwarzanych w Straży Granicznej informacji.
17. Jeżeli w związku z realizacją umowy, zostaną wytworzone informacje niejawne, odpowiednią klauzulę tajności nadaje osoba po stronie Zamawiającego, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału zgodnie ze wskazówkami zawartymi w niniejszej Instrukcji, a w przypadku ich braku, po uzgodnieniu z osobą, o której mowa w pkt. 13.
18. Zniesienie lub zmiana klauzuli tajności w stosunku do dokumentów niejawnych, wytworzonych w związku z realizacją umowy realizuje uprawniona osoba po stronie Zamawiającego.
- Zamawiający zastrzega sobie prawo w zakresie przyznawania, zmiany lub znoszenia klauzuli tajności oraz określania okresu, przez jaki informacja niejawna podlega ochronie wobec dokumentów niejawnych wytworzonych podczas wykonywania umowy.
19. W przypadku konieczności wykonywania migracji danych podlegających ochronie Wykonawca przedstawi Zamawiającemu procedurę wykonania migracji danych zawierającej planowane do wykonania czynności. Procedura migracji danych podlega akceptacji Zamawiającego.
20. Zabrania się wykonywania kopii dokumentów bez zgody kierownika jednostki organizacyjnej Straży Granicznej lub uprawnionego kierownika komórki organizacyjnej Komendy Głównej Straży Granicznej.
21. Wszystkie dokumenty i materiały udostępnione Wykonawcy podlegają ewidencji we właściwych kancelariach jednostek organizacyjnych i komórkach organizacyjnych Straży Granicznej przekazujących przedmiotowe dokumenty i materiały.
22. Po zakończeniu realizacji umowy wszystkie materiały i dokumenty udostępnione, zawierające informacje (w tym informacje niejawne, dane osobowe, inne informacje prawnie chronione, powstałe w wyniku realizacji umowy) muszą być zwrócone przez Wykonawcę do Zamawiającego lub zniszczone protokolarnie za zgodą Zamawiającego, chyba że przepisy prawa stanowią inaczej. Kopia protokołu powinna zostać przekazana do Zamawiającego. Dalsze przetwarzanie materiałów i dokumentów przez Wykonawcę jest dopuszczalne tylko i wyłącznie po uzyskaniu pisemnej zgody ze strony Straży Granicznej.
- Materiały i dokumenty, które zostaną udostępnione w trakcie realizacji umowy muszą być zwrócone w ciągu 14 od zakończenia realizacji umowy.
23. Zamawiający ma prawo do żądania od Wykonawcy danych osobowych osób realizujących w Straży Granicznej umowę w zakresie niezbędnym dla potrzeb zapewnienia ochrony budynków i pomieszczeń Straży Granicznej, wydania niezbędnych upoważnień oraz zapewnienia kontroli nad tym, jakie informacje, kiedy i przez kogo oraz komu zostały przekazywane.
24. Wejście pracowników Wykonawcy do obiektów Straży Granicznej i przebywanie w nich może odbywać się tylko na podstawie przepustki wydanej przez właściwy podmiot Straży Granicznej zgodnie z obowiązującymi procedurami. Przepustki terminowe będą wydawane na podstawie pisemnego wniosku Wykonawcy. W uzasadnionych wypadkach Zamawiający zastrzega sobie prawo do odmowy wydania przepustki, o czym Wykonawca zostanie powiadomiony.

25. Uprawnieni pracownicy Straży Granicznej mogą kontrolować zasadność i sposób przebywania pracowników Wykonawcy na terenie Straży Granicznej.
26. Wykonawca zastosuje się do przyjętego w obiektach Straży Granicznej systemu kontroli osób oraz wwożonych i wywożonych materiałów.
27. Zabrania się Wykonawcy umowy, bez uzyskania wcześniejszej zgody Zamawiającego:
  - a. wnoszenia do obiektów Straży Granicznej materiałów i przedmiotów niebezpiecznych,
  - b. wnoszenia do obiektów Straży Granicznej informatycznych nośników danych oraz urządzeń służących do przesyłania i rejestrowania informacji (komputerów, magnetofonów, aparatów fotograficznych itp.) bez uzyskania wcześniejszej zgody Zamawiającego,
  - c. utrwalania obrazu i dźwięku, w tym robienia zdjęć, nagrywania rozmów i wywiadów,
  - d. pozostawiania przedmiotów i materiałów bez nadzoru,
  - e. przebywania po urzędowych godzinach pracy w obiektach Straży Granicznej bez uzyskania wcześniejszej zgody Zamawiającego.
28. Wszystkie informatyczne nośniki danych wykorzystywane przez Wykonawcę mogą podlegać procedurze kontroli przez Wykonawcę i Zamawiającego na obecność oprogramowania złośliwego.
29. Wszystkie informatyczne nośniki danych wielokrotnego zapisu przekazane przez Wykonawcę i użyte w systemach informatycznych Straży Granicznej i innych, muszą pozostać u administratora systemu. Zwrot nośników może nastąpić dopiero po usunięciu wszystkich informacji zawartych na nośniku przez administratora systemu. W przypadku niemożliwości usunięcia informacji nośniki nie zostają zwrócone.
30. Jeżeli w ramach realizacji umowy wyniknie potrzeba dostępu do systemów teleinformatycznych Straży Granicznej, pracownicy Wykonawcy muszą uzyskać zgodę gestora (kierownika jednostki organizacyjnej lub osoby upoważnionej) przedmiotowego systemu. Dostęp do tych systemów będzie realizowany zgodnie z przyjętymi procedurami, politykami, oraz instrukcjami bezpieczeństwa, z którymi w niezbędnym zakresie zostanie zapoznany Wykonawca.
31. Zabrania się kopiowania jakichkolwiek informacji z systemów Straży Granicznej i wynoszenie ich poza miejsce zainstalowania systemów teleinformatycznych, bez zgody Zamawiającego.
32. Zabrania się wynoszenia wszelkich elementów wchodzących w skład systemu teleinformatycznego (zwłaszcza informatycznych nośników danych).
33. Jeżeli w ramach realizacji umowy wyniknie potrzeba przeprowadzenia kontroli poprawności działania systemu, Wykonawca zobowiązany jest przeprowadzić testy wykorzystując wprowadzone i przygotowane przez siebie dane testowe. Użycie systemów i programów przy wykorzystaniu danych rzeczywistych może odbywać się wyłącznie na terenie obiektów Straży Granicznej i za zgodą Zamawiającego.
34. Informacje (w tym informacje niejawne, dane osobowe, inne informacje prawnie chronione) mogą być udostępniane Wykonawcy i przetwarzane przez niego tylko na terenie obiektów Straży Granicznej lub w miejscach, w których są one przetwarzane przez Straży Granicznej.
35. Udostępnianie przez Wykonawcę innym podmiotom (np. podwykonawcom) informacji związanych z wykonaniem umowy i podlegających ochronie, może odbywać się wyłącznie za zgodą Zamawiającego.
36. Pracownicy Wykonawcy zobowiązani są do poinformowania Straży Granicznej o sytuacjach mogących naruszać przepisy ustawy o ochronie informacji niejawnych, danych osobowych oraz zapisy niniejszej Instrukcji Bezpieczeństwa Przemysłowego.
37. W przypadku naruszenia przepisów o ochronie informacji niejawnych, danych osobowych, innych dot. informacji prawnie chronionych oraz zapisów niniejszej Instrukcji Bezpieczeństwa Przemysłowego, Zamawiający i Wykonawca podejmą działania zmierzające do wyjaśnienia okoliczności naruszenia oraz



spowodują właściwe zabezpieczenie materialnych śladów działania lub jego zaniechania, które były związane ze zdarzeniem.

38. W przypadku niewykonania lub nienależytego wykonania obowiązków wynikających z ustaw o ochronie informacji niejawnych, danych osobowych, nieprzestrzegania wymagań określonych niniejszą Instrukcją Bezpieczeństwa Przemysłowego, Zamawiający ma prawo rozwiązać umowę z winy Wykonawcy, a powstałe z tego faktu skutki finansowe i prawne obciążą Wykonawcę.
39. Wykonawca, pracownicy Wykonawcy, mający dostęp do informacji (w tym informacji niejawnych, danych osobowych, innych informacji prawnie chronionych) Zamawiającego, zobowiązani są zarówno podczas realizacji umowy, jak również po jej zakończeniu lub odstąpieniu od jej wykonania, do:
- a) zapewnienia ochrony i bezpieczeństwa wszelkich informacji uzyskanych od Zamawiającego lub wytworzonych w związku z realizacją umowy, zgodnie z obowiązującymi przepisami prawa oraz na warunkach i zasadach określonych w niniejszej Instrukcji Bezpieczeństwa Przemysłowego,
  - b) zachowania poufności informacji, w których posiadanie wejdzie w trakcie realizacji umowy,
  - c) niewykorzystywania informacji do innych celów niż wykonywanie czynności wynikających z umowy,
  - d) zapewnienia kontroli nad tym, jakie informacje, kiedy i przez kogo oraz komu zostały przekazywane,
  - e) zachowania w tajemnicy informacji i sposobów ich zabezpieczenia, również po zakończeniu umowy,
  - f) nie ujawniania informacji związanych z wykonaniem umowy osobom nieupoważnionym,
  - g) umożliwienia Zamawiającemu, przeprowadzania kontroli stanu ochrony informacji udostępnionych lub wytworzonych w związku z realizacją umowy.
40. Wszyscy pracownicy Wykonawcy mający dostęp do informacji udostępnionych w ramach realizacji umowy są zobowiązani do zapoznania się oraz przestrzegania zasad i postanowień zawartych w niniejszej Instrukcji Bezpieczeństwa Przemysłowego.
41. Ochronie podlegają także wszystkie pozostałe informacje, nieoznaczone żadną klauzulą tajności, a objęte ochroną innymi przepisami.
42. Materiały jawne i materiały niejawne podlegające ochronie nie mogą być wykorzystywane do żadnych innych celów niż te, które określono w umowie. Zabrania się wykorzystywania tych materiałów, w tym do celów propagandowych oraz prezentowania ich w mediach bez wiedzy i zgody Zamawiającego.
43. Wykaz informacji niejawnych, do których Wykonawca może mieć dostęp lub, które mogą być wytworzone przez Wykonawcę podczas realizacji umowy. Zamawiający zastrzega sobie prawo do zmiany lub rozszerzenia listy dokumentów lub spraw zawartych w wykazie. Zmiana w tym zakresie nie będzie wymagała podpisania aneksu do umowy.

L.p.	Nazwa dokumentu lub sprawy	Maksymalna klauzula tajności
1.		
2.		

3.		
----	--	--

44. Wykonawca ma obowiązek niezwłocznego informowania Zamawiającego, o naruszeniu przepisów o ochronie informacji niejawnych przez pracowników Wykonawcy, zgodnie z Art.71 ust.5 pkt.1 Ustawy.
45. Zamawiający ma prawo postawić dodatkowe warunki w zakresie ochrony informacji niejawnych, danych osobowych i innych informacji prawnie chronionych, wynikające ze zmiany obowiązujących przepisów.
46. Wykonawca zaakceptuje wymagania określone w niniejszej Instrukcji Bezpieczeństwa Przemysłowego poprzez podpisanie umowy.
47. Ustalenia zawarte w niniejszej Instrukcji Bezpieczeństwa Przemysłowego dotyczą wszystkich osób, które w imieniu Wykonawcy będą wykonywały umowę, w tym także podwykonawców – jeśli ich wykonywanie umowy wiąże się z dostępem do informacji niejawnych, danych osobowych, innych informacji prawnie chronionych Zamawiającego. Wykonawca zobowiązuje się zawrzeć analogiczne postanowienia w umowach zawieranych z podwykonawcami, zgodnie z Art.54 ust.6 Ustawy.

Wykonał: Andrzej Pindor  
tel.: +48 500 40 44  
Dnia: .....r.



pieczęć Wykonawcy

**ZOBOWIĄZANIE**  
**do oddania do dyspozycji niezbędnych zasobów na potrzeby wykonania**  
**(dotyczy części 2 zamówienia)**

1. Ja(/My) niżej podpisany(/ni) .....  
(imię i nazwisko składającego oświadczenie)

będąc upoważnionym(/mi) do reprezentowania:

.....  
(nazwa i adres podmiotu oddającego do dyspozycji zasoby)

**oświadczam(y),**

że wyżej wymieniony podmiot, stosownie do art. 22a ustawy z dnia 29 stycznia 2004 r. –  
Prawo zamówień publicznych (Dz. U. z 2015 r., poz. 2164 z późn. zm.), odda Wykonawcy:

.....  
(nazwa i adres Wykonawcy składającego ofertę)

do dyspozycji w trakcie realizacji zamówienia niezbędne zasoby<sup>1)</sup> .....

.....  
(zakres udostępnianych zasobów)

na potrzeby wykonania niżej wymienionego zamówienia:

**„Rozbudowa systemu telekomunikacyjnego Straży Granicznej”**  
**– numer sprawy 14/BF/BŁil/17**

2. Sposób wykorzystania ww. zasobów przez Wykonawcę przy wykonywaniu zamówienia:<sup>2)</sup>

3. Charakteru stosunku, jaki będzie łączył nas z Wykonawcą:<sup>3)</sup>

**Niniejsze oświadczenie potwierdza ww. okoliczności na dzień składania ofert.**

.....  
(miejsce i data złożenia oświadczenia)

.....  
(pieczęć i podpis osoby uprawnionej do  
składania oświadczeń woli w imieniu podmiotu  
oddającego do dyspozycji zasoby)

- <sup>1)</sup> Zakres udostępnianych zasobów osobowych niezbędnych do potwierdzenia spełnienia warunku udziału w postępowaniu:  
– 1 inżynier producenta urządzeń ze stopniem certyfikacji co najmniej Cisco Certified Internetwork Expert – CCIE – CCIE Routing&Switching lub równoważnym,  
– 1 inżynier producenta ze stopniem certyfikacji dla bezpieczeństwa co najmniej Cisco Certified Internetwork Expert – CCIE Security lub równoważnym,  
– 1 inżynier producenta ze stopniem certyfikacji co najmniej Cisco Certified Internetwork Expert – CCIE Voice lub równoważnym  
W punkcie 1 należy określić która(e) z ww. osób zostaną udostępnione Wykonawcy do realizacji zamówienia.
- <sup>2)</sup> np. podwykonawstwo. Z uwagi na okoliczność, że przedmiotem udostępnienia są zasoby nierozzerwalnie związane z podmiotem ich udostępniającym, niemożliwe do samodzielnego obrotu i dalszego udzielenia ich bez zaangażowania tego podmiotu w wykonanie zamówienia, powyższe zobowiązanie powinno zawierać wyraźne nawiązanie do uczestnictwa tego podmiotu w wykonaniu zamówienia.
- <sup>3)</sup> np. umowa przedwstępna, umowa o podwykonawstwo, umowa o współpracy, porozumienie pomiędzy pracodawcami o delegowaniu pracowników w celu wykonywania pracy u Wykonawcy itp.



Oświadczenia zawarte w Załącznikach nr 5 – 7 do niniejszej SIWZ  
winny być złożone przez Wykonawcę wyłącznie na wezwanie  
Zamawiającego (zgodnie z treścią Rozdziału VIII pkt 2 SIWZ)

(pieczęć Wykonawcy)

## OŚWIADCZENIE

Ja (my), niżej podpisany(ni) .....

działając w imieniu i na rzecz: .....

.....  
(pełna nazwa i adres siedziby Wykonawcy)

w związku z udziałem w postępowaniu o udzielenie zamówienia publicznego pn:

**„Rozbudowa systemu telekomunikacyjnego Straży Granicznej” -  
numer sprawy 14/BF/BŁii/17**

oświadczamy, że nie orzeczono wobec naszej firmy tytułem środka zapobiegawczego zakazu ubiegania się o zamówienie publiczne.

....., dn. ....

.....  
(podpis osób/osoby uprawnionej do reprezentacji Wykonawcy  
i składania oświadczeń woli w jego imieniu)

(pieczęć Wykonawcy)

## OŚWIADCZENIE

Ja (my), niżej podpisany(ni) .....

działając w imieniu i na rzecz: .....

.....  
(pełna nazwa i adres siedziby Wykonawcy)

w związku z udziałem w postępowaniu o udzielenie zamówienia publicznego pn:

**„Rozbudowa systemu telekomunikacyjnego Straży Granicznej”**

– numer sprawy 14/BF/BŁil/17

oświadczam(y), że:

(należy zaznaczyć/wypełnić odpowiednie pole poniżej)

- wobec naszej firmy **nie wydano** prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne

wobec naszej firmy **wydano**

- prawomocny wyrok sądu** o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne.

Wobec powyższego w załączeniu składam dokumenty potwierdzające dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami/dokumenty potwierdzające zawarcie wiążącego porozumienia w sprawie spłat tych należności.

- ostateczną decyzję administracyjną** o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne.

Wobec powyższego w załączeniu składam dokumenty potwierdzające dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami/dokumenty potwierdzające zawarcie wiążącego porozumienia w sprawie spłat tych należności.

....., dn. ....

.....  
(podpis osób/osoby uprawnionej do reprezentacji  
Wykonawcy i składania oświadczeń w jego imieniu)





pieczęć Wykonawcy

### WYKAZ OSÓB,

które zostaną skierowane przez Wykonawcę do realizacji zamówienia odpowiedzialnych za świadczenie usługi wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia, a także zakresu wykonywanych przez nie czynności oraz z informacją o podstawie do dysponowania tymi osobami

1. Ja (My), niżej podpisany (i).....  
działając w imieniu i na rzecz .....

.....  
w odpowiedzi na ogłoszenie o przetargu nieograniczonym pn.: „Rozbudowa systemu telekomunikacyjnego Straży Granicznej” - numer sprawy 14/BF/BŁil/17- oświadczamy, że dysponujemy lub będziemy dysponować inżynierami Network Consulting Engineer Cisco Advanced Services, którzy będą odpowiedzialni w trakcie realizacji zamówienia za świadczenie wsparcia technicznego dla systemu telekomunikacyjnego Straży Granicznej, posiadającymi wymagane przez Zamawiającego kwalifikacje zawodowe:

Lp.	Imię i nazwisko	Minimalne wymagane kwalifikacje (certyfikaty)	Rodzaj posiadanych kwalifikacji (certyfikatów) <sup>2),3)</sup>	Wystawca i data ważności certyfikatu	Informacja o podstawie do dysponowania osobą <sup>4)</sup>
1.		Cisco Certified Internetwork Expert – <b>CCIE Routing&amp;Switching</b> lub równoważny <sup>1)</sup>			
2.		Cisco Certified Internetwork Expert – <b>CCIE Security</b> lub równoważny <sup>1)</sup>			
3.		Cisco Certified Internetwork Expert – <b>CCIE Voice</b> lub równoważny <sup>1)</sup>			
4.					

1) Poprzez pojęcie „certyfikat równoważny” Zamawiający rozumie certyfikat analogiczny co do zakresu z przykładowymi certyfikatami wskazanymi z nazwy dla danej roli, co jest rozumiane jako: analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat; analogiczny stopień poziomu kompetencji; analogiczny poziom doświadczenia wymaganego do otrzymania danego certyfikatu; certyfikat potwierdzony jest egzaminem (dotyczy przypadku certyfikatów, które muszą być potwierdzone egzaminem); autoryzowany przez producenta urządzeń posiadanych przez Zamawiającego.

2) Zamawiający dopuszcza również do realizacji zamówienia osoby legitymujące się nowszymi odpowiednikami wymaganych certyfikatów.

3) Osoba posiadająca certyfikat, który utraci ważność w okresie realizacji zamówienia jest zobowiązana do ponownego przedstawienia Zamawiającemu ważnego certyfikatu.

4) należy określić tytuł prawny do dysponowania osobami zdolnymi do wykonania zamówienia wskazanymi w tabeli powyżej, tj. należy określić czy jest to:

– dysponowanie bezpośrednie (oznaczające stosunek prawny istniejący bezpośrednio pomiędzy Wykonawcą i osobą (osobami) wskazanymi w zestawieniu powyżej) i jeśli tak to jaki jest charakter prawny tego stosunku (np. umowa o pracę, umowa o świadczenie usług, umowa przedwstępna, samozatrudnienie się osoby fizycznej prowadzącej działalność gospodarczą itp.)

lub

– dysponowanie pośrednie na podstawie załączonego do oferty zobowiązania podmiotu trzeciego do oddania do dyspozycji Wykonawcy osoby/osób zdolnych do wykonania zamówienia wskazanych w tabeli powyżej.

2. Ponadto oświadczamy, że wskazani przez nas inżynierowie będą mieli bezpośredni dostęp do wewnętrznych baz danych producenta oraz do ekspertów technicznych w celu zapewnienia skutecznej diagnostyki sieci oraz szybkiej reakcji na awarie, a w szczególności będą posiadać:
  - a) bezpośredni dostęp do zasobów stanowiących własność intelektualną producenta. Zakres dostępu musi obejmować co najmniej wewnętrzną bazę wiedzy producenta na temat konfiguracji, wewnętrzną bazę danych na temat błędów w oprogramowaniu, bazę wiedzy producenta (Technical Knowledge Library),
  - b) możliwość bezpośredniej zmiany priorytetów i kolejowania zgłoszeń serwisowych,
  - c) dostęp pozwalający na uzupełnianie i zmianę numerów seryjnych urządzeń w bazach danych producenta
3. Potwierdzamy również, że wskazani przez nas inżynierowie będą wykonywać w ramach realizacji zamówienia m. in. następujące czynności:
  - a) szczegółową analizę i pomoc w rozwiązywaniu zgłoszeń serwisowych dotyczących awarii oraz włamań do systemu;
  - b) prowadzić analizę trendów zgłoszeń serwisowych w oparciu o dane zawarte w systemie producenta;
  - c) prowadzić analizę błędów oraz wartości parametrów obciążenia poszczególnych elementów sieci;
  - d) przygotowywać zalecenia konfiguracyjne dla administratorów Straży Granicznej w celu optymalizacji pracy sieci pod względem wydajności i niezawodności;
  - e) prowadzić analizę sieci pod kątem bezpieczeństwa oraz przygotowywanie zaleceń konfiguracyjnych dla administratorów Straży Granicznej w celu poprawy bezpieczeństwa sieciowego;
  - f) prowadzić wewnętrzne szkolenia dla administratorów Straży Granicznej o tematyce związanej z rozwiązaniami stosowanymi w sieci Straży Granicznej, przy czym ww. szkolenia będą prowadzone w Centralnym Węźle Teletransmisyjnym Straży Granicznej dla wskazanej przez Zamawiającego grupy inżynierów;
  - g) realizować inne zleczone przez Zamawiającego bieżące zadania projektowe i diagnostyczne systemu telekomunikacyjnego Straży Granicznej w ramach ustalonego czasu pracy.
4. Potwierdzamy również, że wskazane powyżej osoby będą porozumiewać się biegle w języku polskim w mowie i w piśmie.
5. Oświadczamy również, że wskazane powyżej osoby będą posiadać:
  - poświadczenie bezpieczeństwa lub pisemne upoważnienie do dostępu do informacji niejawnych o klauzuli tajności „zastrzeżone” wydane przez kierownika jednostki organizacyjnej Wykonawcy, jeżeli osoba nie posiada poświadczenia bezpieczeństwa,
  - zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych i ochrony danych osobowych..

....., dn. ....

.....  
(pieczętka i podpis upoważnionego przedstawiciela Wykonawcy)