

Umowa nr [●]/[●] zawarta w [●] w dniu [●]* / w formie elektronicznej**, pomiędzy:

Skarbem Państwa - Ministrem Sprawiedliwości, adres do doręczeń: Aleje Ujazdowskie 11, 00-567 Warszawa, zwanym dalej „**Zamawiającym**” – w imieniu którego działa:

[●] – [●], na podstawie [●],

a

[●], zwaną dalej „**Wykonawcą**”.

Zamawiający i Wykonawca mogą być też zwani każdy z osobna „Stroną” lub łącznie „Stronami”.

Preambuła

W wyniku rozstrzygniętego postępowania o udzielenie zamówienia nr DIRS-XX.044.1.2025 na „Usługę dostępu do sieci Internet”, do którego nie stosuje się przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (na podstawie art. 2 ust. 1 w zw. z art. 30 ust. 4 tej ustawy, tj. z uwagi na jego wartość netto [●] złotych netto, która nie przewyższa 20% wartości całego zamówienia, a przy tym nie przekracza progu stosowania ustawy, tj. 130 000 złotych netto), Strony zawierają Umowę o następującej treści:

Definicje

Ilekoć niniejsza Umowa posługuje się pojęciem:

- 1) Atak DDoS (ang. Distributed Denial of Service) – rozumie się atak na systemy komputerowe dostawców treści i usług internetowych lub serwisy internetowe udostępnione przez Zamawiającego w sieci Internet, polegający na próbie uniemożliwienia działania systemów, usług lub serwisów poprzez zajęcie wolnych zasobów;
- 2) Awaria – rozumie się przez to uszkodzenie powodujące przerwę lub uniemożliwiające korzystanie przez Zamawiającego z Usługi;
- 3) Czas niedostępności (CN) – rozumie się przez to wyrażony w godzinach parametr określający sumę wszystkich CUA w danym miesiącu kalendarzowym, zaokrągloną w górę do pełnych godzin;
- 4) Czas reakcji (CR) – rozumie się przez to czas od wykrycia Awarii przez Wykonawcę lub od zgłoszenia Awarii przez Zamawiającego do podjęcia przez Wykonawcę niezbędnych działań naprawczych, zgodnie z § 5 Umowy;
- 5) Czas reakcji na Atak DDoS (CRA) – rozumie się przez to czas, jaki upłynie od wykrycia Ataku DDoS do skutecznego poinformowania Zamawiającego o tym Ataku przez ustalone kanały komunikacji (telefonicznie lub pocztą elektroniczną);
- 6) Czas reakcji na zlecenie oczyszczania ruchu (CRZ) – rozumie się przez to czas, jaki upłynie od przekazania zlecenia przez Zamawiającego z żądaniem włączenia lub wyłączenia oczyszczania po zarejestrowanym Ataku DDoS;
- 7) Czas usunięcia Awarii (CUA) – rozumie się przez to czas usunięcia Awarii, liczony od chwili (godzina.minuta) wykrycia Awarii przez Wykonawcę lub zgłoszenia przez Zamawiającego, zgodnie z § 5 Umowy, do chwili (godzina.minuta) jej usunięcia;
- 8) Dostępność miesięczna (DM) – rozumie się przez to zdolność do transmisji danych z wykorzystaniem protokołu internetowego pomiędzy urządzeniami punktów zakończenia sieci Wykonawcy a routerem brzegowym Zamawiającego oraz zapewnienie pozostałych świadczeń wchodzących w zakres Usługi; parametr ten wyrażony jest w procentach, a wyliczany zgodnie z wzorem: $DM = (720 - CN) / 720 * 100\%$;

- 9) dzień roboczy – rozumie się przez to dzień przypadający od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy;
- 10) Informacje – dane techniczne, technologiczne, organizacyjne, w szczególności dotyczące struktury, konfiguracji i systemów zabezpieczeń, lub inne informacje poufne, czyli takie, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób i co do których uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności), niezależnie od formy przekazania tych informacji oraz ich źródła;
- 11) łącze – rozumie się przez to połączenie zestawione pomiędzy routerem brzegowym Zamawiającego a siecią Wykonawcy, w celu korzystania z Usługi;
- 12) Okno serwisowe – rozumie się przez to uzgodniony z Zamawiającym z wyprzedzeniem co najmniej 4 dni roboczych przedział czasu przeznaczony na wykonywanie prac konserwacyjnych lub modernizacyjnych w sieci Wykonawcy, w którym może wystąpić przerwa w świadczeniu Usługi. Zamawiający dopuszcza nie więcej niż dwa Okna serwisowe w miesiącu kalendarzowym, przy czym muszą one przypadać w godzinach od 00.00 do 4.00 rano lub w soboty, niedziele i w dni ustawowo wolne od pracy w godzinach od 22.00 do 6.00 rano;
- 13) Umowa – rozumie się przez to niniejszą umowę;
- 14) Usługa – rozumie się przez to zapewnienie Zamawiającemu dostępu do sieci Internet w oparciu o zestawione i utrzymywane przez Wykonawcę łącze dostępowe wraz z niezbędnymi urządzeniami teletransmisyjnymi oraz usługą ochrony przed Atakami DDoS.

§ 1

Przedmiot Umowy

1. Przedmiotem Umowy jest świadczenie przez Wykonawcę, na rzecz Zamawiającego usługi dostępu do sieci Internet w oparciu o zestawione i utrzymywane przez Wykonawcę łącze dostępowe wraz z niezbędnymi urządzeniami teletransmisyjnymi oraz usługą ochrony przed Atakami DDoS, obejmujące:
 - 1) zestawienie, uruchomienie i udostępnienie przez całą dobę, przez cały okres realizacji Umowy, stałego symetrycznego łącza dostępowego, wraz z niezbędnym do podłączenia do infrastruktury Zamawiającego sprzętem, w tym urządzeniami teletransmisyjnymi (m.in. w tym routery, przełącznice), zapewniającego szerokopasmowy dostęp do Internetu o przepustowości gwarantowanej co najmniej 3 Gb/s (+/-5%), przyłączonego po stronie Zamawiającego do routera brzegowego za pośrednictwem interfejsu SFP-10G-LR, zlokalizowanego w obiekcie na terenie miasta stołecznego Warszawy;
 - 2) dostęp do wszystkich usług i serwisów internetowych krajowych i zagranicznych;
 - 3) obsługę adresów IPv4 PI (Provider Independent) posiadanych przez Zamawiającego;
 - 4) obsługę ruchu generowanego przez Zamawiającego przy pomocy dynamicznego protokołu routingu BGP (Border Gateway Protocol);
 - 5) konfigurację routera brzegowego w siedzibie Zamawiającego w zakresie przyłączenia łącza Internetowego (zestawienie sesji BGP) w porozumieniu z obecnym dostawcą usługi dostępu do Internetu;
 - 6) utrzymanie secondary DNS dla domeny ms.gov.pl;
 - 7) zapewnienie Zamawiającemu możliwości całodobowego monitoringu łącza i jego wykorzystania, np. poprzez MRTG (ang. Multi Router Traffic Grapher);

- 8) możliwość odfiltrowania ruchu sieciowego niepożądanego przez Zamawiającego na urządzeniach dostępowych Wykonawcy;
- 9) zapewnienie Zamawiającemu usługi ochrony przed Atakami DDoS, w tym atakami wolumetrycznymi, na usługi uruchomione przez Zamawiającego w publicznej sieci Internet w trybie 24/7/365 (24/7/366 w roku przestępnym):
 - a) Zamawiający wymaga, aby usługa ochrony przed Atakami DDoS realizowana była w sposób proaktywny na urządzeniach Wykonawcy, bez przekierowywania ruchu poza teren Rzeczypospolitej Polskiej,
 - b) szczegółowe wymagania dla usługi ochrony przed Atakami DDoS zawarto w Załączniku nr 1 do Umowy.
2. W ramach Umowy, Wykonawca zobowiązany jest do:
 - 1) wykonania projektu technicznego konfiguracji urządzeń wraz z projektem wykonawczym usługi proaktywnej ochrony przed Atakami DDoS zgodnie z pkt 11 Załącznika nr 1 do Umowy. Projekt techniczny powinien zawierać co najmniej: lokalizację przyłącza wraz z trasą przebiegu kabla do budynku i wewnątrz budynku, schemat logiczny przyłącza, konfigurację urządzeń, warunki testowania przepustowości;
 - 2) przyłączenia routera brzegowego w siedzibie Zamawiającego do łącza zapewniającego połączenie z Internetem,
 - 3) wykonania rekonfiguracji adresacji, ACL, mechanizmów bezpieczeństwa, QoS na urządzeniu brzegowym (dostarczonym przez Wykonawcę do Zamawiającego oraz posiadanym przez Zamawiającego o modelu: Catalyst 8300) w siedzibie Zamawiającego. Wszelkie prace konfiguracyjne urządzeń Zamawiającego będą wykonywane przez pracowników Zamawiającego przy współpracy z Wykonawcą,
 - 4) wykonania testów funkcjonowania łącza z uwzględnieniem dynamicznego przekierowania ruchu do drugiej lokalizacji Zamawiającego Al. Ujazdowskie 11 w Warszawie / ul. Czerniakowska 100 w Warszawie, w przypadku Awarii łącza,
 - 5) opracowania dokumentacji powykonawczej, zawierającej zaktualizowany projekt techniczny wraz z projektem wykonawczym usługi proaktywnej ochrony przed Atakami DDoS.
3. Wykonawca zobowiązany jest w terminie 30 dni od dnia uruchomienia Usługi, o którym mowa w § 2 ust. 1 i 2, przesłać Zamawiającemu dokumentację powykonawczą, o której mowa w ust. 2 pkt 5, w języku polskim, w postaci elektronicznej (skan oryginału oraz wersja edytowalna .docx) na adres poczty elektronicznej Zamawiającego wskazany w Załączniku nr 4 do Umowy. Zamawiający w terminie 3 dni roboczych od otrzymania dokumentacji powykonawczej dokona jej akceptacji lub zgłosi swoje uwagi, przesyłając je na adres poczty elektronicznej Wykonawcy wskazany w Załączniku nr 4 do Umowy. Wykonawca zobowiązany jest w terminie 3 dni roboczych od dnia otrzymania uwag do ich uwzględnienia i przedstawienia poprawionej wersji dokumentacji powykonawczej.

§ 2

Termin realizacji przedmiotu Umowy

1. Zestawienie stałego symetrycznego łącza dostępowego oraz skonfigurowanie i uruchomienie Usługi zgodnie z § 1 ust. 1 pkt 1 nastąpi w terminie do 30 dni od dnia zawarcia Umowy. Odbiór będzie polegał na weryfikacji poprawności wykonania czynności w ramach uruchomienia Usługi i potwierdzeniu uruchomienia Usługi o parametrach wskazanych w Umowie oraz poprawności działania łącza. Wzór Protokołu uruchomienia Usługi dołączono w Załączniku nr 2 do Umowy.

2. Wykonawca będzie świadczył Usługę przez okres 12 miesięcy, poczynając od dnia uruchomienia Usługi, potwierdzonego w Protokole uruchomienia Usługi.

§ 3

Oświadczenia i zobowiązania Stron

1. Strony zobowiązane są współdziałać w celu należytej realizacji przedmiotu Umowy.
2. Wykonawca zobowiązuje się współdziałać z jednostkami organizacyjnymi lub osobami trzecimi wskazanymi przez Zamawiającego, w celu zapewnienia ciągłości procesów biznesowych Zamawiającego.
3. Wykonawca zobowiązuje się do wykonywania przedmiotu Umowy z należytą starannością profesjonalisty, zgodnie z aktualnym stanem wiedzy fachowej, zasadami cyberbezpieczeństwa i dobrymi praktykami stosowanymi w branży IT, przy czym w zakresie świadczeń o charakterze dzieła Wykonawca ponosi odpowiedzialność jak za dzieło.
4. Wykonawca zobowiązuje się przy wykonywaniu Umowy:
 - 1) przestrzegać przepisów prawa, zasad BHP, regulaminów wewnętrznych Ministerstwa Sprawiedliwości oraz procedur obowiązujących w obiektach Ministerstwa Sprawiedliwości, o ile mają zastosowanie;
 - 2) stosować instrukcje obiektów i wyposażenia, karty charakterystyki (o ile mają zastosowanie) oraz instrukcje lub inne wytyczne producentów poszczególnych elementów infrastruktury (sprzętów, urządzeń i instalacji) oraz oprogramowania;
 - 3) zapewnić obsługę przez personel posiadający stosowne umiejętności i wiedzę, wyposażony w sprzęt i narzędzia niezbędne do profesjonalnego świadczenia usług objętych przedmiotem Umowy;
 - 4) zapewnić, aby z przyczyn leżących po stronie Wykonawcy nie doszło na etapie realizacji Umowy do zakłócenia normalnego funkcjonowania infrastruktury Ministerstwa Sprawiedliwości ani systemów teleinformatycznych pozostających w dyspozycji Zamawiającego, w tym incydentów związanych z bezpieczeństwem informacji ani obowiązków ciążyących na Zamawiającym jako administratorze danych osobowych;
 - 5) niezwłocznie poddać się kontroli w zakresie prawidłowości realizacji niniejszej Umowy przez Ministerstwo Sprawiedliwości lub inne upoważnione podmioty, na wezwanie Zamawiającego.
5. Zamawiający zobowiązuje się do udostępnienia procedur i dokumentów, o których mowa w ust. 4 pkt 1 i 2 powyżej, przed przystąpieniem przez Wykonawcę do realizacji stosownych zadań w ramach przedmiotu Umowy, bez uszczerbku dla ust. 15. Zakres oraz sposób udostępniania tej dokumentacji określi Zamawiający, po konsultacji z Wykonawcą.
6. W przypadku, gdy należyta realizacja przedmiotu Umowy wymaga podjęcia określonego działania przez Zamawiającego, Wykonawca niezwłocznie poinformuje o tym Zamawiającego w formie pisemnej albo w formie elektronicznej, wskazując na zakres i uzasadnienie konieczności takiego działania.
7. Wykonawca zobowiązuje się do niezwłocznego informowania Zamawiającego o wszelkich zdarzeniach, które mogą mieć wpływ na jakość, terminowość bądź zakres realizacji przedmiotu Umowy.
8. Zaniechanie terminowego wykonania zobowiązań, o których mowa w ust. 6 lub 7, o ile Wykonawca w danym zakresie wiedzę posiada lub przy uwzględnieniu wymaganej Umową staranności powinien ją posiadać, uprawnia Zamawiającego do obciążenia Wykonawcy poniesionymi kosztami i wydatkami.

9. Na wezwanie Zamawiającego, Wykonawca niezwłocznie zapewni wgląd w dokumentację związaną z realizacją przedmiotu Umowy oraz poinformuje Zamawiającego o szczegółach przebiegu realizacji Umowy w formie pisemnej albo w formie elektronicznej.
10. Zamawiający umożliwi Wykonawcy dostęp do obiektów, danych i informacji, w tym objętych poufnością lub chronionych, w zakresie niezbędnym do realizacji przedmiotu Umowy. Zakres oraz warunki udostępniania obiektów, danych i informacji określi Zamawiający.
11. Wykonawca ponosi odpowiedzialność za właściwą organizację, bezpieczeństwo i jakość wykonywania przedmiotu Umowy.
12. Wykonawca ponosi odpowiedzialność za działania lub zaniechania związane z realizacją Umowy, chyba że szkoda nastąpiła wskutek siły wyższej, o której mowa w § 13 albo z wyłącznej winy Zamawiającego.
13. Wykonawca ponosi odpowiedzialność za udostępnione mu przez Zamawiającego mienie w związku z realizacją Umowy. Zamawiający upoważniony jest do obciążenia Wykonawcy kosztami odpowiednio naprawy lub wymiany, jeżeli uszkodzenie mienia wynikało z działania lub zaniechania Wykonawcy. Postanowienia zdań poprzedzających stosuje się odpowiednio do powierzonych danych.
14. W zakresie, w jakim Umowa przewiduje wskazanie przez Zamawiającego lub uzgodnienie przez Strony szczegółów odnośnie sposobu realizacji przedmiotu Umowy, stosowanie się do takich wskazówek / uzgodnień, nie zwalnia Wykonawcy z odpowiedzialności za niewykonanie lub nienależyte wykonanie Umowy, w tym za wady przedmiotu Umowy, chyba że Wykonawca poinformował Zamawiającego w formie pisemnej albo w formie elektronicznej o ryzyku jakie wiąże się z przestrzeganiem tych wskazówek / uzgodnień.
15. Zamawiający zobowiązuje się do:
 - 1) dostarczenia Wykonawcy, w terminie 5 dni od dnia zawarcia Umowy, informacji i danych niezbędnych do jej realizacji, a w szczególności do udostępnienia niezbędnych dokumentów, w tym rzutów budynków oraz pomieszczeń w lokalizacji Zamawiającego koniecznych do instalacji elementów aktywnych;
 - 2) zapewnienia warunków do instalacji stałego symetrycznego łącza dostępowego, o którym mowa w § 1 ust. 1 pkt 1, poprzez:
 - a) zapewnienie w swoich obiektach miejsca do instalacji urządzeń sieciowych i łącza;
 - b) udostępnienie zasilania elektrycznego dla niezbędnych urządzeń dostarczonych przez Wykonawcę.
16. Wykonawca ma prawo, po uprzednim pisemnym poinformowaniu Zamawiającego oraz po upływie 7 dni od pisemnego potwierdzenia przez Zamawiającego otrzymania informacji, do odłączenia Zamawiającego od sieci Internet bez odszkodowania w przypadku stwierdzenia:
 - 1) dopuszczenia do sieci osób nieuprawnionych, o ile Zamawiający nie zareaguje na wcześniejsze poinformowanie ze strony Wykonawcy potwierdzone przez Zamawiającego,
 - 2) działania na szkodę innych abonentów lub operatorów sieci współpracujących z Wykonawcą, w tym także na skutek niedołożenia należytej staranności w zakresie zapewnienia ochrony nad zarządzaną przez siebie infrastrukturą, o ile Zamawiający nie zareaguje na wcześniejsze poinformowanie ze strony Wykonawcy potwierdzone przez Zamawiającego.
17. Wykonawca gwarantuje:
 - 1) całodobowe świadczenie Usługi na poziomie DM nie niższym niż 99,72 % w skali miesiąca, co oznacza, że CN nie może przekroczyć 2 godzin w skali miesiąca,

- 2) gotowość Wykonawcy do potwierdzenia i usunięcia Awarii w trybie 24/7/365, tj. przez 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku (a w roku przestępnym 366 dni), w tym również w soboty, niedziele oraz dni ustawowo wolne od pracy, przez cały okres realizacji Usług,
 - 3) Czas Reakcji (CR) na Awarię wynoszący do 30 minut od wykrycia przez Wykonawcę lub zgłoszenia przez Zamawiającego.
18. Dostępna przepustowość, która jest określona w § 1 ust. 1 pkt 1, jest gwarantowana przez Wykonawcę w punktach styku sieci IP Wykonawcy z sieciami IP operatorów Internetu, z którymi Wykonawca wymienia bezpośrednio ruch internetowy.
19. Wykonawca gwarantuje także:
- 1) brak limitów ruchu – dostęp do Internetu musi być zapewniony bez jakichkolwiek limitów czasu dostępu, bez względu na liczbę użytkowników czy też liczbę przesłanych lub odebranych danych;
 - 2) to, że łącze internetowe pozwala na wykorzystanie pełnego pasma, dla pojedynczych sesji.
20. Każda ze Stron zobowiązuje się do podejmowania działań mających na celu zapewnienie bezpieczeństwa transmisji danych w ramach korzystania z usługi dostępu do Internetu, zgodnie z obowiązującymi przepisami prawa oraz przyjętymi standardami technicznymi i organizacyjnymi. W szczególności Wykonawca zobowiązuje się do stosowania środków ochrony sieci przed nieautoryzowanym dostępem, złośliwym oprogramowaniem oraz innymi zagrożeniami teleinformatycznymi.
21. Informacje Zamawiającego przesyłane przez sieć telekomunikacyjną podlegają ochronie zgodnie z powszechnie obowiązującymi przepisami prawa.
22. Wykonawca nie ponosi odpowiedzialności za treść danych przesyłanych przez użytkowników za pośrednictwem świadczonej usługi, ani za skutki ich wykorzystania przez osoby trzecie.
23. Wykonawca zapewnia sprawność sieci telekomunikacyjnej na odcinku od urządzeń transmisji danych Wykonawcy instalowanych w lokalizacji Zamawiającego i zarządzanych przez Wykonawcę na potrzeby świadczenia Usługi do punktu styku z siecią innych przedsiębiorców telekomunikacyjnych, a także sprawność wymienionych wyżej urządzeń Wykonawcy przez cały okres realizacji Umowy.

§ 4

Przedstawiciele Stron

1. Do bieżącej współpracy Stron w zakresie realizacji niniejszej Umowy (w tym podpisywania protokołów), Zamawiający wskazuje dane i upoważnia osoby zestawione w tabeli 1 w Załączniku nr 4 do Umowy.
2. Do bieżącej współpracy Stron w zakresie realizacji niniejszej Umowy (w tym podpisywania protokołów), Wykonawca wskazuje dane i upoważnia osoby zestawione w tabeli 2 w Załączniku nr 4 do Umowy.
3. Osoby zestawione w Załączniku nr 4 do Umowy, upoważnione są do wykonywania w imieniu mocodawcy czynności określonych w niniejszej Umowie, z wyłączeniem zmiany postanowień tej Umowy, jej rozwiązania lub odstąpienia od Umowy.
4. Zmiana danych zestawionych w Załączniku nr 4 do Umowy powyżej nie będzie stanowiła zmiany Umowy i będzie skuteczna od dnia doręczenia zawiadomienia Strony, której dane się zmieniły, wraz ze wskazaniem nowych danych kontaktowych – wystosowanego w formie pisemnej albo w formie elektronicznej – drugiej Stronie.

5. W przypadku zmian osób wskazanych w ust. 1 i 2 powyżej, postanowienie ust. 4 powyżej stosuje się odpowiednio.
6. Wszelka korespondencja dotycząca Umowy, prowadzona będzie w postaci elektronicznej (zwykłą pocztą elektroniczną, tj. bez opatrywania jej kwalifikowanym podpisem elektronicznym), chyba że określone postanowienie Umowy wprost wskazuje na wymóg dochowania danej czynności w określonej formie.
7. Korespondencja dostarczana osobiście lub wysłana pocztą lub kurierem na adres Strony, będzie uznana za skutecznie doręczoną we wcześniejszej z dat: (i) z dniem, w którym Strona odebrała przesyłkę, (ii) z dniem, w którym Strona odmówiła odbioru przesyłki, (iii) z upływem terminu wskazanego w awizo przesyłki wysłanej listem poleconym.
8. Korespondencja wysłana pocztą elektroniczną na adres e-mail odbiorcy będzie uznana za skutecznie doręczoną we wcześniejszej z dat: (i) w dacie jej dostarczenia do serwera poczty odbiorcy, (ii) w dacie pierwszej próby dostarczenia do serwera poczty odbiorcy, w razie stwierdzenia niemożności dostarczenia, chyba że adresat wykazał, że brak możliwości dostarczenia spowodowany był wadą teletransmisyjną lub techniczną z przyczyn nieleżących po stronie adresata lub zdarzeniem o charakterze siły wyższej, o której mowa w § 13.

§ 5

Odbiór przedmiotu Umowy

1. Przedmiot Umowy podlega protokolarnemu odbiorowi przez Zamawiającego.
2. O gotowości uruchomienia Usługi, Wykonawca zawiadomi Zamawiającego z co najmniej tygodniowym wyprzedzeniem. Do protokołu dotyczącego uruchomienia Usługi dołącza się wyniki testowania i aktywacji Usługi.
3. Jeżeli podczas testowania i aktywacji Usługi okaże się, że Wykonawca nie wykonał wszystkich czynności przewidzianych Umową dla uruchomienia Usługi lub parametry Usługi wskazane w Umowie nie są spełnione, Zamawiający może wstrzymać się z podpisaniem protokołu uruchomienia Usługi albo wyrazić zgodę na warunkowe uruchomienie Usługi, wskazując w protokole swoje zastrzeżenia. Taki odbiór z zastrzeżeniami (warunkowy) nie stanowi podstawy do rozpoczęcia odpłatnego świadczenia Usługi.
4. W przypadku dokonania przez Zamawiającego odbioru warunkowego, Wykonawca zobowiązany będzie usunąć wszystkie wady lub inne niezgodności z Umową i przedstawić uruchomienie Usługi ponownie do odbioru w terminie wyznaczonym przez Zamawiającego w protokole odbioru warunkowego.
5. Z czynności odbioru świadczonej Usługi, Strony sporządzą co miesiąc protokół.
6. Protokół, o którym mowa w ust. 5 stanowi podstawę do wystawienia przez Wykonawcę faktury z tytułu Usługi świadczonej w miesiącu kalendarzowym, którego protokół dotyczy.
7. Wzory protokołów odbioru przedmiotu Umowy zawiera Załącznik nr 2 do Umowy. Protokoły sporządzane będą w formie pisemnej albo w formie elektronicznej, według wskazania Zamawiającego.

§ 6

Wynagrodzenie

1. Maksymalna wartość nominalna zobowiązania Zamawiającego wynikającego z Umowy wynosi [●] złotych, w tym należny podatek od towarów i usług.

2. Z tytułu należytej realizacji przedmiot Umowy, Wykonawcy należy się wynagrodzenie wyliczone w oparciu o ceny jednostkowe wynikające z oferty Wykonawcy dołączonej jako Załącznik nr 3 do Umowy, tj.:
 - 1) jednorazowa opłata instalacyjna w kwocie [●] zł, powiększonej o należyty podatek od towarów i usług, tj. [●] zł brutto, co stanowi [●]% kwoty wskazanej w ust. 1 [oferowana cena jednorazowej opłaty instalacyjnej nie może przewyższyć 10% łącznej wartości oferowanej za realizację zamówienia];
 - 2) abonament w kwocie [●] zł miesięcznie, powiększonej o należyty podatek od towarów i usług, tj. [●] zł brutto miesięcznie, tj. łącznie (za cały okres świadczenia Usługi objęty Umową) do [●] zł, powiększone o należyty podatek od towarów i usług, tj. [●] zł brutto.
3. Wynagrodzenie, o którym mowa w ust. 2 powyżej, obejmuje wszelkie koszty i wydatki związane z realizacją przedmiotu Umowy, w szczególności uwzględnia opłaty należne za dzierżawę wewnętrznej infrastruktury firm trzecich.
4. Jednorazowa opłata instalacyjna, o której mowa w ust. 2 pkt 1 płatna jest jednorazowo na podstawie faktury wystawionej przez Wykonawcę po odbiorze protokolem potwierdzającym uruchomienie Usługi bez zastrzeżeń Zamawiającego dokonany stosownie do § 5, przelewem na rachunek bankowy Wykonawcy wskazany na tej fakturze.
5. Abonament, o którym mowa w ust. 2 pkt 2 płatny jest miesięcznie z dołu, każdorazowo na podstawie faktury wystawionej przez Wykonawcę do 15. dnia miesiąca następującego po zakończeniu danego okresu rozliczeniowego (okresem rozliczeniowym jest miesiąc kalendarzowy; w razie świadczenia Usługi przez niepełny miesiąc kalendarzowy, abonament należny za ten okres rozliczeniowy oblicza się w oparciu o proporcję liczby dni, w których Wykonawca faktycznie i należycie świadczył Usługi do liczby 30) i miesięcznego protokołu odbioru Usługi dokonanego stosownie do § 5.
6. Faktury tytułem należnego mu wynagrodzenia Wykonawca wystawi na płatnika: Ministerstwo Sprawiedliwości, Aleje Ujazdowskie 11, 00-567 Warszawa, NIP: 5261673166.
7. Termin płatności wynagrodzenia wynosi 30 dni od otrzymania przez Zamawiającego dokumentów niezbędnych do rozliczenia płatności, tj. podpisanego przez Strony protokołu odbioru i prawidłowo wystawionej faktury, przy czym Strony zgodnie postanawiają, że Wykonawca prześle te dokumenty pocztą elektroniczną na adres faktury.dirs@ms.gov.pl, względnie dostarczy je na adres: Departament Informatyzacji i Rejestrów Sądowych Ministerstwa Sprawiedliwości, ul. Czerniakowska 100, 00-454 Warszawa.
8. Za dotrzymanie terminu zapłaty uważa się złożenie przez Zamawiającego w terminie płatności polecenia przelewu w banku obsługującym Zamawiającego.

§ 7

Kary umowne

1. Wykonawca zapłaci Zamawiającemu kary umowne w następujących okolicznościach i wysokościach:
 - 1) w wysokości 20% wartości Umowy wskazanej w § 6 ust. 1, w razie odstąpienia od Umowy z powodu okoliczności po stronie Wykonawcy;
 - 2) w wysokości po 0,2% wartości Umowy wskazanej w § 6 ust. 1 za każdy dzień zwłoki w uruchomieniu Usługi w terminie wynikającym z § 2 ust. 1;
 - 3) w wysokości po 0,02% wartości Umowy wskazanej w § 6 ust. 1 za każdy dzień zwłoki w przedłożeniu dokumentacji powykonawczej w terminie wynikającym z § 1 ust. 3;

- 4) w wysokości po 1,5% ceny jednostkowej - stawki abonamentu miesięcznego brutto wskazanej w § 6 ust. 2 pkt 2 za każdą rozpoczętą godzinę niedostępności Usługi powyżej liczby godzin Czasu niedostępności (CN) określonej w § 3 ust. 17 pkt 1 w skali miesiąca [tj. w przypadku niedotrzymania zagwarantowanego w § 3 ust. 17 pkt 1 poziomu Dostępności Miesięcznej (DM)], przy czym naliczone z tego tytułu kary umowne nie mogą przewyższyć wartości abonamentu za dany okres rozliczeniowy;
 - 5) w wysokości 100 000 złotych za każdy przypadek naruszenia zasad poufności lub bezpieczeństwa informacji wskazanych w § 10, o ile skutkiem naruszenia był wyciek lub utrata informacji poufnych przetwarzanych w systemie teleinformatycznym Zamawiającego;
 - 6) w wysokości 5000 złotych za każdy przypadek naruszenia zasad poufności lub bezpieczeństwa informacji nieobjętych pkt 6 powyżej.
2. Kary umowne należą się Zamawiającemu, o ile uchybienie nie wynikało z okoliczności siły wyższej, o której mowa w § 13 lub z wyłącznej winy Zamawiającego, przy czym każde uchybienie w terminowej realizacji przedmiotu Umowy przez Wykonawcę będzie traktowane przez Strony za zwłokę, chyba że Wykonawca udowodni, że opóźnienie wynikało z okoliczności siły wyższej, o której mowa w § 13 lub z wyłącznej winy Zamawiającego.
 3. Kary umowne podlegają sumowaniu, co oznacza, że naliczenie kary umownej z jednego tytułu nie wyłącza możliwości naliczenia kary umownej z innego tytułu, jeżeli istnieją ku temu podstawy. Zastrzega się zarazem, że w przypadku gdyby za to samo zdarzenie miała być naliczona więcej niż jedna kara umowna, na poczet kwotowo najwyższej zalicza się pozostałe.
 4. Kary umowne Zamawiający może wg swojego uznania potrącić z należnego Wykonawcy wynagrodzenia lub z zabezpieczenia należytego wykonania Umowy.
 5. Łączna maksymalna wysokość kar umownych, których Zamawiający może dochodzić od Wykonawcy na podstawie niniejszej Umowy równa jest 30% wartości Umowy wskazanej w § 6 ust. 1.
 6. Niezależnie od kar umownych, Zamawiający może dochodzić od Wykonawcy również odszkodowania na zasadach ogólnych.
 7. Strony wyłączają odpowiedzialność z tytułu utraconych korzyści.

§ 8

Prawa własności intelektualnej

1. Wykonawca zobowiązuje się przenieść na Zamawiającego, w ramach wynagrodzenia umownego, autorskie prawa majątkowe do wszelkiej dokumentacji wytworzonej na potrzeby Umowy (projekt techniczny, projekt wykonawczy, dokumentacja powykonawcza), jak również wszelkich innych utworów w rozumieniu Ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych dostarczonych lub stworzonych w ramach Umowy, jak również poszczególnych ich elementów, na polach eksploatacji, o których mowa w art. 50 ww. ustawy, w tym:
 - 1) trwałe lub czasowe zwielokrotnianie utworów w całości lub w części, jakimikolwiek środkami i w jakiegokolwiek formie, w tym także utrwalanie i zwielokrotnianie utworów dowolną techniką, w tym techniką zapisu magnetycznego lub techniką cyfrową, taką jak zapis na płycie CD, DVD, Blu-ray, urządzeniu z pamięcią flash lub jakimkolwiek innym nośniku pamięci;
 - 2) obrót utworami, w tym wprowadzanie do obrotu, użyczanie lub najem utworów, a także rozpowszechnianie utworów w inny sposób, w tym ich publiczne wykonywanie, wystawianie, wyświetlanie, odtwarzanie, a także publiczne udostępnianie w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i w czasie przez siebie wybranym.

2. Dla uniknięcia wątpliwości Strony potwierdzają, że Zamawiający ma prawo do dowolnej modyfikacji takich utworów. Wykonawca zobowiązuje się przenieść na Zamawiającego:
 - 1) prawo zezwalania na wykonywanie zależnych praw autorskich do wszelkich opracowań utworów (lub ich poszczególnych elementów), tj. prawo zezwalania na rozporządzanie i korzystanie z takich opracowań na polach eksploatacji wskazanych powyżej,
 - 2) własność wydanych Zamawiającemu nośników, na których zostały utrwalone utwory (lub ich poszczególne elementy) w celu ich przekazania Zamawiającemu, z chwilą wydania tych nośników Zamawiającemu.
3. Przeniesienie praw, o którym mowa powyżej, nastąpi z chwilą wydania nośnika, względnie pierwszego udostępnienia Zamawiającemu danego utworu.
4. Wykonawca zobowiązuje się do niewykonywania praw osobistych do ww. utworów, jak również zobowiązuje się, iż osoby uprawnione z tytułu osobistych praw do ww. utworów (lub ich poszczególnych elementów), nie będą wykonywać tych praw, w tym w szczególności prawa do:
 - 1) decydowania o pierwszym publicznym udostępnieniu;
 - 2) decydowania o wycofaniu z obrotu;
 - 3) nadzoru autorskiego;
 - 4) nienaruszalności formy i treści oraz ich rzetelnego wykorzystania;
 - 5) oznaczenia swoim nazwiskiem lub pseudonimem.
5. Niezależnie od postanowień ustępów powyżej, Wykonawca zezwala Zamawiającemu na korzystanie z wiedzy technicznej, organizacyjnej i innej, zawartej w materiałach przekazanych Zamawiającemu w ramach realizacji Umowy. Wiedza ta może być wykorzystana w dowolny sposób przez Zamawiającego, w tym udostępniana osobom trzecim.
6. W przypadku zgłoszenia przez osoby trzecie roszczeń dotyczących naruszenia praw własności intelektualnej, w tym praw autorskich, w związku z korzystaniem przez Zamawiającego z ww. utworów, będzie je kierował wprost do Wykonawcy, zaś Wykonawca niezwłocznie:
 - 1) wstąpi w miejsce Zamawiającego, a jeśli to niemożliwe przystąpi, do wszelkich postępowań sądowych lub pozasądowych toczących się z udziałem Zamawiającego w związku z tymi roszczeniami;
 - 2) zapewni należytą ochronę interesów Zamawiającego w pełnym zakresie;
 - 3) wyrówna uszczerbek doznany przez Zamawiającego na skutek naruszenia praw osób trzecich;
 - 4) przejmie zobowiązania i w tym zakresie zwolni Zamawiającego z wszelkich zobowiązań z tytułu naruszenia praw osób trzecich poprzez ich wykonanie, a zwłaszcza spełnienie świadczeń wynikających z orzeczeń nakazujących Zamawiającemu zapłatę;
 - 5) zwolni Zamawiającego od odpowiedzialności w stosunku do takich osób trzecich, w szczególności twórców, o których mowa w ust. 4;
 - 6) zwróci Zamawiającemu wszelkie koszty i wydatki, które Zamawiający poniósł w celu zmniejszenia rozmiaru szkód oraz ochrony przed roszczeniami, w tym wypłacone odszkodowania.

§ 9

Gwarantowany serwis techniczny

1. Wykonawca zapewni monitoring sprawności działania łącza oraz obsługę zgłoszeń w zakresie problemów eksploatacyjnych 365 dni w roku, 7 dni w tygodniu, 24 godziny na dobę, w tym również

w soboty, niedziele oraz dni ustawowo wolne od pracy (24/7/365, a w roku przestępnym 24/7/366).

2. Wykonawca gwarantuje, że usługa serwisu technicznego obejmuje usuwanie Awarii po ich wykryciu przez Wykonawcę lub po ich zgłoszeniu przez Zamawiającego. Zamawiający wymaga zapewnienia co najmniej następujących form zgłaszania Awarii:
 - 1) na specjalnie do tego celu wydzielony bezpłatny numer telefoniczny,
 - 2) na adres poczty elektronicznej.
3. Zamawiający wymaga od Wykonawcy zapewnienia, aby wszystkie z wyżej wymienionych form zgłaszania Awarii były dostępne przez 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku (24/7/365, a w roku przestępnym 24/7/366).
4. Zamawiający wymaga, aby Wykonawca w przypadku wystąpienia Awarii odnotował to zdarzenie w dedykowanym serwisie obsługi zgłoszeń i przystąpił do jej usunięcia. Zamawiający wymaga aktualizowania na bieżąco statusu zgłoszenia tak, aby zawierał co najmniej datę oraz czas wykrycia lub zgłoszenia Awarii, datę oraz czas zakończenia realizacji zgłoszenia oraz przyczynę Awarii i sposób obsługi zgłoszenia. Wykonawca zapewni Zamawiającemu dostęp do dedykowanego serwisu w trybie „tylko do odczytu” poprzez przeglądarkę internetową.
5. Zamawiający zastrzega sobie możliwość samodzielnego zgłaszania Awarii niewykrytych przez Wykonawcę, niezwłocznie po ich stwierdzeniu, w sposób podany w ust. 2.
6. Wykonawca niezwłocznie po wykryciu Awarii lub otrzymaniu informacji, o której mowa w ust. 5, w czasie nie dłuższym niż CR określony w § 3 ust. 17 pkt 3, ewidencjonuje zgłoszenie w serwisie obsługi zgłoszeń, przystępuje do jej usunięcia oraz informuje Zamawiającego o przyjętym zgłoszeniu.
7. Potwierdzenie przyjęcia zgłoszenia, o którym mowa w ust. 5, w czasie nie dłuższym niż CR określony w § 3 ust. 17 pkt 3, polega na poinformowaniu Zamawiającego przez Wykonawcę pocztą elektroniczną lub telefonicznie o zarejestrowaniu zgłoszenia, wraz z podaniem co najmniej numeru zgłoszenia oraz daty i godziny zgłoszenia.
8. Awarię uznaje się za usuniętą po jej usunięciu i przywróceniu Usługi o parametrach wskazanych w Umowie oraz poinformowaniu o tym Zamawiającego, o ile Zamawiający nie poinformuje Wykonawcy, że nadal nie jest możliwe korzystanie z Usługi. Informacja dla Zamawiającego zawiera co najmniej numer i godzinę zgłoszenia oraz godzinę usunięcia Awarii.
9. Zgłoszenia Awarii przez Zamawiającego, polegające na poinformowaniu Wykonawcy o jej wystąpieniu, będą przekazywane zgodnie z ust. 2 na numer telefonu i adres e-mail przeznaczony przez Wykonawcę do tego celu i wpisany w tabeli 2 w Załączniku nr 4 do Umowy. Natomiast zawiadomienia o wykryciu Awarii przez Wykonawcę będą przekazywane Zamawiającemu telefonicznie lub pocztą elektroniczną, na numer telefonu i adres e-mail przeznaczony przez Zamawiającego do tego celu i wpisany w tabeli 1 w Załączniku nr 4 do Umowy.
10. Na wezwanie Zamawiającego Wykonawca zobowiązany jest informować Zamawiającego o statusie zgłoszenia we wskazany sposób.
11. Do CN nie wlicza się:
 - 1) Okien serwisowych;
 - 2) okresu, w którym zaistniał brak dostępu pracowników Wykonawcy do pomieszczeń Zamawiającego, do których dostęp jest niezbędny do usunięcia Awarii. W takim przypadku Wykonawca zobowiązany jest niezwłocznie telefonicznie lub pocztą elektroniczną powiadomić Zamawiającego o braku możliwości dostępu do pomieszczeń. Zamawiający po otrzymaniu

- zgłoszenia telefonicznego lub wiadomości pocztą elektroniczną niezwłocznie poinformuje Wykonawcę o terminie, w którym dostęp do pomieszczeń zostanie zapewniony;
- 3) okresu, w którym zaistniał brak zasilania urządzeń w pomieszczeniach Zamawiającego;
 - 4) okresu niedostępności spowodowanej siłą wyższą, o której mowa w § 13;
 - 5) przerw w świadczeniu Usługi spowodowanych uszkodzeniem urządzeń telekomunikacyjnych, za które odpowiedzialność ponosi Zamawiający.
12. Wykonawca udziela Zamawiającemu informacji na piśmie wraz z uzasadnieniem w przypadku niezakwalifikowania Awarii i jej CUA do CN.
13. W razie niewykonania zobowiązań wynikających z gwarantowanego serwisu technicznego, Zamawiający będzie uprawniony, po bezskutecznym upływie terminu 14 dni wyznaczonego Wykonawcy, powierzyć osobie trzeciej wykonanie takiego zobowiązania na koszt i ryzyko Wykonawcy, bez upoważnienia przez sąd (zastępcze wykonanie zobowiązania). Wykonawca zwróci Zamawiającemu na wezwanie, udokumentowane koszty i wydatki związane z zastępczym wykonaniem zobowiązania, w terminie wskazanym w wezwaniu, nie krótszym niż 14 dni.
14. Postanowienia ust. 13 stosuje się analogicznie w przypadku nienależytego wykonywania zobowiązań wynikających z gwarantowanego serwisu technicznego, jeżeli w wyznaczonym terminie Wykonawca nie przystąpił do należytego ich wykonywania lub nie usunął skutków nienależytego ich wykonywania.

§ 10

Klauzula poufności i bezpieczeństwa informacji

1. Wykonawca zobowiązuje się do zachowania w poufności wszelkich Informacji, do których uzyskał dostęp lub zapoznał się z nimi w związku z realizacją Umowy lub choćby przy tej okazji. Poufnością objęte są także Informacje przekazane Wykonawcy w toku postępowania poprzedzającego zawarcie Umowy, oznaczone jako poufne lub co do których Zamawiający w inny sposób poinformował Wykonawcę, że traktuje je jako poufne.
2. Dla uniknięcia wątpliwości Strony potwierdzają, że:
 - 1) poufnością objęte są Informacje bez względu na ich postać lub formę przekazania;
 - 2) nie są uważane za poufne Informacje, które Zamawiający obowiązany jest na mocy ustawy podać do publicznej wiadomości lub w inny sposób ujawnić.
3. Wykonawca zobowiązuje się:
 - 1) nie ujawniać innym podmiotom Informacji, co do których Wykonawca nie uzyskał uprzednio stosownej zgody Zamawiającego wyrażonej formie pisemnej lub w formie elektronicznej pod rygorem nieważności;
 - 2) Informacje wykorzystywać wyłącznie w zakresie niezbędnym do realizacji Umowy;
 - 3) przetwarzać Informacje wyłącznie w takiej formie, w jakiej uzyskał do nich dostęp, chyba że Strony uzgodnią inaczej lub zmiana jest przewidziana przepisami prawa;
 - 4) nie powielać Informacji w zakresie szerszym, niż jest to potrzebne dla realizacji Umowy;
 - 5) zabezpieczać Informacje w stopniu niezbędnym do zachowania ich poufnego charakteru, a przynajmniej w takim samym stopniu, jak postępuje wobec własnej tajemnicy przedsiębiorstwa;
 - 6) przestrzegać wytycznych Zamawiającego o ochronie Informacji, w tym Polityki bezpieczeństwa informacji Ministerstwa Sprawiedliwości oraz Polityki bezpieczeństwa systemów teleinformatycznych Ministerstwa Sprawiedliwości.

4. W zakresie niezbędnym do realizacji Umowy, Wykonawca może udostępniać Informacje swojemu personelowi, podwykonawcom oraz doradcom prawnym z tym zastrzeżeniem, że przetwarzanie Informacji przez takie osoby i podmioty nie może wykraczać poza zakres, w którym Wykonawca może je przetwarzać. Wykonawca zobowiązany jest:
 - 1) zapewnić kontrolę nad tym, jakie Informacje, kiedy, przez kogo oraz komu są przekazywane;
 - 2) zapewnić, aby te osoby i podmioty zachowywały w poufności informacje oraz sposoby ich zabezpieczeń, przestrzegając przy tym zasad i warunków wynikających z ust. 3.
5. Wykonawca odpowiedzialny jest za naruszenia spowodowane przez te osoby i podmioty jak za własne działania i zaniechania.
6. Przed uzyskaniem przez osoby, o której mowa w ust. 4 dostępu do Informacji, Wykonawca zobowiązany jest przekazać Zamawiającemu podpisane przez daną osobę oświadczenie o zachowaniu poufności Informacji, którego wzór stanowi Załącznik nr 5 do Umowy.
7. Na wniosek Zamawiającego złożony w formie pisemnej lub w formie elektronicznej, Wykonawca niezwłocznie zniszczy dokumenty lub materiały zawierające Informacje.
8. Z chwilą rozwiązania lub wygaśnięcia Umowy, Wykonawca:
 - 1) zwróci Zamawiającemu wszelkie dokumenty i materiały zawierające Informacje posiadane przez Wykonawcę lub osoby i podmioty, o którym mowa w ust. 4;
 - 2) Informacje przetwarzane w postaci elektronicznej usunie ze swoich zasobów i nośników oraz zapewni, że osoby i podmioty, o których mowa w ust. 4 usuną je ze swoich zasobów i nośników.
9. Wykonawca zobowiązany jest do natychmiastowego powiadamiania o każdym nieuprawnionym ujawnieniu lub udostępnieniu Informacji oraz o innym naruszeniu bezpieczeństwa Informacji, a następnie raportowania Zamawiającemu o podejmowanych działaniach naprawczych:
 - 1) telefonicznie, na numer telefonu [●];
 - 2) pocztą elektroniczną, na adres e-mail [●];
 - 3) poprzez wykorzystywany przez Zamawiającego system zgłoszeniowy.

Powiadomienie dokonane telefonicznie musi zostać potwierdzone poprzez jeden ze sposobów wskazanych w pkt 2-3 w terminie jednej godziny od dokonania powiadomienia.
10. Strony zobowiązują się zawrzeć umowę o powierzenie przetwarzania danych osobowych, których administratorem jest Zamawiający lub które zostały powierzone Zamawiającemu do przetwarzania, o treści zasadniczo zgodnej ze wzorem stanowiącym Załącznik nr 6 do Umowy. Ponadto Wykonawca, w terminie 7 dni od dnia zawarcia Umowy przekaze Zamawiającemu imienną listę osób skierowanych przez Wykonawcę do świadczenia usług stanowiących przedmiot Umowy, przy których może być wymagane przetwarzanie danych osobowych powierzonych przez Zamawiającego. Lista powinna zawierać dane niezbędne do jednoznacznej identyfikacji każdej z tych osób oraz określać dla każdej z tych osób zakres czynności powierzanych przez Wykonawcę w ramach realizacji Umowy.
11. Wykonawca oświadcza, że zapoznał się z Informacją o przetwarzaniu danych osobowych udostępnioną na stronie internetowej pod adresem <https://www.gov.pl/web/sprawiedliwosc/informacja-o-przetwarzaniu-danych-osobowych> oraz zobowiązuje się zapoznać z nią swoich pracowników i inne osoby, którymi posługuje się przy realizacji Umowy, a których dane osobowe mają być przetwarzane przez Zamawiającego jako administratora danych osobowych.

Zabezpieczenie należytego wykonania Umowy

(celowo pominięto)

§ 12

Podwykonawstwo

1. Wykonawca uprawniony jest do powierzenia podwykonawcom wykonania części przedmiotu Umowy, z zastrzeżeniem przepisów ustawy PZP i poniższych postanowień.
2. Wykonawca wykona przedmiot Umowy przy udziale następujących podwykonawców:
 - 1) [firma, siedziba, adres, dane kontaktowe przedstawicieli podwykonawcy] – w zakresie [wskazać zakres];
3. Wykonawca zobowiązany jest do poinformowania Zamawiającego o zmianie podwykonawcy nie później niż w dniu następującym po nastaniu zmiany. Zmiana tych danych nie wymaga zawarcia aneksu do Umowy, lecz wystarcza zawiadomienie w formie pisemnej albo w formie elektronicznej.
4. Powierzenie podwykonawstwa podmiotom niewymienionym w ust. 2 powyżej nie wymaga zawarcia aneksu do Umowy, lecz wystarcza zawiadomienie przez Wykonawcę Zamawiającego w formie pisemnej albo w formie elektronicznej, zawierające firmę, siedzibę, adres, dane kontaktowe przedstawicieli podwykonawcy oraz zakres podwykonawstwa. O zamiarze wykonania przedmiotu Umowy z udziałem podwykonawcy niewskazanego w ust. 2, Wykonawca zobowiązany jest zawiadomić Zamawiającego z co najmniej dwutygodniowym wyprzedzeniem.
5. Realizacja przedmiotu Umowy przy udziale podwykonawców nie zwalnia Wykonawcy z odpowiedzialności za należyte i terminowe wypełnianie zobowiązań umownych. Za działania i zaniechania podwykonawcy, Wykonawca odpowiada jak za swoje własne.
6. Postanowienia ust. 5 powyżej stosuje się odpowiednio do innych osób, którymi Wykonawca posługuje się przy wykonywaniu przedmiotu Umowy.
7. Powierzenie wykonania całości lub części przedmiotu Umowy osobie, która w zakresie swej działalności zawodowej trudni się wykonywaniem takich czynności nie zwalnia Wykonawcy od odpowiedzialności za szkodę wyrządzoną przez taką osobę.

§ 13

Siła wyższa

1. Żadna ze Stron nie będzie odpowiedzialna względem drugiej za zobowiązania określone w niniejszej Umowie, w zakresie w jakim ich wykonanie okaże się niemożliwe z uwagi na działanie siły wyższej tj. przyczynę wyłączną, zewnętrzną, nadzwyczajną, gwałtowną, nieprzewidywalną i nieuchronną, taką jak w szczególności wojna, wojna domowa, zamieszki, rozruchy, akty sabotażu, katastrofy naturalne, takie jak silne burze, huragany, trzęsienia ziemi, powodzie, zniszczenia spowodowane przez piorun, wybuch, pożar, bojkot, strajk, lock-out wszelkiego rodzaju, okupowanie pomieszczeń.
Konsekwentnie, Wykonawca nie ponosi odpowiedzialności za szkody spowodowane brakiem transmisji, nieprawidłową transmisją, opóźnieniem lub przerwą w transmisji, o ile udowodni, że przyczyną braku transmisji, nieprawidłowej transmisji, opóźnienia lub przerwy w transmisji było działanie siły wyższej, bez uszczerbku dla ust. 2-4.
2. Zastrzega się, że wystąpienie zdarzenia o charakterze siły wyższej nie wyłącza odpowiedzialności Strony w zakresie, w jakim działanie z najwyższą starannością zapobiegłoby jego skutkom.
3. W razie wystąpienia zdarzenia o charakterze siły wyższej, która ma lub może mieć wpływ na terminowe lub należyte wykonywanie zobowiązań, Strona, która powzięła wiedzę o takim

zdarzeniu, niezwłocznie (z tym, że nie później niż w następnym dniu po dniu, w którym uzyskała możliwość skontaktować się z drugą Stroną), poinformuje o tym drugą Stronę, w miarę możliwości przedstawiając stosowną dokumentację w tym zakresie. Strony, o ile to będzie możliwe, uzgodnią sposób postępowania wobec tego zdarzenia oraz terminy wykonywania Umowy.

4. Po ustąpieniu działania siły wyższej, Strona zobowiązana jest przystąpić do dalszego wykonywania swoich zobowiązań niezwłocznie, z tym że nie później niż w następnym dniu po dniu, w którym miała na powrót możliwość działania.
5. Jeżeli zdarzenie o charakterze siły wyższej powoduje konieczność wprowadzenia zmian Umowy, Strony podejmą w dobrej wierze negocjacje w celu zmiany Umowy.

§ 14

Zmiany Umowy

Strony zastrzegają możliwość zmiany Umowy w zakresie:

- 1) zmniejszenia zakresu realizacji przedmiotu Umowy oraz odpowiedniego zmniejszenia wynagrodzenia należnego Wykonawcy w przypadku wystąpienia zmiany okoliczności powodującej, że realizacja części przedmiotu Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawierania Umowy;
- 2) parametrów technicznych świadczenia Usługi dla dostosowania do nowych technologii i rozwiązań technicznych, z zachowaniem minimalnych wymagań określonych w Umowie;
- 3) terminu, zakresu lub sposobu realizacji przedmiotu Umowy dla dostosowania do zmiany stanu faktycznego na skutek zdarzenia o charakterze siły wyższej, które nastąpiło po wszczęciu postępowania o udzielenie zamówienia publicznego, a wpływa na termin, zakres lub sposób realizacji przedmiotu Umowy;
- 4) terminu, zakresu lub sposobu realizacji przedmiotu Umowy dla dostosowania do zmiany stanu prawnego, która nastąpiła po wszczęciu postępowania o udzielenie zamówienia publicznego, a wpływa na termin, zakres lub sposób realizacji przedmiotu Umowy;
- 5) zakresu lub sposobu realizacji przedmiotu Umowy dla dostosowania do zmian struktury lub organizacji po stronie Zamawiającego;
- 6) zmiany zasad zgłaszania, obsługi i eskalacji zgłoszeń w ramach serwisu;
- 7) postanowień, które w toku realizacji Umowy z uwagi na okoliczności niezależne od Stron okazały się nieważne lub niewykonalne, w celu ich zastąpienia innymi możliwie najlepiej oddającym pierwotne intencje Stron;
- 8) oczywistych omyłek pisarskich i rachunkowych;
- 9) innych postanowień, wprost wskazanych w Umowie jako podlegające zmianie.

§ 15

Odstąpienie od Umowy i wypowiedzenie Umowy

1. Zamawiającemu przysługuje uprawnienie do odstąpienia od Umowy, gdy:
 - 1) wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w dniu zawarcia Umowy;
 - 2) Wykonawca utracił zdolność do czynności prawnych, stał się niewypłacalny, został postawiony w stan likwidacji lub spełnia warunki do wykreślenia z rejestru/ewidencji z urzędu;
 - 3) uprawnienie takie wynika z Kodeksu cywilnego lub innych przepisów prawa;

- 4) Wykonawca nie dotrzymał terminu uruchomienia Usługi wynikającego z § 2 ust. 1, z powodu okoliczności za które odpowiada Wykonawca;
 - 5) Wykonawca bezzasadnie odmówił zawarcia umowy o powierzenie przetwarzania danych osobowych.
2. Przed odstąpieniem od Umowy na podstawie ust. 1 pkt 4-5, Zamawiający udzieli Wykonawcy dodatkowego terminu co najmniej 7 dni na wykonanie danego zobowiązania, wskazując na rygor odstąpienia od Umowy.
 3. Termin na odstąpienie od Umowy wynosi:
 - 1) 60 dni od powzięcia przez Zamawiającego wiadomości o zaistnieniu przesłanki, o której mowa w odpowiednio ust. 1 pkt 1 i 2;
 - 2) 60 dni od bezskutecznego upływu dodatkowego terminu, o którym mowa w ust. 2.
 4. W odstąpieniu Zamawiający wskaże, czy odstąpienie następuje w całości czy w części oraz czy wywołuje skutki jedynie na przyszłość.
 5. Zamawiający może wypowiedzieć Umowę ze skutkiem natychmiastowym z przyczyn leżących po stronie Wykonawcy, gdy:
 - 1) Wykonawca nienależycie wykonuje Umowę, w szczególności nie stosuje się do zasadnych uwag Zamawiającego lub narusza inne postanowienia Umowy i w przypadku, gdy po upływie 7 dni od wezwania przez Zamawiającego do zaniechania przez Wykonawcę naruszeń postanowień Umowy i usunięcia ewentualnych skutków naruszeń, Wykonawca nie zastosuje się do tego wezwania;
 - 2) w którymkolwiek okresie rozliczeniowym wystąpiło co najmniej 5 Awarii, z wyłączeniem Awarii przypadających w okresie niewliczanym do CN, stosownie do § 9 ust. 11;
 - 3) w którymkolwiek okresie rozliczeniowym wystąpiła przerwa w świadczeniu Usługi trwająca nieprzerwanie dłużej niż 48 godzin, nieprzypadająca w okresie przerw niewliczanych do CN, stosownie w § 9 ust. 11;
 - 4) doszło do rozwiązania umowy o powierzenie przetwarzania danych osobowych.
 6. W przypadku wypowiedzenia, Wykonawca zachowa prawo do wynagrodzenia za Usługi świadczone Zamawiającemu przez okres do dnia wypowiedzenia.
 7. W razie rozwiązania lub wygaśnięcia Umowy, Wykonawca nie później niż w terminie 14 dni od tej daty i w obecności przedstawicieli Zamawiającego sporządzi i przekaze Zamawiającemu sprawozdanie, które będzie zawierało opis czynności wykonanych do odpowiednio dnia rozwiązania lub wygaśnięcia Umowy, wraz z dokonaniem ich oceny pod względem możliwości ich zaakceptowania i odbioru przez Zamawiającego. W razie nieprzedłożenia przez Wykonawcę sprawozdania, Zamawiający powoła komisję w celu sporządzenia sprawozdania, które będzie wiążące dla Stron.
 8. Wygaśnięcie Umowy na skutek odstąpienia od Umowy pozostaje bez wpływu na odpowiedzialność odszkodowawczą Wykonawcy (dotyczy części, w jakiej Zamawiający od Umowy nie odstąpił) oraz do naliczenia kar umownych należnych na podstawie Umowy.

§ 16

Postanowienia końcowe

1. Umowa wchodzi w życie (obowiązuje) z chwilą zawarcia.
2. Prawo właściwe dla Umowy to prawo obowiązujące w Rzeczypospolitej Polskiej.

3. W sprawach nieuregulowanych niniejszą Umową stosuje się przepisy Kodeksu cywilnego i Prawa komunikacji elektronicznej.
4. Wszelkie zmiany i uzupełnienia niniejszej Umowy, rozwiązanie Umowy za zgodą obu Stron, jak również odstąpienie od Umowy, wymaga zachowania formy pisemnej albo formy elektronicznej pod rygorem nieważności.
5. Wykonawca nie może obciążyć zastawem swoich uprawnień, dokonać cesji (przelewu) przysługujących mu wierzytelności ani przenieść na osobę trzecią jakichkolwiek zobowiązań wynikających z Umowy, bez uprzedniej zgody Zamawiającego wyrażonej w formie pisemnej albo w formie elektronicznej pod rygorem nieważności.
6. Z chwilą wygaśnięcia Umowy, w mocy pozostają postanowienia Umowy, które ze względu na swój charakter, cel oraz znaczenie mogą być stosowane także po jej wygaśnięciu.
7. Niewykonanie przez Zamawiającego któregośkolwiek z uprawnień przysługujących mu na podstawie Umowy nie może być uważane za zrzeczenie się tego uprawnienia, ani zrzeczenie się innych uprawnień wynikających z postanowień Umowy.
8. Wyłącza się możliwość potrąceń wierzytelności Wykonawcy względem Zamawiającego.
9. Postępowanie reklamacyjne będzie prowadzone zgodnie z przepisami Rozdziału 4 ustawy z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1221, z 2025 r. poz. 637, 820).
10. Spory na tle Umowy, których nie udało się Stronom rozwiązać polubownie, rozstrzygać będzie sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
11. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, dwa dla Zamawiającego i jeden dla Wykonawcy* / Umowa została zawarta w formie elektronicznej, tj. podpisana kwalifikowanymi podpisami elektronicznymi.**
12. Integralną część Umowy stanowią załączniki wymienione w poniższej liście:
 - 1) Opis usługi ochrony przed Atakami DDoS;
 - 2) Wzory protokołów odbioru;
 - 3) Oferta Wykonawcy;
 - 4) Dane kontaktowe;
 - 5) Wzór oświadczenia o zachowaniu poufności informacji;
 - 6) Wzór umowy o powierzenie przetwarzania danych osobowych;
 - 7) Odpis z KRS/CEIDG Wykonawcy.

W przypadku sprzeczności, postanowienia Umowy mają pierwszeństwo.

w imieniu WYKONAWCY:

w imieniu ZAMAWIAJĄCEGO:

[imię i nazwisko osoby podpisującej]

[imię i nazwisko osoby podpisującej]

[stanowisko]

[stanowisko]

/podpisano kwalifikowanym podpisem elektronicznym/**

/podpisano kwalifikowanym podpisem elektronicznym/**

* wykreślić, jeżeli umowa ma być podpisana w formie elektronicznej tj. przy użyciu kwalifikowanego podpisu elektronicznego

** wykreślić, jeżeli umowa ma być podpisana w zwykłej formie pisemnej

Opis usługi ochrony przed Atakami DDoS

1. Łączy dostępu do Internetu

- 1) Zamawiający wymaga zapewnienia usługi ochrony przed Atakami DDoS, realizowanej jako usługi powiązanej z symetrycznym łączem dostępu do Internetu, dostarczonym w ramach zamówienia dla całej udostępnionej przepustowości łącza. Usługa będzie świadczona dla całej adresacji IP Zamawiającego na dostarczonym łączu internetowym;
- 2) W ramach realizacji usługi ochrony przed Atakami DDoS Zamawiający wymaga zapewnienia co najmniej:
 - a) analizy ruchu w celu identyfikacji typu i natury Ataku;
 - b) powiadamiania Zamawiającego o podejrzeniu wystąpienia Ataku;
 - c) rozpoczęcia usuwania Ataku w porozumieniu z Zamawiającym (możliwe jest automatyczne uruchamianie obrony dla alarmów o wysokim poziomie zagrożenia), d) modyfikacji zestawu użytych mechanizmów przeciwdziałania tak, by uzyskać maksymalny poziom filtracji ruchu niepożądanego przy minimalnym wpływie na ruch prawidłowy;
 - d) klasyfikacji alarmów typu DDoS jako:
 - ☐ zweryfikowany Atak;
 - ☐ fałszywy alarm;
 - ☐ nagły ruch – znaczący wzrost ruchu, spowodowany inną przyczyną niż Atak na daną usługę Zamawiającego.

2. Wykrywanie zagrożeń

- 1) Zamawiający wymaga zapewnienia efektywnej identyfikacji potencjalnych Ataków DDoS z wykorzystaniem co najmniej poniższych mechanizmów detekcji:
 - a) sygnatury;
 - b) przekroczenie progów dla określonych typów pakietów i protokołów;
 - c) oparte na analizie profilu ruchu Zamawiającego wykrywanie nieoczekiwanych zmian ruchu w odniesieniu do tego profilu;
 - d) Zamawiający dopuszcza wykrywanie ataków warstw wyższych L5-L7 (HTTP GET/POST Flood, SIP Request Flood, SSL Negotiation) na podstawie aproksymacji względem ruchu w L4 pod warunkiem spełnienia pozostałych wymagań określonych w załączniku nr 1 do umowy;
- 2) Usługa ma monitorować ruch do i od chronionej podsieci w czasie rzeczywistym, w tym w odniesieniu do poszczególnych usług Zamawiającego. Lista usług Zamawiającego realizowanych na udostępnionym łączu, zgłoszonych przez Zamawiającego w terminie uruchomienia łącza i ochrony przed Atakami DDoS, jest listą otwartą i może się zmieniać z dnia na dzień w okresie realizacji Umowy, w zależności od uruchamianych / kasowanych usług Zamawiającego;
- 3) Usługa ma zapewniać wykrywanie anomalii polegających na przekroczeniu wartości uważanych za normalne w ruchu internetowym, w szczególności pakietów TCP SYN flood, UDP

flood (w tym DNS reflection), HTTP GET flood, HTTP POST flood, ICMP flood, IGMP flood, invalid packets, IP fragments, IP NULL, DNS flood, SIP request flood, SSL negotiation;

- 4) System realizujący usługę na podstawie danych historycznych ma wyznaczać oczekiwaną wartość ruchu do i od chronionej podsieci o danej porze dnia w danym dniu tygodnia, w odniesieniu do poszczególnych usług Zamawiającego;
- 5) Usługa zapewnia wykrywanie anomalii polegających na znaczącym przekroczeniu wolumenu ruchu oraz wykrywanie potencjalnych Ataków w warstwie aplikacyjnej dla poszczególnych usług Zamawiającego w stosunku do wcześniej wyznaczonych wartości oczekiwanych ruchu.

3. Mitygacja – oczyszczanie ruchu

- 1) Zamawiający wymaga zapewnienia usługi ochrony przed Atakami DDoS, polegającej na usuwaniu Ataku przy możliwie jak najmniejszym wpływie na ruch uprawniony. Efektywne działanie musi stanowić trzy procedury:
 - a) procedura uruchamiana w przypadku podejrzenia wystąpienia Ataku: ruch przekierowany zostanie do dedykowanych do tego celu zasobów wewnętrznych Wykonawcy;
 - b) procedura filtrowania, oparta o wielowarstwową analizę ruchu i mechanizmy przeciwdziałania;
 - c) procedura oparta o kierowanie odfiltrowanego ruchu z powrotem do Zamawiającego;
- 2) Zamawiający wymaga ochrony co najmniej przed następującymi typami Ataków:
 - TCP SYN flood;
 - UDP flood (w tym DNS reflection);
 - HTTP GET flood;
 - HTTP POST flood;
 - ICMP flood IGMP;
 - flood invalid;
 - packets;
 - IP fragments;
 - IP NULL;
 - DNS flood;
 - SIP request flood.

4. Usługa ochrony przed atakami DDoS na warstwy aplikacji

Świadczenie usługi ochrony przed atakami DDoS na warstwę aplikacji przez Wykonawcę w ramach własnej infrastruktury w sposób rozbudowujący podstawową ochronę (opisaną w niniejszym załączniku) przed atakami DDoS o analizę i ochronę przed zagrożeniami w warstwach aplikacji, spełniający poniższe wymagania.

5. Opis wymagań usługi

- 1) Usługa ochrony przed atakami DDoS oferowana musi zapewniać ochronę aplikacji Zamawiającego przed atakami na warstwę L7 modelu ISO/OSI systemów Zamawiającego;
- 2) Usługa ochrony przed atakami musi być realizowana w infrastrukturze Wykonawcy;
- 3) Usługa ochrony przed atakami DDoS świadczona jest w modelu usługowym (ang. *as a service*);
- 4) Usługa jest uruchamiana, konfigurowana, zarządzana i monitorowana przez inżynierów Wykonawcy;

- 5) „Oczyszczanie ruchu” odbywa się poprzez przekierowanie ruchu Zamawiającego do jednostek czyszczących Wykonawcy znajdujących się na terenie Polski lub Unii Europejskiej;
- 6) Infrastruktura sprzętowa świadcząca usługi ochrony DDoS musi być własnością Wykonawcy;
- 7) Usługa ochrony przed atakami DDoS musi zapewniać możliwość odparcia ataków o wolumenie do 80 Gbps i 100 Mpps;
- 8) Po oczyszczeniu ruchu w scrubbing center ruch do Zamawiającego musi być przesłany zgodnie z tablicą routingu, bez konieczności dodatkowej enkapsulacji;
- 9) Nie dopuszcza się by na potrzeby usługi ochrony przed atakami DDoS do zwrotnego przekierowania ruchu używane były tunele GRE;
- 10) Usługa ochrony przed atakami DDoS musi umożliwiać integrację z systemami bezpieczeństwa będącymi w posiadaniu Zamawiającego między innymi takim jak SIEM;
- 11) Usługa ochrony przed atakami DDoS musi w sposób ciągły monitorować ruch do usług Zamawiającego;
- 12) Usługa ochrony przed atakami DDoS musi umożliwiać uruchomienie mitygacji w sposób:
 - a) Automatyczny – dokonywany do 5 min. po wykryciu anomalii;
 - b) Ręczny – po otrzymaniu potwierdzenia przez Zamawiającego – do 30 min.;
- 13) Usługa ochrony przed atakami DDoS posiada możliwość przerywania mitygacji w dowolnym momencie;
- 14) Usługa ochrony przed atakami DDoS zapewnia filtrowanie pakietów minimum według następujących mechanizmów:
 - a) Filtr ograniczający ruch po przekroczeniu progu mitygacji – konfigurowany wg. portów lub protokołów. Może być wykorzystywany do ataków typu „reflected” dla ruchu, który nie jest niezbędny do działania usługi;
 - b) DNS – spoinowanie zapytań UDP;
 - c) Filtr zapewniający możliwość określenia, które z obiektów wykorzystują komunikację UDP;
 - d) Zarządzanie sesjami – filtry pozwalające na monitorowanie oraz zarządzanie sesjami TCP – między innymi zarządzanie sesjami „TCP half-open” itp.;
 - e) Filtr „Porty” – biała oraz czarna lista portów docelowych oraz źródłowych – uwzględniająca usługi działające na dynamicznie lub statycznie zmieniających porty;
 - f) Filtr geolokalizacji IP – usługa ochrony przed atakami DDoS musi umożliwiać zarządzanie ruchem sieciowym zgodnie z adresacją IP z podanych państw, kontynentów – możliwość określenia, czy podczas ataku adresy źródłowe muszą zostać ograniczone do wskazanych obszarów geograficznych;
 - g) Filtry zapewniające możliwość realizacji kierowania ruchu IP zgodnie z poniższą funkcjonalnością:
 - Blacklist;
 - Whitelist;
 - Greylist;
 - przycinanie/limitowanie ruchu powyżej zadanej wartości: Max burst pps;
- 15) System usługi ochrony przed atakami DDoS aplikacyjnymi musi wykrywać minimum poniższe ataki warstw L5 - L7 ISO/OSI:
 - a) SIP Request Flood,
 - b) SSL Abuse

- c) HTTP flood,
- d) NTP reflected/amplification attack
- e) DNS reflected/amplification attack
- f) CLDAP Amplification / Reflection attack
- g) CHARGEN Amplification / Reflection attack
- h) L2TP Amplification / Reflection attack
- i) MSSQL Amplification / Reflection attack
- j) NetBIOS Amplification / Reflection attack
- k) RCPBIND Amplification / Reflection attack
- l) SNMP Amplification / Reflection attack
- m) mDNS Amplification / Reflection attack
- n) SSDP Amplification / Reflection attack
- o) Memcached Amplification / Reflection attack
- p) QOTD Reflection
- q) Invalid packets - Bad UDP Payload length
- r) Ataki typu „Slowloris”

6. Poziom SLA dotyczący powiadomienia o Ataku

1) Czas Reakcji na Atak DDoS (CRA):

- a) przez CRA rozumie się czas, jaki upłynie od wykrycia Ataku DDoS do rozpoczęcia skutecznego poinformowania Zamawiającego, za pośrednictwem poczty elektronicznej, z zastrzeżeniem, że dopuszcza się formę telefoniczną w przypadku braku możliwości przesłania informacji poprzez pocztę elektroniczną
- b) przez skuteczne poinformowanie Zamawiającego rozumie się przekazanie informacji za pośrednictwem poczty elektronicznej lub rozmowę z przedstawicielem Zamawiającego oraz jego poprawną autoryzację,
- c) czas CRA liczony jest od momentu zareportowania na platformie Ataku do czasu zarejestrowania w systemie teleinformatycznym Wykonawcy czasu dokonania pierwszej czynności mającej na celu skuteczne poinformowanie Zamawiającego o Ataku (czas wysłania e-maila, czas wykonania rozmowy telefonicznej),
- d) w przypadku kontaktu Wykonawcy z Zamawiającym za pośrednictwem poczty elektronicznej, CRA liczone jest w następujący sposób: od momentu wykrycia Ataku przez system Wykonawcy do momentu wysłania e-maila z opcją żądania potwierdzenia przeczytania. W przypadku braku potwierdzenia przeczytania e-maila przez Zamawiającego w maksymalnym czasie CRA, Wykonawca podejmuje próbę kontaktu telefonicznego, a w przypadku nieskutecznej pierwszej próby kontaktu telefonicznego Wykonawca wysyła SMS do grupy adresowej z informacją o zanotowanym Ataku,
- e) w przypadku telefonicznego kontaktu Wykonawcy z Zamawiającym, CRA liczone jest w następujący sposób: czas mierzony jest od momentu wykrycia Ataku przez system Wykonawcy do momentu próby wykonania pierwszego telefonicznego kontaktu z Zamawiającym (zgodnie z listą osób/numerów i priorytetami wskazanym przez Zamawiającego). Każda próba kontaktu będzie wykonywana przez Wykonawcę co dwie minuty w maksymalnym czasie CRA. Jeśli nie dojdzie do skutecznego kontaktu w pierwszej próbie, Wykonawca zobowiązany jest do wykonania następnej próby do kolejno

wskazanych osób/numerów z listy kontaktów. W przypadku niemożności uzyskania połączenia z Zamawiającym w maksymalnym czasie CRA we wszystkich próbach kontaktu, Wykonawca wysyła

- f) SMS do grupy adresowej z informacją o zanotowanym Ataku,
- g) w przypadku świadczenia usługi ochrony przed Atakami DDoS na żądanie Zamawiającego ochrona nie będzie włączona do momentu skutecznego kontaktu z Zamawiającym i potwierdzenia decyzji o włączeniu lub braku włączenia ochrony,
- h) wartość parametru CRA wynosi maksymalnie 15 minut.

2) Czas Reakcji na Zlecenie oczyszczania ruchu (CRZ):

- a) przez CRZ rozumie się czas, jaki upłynie od przyjęcia Zlecenia od Zamawiającego z żądaniem włączenia lub wyłączenia oczyszczania po zarejestrowanym Ataku DDoS.
- b) wartość parametru CRZ wynosi maksymalnie 15 minut.

7. Raporty miesięczne

Zamawiający wymaga umieszczania w comiesięcznych Protokołach odbioru Usługi w punkcie dotyczącym usługi ochrony przed Atakami DDoS informacji zawierających co najmniej następujące statystyki:

- a) uśredniony poziom ruchu wchodzącego i wychodzącego,
- b) maksymalne poziomy ruchu,
- c) liczba zarejestrowanych Ataków,
- d) liczba usuniętych Ataków.

8. Raport z incydentu

Zamawiający wymaga każdorazowo po zakończeniu operacji oczyszczania ruchu po zaistniałym Ataku sporządzenia raportu z incydentu. Sposób inicjowania oraz zakończenia procedury zostanie uzgodniony z Zamawiającym w terminie 5 dni od zawarcia Umowy. Informacja w raporcie o incydencie zawierać będzie co najmniej następujące statystyki:

- a) rozmiar Ataku, liczniki pakietów, Gb/s oraz procent całości ruchu,
- b) czas trwania Ataku,
- c) główne źródła Ataku,
- d) typ i natura Ataku,
- e) wdrożone metody eliminacji Ataku,
- f) geograficzna lokalizacja źródeł Ataku,
- g) wielkość oczyszczonego ruchu,
- h) czasy – w szczególności: początek Ataku, powiadomienie, wdrożenie procedur obronnych, zakończenie Ataku, przywrócenie normalnej pracy sieci.

9. Czas świadczenia Usługi

Zamawiający wymaga świadczenia usługi ochrony przed DDoS w trybie 24/7/365 (24/7/366 w roku przestępnym).

10. Procedura przerywania mitygacji – Fall-back Procedure

Jeśli uruchomiona procedura eliminacji Ataków DDoS ma negatywny wpływ na chronione zasoby lub usługi, Zamawiający ma możliwość zlecenia jej przerywania, co następuje w ciągu 15 minut od momentu zlecenia przez Zamawiającego (godzina, minuta). Pomimo przerywania akcji, ruch Zamawiającego cały czas podlega monitorowaniu i istnieje możliwość przywrócenia procedur obronnych w odpowiednio dostosowanym zakresie i analogicznym czasie wdrożenia.

11. Alarmy i sposób powiadamiania Zamawiającego:

Wykryte w ramach realizacji Usługi zdarzenia zostaną przyporządkowane do jednej z niżej opisanych przykładowych grup alarmów:

Kategoria alarmu	Opis	Akcja / Czas reakcji	Przykład
KRYTYCZNA (Servity High)	Alarm o największym stopniu zagrożenia dla Zamawiającego.	Automatyczne rozpoczęcie akcji oczyszczania w sytuacjach uzgodnionych z Zamawiającym. Przystąpienie do rozwiązywania problemu przez Wykonawcę. Do Zamawiającego zostanie wysłane powiadomienie o zaistnieniu potencjalnego Ataku DDoS w czasie zdefiniowanym przez SLA.	Alarmy w tej kategorii zawierają m. in.: • potencjalne ataki DDoS, • utratę komunikacji z monitorowanym i zasobami, • inne alarmy - po uzyskaniu zgody Zamawiającego .
WAŻNA (Servity Medium)	Alarm, który w późniejszym czasie może wymagać akcji ze strony	Podjęcie działań, jeśli to konieczne, ze strony Wykonawcy lub Zamawiającego. Informowanie	Informacje na temat ruchu niezwiązane z wystąpieniem nieprawidłowości.
	Wykonawcy lub Zamawiającego.	Zamawiającego o zaistniałej sytuacji.	
INFORMACYJNA (Servity Low)	Zapis informacji o Ataku.	Brak działania. Brak konieczności informowania Zamawiającego.	Zdarzenia związane z działaniami systemu lub jego rekonfiguracją, np. planowy update sygnatur.

Kryteria definiujące wystąpienie zdarzeń oraz poziom, jaki zostanie przyporządkowany dla poszczególnych zdarzeń, zostaną zastosowane po uzyskaniu zgody Zamawiającego.

12. Implementacja Usługi

1) Projekt wykonawczy

Wykonawca opracuje Projekt wykonawczy usługi proaktywnej ochrony przed Atakami DDoS po podpisaniu Umowy na świadczenie Usługi, przy współpracy z Zamawiającym i przekaże go Zamawiającemu zgodnie z § 1 ust. 3 Umowy. Dokument zawierać będzie m. in.:

- opis techniczny integracji Usługi z siecią Zamawiającego,
- opis procedur powiadamiania i eskalacji,
- testy akceptacyjne,
- opis procedur obsługi zgłoszeń i raportowania.

Jednocześnie Wykonawca przeprowadzi w siedzibie Zamawiającego dla zespołów wyszczególnionych w pkt 1 i 2 tabeli 1 załącznika nr 4 do Umowy instruktaż w zakresie działania Usługi, a w szczególności aspektów dotyczących usługi ochrony przed Atakami DDoS. Zamawiający dopuszcza realizację instruktażu w trybie online (tj. z użyciem narzędzi teleinformatycznych umożliwiających dwukierunkową komunikację audiowizualną w czasie rzeczywistym).

2) Implementacja

Implementacja stanowi rekonfigurację urządzeń Zamawiającego oraz Wykonawcy pod kątem monitorowania ruchu oraz uruchomienia usługi przeciwdziałania Atakom DDoS.

3) Testy akceptacyjne

- a) Po zakończeniu Implementacji Zamawiający wraz z Wykonawcą przeprowadzą testy akceptacyjne, zgodnie z uzgodnionym Projektem wykonawczym, stanowiące test funkcjonalny platformy ochrony przeciwko Atakom DDoS. Testy uwzględnią weryfikację poprawności wdrożonej konfiguracji. Potwierdzeniem przeprowadzenia ww. testów będzie podpisanie przez Strony Protokołu uruchomienia Usługi;
- b) Przed wdrożeniem pełnej funkcjonalności usługi przed Atakami DDoS Zamawiający wymaga przeprowadzenia, w okresie pełnego miesiąca kalendarzowego od terminu uruchomienia Usługi, o którym mowa w § 2 Umowy, Procesu analizy ruchu Abonenta, w którym ruch zdefiniowany w ramach danej lokalizacji kierowany jest do platformy ochrony przed Atakami DDoS Wykonawcy. Ruch podczas tego procesu nie podlega żadnym filtracjom i w sposób niezmieniony kierowany jest do sieci Zamawiającego. Platforma podczas przedmiotowego procesu nauczania zbiera statystyki, na których podstawie jest w stanie określić parametry algorytmów mitygacji (countremeasures) tak, aby w trakcie Ataku zachować ruch użytkowników, a odfiltrować ruch Ataku. Ze względu na specyfikę poszczególnych usług Zamawiającego realizowanych na udostępnionym łączu, dla wybranych usług Zamawiającego termin wdrożenia pełnej funkcjonalności usługi ochrony przed Atakami DDoS może być przedłużony w porozumieniu Zamawiającego z Wykonawcą.

13. Dostęp do infrastruktury Zamawiającego

W uzasadnionych przypadkach świadczenie Usługi może być powiązane z dostępem do urządzeń aktywnych zarządzanych przez Zamawiającego, w celu uzyskania statystyk ruchu otrzymywanego oraz wysyłanego do sieci Wykonawcy.