# Załącznik nr 1 do Umowy – Opis Przedmiotu Zamówienia

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Zakup usług transmisji danych dla jednostek organizacyjnych prokuratury.

**Definicje:**

Ilekroć mowa o:

1. **Aktualizacji** - są to wszystkie nowe wersje Oprogramowania systemowego, (update/upgrade), patche i programy korekcji błędów, poprawki lub inne zmiany, udostępniane przez Wykonawcę/producenta w ramach Umowy bez dodatkowych opłat oraz w okresie trwania Umowy wraz z opracowaną do nich dokumentacją w zakresie powyższych zmian.
2. **Awarii**, rozumie się przez to okres przerwy w świadczeniu Usługi transmisji danych trwający od chwili wykrycia przez Wykonawcę lub dokonania zgłoszenia przez Zamawiającego, do przywrócenia świadczenia usługi;
3. **Braku Dostępności Usługi**, rozumie się przez to Awarię lub Usterkę; w przypadku występowania wielości Awarii lub Usterek w krótkich odstępach czasu, brakiem dostępności Usługi są również okresy pomiędzy nimi;
4. **Czasie Reakcji**, rozumie się przez to okres od wykrycia przez Wykonawcę lub zgłoszenia przez Zamawiającego Braku Dostępności Usługi do podjęcia przez Wykonawcę działań naprawczych;
5. **Czasie Naprawy**, rozumie się przez to okres od wykrycia przez Wykonawcę lub zgłoszenia przez Zamawiającego Braku Dostępności Usługi do przywrócenia świadczenia Usługi;
6. **DDoS - (ang. Distributed Denial of Service)** rozumie się przez toatak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów
7. **Dniach Roboczych**, rozumie się przez to każdy dzień od poniedziałku do piątku
z wyłączeniem dni ustawowo wolnych od pracy.
8. **Dokumentacji Powykonawczej i Dokumentacji Administracyjnej /Dokumentacja** – oznacza dokumentację przygotowaną przez Wykonawcę i dostarczoną Zamawiającemu w ramach realizacji Umowy spełniająca wymagania na produkt typu Dokument.
9. **Dzierżawa ciemnych włókien** - usługa, która polega na tym, że Zamawiający otrzymuje do dyspozycji włókna światłowodowe, na których może realizować dowolną transmisję, bez jakiejkolwiek ingerencji ze strony Wykonawcy;
10. **Gwarantowanej Dostępności Usługi -** gwarantowana przez Wykonawcę, określona procentowo w Rozdziale IV ust 1 pkt 2), liczba godzin w ciągu miesiąca kalendarzowego podczas których Wykonawca zapewnia działanie Łącza bez wystąpienia Braku Dostępności Usługi. Parametr ten wynosi 99,44% dla Lokalizacji POPD PK, ZOPD MS, OPDR oraz 98,88% miesięcznie dla pozostałych Lokalizacji liczony według wzoru: {[(liczba godzin w danym miesiącu kalendarzowym) – (suma wszystkich czasów Braku Dostępności Usługi)]/(liczba godzin w danym miesiącu kalendarzowym)}\*100%
11. **Harmonogramie** –oznacza dokument, przygotowany przez Wykonawcę, potwierdzony podpisem przez Koordynatora Zamawiającego i Wykonawcy, określający poszczególne terminy wykonania Przedmiotu Umowy, spełniający wymagania na produkt typu Dokument określone w Załączniku nr 1 do Umowy.
12. **IP** - protokół transmisji danych używany przez systemy informatyczne (ang. Internet Protocol),
13. **Kanalizacji Kablowej / Kanalizacji Teletechnicznej** – należy przez to rozumieć ciąg rur osłonowych i związanych z nimi pomieszczeń podziemnych (w szczególności studni i zasobników kablowych) dla kabli i ich złączy oraz urządzeń telekomunikacyjnych;
14. **Kanalizacji Wtórnej** - oznacza Kanalizację Kablową umieszczona w innej Kanalizacji Kablowej (Kanalizacji Pierwotnej), stanowiącą dodatkowe zabezpieczenie kabli telekomunikacyjnych
15. **Koordynatorach Stron** - oznaczają osoby wyznaczone przez każdą ze Stron do roboczych kontaktów i koordynowania procesu wykonania Umowy
16. **LAN** - lokalna sieć transmisji danych obejmująca swym zasięgiem pojedynczą jednostkę Zamawiającego (ang. Local Area Network),
17. **Lokalizacji**, rozumie się przez to adres zakończenia Łącza transmisji danych wskazany w Załączniku nr 2;
18. **Łączach dostępowych**, rozumie się przez to Podstawowe i/lub Zapasowe Łącze Dostępowe;
19. **Migracji** – oznacza przeniesienie obecnie eksploatowanej usługi transmisji danych sieci WAN-PROK w danej Lokalizacji do udostępnianej Usługi typu A z zachowaniem możliwości transmisji danych pomiędzy Lokalizacjami w których nastąpiła Migracja oraz Lokalizacjami w których Migracja nie nastąpiła do momentu zakończenia Migracji w ostatniej z Lokalizacji funkcjonującej w obecnie eksploatowanej usłudze transmisji danych sieci WAN-PROK.
20. **Monitorowaniu Łączy**, rozumie się przez to ogół czynności technicznych polegających na weryfikacji parametrów SLA;
21. **Oknie Serwisowym**, rozumie się przez to uzgodniony z Zamawiającym przedział czasu przeznaczony na wykonywanie prac konserwacyjno-modernizacyjnych w sieci Wykonawcy mogących skutkować brakiem dostępu Zamawiającego do Usługi transmisji danych; przerwy w dostarczaniu Usługi spowodowane oknami serwisowymi Zamawiający traktuje, jako zachowanie ciągłości Usługi;
22. **QoS** - parametry definiujące wymagania jakościowe względem łączy telekomunikacyjnych realizowane przez: kształtowanie ruchu, ograniczanie przepustowości, nadawanie priorytetów, zarządzanie parametrami jakościowymi, unikanie przeciążeń w sieci, itp. (ang. Quality of Service),
23. **Oprogramowaniu** – oznacza oprogramowanie narzędziowe lub systemowe wchodzące w skład Urządzeń CE, SMW, SMZ.
24. **OPZ**, rozumie się przez to Załącznik nr 1 do Umowy,
25. **Pasmo transmisyjne IP** - dostępna dla Zamawiającego przepustowość łącza wyrażona w kbps lub Mbps, określająca szybkość przesyłania danych w ramach świadczonej usługi transmisji danych mierzona w warstwie 2 modelu ISO/OSI,
26. **Planie Testów** – dokument określający szczegółowy zakres i harmonogram Testów Usługi.
27. **Podstawowym łączu dostępowym (Łącze podstawowe)** - łącze transmisji danych, które pozwala na połączenie lokalizacji Zamawiającego z węzłem dostępowym sieci transmisji danych Wykonawcy. Łącze to musi być zakończone w każdej lokalizacji Zamawiającego urządzeniem dostępowym (CE) oraz ewentualnie innymi urządzeniami niezbędnymi do realizacji łącza (np.: modemy kablowe, multipleksery, itp.),
28. **Projekcie** – realizowana Umowa zawarta pomiędzy Zamawiającym i Wykonawcą.
29. **Projekcie Technicznym** – dokument określający sposób realizacji Przedmiotu Umowy, opracowany przez Wykonawcę, dostarczony Zamawiającemu w wersji elektronicznej na dowolnym standardowym nośniku optycznym lub pendrive lub za pośrednictwem poczty elektronicznej w postaci edytowalnych zbiorów (doc lub docx).
30. **Routerze PE** – router brzegowy sieci Wykonawcy umieszczony w węźle sieci Wykonawcy, do którego dołączone jest urządzenie dostępowe (CE) za pomocą łącza dostępowego,
31. **Scenariuszach testowych** – oznacza scenariusze Testów, opracowane przez Wykonawcę i zatwierdzone przez Zamawiającego.
32. **SLA**, rozumie się przez to parametry określające niezawodność i jakość Usługi transmisji danych określone w Rozdziale IV Załącznika nr 1 do Umowy (*ang. Service Level Agreement*);
33. **System Monitorowania i Weryfikacji Jakości Świadczonych Usług Zamawiającego (SMZ)** – sprzęt i oprogramowanie dostarczone przez Wykonawcę w ramach realizacji umowy o funkcjonalnościach wyszczególnionych w OPZ w celu monitorowania udostępnionej sieci transmisji danych dla Usługi.
34. **System Monitorowania Sieci Wykonawcy (SMW)** – rozwiązanie służące monitorowaniu udostępnionej sieci Wykonawcy o funkcjonalnościach wyszczególnionych w OPZ zarządzane i utrzymywane przez Wykonawcę
35. **System Monitorowania i Korelacji Logów (SML)** – rozwiązanie służące gromadzeniu, przeszukiwaniu i korelacji logów z urządzeń utrzymujących odpowiedni poziom zabezpieczeń w ramach Usługi. Rozwiązanie posiadane przez Zamawiającego oparte na produkcie Splunk.
36. **Testach** – oznacza Testy funkcjonalne i Testy akceptacyjne opisane w Rozdziale X, potwierdzające wykonanie Przedmiotu Umowy.
37. **Usłudze/Usłudze TD**, rozumie się przez to zapewnienie Zamawiającemu możliwości transmisji danych o parametrach SLA w oparciu o zestawione i utrzymywane przez Wykonawcę łącza dostępowe w ramach Usługi wraz z niezbędnymi urządzeniami teletransmisyjnymi;
38. **Usterce**, rozumie się przez to okres obniżenia parametrów Usługi poniżej SLA, trwający od chwili wykrycia przez Wykonawcę lub dokonania zgłoszenia przez Zamawiającego, do przywrócenia świadczenia Usługi;
39. **Urządzeniu, Urządzeniu dostępowym, Routerze CE –** urządzenie/a w lokalizacji Zamawiającego, dostarczone, zainstalowane we wskazanym przez Zamawiającego miejscu i zarządzane przez Wykonawcę. Urządzenie to stanowi zakończenie łącza dostępowego oraz udostępnia interfejs przyłączeniowy lub interfejsy przyłączeniowe zapewniające podłączenie do urządzeń i sieci lokalnej Zamawiającego oraz realizuje funkcjonalności opisane w OPZ,
40. **Użytkowniku,** rozumie się przez to Zamawiającego i jednostki Zamawiającego wskazane w Załączniku nr 2 - adresy miejsca instalacji łączy oraz przepustowość;
41. **WAN** - rozległa sieć transmisji danych Wykonawcy obejmująca swym zasięgiem wszystkich zdefiniowanych Umową Użytkowników Zamawiającego (ang. Wide Area Network),
42. **Włóknach Światłowodowych** rozumie się przez to pojedyncze światłowody jednomodowe z nieprzesuniętą dyspersją G.652D (typ włókna światłowodowego zoptymalizowanego dla transmisji fali o długości 1310 nm, mogącego być również użyty dla transmisji fali o długości 1550 nm), służące do przesyłania promieniowania świetlnego w kablu światłowodowym; Zamawiający wymaga aby dostarczone włókna światłowodowe były realizowane jako tzw. ciemne włókna bez jakichkolwiek ograniczeń w szybkości transmisji danych i rodzaju obsługiwanych protokołów komunikacyjnych;
43. **VPN** - struktura logiczna sieci kreowana w ramach fizycznej infrastruktury sieci rozległej Wykonawcy, zapewniająca możliwości zestawiania połączeń pomiędzy użytkownikami sieci transmisji danych w warstwie trzeciej modelu OSI (ang. Virtual Private Network),
44. **Zapasowym łączu dostępowym (Łącze zapasowe)** - łącze transmisji danych, które pozwala na połączenie lokalizacji Zamawiającego z węzłem dostępowym sieci transmisji danych Wykonawcy. Łącze to musi być zakończone w każdej lokalizacji Zamawiającego urządzeniem dostępowym (CE) w przypadku wymagania jego realizacji w układzie 2PE-2CE lub może być zakończone na urządzeniu dostępowym CE razem z Łączem podstawowym w przypadku jego realizacji w układzie 2PE-1CE oraz ewentualnie innymi urządzeniami niezbędnymi do realizacji łącza (np.: modemy kablowe, multipleksery, itp.),
45. **2PE-2CE** – układ niezwodnościowy pracy instalowanych w Lokalizacjach Routerów CE oraz Routerów PE w którym dwa Routery CE w Lokalizacji podłączone są do dwóch różnych Routerów PE Wykonawcy i udostępniają wspólny wirtualny interfejs w kierunku sieci LAN Zamawiającego.
46. **2PE-1CE** - układ niezwodnościowy pracy instalowanych w Lokalizacjach Routerów CE oraz Routerów PE w którym Router CE w Lokalizacji podłączony jest do dwóch różnych Routerów PE Wykonawcy.
47. **DC** – centrum przetwarzania danych w POPD i ZOPD
48. **Rozproszone DMZ** – podsieci w prokuraturach okręgowych i regionalnych udostępniające usługi w sieci Internet.
49. **POPD PK** – Podstawowy ośrodek przetwarzania danych
50. **ZOPD PK** – Zapasowy ośrodek przetwarzania danych

1. **Zakres świadczonych usług**
2. Zamawiający wymaga uruchomienia Usługi transmisji danych zapewniającej komunikację pomiędzy wszystkimi lokalizacjami Zamawiającego oraz umożliwiającej dostęp do sieci Internet ( za pomocą centralnych dwóch punktów styku z siecią Internet w POPD i ZOPD) dla wszystkich jednostek organizacyjnych prokuratury. Zamawiający wymaga utworzenia odseparowanego VRF w zasobach Wykonawcy przeznaczonego na realizację Usługi. Wszystkie jednostki organizacyjne prokuratury wskazane w *Załączniku nr 2 do Umowy - adresy miejsca instalacji łączy oraz przepustowość* będą posiadać możliwość korzystania z Usługi.



Rysunek 1 – Schemat topologii sieci

1. Zakres świadczonych usług został opisany w §2 Umowy.
	1. **Wymagania ogólne na Produkty typu Dokument**
2. Zamawiający wymaga, aby wszystkie dokumenty tworzone w ramach realizacji przedsięwzięcia charakteryzowały się wysoką jakością, na którą będą miały wpływ, takie czynniki jak:
	* 1. Struktura dokumentu, rozumiana jako podział danego dokumentu na rozdziały, podrozdziały i sekcje, w czytelny i zrozumiały sposób;
		2. Zachowanie standardów dokumentowania, a także sposób pisania, rozumianych jako zachowanie spójnej struktury, formy i sposobu pisania dla poszczególnych dokumentów oraz fragmentów tego samego dokumentu;
		3. Kompletność dokumentu, rozumiana jako pełne, bez wyraźnych, ewidentnych braków przedstawienie omawianego problemu obejmujące całość z danego zakresu rozpatrywanego zagadnienia;
		4. Spójność i niesprzeczność dokumentu, rozumianych jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumencie, jak i brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach oraz we fragmentach tego samego dokumentu.
3. Dostarczone dokumenty muszą być opracowane w języku polskim, w wersji elektronicznej w niezabezpieczonym/edytowalnym formacie Word, PDF (na płycie CD-ROM lub innym równoważnym nośniku danych) i drukowanej (papierowej), co najmniej w 3 egzemplarzach (dopuszcza się inne formaty zapisu dokumentacji lub formaty wektorowe jak DWG, DXF, należy jednak dołączyć przeglądarkę obsługującą wykorzystane formaty). Dopuszczalne jest dostarczenie dokumentacji technicznej urządzeń oraz oprogramowania systemowego w języku angielskim, o ile producent nie dostarcza jej w wersji polskiej.
4. Harmonogramy należy dostarczyć jako wykresy Gantta w formacie MPP lub w formacie XLS umożliwiającym import do MS Project.
5. Całość dostarczanych w ramach niniejszego projektu dokumentów musi:
	* 1. być wersjonowana (oznaczona numerem wersji oraz datą wytworzenia),
		2. posiadać wskazanego autora,
		3. posiadać krótkie streszczenie kierownicze,
		4. dla plików \*.pdf. \*.rtf oraz \*.doc (\*.docx) musi być zapisana w sposób pozwalający na wyszukiwanie w niej dowolnej frazy.
	1. **Opracowanie Dokumentu Inicjującego Projekt**

Wykonawca zobowiązany jest do przygotowania Dokumentu Inicjującego Projekt (DIP) obejmującego co najmniej:

1. Organizację projektu (strukturę organizacyjną po obu stronach, role, obsadę ról przez osoby).
2. Definicję produktów Projektu.
3. Strategię realizacji wdrożeń Usług TD we wskazanych w *Załączniku nr 2* do *Umowy* lokalizacjach Zamawiającego objętych wdrożeniem.
4. Harmonogram realizacji projektu uwzględniający zapisy niniejszego OPZ oraz uwzględniający strategię wdrożenia Usług w tym Urządzeń CE we wszystkich lokalizacjach Zamawiającego objętych projektem.
5. Harmonogram musi zawierać terminy realizacji zobowiązań Wykonawcy wynikających z Umowy, w tym opracowanie projektu i scenariuszy testów, harmonogramu dostaw, instalacji, konfiguracji, testów z uwzględnieniem miejsc lokalizacji Zamawiającego, odbioru przedmiotu Umowy, przeprowadzenie Szkoleń, z uwzględnieniem wszelkich terminów zastrzeżonych w zakresie procedury odbioru dla Zamawiającego lub Wykonawcy.
6. Komunikację w projekcie (spotkania Kierowników projektów, przepływ informacji w projekcie, raportowanie).
7. Zarządzanie ryzykiem w projekcie (w tym analizę ryzyka aktualizowaną przynajmniej raz w miesiącu).
	1. **Opracowanie Projektu Technicznego**
8. Projekt Techniczny musi być wykonany zgodnie z wymaganiami Produktu typu Dokument.
9. Wykonawca w terminie określonym w zatwierdzonym harmonogramie przedstawi Projekt Techniczny Usługi który musi zawierać co najmniej:
	1. wprowadzenie opisujące cele i zakres przedmiotu zamówienia;
	2. ograniczenia rozwiązania, założenia i zależności;
	3. opis architektury fizycznej i logicznej udostępnianej sieci transmisji danych;
	4. opis zastosowanych technologii i protokołów telekomunikacyjnych;
	5. wykaz dostarczanych Urządzeń dostępowych i oprogramowania, zasady nazewnictwa urządzeń,
	6. opis instalacji dostarczanych urządzeń zawierający co najmniej:
		1. rozmieszczenie dostarczanych urządzeń w szafach dystrybucyjnych, udostępnionych przez Zamawiającego,
		2. schemat połączeń sieciowych LAN (przedstawiający topologię fizyczną i logiczną).
		3. wymagania na zasilanie dla instalowanych urządzeń,
		4. ilości i typy złączy elektrycznych wykorzystanych do zasilania,
		5. konfigurację oprogramowania.
	7. opis instalacji dostarczanego SMZ udostępnianej usługi transmisji danych,
10. rozmieszczenie dostarczanych Urządzeń w szafach dystrybucyjnych, udostępnionych przez Zamawiającego,
11. schemat połączeń sieciowych LAN/WAN (przedstawiający topologię fizyczną i logiczną).
12. wymagania na zasilanie dla instalowanych urządzeń,
13. ilości i typy złączy elektrycznych wykorzystanych do zasilania,
14. konfigurację oprogramowania oraz instrukcję użytkownika która będzie uaktualniana w trakcie realizacji projektu.
	1. adresację IP instalowanych Urządzeń która musi być uzgodniona z Zamawiającym,
	2. konfigurację QoS,
	3. konfigurację eksportu statystyk do SMZ i SMW,
	4. procedury instalacji urządzeń oraz zasady przeprowadzenia testów,
	5. rozwiązanie migracji z obecnie eksploatowanej sieci transmisji danych opisanej poniżej do Usługi będącej przedmiotem Umowy w tym procedury migracji lokalnych DMZ do rozwiązania docelowego,
	6. opis rozwiązania umożliwiający świadczenie usługi SOC ( dostęp do logów i systemów korelacji logów)
	7. opis rozwiązań/mechanizmów niezawodnościowych zastosowanych w POPD i ZOPD dla styku z siecią WAN i Internet
	8. słownik skrótów i pojęć.
	9. **Opis aktualnie eksploatowanej sieci transmisji danych**

Świadczona obecnie usługa transmisji danych składa się z sieci WAN-PROK oraz usługi umożliwiającej dostęp do sieci Internet dla wszystkich jednostek organizacyjnych prokuratury (Usługa A oraz Usługa B). Usługi są odseparowane logicznie w infrastrukturze Operatora.

Sieć WAN-PROK (Usługa A) składa się z dwóch warstw:

1. Warstwa pierwsza jest Siecią Operatora w oparciu o którą wykreowano prywatną sieć WAN w technologii IP VPN MPLS dla połączenia powszechnych jednostek organizacyjnych prokuratury. Topologia zbudowanej sieci umożliwia realizację połączeń pomiędzy lokalizacjami każdy z każdym. Sieć Operatora składa się z następujących elementów:
	1. routerów dostępowych CE które instalowane są w lokalizacjach powszechnych jednostkach organizacyjnych prokuratury. Zainstalowany w jednej lokalizacji, jeden router CE może obsługiwać kilka jednostek prokuratury mieszczących się w tej lokalizacji. Routery dostępowe CE są własnością Operatora i zarządzane są przez Operatora,
	2. routery brzegowe PE umieszczone są w węzłach sieci szkieletowej Operatora. Routery brzegowe PE są własnością Operatora i zarządzane przez Operatora,
	3. łączy dostępowych, które łączą router CE zainstalowany w lokalizacji Zamawiającego z routerem PE zainstalowanym w najbliższym węźle sieci szkieletowej Operatora,
	4. systemu monitorowania sieci Wykonawcy
	5. stacji monitorowania zainstalowanej w Prokuraturze Krajowej umożliwiającej kontrolę jakości usług świadczonych przez Operatora.
2. Warstwa druga, zapewnia bezpieczeństwo sieci WAN-PROK. Zbudowana jest w oparciu o Urządzenia Bezpieczeństwa umożliwiające połączenia przy zachowaniu wymaganego poziomu bezpieczeństwa sieci LAN danej jednostki prokuratury z routerem dostępowym CE. Urządzenia Bezpieczeństwa funkcjonujące w sieci WAN-PROK są własnością Zamawiającego i są przez niego administrowane i zarządzane.
3. Routing pomiędzy routerami PE-CE jest zgodny z protokołem eBGP.
4. Routery CE są własnością aktualnego Wykonawcy.
5. W przypadku gdy dana lokalizacja jest siedzibą kilku jednostek organizacyjnych (np. prokuratury regionalnej i prokuratury okręgowej) wówczas w tej lokalizacji jest tylko jeden router CE do którego podłączonych jest kilka urządzeń bezpieczeństwa Zamawiającego.
6. Routing pomiędzy routerami CE a urządzeniami bezpieczeństwa Zamawiającego jest routingiem statycznym. Istnieje możliwość uruchomienia routingu dynamicznego.
7. Pomiędzy routerami CE a urządzeniem bezpieczeństwa Zamawiającego zastosowana jest adresacja point-to-point. Szczegółowa adresacja zostanie przekazana Wykonawcy po podpisaniu umowy.
8. Wszystkie routery CE podlegają wewnętrznej polityce bezpieczeństwa Operatora, która uwzględnia m.in.:
9. bezpieczny dostęp przez konsolę,
10. bezpieczny dostęp przez VTY uwzględniający AAA + RSA (wyłącznie jeśli użytkownik ma mieć dostęp do CE),
11. enkrypcję haseł,
12. wyłączanie niewykorzystywanych serwisów,
13. włączone snmp traps,
14. baner przy logowaniu,
15. włączony NTP w celu dokładnych korelacji wydarzeń.

**IP VPN MPLS**

**Sieć**

**Szkieletowa**

**Operatora**

**Router CE**

**Operatora**

**Urządzenie**

**Bezpieczeństwa**

**Zamawiającego**

**Przełącznik LAN**

**Zamawiającego**

**VLAN**

**1**

**VLAN N**

**Lokalizacja L**

**1**

**Router CE**

**Operatora**

**Przełącznik LAN**

**Zamawiającego**

**VLAN**

**1**

**VLAN N**

**Lokalizacja Ln**

**Router PE**

**Operatora**

**Router PE**

**Operatora**

**Router PE**

**Operatora**

**Router CE**

**Operatora**

**Urządzenie**

**Bezpieczeństwa**

**Zamawiającego**

**Przełącznik LAN**

**Zamawiającego**

**VLAN N**

**VLAN**

**1**

**Lokalizacja Prokuratury Krajowej**

**Przełącznik LAN**

**Zamawiającego**

**Urządzenie**

**Bezpieczeństwa**

**Zamawiającego**

**Stacja**

**monitorowania**

**sieci Operatora**

Łącza dostępowe

**WAN**

**-**

**PROK**

**Sieć Operatora**

Rysunek 2 Architektura sieci WAN-PROK – Usługa A

Sieć umożliwiająca dostęp do sieci Internet (Usługa B) zbudowana jest analogicznie jak sieć WAN-PROK i również składa się z dwóch warstw:

1. Warstwa pierwsza jest Siecią Operatora w oparciu o którą wykreowano prywatną sieć WAN w technologii IP VPN MPLS w której powszechne jednostki organizacyjne prokuratury poprzez 2 odseparowane geograficznie punkty styku z siecią publiczną uzyskują dostęp do Internetu. Sieć Operatora składa się ze współdzielonych (logicznie) z siecią WAN-PROK elementów w postaci routerów CE oraz routerów PE.
2. Warstwa druga, zapewnia bezpieczeństwo sieci posiadającej dostęp do Internetu. Zbudowana jest w oparciu o Urządzenia Bezpieczeństwa zlokalizowane w punktach styku, lokalizacjach POPD PK, ZOPD MS, OPDR, OPDO, Prokuraturach Regionalnych oraz Prokuraturach Okręgowych. Urządzenia Bezpieczeństwa funkcjonujące w sieci posiadającej dostęp do Internetu są własnością Wykonawcy i są przez niego administrowane i zarządzane. Po zakończeniu realizacji projektu urządzenia nie przechodzą na własność Zamawiającego. W lokalizacjach prokuratur rejonowych nie ma zainstalowanych Urządzeń Bezpieczeństwa zaś kontrola ruchu dla tych lokalizacji odbywa się na poziomie punktów styku.



Rysunek 3 Architektura sieci Usługa B

1. Udostępnienie Usługi A oraz Usługi B realizowane jest na fizycznie różnych interfejsach Routera CE w danej Lokalizacji.
	1. **Warianty instalacji Routerów CE**
2. Ze względów organizacyjnych występują trzy przypadki umiejscowienia jednostek prokuratury w lokalizacjach:
	1. jedna jednostka prokuratury mieści się w jednej lokalizacji,
	2. dwie lub więcej jednostek prokuratury mieszczą się w jednej lokalizacji,
	3. jedna jednostka prokuratury mieści się w dwóch lub więcej lokalizacjach.
3. Zgodnie z umową podpisaną pomiędzy Zamawiającym a Operatorem Routery dostępowe CE zainstalowane są w każdej lokalizacji w której może być jedna lub kilka jednostek prokuratury.

W dalszej części przedstawionych zostanie pięć wariantów podłączenia urządzeń bezpieczeństwa (Zamawiającego w ramach Usługi A lub Wykonawcy w ramach Usługi B) do Routerów CE Wykonawcy. Zakłada się, że w wyjątkowych przypadkach mogą wystąpić odstępstwa od przedstawionych rozwiązań wariantowych.

Wariant 1 instalacji Routerów CE

1. W Wariancie 1 jedna jednostka prokuratury mieści się w jednej lokalizacji.
2. W tym przypadku do Routera Operatora CE dołączone jest jedno urządzenie bezpieczeństwa Zamawiającego dla Usługi A oraz dla lokalizacji POPD PK, ZOPD MS, OPDR, OPDO, Prokuraturach Regionalnych oraz Prokuraturach Okręgowych urządzenie bezpieczeństwa Wykonawcy dla Usługi B do którego będzie podłączony jeden lub kilka przełączników LAN.
3. W jednostce prokuratury na przełącznikach LAN może być utworzonych kilka sieci VLAN. Do sieci VLAN podłączane są serwery oraz stacje robocze. Zakłada się, że nie będzie zmieniana adresacja urządzeń dołączonych do sieci LAN (VLAN). Przełączniki dla Usługi A i Usługi B są fizycznie innymi urządzeniami.



Rysunek 4 Wariant 1 instalacji routerów CE Usługa A

* + 1. Wariant 2 instalacji Routerów CE
1. W Wariancie 2 dwie lub kilka jednostek prokuratury mieści się w jednej lokalizacji.
2. W tym przypadku do Routera CE dołączone są urządzenia bezpieczeństwa Zamawiającego dla Usługi A oraz dla lokalizacji POPD PK, ZOPD MS, OPDR, OPDO, Prokuraturach Regionalnych oraz Prokuraturach Okręgowych urządzenie bezpieczeństwa Wykonawcy dla Usługi B do których podłączone są jeden lub kilka przełączników LAN.
3. W każdej jednostce prokuratury na przełącznikach LAN może być utworzonych kilka sieci VLAN. Do sieci VLAN podłączane są serwery oraz stacje robocze. Zakłada się, że nie będzie zmieniana adresacja urządzeń dołączonych do sieci LAN (VLAN). Przełączniki dla Usługi A i Usługi B są fizycznie innymi urządzeniami.



Rysunek 5 Wariant 2 instalacji Routerów CE – Usługa A

* + 1. Wariant 3 instalacji Routerów CE
1. W Wariancie 3 kilka jednostek prokuratury mieści się w jednej lokalizacji.
2. W tym przypadku do Routera CE dołączone jest jedno urządzenie bezpieczeństwa Zamawiającego dla Usługi A oraz dla lokalizacji POPD PK, ZOPD MS, OPDR, OPDO, Prokuraturach Regionalnych oraz Prokuraturach Okręgowych urządzenie bezpieczeństwa Wykonawcy dla Usługi B zainstalowane w jednej z jednostek prokuratury. Do urządzenia bezpieczeństwa dołączone są przełączniki LAN, które zainstalowane są w jednostkach prokuratury znajdujących się w danej lokalizacji.
3. W każdej jednostce prokuratury znajdującej się w danej lokalizacji na przełącznikach LAN może być utworzone kilka sieci VLAN. Do sieci VLAN podłączane są serwery oraz stacje robocze. Zakłada się, że nie będzie zmieniana adresacja urządzeń dołączonych do sieci LAN (VLAN). Przełączniki dla Usługi A i Usługi B są fizycznie innymi urządzeniami.



Rysunek 6 Wariant 3 instalacji Routerów CE – Usługa A

* + 1. Wariant 4 instalacji Routerów CE
1. W Wariancie 4 dwie lub kilka jednostek prokuratury mieści się w jednej lokalizacji.
2. W tym przypadku do Routera CE dołączone jest jedno urządzenie bezpieczeństwa Zamawiającego dla Usługi A oraz dla lokalizacji POPD PK, ZOPD MS, OPDR, OPDO, Prokuraturach Regionalnych oraz Prokuraturach Okręgowych urządzenie bezpieczeństwa Wykonawcy dla Usługi B do którego jest podłączony jeden lub kilka przełączników LAN obsługujących kilka jednostek prokuratury w danej lokalizacji.
3. Na przełącznikach LAN może być utworzonych kilka sieci VLAN obsługujących jednostki prokuratury w danej lokalizacji. Do sieci VLAN podłączane są serwery oraz stacje robocze. Zakłada się, że nie będzie zmieniana adresacja urządzeń dołączonych do sieci LAN (VLAN). Przełączniki dla Usługi A i Usługi B są fizycznie innymi urządzeniami.



Rysunek 7 Wariant 4 instalacji Routerów CE – Usługa A

* + 1. Wariant 5 instalacji Routerów CE
1. W Wariancie 5 jedna jednostka prokuratury rozlokowana jest w kilku lokalizacjach.
2. W tym przypadku w każdej lokalizacji znajduje się Router CE do którego w każdej lokalizacji dołączone jest jedno urządzenie bezpieczeństwa Zamawiającego dla Usługi A oraz dla lokalizacji POPD PK, ZOPD MS, OPDR, OPDO, Prokuraturach Regionalnych oraz Prokuraturach Okręgowych urządzenie bezpieczeństwa Wykonawcy dla Usługi B do którego jest podłączony jeden lub kilka przełączników LAN.
3. W każdej lokalizacji zainstalowane są przełączniki LAN, które umożliwią utworzenie kilku sieci VLAN. Do sieci VLAN podłączane są serwery oraz stacje robocze. Zakłada się, że nie będzie zmieniana adresacja urządzeń dołączonych do sieci LAN (VLAN). Przełączniki dla Usługi A i Usługi B są fizycznie innymi urządzeniami.



Rysunek 8 Wariant 5 instalacji Routerów CE – Usługa A

1. **Struktura fizyczna sieci**
2. Łącza TD muszą być łączami symetrycznymi o gwarantowanej przepustowości bez jakichkolwiek ograniczeń przesyłanych danych.
3. Usługa powinna być skalowalna, tzn. Zamawiający ma prawo żądania zwiększenia przepustowości ruchu do wartości dwukrotne większej od określonej w Załączniku nr 2 do Umowy w każdej Lokalizacji, w której Wykonawca będzie w stanie technicznie zagwarantować usługę o żądanych przez Zamawiającego parametrach przepustowości łączy. Powyższe skutkować będzie zmianą wysokości abonamentu miesięcznego za dane łącze nie zaś dodatkowymi kosztami ponoszonymi przez Zamawiającego w związku z koniecznością modernizacji infrastruktury Wykonawcy.
4. Zamawiający przy budowie łączy dostępowych dopuszcza następujące rodzaje mediów:
	1. łącza światłowodowe zakończone dedykowanymi urządzeniami teletransmisyjnymi lub jako ciemne włókno bezpośrednio łączące router PE Wykonawcy z routerem CE w lokalizacji Zamawiającego,
	2. łącza radiowe punkt-punkt lub punkt-wielopunkt pracujące w paśmie koncesjonowanym,
5. Podstawowe łącze transmisji danych w danej lokalizacji nie może być zrealizowane za pomocą tego samego fizycznego łącza, na którym zrealizowane będzie łącze zapasowe w tej lokalizacji.
6. W przypadku, jeżeli Wykonawca zdecyduje o instalacji w danej Lokalizacji Łączy Podstawowego i Zapasowego za pomocą dwóch światłowodów, to w takim wypadku pierwszy taki światłowód przeznaczony dla Podstawowego Łącza transmisji danych musi być ciągnięty fizycznie innymi studzienkami telekomunikacyjnymi na odcinku od węzła Wykonawcy do siedziby Zamawiającego niż światłowód przeznaczony dla Łącza Zapasowego. Zniszczenie (awaria) ciągu komunikacyjnego (studzienki telekomunikacyjnej) dla jednego światłowodu nie może powodować awarii drugiego z tych światłowodów. Mapy projektowe (inwentaryzacyjne) wskazujące trasy obu światłowodów muszą być dołączone do dokumentacji powykonawczej.
7. W przypadku, jeżeli Wykonawca zdecyduje o instalacji w danej Lokalizacji Łączy Podstawowego i Zapasowego realizowanych w technologii bezprzewodowej, to w takim wypadku łącza muszą być skierowane w różnych kierunkach. Awaria w węźle dostępowym Wykonawcy obsługującym Łącze Podstawowe nie może powodować awarii węzła dostępowego Wykonawcy obsługującego Łącze Zapasowe i odwrotnie. Mapy projektowe (inwentaryzacyjne) wskazujące lokalizacje węzłów dostępowych muszą być dołączone do dokumentacji powykonawczej.
8. Wykonawca zaprojektuje i wykona udostępnianą infrastrukturę w taki sposób aby awaria pojedynczego Routera PE nie powodowała Awarii Podstawowego i Zapasowego Łącza transmisji danych w żadnej z Lokalizacji. Mapy projektowe (inwentaryzacyjne) wskazujące podłączenia do Routerów PE muszą być dołączone do dokumentacji powykonawczej
9. Dla lokalizacji POPD PK, ZOPD MS, OPDR Zamawiający wymaga realizacji łączy w schemacie 2PE-2CE. Wariant realizacji Łącza Podstawowego i Zapasowego dla poszczególnych Lokalizacji został wskazany w *Załączniku nr 2 do Umowy*.



Rysunek 9 Redundancja łącza w układzie 2PE-2CE



Rysunek 10 Redundancja łącza w układzie 2PE-1CE

1. Łącze transmisji danych Wykonawca wprowadzi do wskazanej przez upoważnionego w danej Lokalizacji pracownika Zamawiającego szafy typu rack 19" w serwerowni i zakończy w montowanym przez Wykonawcę w tej szafie patchpanelem lub w przypadku światłowodu - patchpanelem światłowodowym. Wszelkie urządzenia niezbędne do realizacji przedmiotu umowy zostaną również zamontowane w szafie typu rack 19". W przypadku urządzeń nieposiadających fabrycznych uchwytów lub mniejszej wielkości, Wykonawca zapewni odpowiednie półki do montażu w szafach. Wykonawca zapewni również wszelkie inne niezbędne elementy w tym śruby montażowe, uchwyty, kable zasilające, konwertery interfejsów itp.
2. Dla lokalizacji POPD PK, ZOPD MS, OPDR oraz OPDO Zamawiający obligatoryjnie wymaga wykonania Podstawowego Łącza transmisji danych za pomocą światłowodu jednomodowego.
3. Wszystkie węzły sieci operatora do których będą budowane łącza dostępowe jednostek prokuratury powinny być połączone z siecią operatora co najmniej dwiema niezależnymi drogami (dwa niezależne łącza w górę sieci).
4. Dla zapewnienia odpowiedniej skalowalności infrastruktury sieciowej i bezpieczeństwa transmisji danych oraz zapewnienia prywatności konfigurowanych przez dostawcę usług telekomunikacyjnych, łącza dostępowe nie mogą być budowane:
	1. na bazie zasobów publicznej sieci Internet,
	2. łączy z wykorzystaniem infrastruktury znajdującej się poza terytorium Polski,
	3. łączy asymetrycznych w technologii DSL,
	4. łączy satelitarnych,
	5. telefonicznych łączy komutowanych,
	6. łączy technologii radiowych w paśmie niepodlegającym koncesjonowaniu,
	7. technologii Wi-Fi,
	8. w oparciu o sieci komórkowe, tj. w szczególności technologii GPRS, EDGE, UMTS, HSPA, HSDPA, CDMA, LTE, 5G.
5. Zamawiający wymaga, aby Łącza TD użyte do realizacji sieci były na całej relacji (od danej Lokalizacji do routera PE w sieci Wykonawcy) budowane z zastosowaniem łączy odseparowanych od publicznej sieci Internet.
6. Podstawowe i Zapasowe Łącza TD przeznaczone dla usługi transmisji danych w ramach Usługi na odcinku od węzła Wykonawcy do Routera CE (tzw. ostatnia mila) nie mogą być wykorzystywane do świadczenia przez Wykonawcę jakichkolwiek usług dla klientów innych niż Zamawiający. Od węzła Wykonawcy do Routera PE ruch musi być odseparowany przynajmniej logicznie.
7. Każde Podstawowe i Zapasowe Łącze TD musi być zakończone dedykowanym dla tego Łącza Routerem CE, będącym stykiem infrastruktury fizycznej Wykonawcy z infrastrukturą fizyczną Zamawiającego.
8. Zamawiający wymaga, aby Wykonawca wykorzystał jako Routery CE routery IP dostarczone wraz z niezbędnym okablowaniem, osprzętem i oprogramowaniem umożliwiającym realizowanie założonych funkcjonalności opisanych w SIWZ. Nie dopuszcza się wykorzystywania jako urządzeń dostępowych CE wyłącznie mostów lub modemów oraz innych urządzeń pracujących w warstwie drugiej modelu ISO/OSI.
9. Routery CE muszą komunikować się z wykorzystaniem protokołu TCP/IP z urządzeniami bezpieczeństwa posiadanymi przez Zamawiającego. Routery CE Wykonawcy i urządzenia Zamawiającego muszą być połączone bezpośrednio ze sobą za pomocą skrętki przynajmniej kat.6 i z wykorzystaniem interfejsu RJ45 GigabitEthernet 10/100/1000 (1000Base TX). Wszystkie kable połączeniowe muszą być oznaczone i opisane przez Wykonawcę. Dla lokalizacji POPD PK i ZOPD MS Wykonawca zapewni multimodowe światłowodowe interfejsy (10GBASE-SR ) przyłączeniowe LC o prędkości 10Gbps.
10. Routery CE muszą zapewnić odpowiednią ilość interfejsów przyłączeniowych dostępnych dla Zamawiającego:
11. co najmniej cztery interfejsy przyłączeniowe światłowodowe MM (10GBASE-SR) 10G dla lokalizacji POPD PK, ZOPD MS,
12. co najmniej cztery elektryczne interfejsy przyłączeniowe Eth 10/100/1000 dla lokalizacji OPDR, OPDO,
13. co najmniej dwa elektryczne interfejsy przyłączeniowe Eth 10/100/1000 dla pozostałych lokalizacji Zamawiającego,
14. jeżeli w celu realizacji funkcjonalności wymaganych w OPZ konieczne jest wykorzystanie interfejsów Routerów CE przez Wykonawcę, należy zapewnić odpowiednio większą ich ilość w dostarczanych Urządzeniach.
15. Zamawiający wymaga, aby Wykonawca obsługiwał adresy IP używane przez Zamawiającego w dotychczas eksploatowanych sieciach rozległych z puli określonej w dokumencie RFC 1918 (ang. *Requests For Comments)*. Szczegółowy plan adresacji sieci dla obsługi poszczególnych systemów aplikacyjnych Zamawiającego zostanie przekazany Wykonawcy po podpisaniu Umowy.
16. W celu wykonania instalacji łączy transmisji danych, Wykonawca zobowiązany jest dla każdej Lokalizacji uzyskać w imieniu Zamawiającego wymagane pozwolenia, decyzje i zgody, w szczególności konserwatora zabytków jeżeli są wymagane, oraz wykonać konieczne projekty, roboty budowlane, w tym prace wykończeniowe, porządkowe i inne. Całość procesu budowlanego leży po stronie Wykonawcy.
17. Wszystkie prace i roboty budowlane, a także instalacje, w szczególności trasy kablowe, prowadzone poza terenem Zamawiającego dla każdej Lokalizacji, nie mogą obciążać kosztami prawnymi i ekonomicznymi Zamawiającego.
18. **Struktura logiczna sieci**
19. Struktura logiczna udostępnianej usługi transmisji danych w sieci operatora telekomunikacyjnego musi umożliwiać konfigurację dostępu użytkowników do usług i uwzględniać korzystanie danej jednostki z określonych centralnych oraz rozproszonych zasobów bazodanowych czy aplikacji,
20. Udostępniona sieć MPLS będzie podzielona logicznie na niezależne sieci przy wykorzystaniu mechanizmu VRF (Virtual Routing and Forwarding), z możliwością zwiększania przez Zamawiającego ilości tych sieci niezależnie do każdej Lokalizacji.
21. W ramach struktury logicznej sieci Zamawiającego musi zostać zdefiniowany:
	1. WAN-PROK: obejmujący swoim zasięgiem wszystkie lokalizacje wyszczególnione w *Załączniku nr 2 do Umowy - adresy miejsca instalacji łączy oraz przepustowość*; Zamawiający wymaga aby w ramach tej struktury możliwa była komunikacja „każdy z każdym” (topologia full-mesh).
	2. VRF-BBW – obejmujący swoim zakresem POPD PK, ZOPD PK, OPDR i OPDO.
	3. sieć zarządzająca, w której zostanie umiejscowiona Stacja Monitorowania i weryfikacji jakości świadczonych usług Zamawiającego.
	4. Lokalne struktury na poziomie prokuratur okręgowych i regionalnych (nie więcej niż 10) których wykaz zostanie udostępniony Wykonawcy po podpisaniu umowy.
22. Przełączenie transmisji danych z Łącza Podstawowego na Łącze Zapasowe i odwrotnie nie może powodować przerw w pracy poza wymaganą na odpowiednie rozgłoszenie tras routingu lub wyzwolenia mechanizmów niezawodnościowych.
23. Domyślnie transmisja danych (dla wszystkich VRF) będzie odbywać się poprzez Łącze Podstawowe. W momencie utraty łączności w tym medium transmisyjnym Router CE w Lokalizacji musi, bez zbędnej zwłoki, w sposób automatyczny przełączyć transmisję danych na Łącze Zapasowe. Po ustaniu Awarii, transmisja danych musi ponownie, bez zbędnej zwłoki, przełączyć się automatycznie na Łącze Podstawowe.
24. Przełączanie transmisji danych w Routerze PE nie może wymagać i pociągać za sobą zmiany adresacji IP w jakimkolwiek VRF dla urządzeń podłączanych do Routera CE od strony sieci LAN w każdej Lokalizacji.
25. Wykonawca dokona dla Usługi odpowiedniej konfiguracji urządzeń w celu umożliwienia migracji z obecnie eksploatowanych sieci Usługi A oraz Usługi B. Uzgodnienia w zakresie rozgłoszeń adresacji, tras routingu, protokołów itp. zostaną dokonane po podpisaniu Umowy.
26. Zakres uprawnień w dostępie dla każdej lokalizacji zostanie zdefiniowany indywidualnie na etapie uruchomienia usług i eksploatacji po podpisaniu umowy.
27. W ramach realizacji Usługi Wykonawca dla łączy sieci WAN-PROK w lokalizacjach POPD PK i ZOPD MS dokona konfiguracji umożliwiającej rozgłaszanie wspólnej adresacji tych lokalizacji w udostępnianej sieci dla jednostek prokuratury w konfiguracji odpornej na awarie. Wykonawca opracuje i wdroży uzgodnione na etapie realizacji Umowy scenariusze przełączania pomiędzy lokalizacjami POPD PK i ZOPD MS
28. W ramach realizacji Usługi Wykonawca wykreuje w swojej infrastrukturze co najmniej dwa rozproszone geograficznie (zlokalizowane w POPD PK oraz ZOPD MS) punkty styku z siecią Internet w ramach VRF WAN-PROK. Punkty styku muszą mieć zagwarantowaną przepustowość co najmniej 3 Gbps każdy wraz z uruchomioną usługą AntyDDoS. Wykonawca zobowiązany jest do konfiguracji rozproszonych punktów styku z siecią Internet w taki sposób aby umożliwić rozgłaszanie wspólnej adresacji publicznej tych lokalizacji w konfiguracji odpornej na awarie. Wykonawca opracuje i wdroży uzgodnione na etapie realizacji Umowy scenariusze przełączania pomiędzy lokalizacjami POPD PK i ZOPD MS.
29. W ramach realizacji Usługi Wykonawca zapewni dostęp DC POPD i ZOPD do sieci Internet odseparowany od centralnych punktów styku z siecią Internet i przydzieli im adresacje zgodnie przydzielonym zamówieniem. Ponadto dokona konfiguracji umożliwiającej rozgłaszanie wspólnej adresacji dla obydwu DC POPD i ZOPD.
30. Punkty styku z siecią Internet muszą być aktywne w tym samym czasie tzn. Wykonawca tak skonfiguruje Usługę aby ruch z sieci Internet do zasobów udostępnianych przez Zamawiającego oraz wychodzący do sieci Internet generowany przez użytkowników Zamawiającego, kierowany był dynamicznie z/do obu punktów w zależności od preferencji ustawień protokołu routingu dynamicznego.
31. W ramach realizacji Usługi, Zamawiający wymaga dostarczenia podsieci z przynajmniej 512 stałymi publicznymi adresami IP (maska o wartości /23), przy czym adresy te nie mogą zostać wykorzystane w celu konfiguracji łączy dla usługi dostępu do Internetu od strony Wykonawcy. Adresy dostarczone przez Wykonawcę muszą umożliwiać publikowanie usług w sieci Internet tzw. rozproszone DMZ oraz usługi DC. Nie mogą figurować na black-listach operatorów, być blokowane itp. Zamawiający wymaga aby dostarczona pula adresów publicznych przeszła na własność Zamawiającego w trakcie realizacji usługi jako pula PI. Pula adresów zostanie podzielona przez Zamawiającego na segment „Centralny Dostęp do sieci Internet” oraz na potrzeby rozproszonego DC.
32. Kierowanie ruchu przez jedno lub dwa łącza dla dostępu do Internetu nie może powodować zmian publicznej adresacji IP przydzielonej Zamawiającemu.
33. Zamawiający przewiduje, że w punktach styku z siecią Internet w POPD i ZOPD będzie posiadał po jednym niezależnym klastrze urządzeń typu firewall z wykupionymi odpowiednimi licencjami podnoszącymi bezpieczeństwo tych systemów. Na tych urządzeniach będą realizowane funkcjonalności typu routing, NAT, VPN, IPS, URL filtering, AV. Dla części centrum przetwarzania danych DC będzie przeznaczony oddzielny klaster urządzeń typu firewall w innej adresacji niż centralne punkty styku z Internetem.
Ponadto zamawiający będzie posiadał po jednym niezależnym klastrze urządzeń typu firewall w punktach styku centrum przetwarzania danych DC POPD i ZOPD od strony WANu gdzie zostaną uruchomione funkcjonalności typu routing, VPN, IPS na potrzeby wewnętrznych systemów.

W ramach przedmiotowego zamówienia pomiędzy POPD i ZOPD Zamawiający wymaga zestawienia połączeń typu xWDM w celu realizacji niezawodności konfiguracji urządzeń brzegowych w obydwu ośrodkach przetwarzania danych POPD i ZOPD w przypadku awarii jednego ośrodka zarówno dla części związanej ze stykiem Internet jak i styku z siecią WAN.

1. **Monitorowanie Łączy oraz SLA**
2. Zamawiający wymaga zapewnienia następujących, minimalnych parametrów usług SLA, jakie muszą być gwarantowane przez operatora telekomunikacyjnego w ramach świadczenia Usługi:
	1. gwarancja przepustowości na poziomie 100% dostarczonego pasma,
	2. gwarantowana dostępność usługi na poziomie co najmniej 99,44% dla Lokalizacji POPD PK, ZOPD MS, OPDR oraz 98,88% miesięcznie dla pozostałych Lokalizacji,
	3. czas reakcji na Awarię nie dłużej niż 60 minut, liczonych od chwili wykrycia/zgłoszenia,
	4. czas usunięcia Awarii nie dłużej niż:
		1. dla lokalizacji POPD PK, ZOPD MS, OPDR, OPDO - 2 godziny, liczone od chwili wykrycia/zgłoszenia Awarii,
		2. dla pozostałych lokalizacji - 4 godziny, liczone od chwili wykrycia/zgłoszenia Awarii,
	5. czas usunięcia Usterki nie dłużej niż 24 godziny liczone od chwili wykrycia/zgłoszenia Usterki,
	6. gwarantowane opóźnienie w obu kierunkach (RTD - Round Trip Delay) - nie więcej niż 30 ms,
	7. gwarancja straty pakietów (PLR - Packet Loss Ratio) - nie więcej niż 0,01%.
3. Parametry jakościowe będą mierzone z użyciem 10 pakietów ICMP (lub datagramów UDP) o wielkości 128 bajtów wysyłanych w okresach nie dłuższych niż co 5 minut pomiędzy urządzeniem dostępowym CE w danej lokalizacji a stacją monitorowania jakości świadczonych usług; wyniki pomiarów będą uśredniane w okresach 30 minutowych. Do pomiarów brane będą pomiary wykonane w warunkach obciążenia poszczególnych kolejek danych Routera CE w danej lokalizacji nieprzekraczającego wartości 90% dostępnego pasma dla kolejki. W przypadku, gdy warunki obciążenia nie są respektowane dla jednego z dwóch portów IP, których pomiar dotyczy, pomiar będzie odrzucany.
4. Wymagane szybkości transmisji danych (dalej zamiennie: przepustowości Łączy) są to gwarantowane przez Wykonawcę minimalne szybkości łączy transmisji danych w warstwie aplikacji modelu ISO/OSI dostępne w ramach jednej uruchomionej sesji dla danej aplikacji Zamawiającego działającej w ramach Usługi.
5. Szybkość transmisji danych dla Usługi będzie sprawdzana pomiędzy interfejsem Routera CE od strony udostępnianej Usługi w siedzibie Zamawiającego w Warszawie, a Routerem CE w każdej Lokalizacji przy zastosowaniu usługi FTP. Niedotrzymanie parametru minimalnej gwarantowanej szybkości transmisji danych przez strony Umowy traktowane jest jako Awaria.
6. Szybkość transmisji danych dla punktów styku z siecią Internet będzie sprawdzana na interfejsie każdego z Routerów CE od strony sieci Zamawiającego, w stosunku do serwera referencyjnego udostępniającego co najmniej usługę FTP umiejscowionego wewnątrz infrastruktury telekomunikacyjnej Wykonawcy i wskazanego w momencie przeprowadzania testów akceptacyjnych. Dane serwera referencyjnego będą wpisane do dokumentacji powykonawczej. Serwer referencyjny będzie dostępny dla Zamawiającego przez cały okres świadczenia Usługi. Zmiana serwera referencyjnego musi być protokolarnie potwierdzona przez obie strony Umowy i wymaga wykonania przez Wykonawcę modyfikacji dokumentacji powykonawczej.
7. Kontrola łączności z siecią publiczną Internet odbywać się będzie poprzez generowanie ruchu z przynajmniej z dwoma referencyjnymi stałymi adresami IP dostępnymi w Internecie i nie będącymi w sieci telekomunikacyjnej należącej do Wykonawcy lub kontrolowanej przez Wykonawcę oraz nie będącymi w sieci jednego operatora (właściciela). Adresy IP zostaną uzgodnione z Wykonawcą na etapie wdrożenia.
8. Wszelkie prace serwisowe wymagające dostępu do routerów i modemów, powinny być dokonywane przez operatora zdalnie po wcześniejszym uzgodnieniu terminu i zakresu prac. W przypadkach, gdy zdalny dostęp z przyczyn technicznych nie będzie możliwy, odpowiednie działania mające na celu przywrócenie poprawnej pracy urządzeń i łącza powinny być wykonywane w lokalizacji Zamawiającego.
9. Wykonawca dostarczy i skonfiguruje SMZ wraz z niezbędnym oprogramowaniem umiejscowiony w infrastrukturze Zamawiającego. System będzie zlokalizowany w Prokuraturze Krajowej. Zamawiający wymaga zapewnienia synchronizacji czasu zdarzeń pomiędzy SMW oraz SMZ oraz skonfigurowania co najmniej następujących funkcjonalności dla udostępnianej struktury sieciowej:
	1. monitorowanie parametrów SLA dla całej udostępnianej sieci na potrzeby Usługi, w szczególności parametrów łączy dostępowych, gwarantowanej przepustowości i obciążenia łączy dla poszczególnych klas ruchu QoS, z poziomu jednej konsoli monitorującej,
	2. automatyczne odkrywanie urządzeń znajdujących się w monitorowanej sieci i dodawanie ich do bazy urządzeń podlegających monitorowaniu,
	3. graficzna wizualizacja odpowiedzi monitorowanych urządzeń na pakiety ICMP, ECHO wysyłane przez stację monitorującą,
	4. dynamiczne (w czasie rzeczywistym ), graficzne wyświetlanie mapy logicznej i fizycznej topologii sieci (z routerem w każdej lokalizacji włącznie),
	5. monitorowanie w czasie rzeczywistym (uwzględniając prędkość sieci komputerowej
	i częstotliwość odpytywania) parametrów pracy urządzeń sieciowych,
	6. testowanie poprawności zdalnych połączeń,
	7. gromadzenie bieżących parametrów pracy monitorowanych urządzeń sieciowych dzięki wykorzystaniu protokołu SNMP oraz graficzna wizualizacja całej topologii sieci na podstawie zgromadzonych danych; prezentacja utylizacji łączy z możliwością określenia przedziału czasowego oraz monitorowania w czasie rzeczywistym.
	8. graficzna prezentacja zebranych danych w postaci wykresów tygodniowych, miesięcznych, rocznych wraz z odpowiednim wyskalowaniem w jednostkach Mbps,
	9. generowanie komunikatów w wyniku zdarzeń i symptomów potencjalnych zagrożeń oraz reagowanie na nie za pomocą zdefiniowanych przez użytkownika akcji takich jak wysłanie powiadomienia poprzez email, wysłanie trapów SNMP lub uruchomienie lokalnego/zdalnego programu lub skryptu.
	10. generowanie automatycznych raportów miesięcznych dotyczących spełnienia przez Wykonawcę wymaganych przez Zamawiającego parametrów SLA dla wszystkich uruchomionych łączy dostępowych z uwzględnieniem okien serwisowych w danym okresie z możliwością prezentacji lokalizacji przekraczających zadane wartości SLA, lokalizacji w których wystąpiła Awaria i/lub Usterka, wszystkich lokalizacji.
	11. wizualizacja udostępnionej infrastruktury na mapie konturowej Polski wraz z bieżącą sygnalizacją stanu łącza sprawne/niesprawne/okno serwisowe (np. poprzez zmianę koloru zielony/czerwony/żółty); wyświetlanie informacji o danej lokalizacji po przesunięciu na nią myszką w formie np. dymka zawierającego dane o lokalizacji (adres), przepustowość oraz link do szczegółowych raportów o danej lokalizacji.
	12. dostęp do konsoli SMZ musi być możliwy poprzez przeglądarkę internetową dla minimum 75 administratorów Zamawiającego.
10. Wykonawca zapewni z SMZ stały dostęp SSH do konsoli Routerów CE Wykonawcy (w trybie tylko do odczytu - *ang. read-only*) w zakresie minimum:
	* 1. poleceń służących do sprawdzenia stanu interfejsów, routingu, statystyk kolejek QoS, dopasowań pakietów do poszczególnych klas CoS;
		2. narzędzi diagnostycznych ping i traceroute;
11. Wykonawca skonfiguruje SMZ wraz z zapewnieniem ewentualnych niezbędnych licencji:
	1. do całej sieci, z podziałem na PK i 11 segmentów według właściwości terytorialnej poszczególnych prokuratur regionalnych (dla minimum 5 zdefiniowanych administratorów Zamawiającego) wraz z prezentacją i przeszkoleniem w zakresie użytkowania, w formie warsztatów praktycznych w sposób zdalny dla wszystkich wskazanych administratorów Zamawiającego,
	2. do części sieci - łącza należące do danego obszaru prokuratury regionalnej (dla minimum 5 zdefiniowanych administratorów z danego obszaru prokuratury regionalnej),
	3. SMZ musi zapewniać dostęp do statystyk właściwych Łączy dla danej lokalizacji z uwzględnieniem uprawnień danego administratora:
		1. w widoku dziennym (z ostatnich 24 godzin),
		2. w widoku historia z możliwością wyboru widoku z konkretnych dni (ostatnie 90 dni kalendarzowych) oraz widoku w ujęciu miesięcznym lub rocznym (dane archiwalne za okres 12 miesięcy),
		3. z jednoczesną możliwością wyboru określonych godzin i/lub dni tygodnia (np. statystyki wyłącznie dla godzin dziennych w dni robocze w widoku dziennym i widoku historia).
12. SMW musi wykrywać w czasie rzeczywistym przynajmniej następujące zdarzenia, które mają charakter ciągły i nie krótszy niż 10 sekund, oraz rejestrować datę i godzinę (na podstawie serwerów czasu dla instytucji publicznych), w której dane zdarzenie zostało zarejestrowane dla Łączy realizujących Usługę:
	* 1. po którym Łączu, tj. czy Podstawowym czy Zapasowym, przebiega transmisja danych w danej Lokalizacji Zamawiającego
		2. status każdego, zarówno Podstawowego jak i Zapasowego, Łącza, tj. czy łącze jest aktywne czy uległo Awarii
		3. przekroczenie i powrót do wymaganych parametrów zarówno dla Łącza Podstawowego jak i Zapasowego w każdej Lokalizacji dla każdej klasy QoS, tj.:
			+ - utraty pakietów;
				- opóźnienia (RTD);
				- jitteru.

Jeżeli sposób wykonywania danego pomiaru nie został wskazany wówczas podlega on uzgodnieniu w momencie wdrożenia.

* + 1. brak komunikacji poprzez dane Łącze.
		2. przeciążenie procesora dowolnego z Routerów CE.
1. Informacje historyczne zbierane przez SMW muszą być dostępne przez cały okres obowiązywania umowy.
2. Informacja o każdym zdarzeniu wykrytym przez SMW musi być wysyłana zarówno do Zamawiającego jak i Wykonawcy, przy czym musi być możliwe wysłanie na co najmniej 75 adresów email nie później niż 1 minutę od chwili wykrycia zdarzenia z możliwością przypisania zakresu Lokalizacji i administratora/ów który powinien otrzymać powiadomienie. Informacje o wybranych zdarzeniach (lub grupie zdarzeń) muszą być także wysyłane poprzez bramkę SMS z możliwością powiadamiania przynajmniej 75 odbiorców nie później niż 10 minut od chwili wykrycia zdarzenia. W ramach realizacji umowy Wykonawca zapewni funkcjonowanie bramki SMS przeznaczonej na te potrzeby.
3. Szczegóły związane z klasyfikacją, ilością zdarzeń i ustaleniem progów po przekroczeniu których wysyłane będą informacje mailem lub SMS podlegają ustaleniu w czasie wdrożenia.
4. Bramka SMS musi być fizycznym urządzeniem przeznaczonym do wysyłania takich komunikatów, tj. SMS muszą być wysyłane poprzez sieć operatora telefonii komórkowej bez limitów ilościowych.
5. Wykonawca musi zaprojektować i wykonać odpowiednią konfigurację korelacji zdarzeń rejestrowanych przez SMW w taki sposób, żeby zminimalizować ilość reakcji na te zdarzenia do niezbędnego minimum, wskazującego pierwotną/najważniejszą przyczynę sekwencji zarejestrowanych zdarzeń.
6. **QoS**
7. Zamawiający wymaga skonfigurowania priorytetyzacji ruchu na każdym Podstawowym i Zapasowym Łączu transmisji danych. Podział na poszczególne klasy ruchu, podział procentowy do każdej z klas ruchu oraz określenie priorytetów dla poszczególnych aplikacji biznesowych Zamawiającego, w ramach przepustowości Łącza zostanie ustalony na etapie opracowywania Projektu Technicznego Usługi.
8. **Bezpieczeństwo teleinformatyczne Usługi oraz infrastruktura Zamawiającego**
	* + 1. Zamawiający we wszystkich lokalizacjach posiada jako urządzenia brzegowe do sieci WAN-PROK firewalle Cisco ASA. W zależności od wielkości Lokalizacji i generowanego wolumenu ruchu są to urządzenia Cisco ASA 5506-X, Cisco ASA 5516-X oraz Cisco ASA 5545-X. W lokalizacjach OPDR, OPDO zainstalowane są urządzania Cisco ASA 5545-X. W lokalizacji POPD PK zainstalowany jest klaster urządzeń Cisco ASA 5545-X .

Na powyższych urządzeniach uruchomione są typowe funkcjonalności jakie posiadają urządzenia typu UTM (tunele VPN ,NAT , IPS, firewall itd.).

* + - 1. Zamawiający dla Usługi posiada Centralny System Monitorowania i Korelacji Logów oraz Centralny System Zarządzania urządzeniami wskazanymi w pkt 1 powyżej.
			2. Wykonawca w celu umożliwienia konfiguracji dostępu do Usługi, opracuje konieczne zmiany konfiguracyjne niezbędne do przeprowadzenia w danej Lokalizacji na danym typie urządzenia posiadanego przez Zamawiającego w tej Lokalizacji.
1. **Usługa Anty DDoS**
2. W ramach realizacji Usługi, Wykonawca uruchomi usługę AntyDDoS czyli przeciwdziałanie atakom typu DDoS. Usługa nie może posiadać ograniczeń w ilości analizowanych danych i musi być świadczona w ramach Usługi bez naliczania dodatkowych opłat. Wymagany czas reakcji na zdarzenia nie może być dłuższy niż 20 minut od wykrycia zdarzenia.
3. W celu poprawnego świadczenia usługi AntyDDoS Wykonawca musi posiadać we własnej infrastrukturze i strukturze organizacyjnej:
	1. system monitorowania w czasie rzeczywistym Routerów PE lub innych urządzeń w infrastrukturze, w celu sporządzenia profilu typowego ruchu w kierunkach od i do Zamawiającego;
	2. system wykrywania anomalii ruchu przynajmniej za pomocą sygnatur, przekroczenia zdefiniowanych progów ruchu dla określonego typu pakietów i protokołów, analizy profilu ruchu w oparciu o profil standardowego ruchu;
	3. system usuwania ataku (filtrowania) przy możliwie jak najmniejszym wpływie na pozostały ruch w kierunkach od i do Zamawiającego;
	4. specjalistów dedykowanych do obsługi AntyDDoS w sposób ciągły, przez 24 godziny na dobę.
4. System wykrywania anomalii ruchu musi obejmować przynajmniej:
5. wykrywanie anomalii polegających na przekroczeniu wartości uważanych za normalne w ruchu w sieci Internet, w szczególności pakietów TCP SYN, TCP RST, TCP Null, ICMP, IP Null, IP Fragmented, DNS;
6. wyznaczanie oczekiwanej wartości ruchu w kierunkach do i od Zamawiającego, o danej porze dnia w danym dniu tygodnia;
7. wykrywanie anomalii polegających na znaczącym przekroczeniu wolumenu ruchu w stosunku do wcześniej wyznaczonych wartości oczekiwanych tego ruchu.
8. System usuwania ataku musi obejmować przynajmniej:
9. filtrowanie ruchu z błędnymi nagłówkami IP/TCP/UDP;
10. odrzucanie lub przepuszczanie na bazie zdefiniowanych dla Zamawiającego filtrów operujących na informacjach w nagłówkach L3 i L4 modelu ISO/OSI;
11. filtrowanie ruchu na określonych portach UDP na podstawie zawartości pola danych w oparciu o wyrażenia regularne;
12. filtrowanie ruchu na określonych portach TCP na podstawie zawartości pola danych w oparciu o wyrażenia regularne;
13. ochronę przed atakami z udawanymi adresami źródłowymi IP (spoofing) poprzez autentykację sesji TCP, zapytań DNS oraz zapytań http;
14. filtrowanie nieprawidłowych zapytań DNS;
15. ograniczenie zapytań DNS do zadanej wartości zapytań na sekundę;
16. filtrowanie oparte o wyrażenia regularne definiujące zakres stosowania autentykacji DNS oraz ograniczania liczby zapytań DNS;
17. filtrowanie nieprawidłowych zapytań HTTP;
18. blokowanie ruchu od stacji Zamawiającego przekraczających progi dla operacji HTTP na sekundę na dany serwer lub na dany URL;
19. filtrowanie oparte o wyrażenia regularne definiujące zakres stosowania autentykacji HTTP lub ograniczania liczby zapytań http;
20. filtrowanie ruchu w oparciu o wyrażenia regularne dotyczące nagłówków HTTP;
21. ochronę przez atakami typu Slow Lories poprzez resetowanie połączeń, które pozostają nieaktywne przez zadany okres czasu;
22. ochronę przez atakami typu Slow Lories poprzez resetowanie sesji TCP, której aktywność jest poniżej zadanej liczby bajtów przesyłanej w zadanym okresie czasu;
23. wykrywanie ruchu kierowanego z serwerów CDN proxy i stosowanie algorytmów filtrowania na podstawie oryginalnego źródła ruchu;
24. wykrywanie i filtrowanie pakietów z nieprawidłowymi nagłówkami SSL/TLS lub nagłówkami SSL/TLS, które są poza sekwencją;
25. blokowane sesji jeżeli podczas negocjacji SSL/TLS klient zarządza nadmiernej ilości metod kryptograficznych lub rozszerzeń użytkownika. Próg dla tych wartości musi być definiowalny;
26. wykrywanie i rozłączanie sesji jeżeli negocjacja SSL/TLS nie zakończy się w zadanym czasie;
27. blokowanie ruchu ze stacji, dla których występuje nadmierna liczba nieprawidłowych, nadmiarowych lub niekompletnych sesji SSL;
28. monitorowanie negocjacji SSL dla wszystkich portów, na których można stosować aplikacje zabezpieczone protokołem TLS, przynajmniej: HTTPS, SMTP, IMAP4, POP, LDAP, NNTP, TELNET, FTP i SIP;
29. ochronę przed atakami pochodzącymi od sieci botnetowych (komputerów zainfekowanych w sposób umożliwiające zdalne sterowanie przez hackerów) poprzez filtrowanie na podstawie na bieżąco aktualizowanych sygnatur zawierających listę adresów IP;
30. ochronę przed atakami pochodzącymi z sieci botnetowych poprzez wykrywanie źródeł ataku o wolumenie przekraczającym zadane wartości. Wartości progowe muszą być definiowalne zarówno dla całości ruchu jak i do części ruchu zdefiniowanego za pomocą filtru.
31. Ze względu na wymaganą poufność, monitoring i obróbka ruchu pod kątem ataków DDoS musi odbywać się wyłączenie w infrastrukturze Wykonawcy.
32. Personel techniczny Wykonawcy dedykowany do obsługi AntyDDoS będzie odpowiadał za:
33. analizę ruchu w celu identyfikacji typu i natury ataku;
34. powiadamianie Zamawiającego o podejrzeniu wystąpienia ataku;
35. rozpoczęcie usuwania ataku w porozumieniu z Zamawiającym, przy czym musi być możliwe automatyczne uruchamianie obrony dla alarmów o wysokim poziomie zagrożenia;
36. modyfikację zestawu użytych mechanizmów przeciwdziałania tak, aby uzyskać maksymalny poziom filtracji ruchu niepożądanego przy minimalnym wpływie na ruch prawidłowy;
37. klasyfikację alarmów typu DDoS jako: atak prawdziwy - zweryfikowany, atak fałszywy - zweryfikowany, nagły wzrost ruchu - zweryfikowany (pożądany).
38. Szczegółowy sposób powiadamiania Zamawiającego, inicjowania, awaryjnego przerwania i zakończenia procedury filtrowania w przypadku wykrycia ataku zostanie uzgodniony na etapie wdrożenia.
39. Po zakończeniu operacji filtrowania ruchu po zaistniałym ataku DDoS każdorazowo wymaga się sporządzania przez Wykonawcę i przekazywania Zamawiającemu raportu z wykrytego ataku. Raport musi zawierać przynajmniej następujące informacje:
40. rozmiar ataku, liczniki pakietów, procent całości ruchu wyrażony także w Gb/s;
41. czas trwania ataku;
42. główne źródła ataku wraz z geograficznym położeniem tych źródeł;
43. typ i naturę ataku;
44. wdrożone metody eliminacji ataku;
45. wielkość oczyszczonego ruchu;
46. czasy związane z wykonywaniem usługi AntyDDoS, tj.: godzina początku ataku, godzina powiadomienia Zamawiającego, godzina wdrożenia procedur obronnych, godzina zakończenia ataku, godzina przywrócenia normalnej pracy sieci.
47. Wykonawca sporządzi i przekaże Zamawiającemu w każdym Miesiącu Rozliczeniowym, do 10 dnia danego Miesiąca Rozliczeniowego, raport za poprzedni Miesiąc Rozliczeniowy zawierających przynajmniej:
48. statystykę ruchu w kierunkach od i do Zamawiającego;
49. maksymalne wartości ruchu;
50. listę zarejestrowanych ataków wraz z ich klasyfikacją;
51. listę usuniętych ataków
52. **Usługa DNS**
53. Zamawiający wymaga, aby Wykonawca skonfigurował w swojej infrastrukturze przynajmniej dwa publiczne serwery DNS:
54. typu primary dla domen prostych i odwrotnych wykorzystywanych obecnie przez jednostki prokuratury, wraz ze zdalnym systemem dostępowym umożliwiającym Zamawiającemu pełną modyfikację stref 24 godziny na dobę;
55. typu secondary dla domen prostych i odwrotnych wykorzystywanych obecnie przez jednostki prokuratury, wraz ze zdalnym systemem dostępowym umożliwiającym Zamawiającemu pełną modyfikację stref 24 godziny na dobę;
56. Serwery muszą być skonfigurowane w trybie wskazującym dodatkowo na serwer pracujący w trybie secondary dla domen prostych i odwrotnych znajdujących się w infrastrukturze wewnętrznej Zamawiającego. Wykonawca odpowiednio skonfiguruje strefy tego serwera DNS.
57. Zmiana wpisu dla domen prostych lub odwrotnych dokonana przez Zamawiającego musi spowodować automatyczną aktualizację wpisów w serwerach typu secondary oraz rozpropagowanie się aktualizacji domen w całej sieci Internet.
58. Zmiana delegacji domen wykorzystywanych obecnie przez jednostki prokuratury na adresację IP wskazującą na serwery DNS i adresację IP przydzieloną przez Wykonawcę leży po stronie Zamawiającego.
59. **Ciemne włókna oraz połączenia xWDM**
60. W ramach realizacji Umowy Wykonawca zrealizuje połączenia pomiędzy lokalizacjami na terenie Warszawy z wykorzystaniem infrastruktury światłowodowej
61. dzierżawionego ciemnego włókna światłowodowego zestawionego w postaci światłowodu jednomodowego w relacji Postępu 3, Warszawa (Prokuratura Krajowa) – Domaniewska 36/38, Warszawa (Komenda Główna Policji) o ilości włókien 14J,
62. wymiany danych jako usługi telekomunikacyjnej z wykorzystaniem systemu teletransmisyjnego xWDM**, zapewniając redundancje tych połączeń przy pomocy dwóch niezależnych ścieżek** realizowanej przez Wykonawcę w relacjach:
	* 1. Postępu 3, Warszawa (Prokuratura Krajowa) – Czerniakowska 100, Warszawa (Ministerstwo Sprawiedliwości)
		2. Postępu 3, Warszawa (Prokuratura Krajowa) – Rakowiecka 37a, Warszawa (Centralny Zarząd Służby Więziennej).
63. Włókna wskazane w ust 1 pkt a) muszą być udostępnione i zestawione jako tzw. „ciemne włókna” bez jakichkolwiek ograniczeń w szybkości transmisji danych i rodzaju obsługiwanych protokołów komunikacyjnych. Infrastruktura światłowodowa musi być umieszczona w Kanalizacji Wtórnej (w kanalizacji zostanie zaciągnięty kabel z włóknami światłowodowymi dedykowanymi dla Zamawiającego). Kabel światłowodowy musi zostać zabudowany przełącznicami światłowodowymi w istniejących szafach Zamawiającego 19” w standardzie SC/APC we wskazanych lokalizacjach.
64. Udostępnione włókna światłowodowe muszą spełniać poniższe parametry techniczne:
	* 1. Właściwości optyczne:
65. włókna światłowodowe typu matched cladding (z nieprzesuniętą dyspersją) , zgodne z ITU - T G.652d,
66. praca w oknie 1310 nm i 1550 nm,
67. tłumienność włókien:
* < 0,40 dB/km dla fali o długości 1310 nm,
* < 0,25 dB/km dla fali o długości 1550 nm;
1. dyspersja chromatyczna:
* < 3,5 ps/nm/km dla fali z zakresu 1285 - 1330 nm,
* < 20 ps/nm/km dla fali z zakresu 1525 - 1575 nm;
1. długość fali zerowej dyspersji chromatycznej: 1310 +/- 10 nm,
2. średnica pola modu: 9,4 +/- 0,6 nm,
3. długość fali odcięcia: < 1260 nm.
	* 1. Właściwości geometryczne i mechaniczne:
4. średnica płaszcza: 125 +/- 2 µm.,
5. eliptyczność płaszcza: < 2 %,
6. niecentryczność pola modowego: < 1,0 µm,
7. średnica powłoki zewnętrznej: 250 +/- 15 µm,
8. niecentryczność powłoki: < 25 µm,
9. konstrukcja tubowa, dopuszczalny promień gięcia: 72 mm
10. We wskazanych w ust 1 pkt b) relacjach, Wykonawca zapewni następujące ilości i typy połączeń:
11. Postępu 3, Warszawa (Prokuratura Krajowa) – Czerniakowska 100, Warszawa (Ministerstwo Sprawiedliwości) w ilości 4x1Gbps Ethernet 1000BASE-T , 4x1Gbps Ethernet 1000BASE-SX, 4x1Gbps Ethernet 1000BASE-LX, 24x10Gbps Ethernet 10GBASE-SR, 4x40Gbps Ethernet (40GBASE-X), 4x100Gbps Ethernet (100GBASE-X), 12x 16Gbps FC
12. Postępu 3, Warszawa (Prokuratura Krajowa) – Rakowiecka 37a, Warszawa (Centralny Zarząd Służby Więziennej) w ilości 4x1Gbps Ethernet 1000BASE-T, 4x1Gbps Ethernet 1000BASE-SX, 4x1Gbps Ethernet 1000BASE-LX, 4x10Gbps Ethernet 10GBASE-SR w każdej relacji.

Wykonawca zapewni współpracę wskazanych interfejsów z posiadanymi przez Zamawiającego w danych lokalizacjach przełącznikami wyposażonymi w interfejsy o tej samej przepustowości producentów Cisco, Arista i Brocade.

1. Włókna światłowodowe wykorzystywane na potrzeby przedmiotowego zamówienia muszą:
2. być włóknami jednomodowymi i spełniać parametry jakościowe zgodne z zaleceniami: ITU - T G.652/655,
3. umożliwiać Zamawiającemu realizację dowolnej transmisji bez jakichkolwiek ingerencji Wykonawcy,
4. być zestawione w relacjach wskazanych w ust. 2,
5. być zakończone na przełącznicach światłowodowych znajdujących się w pomieszczeniach w wyżej wymienionych lokalizacjach (Punktach Styku).

Dodatkowo Wykonawca musi przewidzieć pozostawienie dodatkowych zapasów kabla światłowodowego zamontowanego w skrzyniach we wskazanych pomieszczeniach o długości 30 m po każdej stronie.

1. Urządzenia xWDM muszą posiadać budowę modularną, umożliwiającą rozbudowę i zwiększanie liczby portów, pozwalającą na wymianę komponentów w trakcie pracy bez konieczności przerw serwisowych. Usuwanie lub dodawanie dowolnej karty liniowej interfejsów nie może degradować usług na pozostałych kartach liniowych interfejsów. Urządzenia xWDM muszą obsługiwać co najmniej 2 razy więcej kanałów optycznych od ilości wskazanych w ust. 3 zgodnie z siatką kanałów określoną normach ITU-T G.694.1. Matryca przełączająca musi posiadać architekturę “non-blocking” umożliwiającą pracę wszystkich portów z pełną prędkością łącza na każdym ze slotów każdego z urządzeń. Redundancja matrycy przełączającej powinna zapewnić pracę bez utraty wydajności zainstalowanych i podwojonych portów łącznie nawet w przypadku awarii jednego z modułów przełączających. Wymagane jest zastosowanie urządzeń o architekturze rozdzielającej funkcjonalnie warstwę kontrolną od warstwy przełączającej. Urządzenia instalowane w lokalizacjach wskazanych w ust. 1 muszą pochodzić z legalnego kanału dystrybucji urządzeń na terenie UE i nie mogą być przeznaczone do innych projektów Wykonawcy. Urządzenia muszą posiadać wkładki interfejsów (m.in. SFP/SFP+/XFP), zgodnie z ilościami wskazanymi w ust 3, których zamontowanie nie spowoduje utraty gwarancji producenta urządzenia, w którym będą pracować. Każde z urządzeń musi posiadać redundantny system zasilania i chłodzenia. W przypadku awarii jednego z zasilaczy, każdy kolejny zasilacz musi przejąć system w pełni obciążony. Urządzenia muszą posiadać zapas miejsc na w kartach liniowych przeznaczony na wkładki co najmniej w ilości umożliwiającej Zamawiającemu podwojenie ilości połączeń w danej relacji bez ponoszenia innych kosztów niż koszt wkładki danego rodzaju.
2. Urządzenia xWDM muszą być urządzeniami możliwymi do zamontowania w szafie 19’ RACK lub szafie dedykowanej. W przypadku montażu w szafie dedykowanej, szafę taką należy dostarczyć obligatoryjnie. Urządzenia możliwe do montażu w standardowej szafie 19’ również muszą zostać dostarczone wraz z szafą. Zamawiający w zależności od możliwości technicznych może podjąć decyzję o braku konieczności dostarczenia standardowej szafy 19’.
3. Urządzenia pełniące funkcję xWDM muszą komunikować się za pomocą światłowodu jednomodowego G-652D wykorzystując jedną parę włókien w każdym kierunku.
4. Po zestawieniu relacji optycznych pomiędzy wskazanymi węzłami sieci Wykonawca musi wykonać pomiary wymagane normami dla każdego włókna światłowodowego w kablu:
5. pomiary reflektometryczne OTDR z przełącznic światłowodowych,
6. pomiary tłumienia metodą transmisyjną,
7. pomiary tłumienia odbiciowego,
8. pomiar reflektancji złączy optycznych dla każdego złącza.

Pomiary OTDR i transmisyjne należy wykonać dla minimum trzech długości fali - 1310 nm, 1550 nm i 1620 nm.

1. Instalacja kabli światłowodowych w kanalizacji powinna przebiegać zgodnie z normami technicznymi z uwzględnieniem parametrów mechanicznych kabla światłowodowego (maksymalny naciąg instalacyjny kabla, promień gięcia, temperatura układania, etc.) określonymi przez producenta kabla w dokumentacji technicznej.
2. Metoda instalacji kabli powinna być zgodna z zaleceniami producenta i typem kabla.
3. Identyfikację kabli powinny umożliwić trwałe napisy znacznikowe na powłoce kabla, wykonywane w sposób zapewniający trwałość oznaczenia. Napis na kablu musi zawierać oznaczenie producenta kabla, typ kabla, ilość włókien i ich rodzaj, datę produkcji, długość bieżącą, ewentualnie dane Inwestora.
4. **Testy Usługi**
5. Wykonawca przygotuje plan testów w którym określona będzie organizacja przeprowadzenia testów oraz harmonogram przeprowadzenia testów.
6. Plan testów oraz scenariusze testów podlegają odbiorowi przez Zamawiającego zgodnie z procedurą odbioru Produktu typu Dokument.
7. W ramach planowanych Testów Zamawiający wymaga przygotowania Scenariuszy testowych dla co najmniej następującego zakresu Testów:
	1. testy funkcjonalne przeprowadzane w każdej Lokalizacji. Testy będą miały na celu sprawdzenie zgodności z Projektem Technicznym oraz wymaganiami określonymi w Umowie,
	2. testy akceptacyjne - po wdrożeniu całego rozwiązania. Testy będą miały na celu sprawdzenie zgodności wykonania z Projektem Technicznym oraz wymaganiami określonymi w Umowie,
8. Testy akceptacyjne muszą zostać tak przygotowane przez Wykonawcę, aby było możliwe ich przeprowadzenie z siedziby Zamawiającego w Warszawie.
9. Scenariusze dla testów muszą być tak przygotowane, aby mogły być wykonane przez osoby spoza personelu Wykonawcy a wskazane przez Zamawiającego.
10. Sposób przygotowania scenariuszy testowych musi pozwolić na zweryfikowanie spełnienia wymagań określonych w niniejszym zamówieniu. W szczególności musi istnieć możliwość łatwego:
	1. zidentyfikowania wymagań OPZ weryfikowanych przez scenariusz,
	2. zidentyfikowania wymagań zawartych w Projekcie Technicznym.
11. Scenariusz testowy musi zawierać:
12. numer scenariusza – umożliwiający jego łatwą i bezbłędną identyfikację,
13. wskazanie testowanego zakresu oraz odniesienia do dokumentacji,
14. warunki wejściowe – lista warunków, jakie muszą być spełnione, aby można było rozpocząć wykonanie scenariusza,
15. oczekiwane wyniki testu,
16. zawierać opis działań osoby realizującej test w postaci kolejnych kroków, ze wskazaniem danych, których należy użyć. Opis winien być wyrażony w sposób prosty, przystępny dla osoby w ograniczonym stopniu zapoznanej z urządzeniami,
17. umożliwiać realizację scenariusza testowego w krótkim czasie, bez konieczności czasochłonnej lektury dużych fragmentów tekstu, lub odwoływania się do dokumentacji technicznej, przed jego wykonaniem,
18. prezentować oczekiwany wynik wykonania – opis pozwalający na jednoznaczną ocenę, czy przypadek testowy zakończył się sukcesem lub czy błędem,
19. jeżeli dla sprawdzenia wyniku przypadku testowego konieczne jest wykonanie pewnej sekwencji działań, to musi być ona również opisana w postaci kolejnych kroków,
20. każdy scenariusz w zbiorze scenariuszy musi cechować:
	* 1. prostota opisu – scenariusz powinien być opisany w sposób prosty, zrozumiały dla osoby nie znającej urządzeń lub zapoznanej z nim w ograniczony sposób,
		2. powtarzalność – powinno być możliwe wielokrotne wykonanie scenariusza w identyczny sposób na podstawie jego opisu,
		3. jednoznaczność – scenariusz przy spełnieniu wymagań wejściowych oraz realizacji wg. opisu powinien mieć ten sam przebieg oraz identyczny wynik,
		4. możliwość automatyzacji – w przypadku scenariuszy, w których automatyzacja jest możliwa.
21. Zamawiający będzie uważał Test za zaliczony, jeżeli rzeczywiste wyniki pomiarowe nie będą przekraczały parametrów granicznych wskazanych w spodziewanych wynikach pomiarowych dla tego testu.
22. Kierownik Projektu Wykonawcy w sposób pisemny lub pocztą elektroniczną poinformuje kierownika projektu Zamawiającego o przełączeniu rozgłaszania lokalnych sieci Zamawiającego do Routerów CE we wszystkich Lokalizacjach i o gotowości do przeprowadzenia drugiej części Testów – testów akceptacyjnych.
23. Przeprowadzanie testów akceptacyjnych rozpocznie się w terminie uzgodnionym z kierownikiem projektu Zamawiającego jednak nie później niż 5 Dnia Roboczego od dnia wpłynięcia zawiadomienia od Wykonawcy.
24. W przypadku jeżeli chociaż jeden test z grupy testów przeprowadzonych przez Wykonawcę w ramach Testów nie zostanie zaliczony, Wykonawca bez zbędnej zwłoki usunie przyczyny związane z niepowodzeniem danego testu lub testów i ponownie zgłosi gotowość do przeprowadzenia Testów. Przeprowadzanie Testów rozpocznie się w terminie uzgodnionym z kierownikiem projektu Zamawiającego jednak nie później niż 3 Dnia Roboczego od dnia wpłynięcia ponownego zawiadomienia od Kierownika Projektu Wykonawcy.
25. W ramach Testów funkcjonalnych, Wykonawca musi zmierzyć przynajmniej:
26. minimalną przepustowość w obu kierunkach w każdej Lokalizacji dla Usługi;
27. maksymalną utratę pakietów dla każdej klasy QoS w każdej Lokalizacji dla Usługi;
28. maksymalne opóźnienie (RTD) dla każdej klasy QoS w każdej Lokalizacji dla Usługi;
29. maksymalny Jitter dla klas QoS: w każdej Lokalizacji dla Usługi;
30. Testy parametrów łączy xWDM, tj. RTD, utratę pakietów i Jitter, a także testy przepustowości łączy w Lokalizacjach Zamawiającego dla Usługi należy wykonać miernikiem zgodnie ze standardem RFC 2544, przy następujących założeniach:
31. dla minimum trzech zdefiniowanych długości ramki, tj. dla minimum 256, 512 i 1518 bajtów;
32. parametr „throughput” ustawiony w taki sposób, aby wykonać pomiar dla 100% wymaganej przepustowości łączy;
33. warstwa modelu ISO/OSI: L3;
34. tolerancja pomiaru: nie większa niż 1 %;
35. czas prowadzenia każdego testu: minimum 5 minut;
36. ilość prób przeprowadzenia danego testu: 1 próba.
37. Miernik pomiarowy użyty do pomiarów łączy musi posiadać certyfikację organu upoważnionego aktualną na dzień prowadzenia pomiaru. Z certyfikacji musi wynikać, że miernik pracuje poprawnie, oraz że został on prawidłowo skalibrowany. Kopię takiego dokumentu Wykonawca zobowiązany jest przedstawić Zamawiającemu do wglądu przed rozpoczęciem wykonywania testów, a także zobowiązany jest dołączyć ją do dokumentacji powykonawczej.
38. Testy systemu xWDM będą obejmowały minimalnie następujące elementy:
39. Test 24h BER;
40. Pomiar mocy optycznych (nadawanych, odbieranych), czułości;
41. Pomiary parametrów właściwych dla systemów xWDM np. przesłuchy międzykanałowe, częstotliwości środkowych prążków, szerokości widmowe;
42. Testy alarmów sprzętowych i zewnętrznych.
43. Wykonawca może przystąpić do wykonywania Testów akceptacyjnych jeżeli jednocześnie spełni następujące trzy warunki:
44. uzyska odbiór wyników Testów funkcjonalnych;
45. uzyska odbiór propozycji Testów akceptacyjnych;
46. we wszystkich Lokalizacjach dokona migracji obecnie eksploatowanej sieci WAN-PROK oraz obecnej usługi transmisji danych z dostępem do sieci Internet do udostępnianej Usługi.
47. W ramach Testów akceptacyjnych Wykonawca musi przeprowadzić przynajmniej:
48. weryfikację poprawności konfiguracji i działania routingu dla każdego VRF na Routerze CE w każdej Lokalizacji;
49. weryfikację poprawności trasy domyślnej do centralnych styków z siecią Internet w każdej lokalizacji
50. weryfikację poprawności konfiguracji i działania usługi Anty DDoS;
51. weryfikację poprawności konfiguracji i kierowania określonego ruchu do danej klasy QoS;
52. weryfikację poprawności konfiguracji i działania automatycznego przełączania ruchu pomiędzy Podstawowym i Zapasowym Łączem transmisji danych w przypadku Awarii dla routerów na styku z DC oraz routerów odpowiedzialnych za centralny styk z siecią Internet;
53. weryfikację poprawności konfiguracji i działania automatycznego przełączania ruchu pomiędzy punktami styku do sieci Internet;
54. weryfikację poprawności konfiguracji i działania SMZ w zakresie wykrywania Awarii, zbierania i eksportowania statystyk, korelacji zdarzeń, wysyłania email i SMS z powiadomieniami o Awariach;
55. weryfikację poprawności konfiguracji i działania głównego oraz zapasowego DNS i revDNS;
56. weryfikację dostępności przynajmniej 5 podsieci DMZ z sieci Internet.
57. Szczegółowy zakres Testów akceptacyjnych Wykonawca zaproponuje oraz uzgodni z Kierownikiem Projektu Zamawiającego podczas realizacji Projektu.
58. Poprawna realizacja uzgodnionych testów funkcjonalnych będzie podstawą do podpisania Protokołu Odbioru Lokalizacji dla danej Lokalizacji.
59. Poprawna realizacja testów akceptacyjnych będzie podstawą do podpisania Protokołu Odbioru Końcowego.
60. **Szkolenia i Warsztaty**
61. Wykonawca w ramach umowy przeprowadzi warsztaty:
	1. warsztaty organizacyjne,
	2. warsztaty z zakresu wykorzystania SMZ,
	3. warsztaty z zakresu realizacji zadań SOC,
62. Wykonawca przeprowadzi warsztaty organizacyjne personelu technicznego Zamawiającego dla 75 osób w postaci warsztatów technicznych z zakresu wdrażanej Usługi. Warsztaty przeprowadzone będą w maksymalnie 20 osobowych grupach. Warsztaty trwać będą 3 dni robocze. Warsztaty będą prowadzone w języku polskim. Warsztat organizacyjny musi obejmować zagadnienia organizacyjne realizacji projektu oraz informacje techniczne z zakresu planowanego wdrożenia.
63. Wykonawca przeprowadzi warsztaty z zakresu realizacji zadań SOC personelu technicznego Zamawiającego dla 15 osób w postaci warsztatów technicznych. Warsztaty trwać będą 3 dni robocze. Warsztaty będą prowadzone w języku polskim. Warsztat musi obejmować zagadnienia organizacyjne współpracy SOC z personelem technicznym Zamawiającego, realizacja i definicja scenariuszy obsługi incydentów, zakres świadczenia usług przez I i II linię wsparcia, realizacja zgłoszeń badania próbek oprogramowania z zakresu planowanego wdrożenia itp.
64. Wykonawca przeprowadzi warsztaty z zakresu wykorzystania SMZ dla personelu technicznego Zamawiającego dla 75 osób w postaci warsztatów technicznych z zakresu SMZ. Warsztaty trwać będą 1 dzień roboczy. Warsztaty będą prowadzone w języku polskim i zostaną przeprowadzone w formie zdalnej.
65. Warsztaty określone w pkt 1 ppkt a Wykonawca przeprowadzi w terminie do 56 dni od dnia podpisania Umowy, po odbiorze Projektu Technicznego Usługi.
66. Szkolenie określone w pkt 1 ppkt b i c Wykonawca przeprowadzi nie później niż 30 dni przed terminem odbioru zestawienia i uruchomienia łączy realizujących Usługę.
67. Szkolenia/warsztaty zostaną przeprowadzone w ciągu następujących po sobie dni (w dni robocze tj. od poniedziałku do piątku, z wyłączeniem dni świątecznych).
68. W zakresie warsztatów o których mowa w ust. 1 pkt a. oraz pkt c. zadaniem Wykonawcy jest zapewnienie:
	1. bazy noclegowej – dla organizatorów i uczestników
		1. Obiekt nie może być w trakcie prac remontowych w czasie trwania spotkania.
		2. Wykonawca zapewnia wszystkie miejsca noclegowe w sposób zapewniający samodzielny pobyt w pokoju (Zamawiający dopuszcza zakwaterowanie samodzielne jednego uczestnika w pokoju dwuosobowym)
		3. Każdy z pokoi noclegowych z łazienką, TV, łącze internetowe (Wi-Fi) posiadających otwierane okna lub działającą klimatyzację.
		4. Obiekt co najmniej \*\*\* (trzy gwiazdki), w rozumieniu przepisów § 2 ust. 2 pkt 1 rozporządzenia Ministra Gospodarki i Pracy z dnia 19 sierpnia 2004 r. w sprawie obiektów hotelarskich i innych obiektów, w których są świadczone usługi hotelarskie (Dz. U. z 2006 r., Nr 22, poz. 169 ze zm.). Na każde żądanie Zamawiającego Wykonawca obowiązany jest okazać kopię decyzji właściwego Marszałka Województwa o nadaniu kategorii hoteli na podstawie art. 38 ust.1 i art. 42 ustawy z dnia 29 sierpnia 1997 r. o usługach turystycznych (Dz. U. z 2014 r., poz. 196 ze zm.),
		5. Na terenie obiektu lub w bezpośrednim jego sąsiedztwie powinien znajdować się bezpłatny parking.
		6. Obiekt powyżej trzech pięter powinien zostać wyposażony w windę
		7. Warsztaty, nocleg oraz wyżywienie powinny odbywać się na terenie tego samego obiektu.
		8. Obiekt zlokalizowany w promieniu 50 km od centrum Warszawy.
	2. odrębnych sal szkoleniowych dla każdej, równolegle szkolonej grupy. Każda z sal wykładowych przeznaczona jest maksymalnie dla 20 osób ze stanowiskiem dla wykładowców oraz miejscem na sprzęt multimedialny. Wszystkie sale szkoleniowe muszą być klimatyzowane i posiadać dostęp do światła dziennego oraz zapewniać komfortowe warunki do prowadzenia w nich szkoleń/warsztatów (tj. odpowiednie oświetlenie, odpowiednia temperatura).
	3. każda sala szkoleniowa musi być wyposażona w rzutnik multimedialny, ekran do wyświetlania prezentacji, tablicę do pisania lub flipchart z arkuszami papieru i pisakami, skaner, stację zarządzającą i stanowiska szkoleniowe dla każdej ze szkolonych osób, wyposażone w stację roboczą i zestaw 2-monitorowy. Wykonawca zapewni w miejscu przeprowadzania szkoleń/warsztatów urządzenia sieciowe umożliwiające wykreowanie tuneli VPN celem połączenia ze środowiskiem warsztatowym zorganizowanym po stronie Wykonawcy. Czas wykorzystania sal pierwszego dnia od godz. 12.00 do 20.00, pozostałe dni od godz. 8.00 do 19.00.
	4. noclegów dla uczestników szkolenia/warsztatów w pokojach jednoosobowych z łazienkami lub dwuosobowych z łazienkami do samodzielnego wykorzystania **(Wykonawca ma obowiązek zapewnić nocleg każdej osobie w odrębnym pokoju).** Czas trwania doby hotelowej od godz. 11.00 pierwszego dnia szkolenia do godz. 16.00 ostatniego dnia szkolenia. Miejsca noclegowe muszą znajdować się na terenie tego samego obiektu, co sale wykładowe.
	5. Wyżywienia dla uczestników szkolenia składającego się z:
69. śniadania podawanego w formie bufetu, obejmujące:

- pieczywo jasne i ciemne,

- wędliny (3 rodzaje),

- ser żółty

- ser biały

- jaja

- dżem

- miód

- ciepłe mleko

- płatki śniadaniowe (co najmniej 2 rodzaje)

- jogurt

- jedno danie ciepłe

- świeże warzywa (co najmniej 3 rodzaje)

- napoje (kawa, herbata, woda mineralna, sok 100%)

- masło, cytryna, mleko, cukier

1. obiadu w formie bufetu obejmującego:

- zupę,

- sałatki (minimum 2 rodzaje)

- dania ciepłe (rybne, mięsne, warzywne)

- dodatki skrobiowe

- desery

- napoje (kawa, herbata, woda mineralna, sok 100%)

1. kolacji w formie bufetu obejmującej:

- sałatki (minimum 2 rodzaje)

- pieczywo jasne i ciemne,

- wędliny (3 rodzaje),

- ser (3 rodzaje)

- dania ciepłe (rybne, mięsne, warzywne)

- napoje (kawa, herbata, woda mineralna, sok 100%)

- masło, cytryna, mleko, cukier

1. przerw kawowych (całodziennych, uzupełniany serwis konferencyjny), składający się:

- świeżo parzoną gorącą kawę naturalną oraz herbatę w torebkach

- cytrynę, cukier, mleko,

- sok owocowy 100%,

- butelkowana woda mineralna gazowana i niegazowana,

- co najmniej 3 rodzaje kruchych ciasteczek.

1. Posiłki, które będą podawane podczas szkoleń/warsztatów muszą być przygotowywane na terenie obiektu w którym odbywa się szkolenie. Wyklucza się ich dowożenie. W zakresie wyżywienia Wykonawca zobowiązany jest do:
2. Terminowego przygotowania posiłków zgodnie z ustalonym harmonogramem.
3. Zachowania zasad higieny i obowiązujących przepisów sanitarnych przy przygotowywaniu posiłków.
4. Przygotowywania posiłków zgodnie z zasadami racjonalnego żywienia, urozmaiconych (każdego dnia szkolenia inne menu), przygotowywanych ze świeżych produktów z ważnymi terminami przydatności do spożycia.
5. Wyżywienie dla trenerów oraz innych osób zaangażowanych w obsługę szkolenia/warsztatów Wykonawca zapewnia na swój koszt.
6. Zakres i szczegółowy plan szkoleń/warsztatów Wykonawca przedstawi Zamawiającemu do akceptacji minimum 10 dni roboczych przed rozpoczęciem pierwszego szkolenia/warsztatu.
7. Dla każdego typu szkoleń i warsztatów Wykonawca przygotuje materiały szkoleniowe, które zostaną przekazane Zamawiającemu do akceptacji minimum na 10 dni przed rozpoczęciem szkolenia.
8. Wykonawca zapewni prowadzenie szkoleń/warsztatów przez wykwalifikowaną kadrę posiadającą wiedzę teoretyczną i praktyczną z zakresu przedmiotu zamówienia oraz profesjonalny przebieg i organizację.
9. Przeprowadzane szkolenia/warsztaty zostaną potwierdzone protokołem odbioru szkolenia/warsztatu sporządzonym w dwóch jednobrzmiących egzemplarzach, po jednym dla Zamawiającego i Wykonawcy, zawierającym:
10. nazwę, tematykę i czas trwania szkolenia/warsztatów,
11. datę i miejsce szkolenia/warsztatów,
12. imienną listę osób uczestniczących w szkoleniach/warsztatach,
13. imię i nazwisko oraz specjalizację osób prowadzących szkolenia/warsztaty.
14. Protokół z przeprowadzenia szkoleń/warsztatów podlegać będzie zatwierdzeniu przez Zamawiającego.
15. Wszystkie szkolenia/warsztaty Wykonawca przeprowadzi w języku polskim, zapewniając materiały szkoleniowe (w języku polskim lub angielskim jeżeli nie są dostępne materiały szkoleniowe w języku polskim) dla uczestników warsztatów. W przypadku warsztatów organizowanych przez Wykonawcę, Wykonawca przeniesie na Zamawiającego prawa autorskie do opracowanych materiałów szkoleniowych.
16. Wykonawca dostarczy Zamawiającemu multimedialne materiały szkoleniowe w postaci zapisu na płycie CD-ROM (lub innym równoważnym nośniku).
17. Każdy uczestnik szkolenia otrzyma certyfikat udziału w szkoleniu/warsztacie.
18. Szkolenia/warsztaty realizowane przez Wykonawcę, będą realizowane w formie stacjonarnej. Zamawiający dopuszcza realizację w formie zdalnej w zależności od aktualnej sytuacji epidemiologicznej w okresie realizacji Umowy.
19. **Dokumentacja**
20. Wykonawca opracuje i przekaże Zamawiającemu Dokumentację Powykonawczą opracowaną na podstawie Projektu Technicznego z uwzględnionymi zmianami oraz uzupełnieniami wynikającymi z przeprowadzenia instalacji i konfiguracji Usługi.
21. Dokumentację powykonawczą dotyczącą robót budowlanych Wykonawca opracuje zgodnie z obowiązującymi przepisami prawa. W ramach dokumentacji dotyczącej robót budowlanych dla każdej Lokalizacji w obrębie budynków, na i w budynkach Zamawiającego muszą znajdować się przynajmniej:
22. mapy projektowe z naniesionymi trasami przyłączy i studzienek rewizyjnych - jeżeli wykonano lub użyto istniejących;
23. projekty wykonawcze instalacji;
24. projekty wykonawcze budowlano-konstrukcyjne;
25. wszelkie zgody i decyzje wynikające z przepisów Prawo budowlane i pokrewnych uzyskane przez Wykonawcę w imieniu Zamawiającego;
26. wszelką korespondencję i decyzje konserwatora zabytków uzyskane przez Wykonawcę w imieniu Zamawiającego, jeżeli wymagane;
27. zgoda na użytkowanie pasma koncesjonowanego, zgodnie z wymaganiami przepisów prawa - dla każdego zamontowanego bezprzewodowego łącza telekomunikacyjnego;
28. dokumenty stwierdzające dopuszczenie użytych materiałów do stosowania w budownictwie;
29. oświadczenie Wykonawcy o wykonaniu robót budowlanych w Lokalizacjach zgodnie z aktualnymi przepisami;
30. dokumenty potwierdzające utylizację odpadów powstałych w toku wykonywanych w Lokalizacjach robót.
31. Dokumentacja dotycząca robót budowlanych złożona u Zamawiającego musi zawierać wymagane pieczęcie i podpisy osób uprawnionych do przygotowania tej dokumentacji, w szczególności oświadczenie, podpis i pieczęć osoby uprawnionej stwierdzające wykonanie robót zgodnie z projektem.
32. Jeden egzemplarz dokumentacji dotyczącej robót budowlanych musi pozostać w Lokalizacji, której dotyczy ta dokumentacja, a drugi Wykonawca dostarczy do siedziby Zamawiającego w Warszawie i dołączy do Protokołu Odbioru Końcowego Usługi.
33. Dokumentacja Powykonawcza powinna dodatkowo zawierać co najmniej:
34. podania typu i parametrów katalogowych producenta Routerów CE oddzielnie dla każdego rodzaju routera;
35. podania rzeczywistych parametrów łączy Wykonawcy i fizycznego rodzaju każdego z Łączy dla każdej Lokalizacji;
36. podania spisu oraz wartości księgowej brutto na dzień instalacji zainstalowanych w każdej Lokalizacji urządzeń Wykonawcy podlegających zwrotowi po zakończeniu Umowy, w szczególności Routerów CE;
37. dołączenia kopii licencji na oprogramowanie - jeżeli zostanie takowe wykorzystane w urządzeniach Wykonawcy, w szczególności w systemie monitoringu;
38. dokumentacji (wraz z wynikami pomiarów) wykonanych testów akceptacyjnych;
39. dołączenia certyfikatów, instrukcji obsługi i eksploatacji, haseł, kart gwarancyjnych i innych koniecznych;
40. podania dostępu do baz wiedzy dotyczących obsługi i konfiguracji dostarczonego Routera CE oraz informacji
41. producenta na temat bezpieczeństwa oprogramowania i aktualizacji oprogramowania routera;
42. podania dokładnego opisu i rysunku topologii dla udostępnianej sieci dla Usługi;
43. podania dokładnego opisu systemu monitoringu, w szczególności instrukcji jego użytkowania w zakresie historycznych danych oraz komunikatów wysyłanych przez ten system;
44. podania danych kontaktowych serwisu Wykonawcy;
45. podania innych danych nie wymienionych powyżej, a koniecznych do kompletacji dokumentacji powykonawczej.
46. Dokumentacja powykonawcza musi być każdorazowo aktualizowana przez Wykonawcę w okresie świadczenia Usługi TD w przypadku dokonywania zmian.
47. **Świadczenie usługi SOC**
	1. **Definicje**

**Best Effort -** Stan realizacji usługi, w którym zostały przekroczone ograniczenia SLA ze względu na wystąpienie zwiększonego zapotrzebowania na usługę. W przypadku przekroczenia ograniczeń SLA Wykonawca niezwłocznie poinformuje Zamawiającego o zaistniałej sytuacji.

**Cyberbezpieczeństwo** - Adekwatny do potrzeb stan ochrony zapewniający możliwość wykrycia oraz reagowania na zdarzenia niepożądane oraz wskazane w dokumentacji systemu zarządzania bezpieczeństwem informacji Zamawiającego.

**Cyberprzestrzeń** - Przestrzeń, w której następuje wymiana, gromadzenie i udostępnianie informacji za pośrednictwem komputerów oraz komunikacja między człowiekiem i komputerem.

**Incydent Bezpieczeństwa Informacji (Incydent)** - Pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

**KSC** Ustawa o Krajowym Systemie Cyberbezpieczeństwa z 5 lipca 2018 roku (dziennik ustaw nr 1560/2018)

**Miejsce świadczenia usługi monitorowania cyberbezpieczeństwa** - Miejsce świadczenia usługi Monitorowania Cyberbezpieczeństwa przez zespół Wykonawcy spełniające wymagania ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).

**Pierwsza Linia Wsparcia** - Pierwsza Linia Wsparcia SOC - usługa realizująca w szczególności zadania:

* + - * 1. Monitoringu;
				2. Identyfikacji zdarzeń;
				3. Analizy i eliminacji prostszych znanych zdarzeń określonych w ramach Scenariusza Reakcji.

**Druga Linia Wsparcia -** Druga Linia Wsparcia SOC - usługa realizująca w szczególności zadania:

* + - * 1. Współpracy w reakcji na zdarzenia skomplikowane i nieznane;
				2. Tworzenie Scenariuszy Reakcji na powtarzalne zdarzenia;
				3. Nadzór nad poprawnością działania konfiguracji scenariuszy użycia;
				4. Wykonywanie comiesięcznych sprawdzeń działania systemów monitoringu (testy funkcjonalne).

**On-call -** Dyżur pod telefonem, czekanie w gotowości na zgłoszenie Drugiej Linii Wsparcia, wyłącznie dla Incydentów o priorytecie Poważnym.

**CTI/OSINT -** ang. *Cyber Threat Inelligence/OpenSource Inteligence* - narzędzia dostarczające szczegółowe informacje o technikach hakerskich, zagrożeniach, podatnościach, artefaktach lub umiejętności ich interpretowania i dekodowania oraz czynności pozwalające na pozyskanie informacji z powszechnie dostępnych źródeł umożliwiających powiększenie zakresu wiedzy na temat potencjalnych zagrożeń.

**PAM** - ang. *Privileged Access Management* - narzędzie wspierające nadzór nad sesjami uprzywilejowanymi oraz monitorowanie i zarządzanie uprzywilejowanymi kontami.

**PUODO -** Prezes Urzędu Ochrony Danych Osobowych - organ właściwy do spraw ochrony danych osobowych na terytorium Polski, utworzony ustawą z 10 maja 2018 roku o ochronie danych osobowych. Jest również organem nadzorczym w rozumieniu ogólnego rozporządzenia o ochronie danych.

**RODO -** Ustawa o ochronie danych osobowych z dnia 28 maja 2018 roku uszczegółowiające wymagania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) jest odpowiedzią na wyzwania związane ze zmieniającą się gospodarką danymi osobowymi.

**SOC -** Security Operations Center - centrum operacji bezpieczeństwa, którego zadaniem jest całodobowe monitorowanie, zapobieganie, wykrywanie, badanie i reagowanie na cyberzagrożenia.

**Scenariusz Reakcji -** Dokument opisujący wymagane czynności w przypadku wykrycia zdarzenia nieporządnego, składający się z:

* + - * 1. Zestawu możliwości technicznych wykrycia zdarzenia;
				2. Zdefiniowanych warunków wywołania zdarzenia niepożądanego;
				3. Opisu identyfikacji zdarzeń zależnych;
				4. Instrukcji reakcji na zdarzenie;
				5. Instrukcji uruchomienia działań korekcyjnych;
				6. Instrukcji wykonywania działań informacyjnych;
				7. Ogólnych i szczegółowych ścieżek eskalacyjnych.

**Scenariusz użycia systemu bezpieczeństwa -** Dokument opisujący zestaw zadań wymaganych do wykonania w ramach Drugiej Linii Wsparcia, w skład którego wchodzą między innymi:

* + - * 1. Skonfigurowanie jednego lub kilku źródeł zdarzeń;
				2. Opisanie procesu normalizacji;
				3. Przygotowanie Scenariuszy Reakcji w zakresie czynności wykonywanych przez Pierwszą Linię Wsparcia.

**System SIEM (SML)** - System zarządzania informacjami i zdarzeniami bezpieczeństwa informatycznego Zamawiającego, w którym zbierane są logi z systemów poddawane korelacji w celu wykrycia Incydentów. Zamawiający posiada System SIEM - Splunk.

**Usługa monitorowania Cyberbezpieczeństwa/Usługa SOC -** Zestaw czynności wykonywanych przez Wykonawcę w ramach umowy w celu identyfikacji Incydentów Bezpieczeństwa Informacji.

**Zdarzenia niepożądane -** Zdarzenie mogące wskazywać na wystąpienie incydentu bezpieczeństwa w środowisku chronionym.

**Zdarzenie False-Negative -** Wykrycie przez Drugą Linię Wsparcia, zdarzenia niepoprawnie rozpoznanego przy zastosowaniu ustalonych i zaakceptowanych procedur bezpieczeństwa. Realizacja i rozpoznawanie zdarzeń „ False-Negative".

**Zdarzenie False-Positive -** Wykrycie przez automatyczne systemy zdarzenia, które po analizie zostało uznane jako zdarzenie poprawne. W przypadku notorycznego występowania, statystycznie rozumianego jako więcej niż 100 zdarzeń „False - Positive" na 1 incydent bezpieczeństwa w miesiącu, należy uznać regułę automatyczną tworzącą takie zdarzenia jako błędną konfigurację systemu bezpieczeństwa.

**Przypadek testowy -** Celowe wykonanie pełnego przebiegu zdarzenia od momentu wystąpienia sytuacji niepożądanej do momentu zakończenia przetwarzania fazy analizy incydentu. Gdy jest to możliwe, obejmuje wykonanie odwracalnych kroków reakcji na incydent, sprawdzenie scenariusza end-to-end łącznie z zablokowaniem wskaźników kompromitacji w narzędziach prewencyjnych.

* 1. **Wymagania ogólne**
		+ 1. W ramach realizacji Umowy Wykonawca zapewni świadczenie Usługi monitorowania Cyberbezpieczeństwa. Zamawiający w celu realizacji usługi udostępni wskazanym pracownikom Wykonawcy (nie więcej niż 10 osób) posiadany SML. Świadczenie usługi będzie odbywało się w trybie 24/7/365.
			2. Wykonawca gwarantuje, że miejsce świadczenia Usługi wskazane w ofercie spełnia wymagania ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).
			3. Wykonawca do świadczenia usługi będzie wykorzystywał narzędzia udostępnione przez Zamawiającego - SML. Dostęp do SML pracowników Wykonawcy zostanie zrealizowany przez szyfrowane połączenie oraz posiadany przez Zamawiającego system klasy PIM/PAM nagrywający sesje osoby łączącej się. Parametry dostępu zostaną ustalone na etapie realizacji Projektu .
	2. **Wymagania dla Usługi monitorowania Security Operations Center.**

W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w SML zgodnie z opisanymi poniżej wymaganiami.

* + 1. **Pierwsza Linia Wsparcia**
			1. W ramach realizacji zadań Pierwszej Linii Wsparcia Wykonawca będzie odpowiedzialny za:
1. Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa w trybie 24 / 7 / 365, zgodnie z określonymi warunkami SLA.
2. Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji.
3. Analizę i eliminację najprostszych znanych zdarzeń określonych w ramach Scenariusza Reakcji.
4. Łączenie (korelowanie) zdarzeń i incydentów cyberbezpieczeństwa.
5. Dokumentowanie wykonanych czynności zgodnie z przygotowanymi i zaakceptowanymi Scenariuszy Reakcji.
6. Eskalowanie zdarzenia zgodnie w ramach ustalonego Scenariusza Reakcji.
7. Zamykanie zdarzeń błędnie rozpoznanych przez system bezpieczeństwa jako zagrożenie (tzw. False-Positive).
8. Priorytetyzowanie i kategoryzowanie zdarzeń bezpieczeństwa.
9. Przygotowywanie dziennych raportów wykrytych zdarzeń bezpieczeństwa.
	* 1. **Druga Linia Wsparcia**
10. W ramach realizacji zadań Drugiej Linii Wsparcia Wykonawca będzie odpowiedzialny za:
	1. Dostępność usługi dla Zamawiającego zgodnie z określonymi warunkami SLA.
	2. Analizę zgłoszonych przez Pierwszą Linię Wsparcia Incydentów cyberbezpieczeństwa oraz przygotowanie raportów i zaleceń poincydentalnych.
	3. Przygotowywanie i realizację Scenariuszy użycia systemu bezpieczeństwa zgodnie z wymaganiami przedstawionymi przez Zamawiającego.
	4. Przygotowanie Scenariuszy Reakcji.
	5. Przygotowanie Miesięcznych raportów z realizacji prac.
		1. **Scenariusze**
11. Scenariusz użycia systemu bezpieczeństwa.

Zamawiający wymaga przygotowania i wdrożenia co najmniej 50 scenariuszy użycia dla zidentyfikowanych ryzyk. Analiza ryzyka zostanie przeprowadzona na etapie realizacji Projektu. Każdorazowo Scenariusz użycia musi zostać zaakceptowany przez Zamawiającego. Zamawiający posiada listę przykładowych scenariuszy użycia, które należy przygotować i wdrożyć. Przykładowe scenariusz użycia:

1. Wykrywanie logowania z ominięciem systemu klasy PAM
2. Wykrywanie utworzenia użytkownika (lokalnego i domenowego)
3. Wykrycie złośliwego oprogramowania na chronionym obiekcie
4. Minimalny zakres zadań, z których ma być zbudowany Scenariusz użycia sytemu bezpieczeństwa zawiera:
5. Skonfigurowanie jednego lub kilku źródeł zdarzeń,
6. Opisanie procesu normalizacji,
7. Stworzenie reguł korelacyjnych w systemie SIEM mających na celu analizowanie w referencji do listy i/lub pól wyliczeniowych i/lub analizy statystycznej, lub w inny sposób mający ujawnić incydent bezpieczeństwa,
8. Stworzenie Scenariusza Reakcji w zakresie czynności wykonywanych przez Pierwszą Linię Wsparcia,
9. Opisanie szczegółowej ścieżki eskalacji,
10. Opracowanie scenariusza manualnego lub automatycznego sprawdzania poprawności działania. W przypadku pojawienia się nowych skuteczniejszych technik identyfikacji zagrożeń, Wykonawca ma obowiązek zaktualizować w porozumieniu z Zamawiającym istniejące Scenariusze użycia sytemu bezpieczeństwa.
11. Scenariusz Reakcji

Przygotowany przez Wykonawcę oraz zatwierdzony przez Zamawiającego Scenariusz Reakcji określa minimalny zestaw czynności konieczny do udokumentowania oraz wyciagnięcia powtarzalnych wniosków, na podstawie których zostaną podjęte określone czynności. Scenariusz Reakcji składa się z podzadań realizujących funkcje:

1. Wzbogacenia wiedzy o artefaktach tj. adresy IP, domeny, hash'e plików, nazwy plików, rozpoznawalność wskaźników kompromitacji przez narzędzia klasy CTI / OSINT, w celu wyciągania adekwatnych wniosków i podejmowania trafnych decyzji,
2. Analizy zidentyfikowanego zdarzenia, w tym w szczególności potwierdzenia, że zagrożenie w przypadku uruchomienia w środowisku Zamawiającego może stać się incydentem lub jest incydentem, jak również rozpoczęcia pobierania lub zabezpieczenia dodatkowych danych z zaatakowanego źródła ataku zasobu na potrzeby realizacji Pierwszej Linii Wsparcia,
3. Reakcji rozumianej jako ograniczenie możliwości wystąpienia zdarzenia niepożądanego, uruchomienia procesu eskalacyjnego lub innych czynności stosownych do zagrożenia w zakresie uzgodnionym z Zamawiającym,
4. Informowania i raportowania obejmującego dokumentowanie wykonanych czynności oraz rezultatów przeprowadzonej analizy lub zasadności czynności reakcji.
	* 1. **Raport Poincydentalny**
5. Zamawiający wymaga przygotowania Raportu Poincydentalnego dla incydentów o priorytecie Poważnym i Wysokim nie później niż do 2 dni roboczych od zakończenia realizacji zawierającego informacje:
6. Unikalny identyfikator zdarzenia
7. Kiedy incydent wystąpił?
8. Kiedy incydent został zauważony / wykryty?
9. Kto lub jaki proces był sprawcą incydentu?
10. Co się wydarzyło?
11. Gdzie wydarzenie miało miejsce?
12. Dlaczego zdarzenie mogło wystąpić?
13. Jakie czynności zostały przeprowadzone w celu powstrzymania incydentu?
14. Zalecenia Poincydentalne zawierające informację jakie zabezpieczenia zostały ustanowione lub powinny zostać ustanowione w celu zapobieżenia ponownemu wystąpieniu incydentu.
15. W przypadku przygotowania zaleceń, dla których konieczne jest wprowadzenie istotnych zmian do systemów bezpieczeństwa lub jakiejkolwiek rekonfiguracji systemów Zamawiającego Koordynator Wykonawcy przedstawi do akceptacji Koordynatorowi Zamawiającego zakres i szczegółową listę zmian. Zwolnione z takiej czynności są Zalecenia Poincydentalne konieczne do powstrzymania zidentyfikowanego Incydentu zagrażającego cyberbezpieczeństwu infrastruktury lub danych Zamawiającego.
	* 1. **Systemy Zamawiającego wymagające monitorowania**
16. Usługa monitorowania, będąca przedmiotem zamówienia, w szczególności będzie obejmowała logi/dane z poniższych systemów Zamawiającego ( źródło logów):

|  |  |
| --- | --- |
| **Rodzaj usługi lub urządzenia** | **Liczba urządzeń / nodów będących źródłami logów** |
| Active Directory (liczba serwerów) | 16 |
| Windows Server | 500 |
| Linux Server SUSE | 20 |
| Linux Server CENTOS / REDHAT  | 40 |
| DNS | 16 |
| Systemy bezpieczeństwa np.: serwer systemu antywirusowego, firewall, web application firewall, inne | 450 |
| Centralny Firewall | 6 |
| Pomocniczy Firewall | 8 |
| IPS/IDS | 6 |
| VPN | 6 |
| WAF  | 6 |
| System autoryzacji użytkowników sieci | 6 |

* 1. **Analiza złośliwego oprogramowania**
		+ 1. W ramach realizacji umowy, Zamawiający będzie mógł zlecić Wykonawcy wykonanie analizy złośliwego oprogramowania, w tym z wykorzystaniem technik inżynierii odwrotnej (ang. reverse engineering) nie większym niż 15 w ciągu roku. Sposób zgłaszania analizy złośliwego oprogramowania zostanie uzgodniony po podpisaniu umowy.
1. Zakres analizy złośliwego oprogramowania będzie nie mniejszy niż:
2. Analiza statyczna wskazanej próbki złośliwego oprogramowania,
3. Analizy dynamiczna w kontrolowanym środowisku pozwalającym na wyłączenie funkcji ukrywania lub wykrywania analizy,
4. Proces odwrotny do obfuskacji umożliwiający analizę kodu zaciemnionego,
5. Analiza występowania modułów pozwalających na kontrolę w tym szczegółowego określenia zaimplementowanych funkcji,
6. W przypadku wykorzystywania rodziny malware określenia wersji
7. Każdorazowo po wykonanej analizie złośliwego oprogramowania Wykonawca przekaże drogą mailową raport z wykonanej analizy. Zakres raportu zostanie ustalony po podpisaniu umowy.
	1. **Ogólne warunki SLA**

Wykonawca zapewni świadczenie Usługi SOC zgodnie z określonym poziomem SLA.

* 1. Pierwsza Linia Wsparcia
1. Czasy dla pierwszych Incydentów każdego dnia - nie mniej niż 50 i nie więcej niż 75, pozostałe zadania realizowane w trybie „Best Effort”. Dostępność usługi w trybie 24/7/365.

|  |  |
| --- | --- |
| Priorytet incydentu | Czas od wykrycia do |
| Podjęcia | Realizacji |
| Poważny | 15 min | 2 h |
| Wysoki | 60 min | 6 h |
| Średni | 2 h | 12 h |
| Niski | 4 h | 24 h |

* 1. Druga Linia Wsparcia
1. Czasy dla pierwszych Incydentów każdego dnia - nie mniej niż 5 i nie więcej niż 10, pozostałe zadania realizowane w trybie „Best Effort”. Dostępność usługi w dni robocze pomiędzy godzinami 7:00 a 18:00. Dodatkowo dla Incydentów o priorytecie Poważnym - w trybie „on-call":
	1. w dni robocze w godzinach 00:00 do 7:00 i 18:00 do 24:00
	2. w pozostałe dni w trybie „on-call" w godzinach 00:00 do 23:59

|  |  |
| --- | --- |
| Priorytet | Czas od eskalacji |
| incydentu | pierwszej linii wsparcia |
|  | do |  |
|  | Podjęcia | Realizacji |
| Poważny | 30 min | 24 h |
| Wysoki | 60 min | 2 dni |
| Średni | 2 h | 4 dni |

* 1. Analiza złośliwego oprogramowania

Przeprowadzenie analizy w terminie do 2 dni roboczych od przekazania podejrzanej próbki oprogramowania przez Koordynatora Zamawiającego do Koordynatora Wykonawcy oraz potwierdzenia otrzymania próbki przez Koordynatora Wykonawcy.

Czas podjęcia Incydentu będzie liczony jako delta czasu pomiędzy odnotowaniem wystąpienia zdarzenia w logach SML a czasem zweryfikowania poprawności nadania priorytetu.

Czas realizacji Incydentu będzie jako delta czasu pomiędzy podjęciem incydentu a zakończeniem obsługi podsumowanym wydanymi rekomendacjami i/lub raportem, w zależności od przypisanego scenariusza reakcji.

Zamawiający wyróżnia cztery poziomy incydentów: Poważny, Wysoki, Średni, Niski. Domyślnie każdy incydent zarejestrowany, jeżeli nie zostanie to uszczegółowione inaczej ma priorytet Średni.

Zgłoszenie incydentu Poważnego skutkuje bezzwłocznym uruchomieniem u Zamawiającego procesu eskalacyjnego;

|  |  |
| --- | --- |
| Priorytet | Opis  |
| Poważny | Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika:1. Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) trwającej co najmniej od 30 minut w tym aktywnie wykorzystywanego (więcej niż 1kb/min);
2. Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych;
3. Informacja od CSIRT NASK lub inny CSIRT;
4. Potwierdzona informacja od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową;
5. Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego;
6. Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności;
7. Nieautoryzowane dysponowanie uprawnieniami administracyjnymi;
8. Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, przesłanie na dyski webowe lub danych z wykorzystaniem nieautoryzowanych nośników przenośnych;
9. Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego wspierającego działanie usługi kluczowej;
 |

|  |  |
| --- | --- |
| Wysoki | Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym:1. Ujawnienie zestawionej sesji zwrotnej z C&C, trwającej co najmniej od 30 minut, aktywnie wykorzystywanej przez atakującego (więcej niż 1kb/min);
2. Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych w strefie chronionej;
3. Informacja od CSIRT NASK lub inny CSIRT;
4. Potwierdzona Informacja od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową;
5. Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego;
6. Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na utworzenie tylnej furtki, podsłuchu transmisji lub wykorzystania podatności;
7. Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, upload na dyski webowe lub przenoszenie przez nieautoryzowane pendrive;
8. Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamywania zabezpieczeń (tzw. grayware);
9. Ujawnienie nieznanego przez VirusTotal lub inne bazy reputacyjne oprogramowania mającego złośliwe funkcje pozwalające operatorowi na uruchomienie nieautoryzowanych skryptów lub kodu;
10. Celowany atak na personel Zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;
 |
| Średni | Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym:1. Atak na personel Zamawiającego mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;
2. Wszystkie przypadki wystąpienia na chronionych systemach komputerowych złośliwego oprogramowania, które jest rozpoznawane przez system antywirusowy ale nie zostało zatrzymane przez inny system bezpieczeństwa;
3. Wszystkie potwierdzone przypadki z naruszenia poufności, dostępności lub integralności wykryte przez systemy bezpieczeństwa dla których użytkownik wyklucza świadome lub nieświadome działanie; częściowo personalizowany atak na personel Zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;
 |

|  |  |
| --- | --- |
| Niski | Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu zdefiniowanego zdarzenia bezpieczeństwa opisanego scenariuszem reakcji, ale udało się potwierdzić że wywołanie zdarzenia było efektem realizacji autoryzowanych czynności służbowych z pominięciem ustalonych procedur bezpieczeństwa. |

* 1. **Transfer wiedzy**
1. Zamawiający wymaga aby w każdym półroczu trwania umowy, Wykonawca przeprowadził dla grupy nie większej niż 10 osób wskazanych przez Koordynatora Zamawiającego warsztaty. Jedno spotkanie Warsztatowe trwa nie mniej niż 4 godziny i nie więcej niż 8 godzin. Warsztaty swoim zakresem będą obejmować metody analizy i procedury monitorowania zdarzeń.
2. Szczegółowy harmonogram warsztatów oraz lista uczestników zostaną uzgodnione przez Koordynatorów stron.
	1. **Raportowanie i rozliczanie pracy**
		1. **Miesięczny Raport Rozliczenia Usług**
3. Każdy miesiąc świadczenia Usług potwierdzony zostanie Protokołem Odbioru.
4. Zamawiający zastrzega prawo zgłoszenia zastrzeżeń do Raportu, w terminie do 5 Dni roboczych od dnia jego otrzymania i zażądać uzupełnienia lub poprawy Raportu. Po uwzględnieniu przez Wykonawcę uwag do Protokołu Odbioru, w tym również Raportu Prac, Zamawiający w terminie kolejnych 3 Dni roboczych zweryfikuje ostateczną treść Protokołu Odbioru oraz Raportu Prac przed jego podpisaniem. W przypadku odmowy podpisania Raportu Prac przez Wykonawcę podstawę rozliczenia stanowi Raport Prac podpisany jednostronnie przez Zamawiającego.
5. Podpisany przez Strony Protokół Odbioru wraz z Raportem Prac stanowi podstawę do rozliczenia wynagrodzenia za świadczenie Usługi w miesiącu, którego dotyczą i podstawę do ewentualnego naliczenia kar umownych za miesiąc, w którym nastąpiło przekroczenie parametrów SLA .
6. Poza pierwszym raportem, każdy kolejny obejmuje okres od godziny 0:00 pierwszego dnia miesiąca kalendarzowego do ostatniego dnia miesiąca kalendarzowego do godziny 23:59.
7. Raport praca składa się z sekcji:
	* 1. Monitorowanie cyberbezpieczeństwa
* Data świadczenia usług
* Zestawienie poprawnie obsłużonych incydentów
* Identyfikator incydentu
* Nazwa
* Klasyfikacja priorytetu Incydentu
* Dokładna data i godzina ujawienia incydentu,
* Dokładna data i godzina podjęcia incydentu
* Dokładna data i godzina realizacji obsługi incydentu
* Statusy końcowe
* Liczba przygotowanych rekomendacji i raportów poincydentalnych
* Zestawienie niepoprawnie nieobsłużonych incydentów zgodnie z SLA
* Identyfikator incydentu
* Nazwa
* Klasyfikacja priorytetu Incydentu
* Dokładna data i godzina ujawnienia incydentu,
* Dokładna data i godzina podjęcia incydentu
* Dokładna data i godzina realizacji obsługi incydentu
* Statusów końcowych zdarzenia (false-positive, zamknięty)
* Ogólne rekomendacje i zalecenia Wykonawcy w zakresie cyberbezpieczeństwa w nawiązaniu do obsłużonych Incydentów w celu eliminacji możliwości pojawienia się incydentów w przyszłości.
	+ 1. Analiza złośliwego oprogramowania
* Data świadczenia usług
* Lista zgłoszonych analiz złośliwego oprogramowania
* Liczba analiz przeprowadzonych zgodnie z SLA
	1. **Audyt**
1. Wykonawca zobowiązuje się umożliwić Zamawiającemu lub wskazanemu przez niego podmiotowi przeprowadzanie audytów jakości prac Wykonawcy związanych z realizacją Umowy, w tym zgodności prowadzonych prac z postanowieniami Umowy. Wykonawca ma obowiązek zapewnić możliwość kontroli swoich prac, w szczególności niezwłocznie przekazać podmiotowi prowadzącemu audyt informacje i wyjaśnienia związane bezpośrednio z realizacją Umowy. Informacja o audycie i przedmiocie audytu zostanie przekazana Wykonawcy najpóźniej na 2 Dni Robocze przed terminem rozpoczęcia przeprowadzenia audytu. Z wykonania audytu Zamawiający sporządzi na piśmie protokół zaleceń poaudytowych i przekaże go Wykonawcy. Wykonawca zobowiązany jest do wprowadzenia na własny koszt i ryzyko zaleceń poaudytowych, wykazujących niezgodności w realizacji przez Wykonawcę Umowy. Wprowadzenie tych zaleceń poaudytowych nastąpi w terminie uzgodnionym przez Koordynatorów. W przypadku braku porozumienia co do terminu wprowadzenia ww. zaleceń poaudytowych obowiązuje termin wskazany przez Zamawiającego.
2. Zamawiający ma prawo do korzystania w związku z realizacją Umowy (w szczególności w związku z przeprowadzeniem kontroli realizacji Umowy, audytem, odbiorami lub jakimikolwiek innymi działaniami realizowanymi przez Zamawiającego) z usług upoważnionych przez niego podmiotów zewnętrznych. Zamawiający zobowiąże wskazane powyżej podmioty do zachowania poufności w odniesieniu do wszystkich informacji, w jakich posiadanie wejdą one w związku z prowadzonymi przez siebie czynnościami oraz do niewykorzystywania tych informacji w celu innym niż świadczenie prac na rzecz Zamawiającego. Wykonawca jest zobowiązany do współpracy z upoważnionymi podmiotami w pełnym zakresie wynikającym z upoważnienia, na zasadach określonych w Umowie względem Zamawiającego. W przypadku cofnięcia upoważnienia dla podmiotów zewnętrznych, Zamawiający jest zobowiązany do niezwłocznego poinformowania Wykonawcy o tym fakcie.
	1. Wykonawca nie może odmówić wstępu do pomieszczeń, w których jest realizowana Umowa, udostępnienia żądanych informacji, dokumentów lub produktów związanych z realizacją Umowy, w tym mających wpływ na dochowanie terminów oraz zachowanie jakości, nawet jeśli objęte są tajemnicą przedsiębiorstwa. Zamawiający oraz osoby działające na jego rzecz zobowiązani są zachować informacje objęte tajemnicą przedsiębiorstwa Wykonawcy w poufności i mogą wykorzystać uzyskane w ten sposób informacje wyłącznie dla potrzeb kontroli, audytu, odbiorów lub innych działań realizowanych przez Zamawiającego.
	2. Pozyskanie informacji niezbędnych do dokonania kontroli lub przeprowadzenia audytu nie może wiązać się dla Zamawiającego z dodatkowymi kosztami. W szczególności, na wniosek Zamawiającego Wykonawca zapewni obecność osób niezbędnych do zrealizowania zadań audytorskich w siedzibie Zamawiającego.