# REGULAMIN

**ŚWIADCZENIA PUBLICZNIE DOSTĘPNEJ USŁUGI TELEKOMUNIKACYJNEJ**

**OCHRONY INFRASTRUKTURY ABONENTA PRZED ATAKAMI TYPU DDoS**

**(Distributed Denial of Service) dla Podmiotów realizujących zadania publiczne oraz Podmiotów istotnych z punktu widzenia bezpieczeństwa RP**

obowiązujący od dnia[*] 2023 roku

(*z chwilą zatwierdzenia poprzez opatrzenie kwalifikowanym podpisem elektronicznym)

## § 1

## Postanowienia wstępne

1. Niniejszy Regulamin świadczenia publicznie dostępnej usługi telekomunikacyjnej ochrony Infrastruktury Abonenta przed Atakami DDoS dla Podmiotów realizujących zadania publiczne oraz Podmiotów istotnych z punktu widzenia bezpieczeństwa RP (dalej zwany "**Regulaminem**"), określa zasady świadczenia na rzecz Podmiotów realizujących zadania publiczne i Podmiotów istotnych z punktu widzenia bezpieczeństwa RP, publicznie dostępnych usług telekomunikacyjnych przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (dalej zwany „**Wykonawcą**" lub „**NASK**") z siedzibą w Warszawie, ul. Kolska 12, 01-045 Warszawa, wpisaną do Krajowego Rejestru Sądowego pod numerem 0000012938 przez Sąd Rejonowy dla m.st. Warszawy.
2. Podstawą wykonywania działalności telekomunikacyjnej przez NASK jest wpis do rejestru przedsiębiorców telekomunikacyjnych prowadzonego przez Prezesa Urzędu Komunikacji Elektronicznej.
3. NASK może wprowadzić odrębne regulaminy dla świadczonych przez siebie Usług.
4. Postanowienia Porozumienia oraz odrębnych regulaminów odmienne od postanowień zawartych w Regulaminie, znajdują pierwszeństwo przed postanowieniami Regulaminu.
5. NASK dla świadczenia Usług może posługiwać się podwykonawcami.

## § 2

## Definicje

1. Określenia użyte w liczbie pojedynczej lub mnogiej w Regulaminie lub Porozumieniach, do których ma zastosowanie Regulamin, oznaczają:

1. **Abonent** – Podmiot realizujący zadania publiczne lub Podmiot istotny z punktu widzenia bezpieczeństwa RP, który zawarł Porozumienie z Wykonawcą;
2. **Ankieta techniczna** – dokument stanowiący załącznik do Porozumienia, który Abonent zobowiązany jest dostarczyć Wykonawcy przed podpisaniem Porozumienia. Ankieta techniczna określa wymagania Abonenta odnośnie chronionych zasobów (adresacji IP lub nazw domenowych serwisów/aplikacji internetowych), szacunkowy wolumen obsługiwanego ruchu oraz możliwości techniczne zasobów informatycznych Abonenta. Na podstawie danych wprowadzonych przez Abonenta do Ankiety technicznej NASK określa Wariant Usługi anty-DDoS, który jest najbardziej optymalny dla Abonenta;
3. **Aplikacje Abonenta** – aplikacje internetowe Abonenta wskazane w Ankiecie technicznej i objęte Usługą anty-DDoS na mocy Porozumienia;
4. **Atak DDoS** – wolumetryczny lub aplikacyjny atak typu DDoS (ang. Distributed Denial of Service) na Aplikacje Abonenta lub Infrastrukturę Sieciową Abonenta w celu uniemożliwienia działania Abonenta poprzez zajęcie dostępnych zasobów lub pasma sieci internetowej;
5. **Awaria** - przerwa w świadczeniu Usługi anty-DDoS lub obniżenie poziomu świadczenia Usługi anty-DDoS w stosunku do poziomu deklarowanego przez Wykonawcę. Nie stanowią Awarii przerwa w świadczeniu Usługi anty-DDoS lub obniżenie jakości świadczenia Usługi anty-DDoS związane z urządzeniami, elementami infrastruktury lub innymi zasobami należącymi do Abonenta;
6. **Centrum Czyszczenia** – infrastruktura Wykonawcy służąca do czyszczenia ruchu kierowanego do Infrastruktury Abonenta z Ataków DDoS;

**NASK-PIB**
ul. Kolska 12
01–045 Warszawa

nask@nask.pl
+48 22 380 82 00
+48 22 380 82 01

Projekt finansowany ze środków Ministra Cyfryzacji

7. **Centrum Kontaktu** – wydzielona struktura Wykonawcy odpowiedzialna za bieżący kontakt NASK z Abonentem, w tym za przyjmowanie Ankiety technicznej, przyjmowanie i obsługę Zgłoszeń Awarii i reklamacji, lub informowanie o kwestiach technicznych dotyczących Usługi anty DDoS;
8. **Czas Automatycznej Mitygacji/CAM** – CAM mierzony jest dla Usługi anty-DDoS w Wariancie I; oznacza czas pomiędzy automatycznym wykryciem Ataku DDoS, a przystąpieniem przez Wykonawcę do automatycznej Mitygacji Ataku DDoS;
9. **Czas Reakcji na Atak/CRA** – CRA mierzony jest dla Usługi anty-DDoS w Wariancie II lub Wariancie III obejmującym Infrastrukturę Sieciową Abonenta; oznacza czas pomiędzy pojawieniem się informacji o Ataku DDoS na Koncie w Portalu Administracyjnym, a:
   a. przystąpieniem przez Wykonawcę do automatycznej Mitygacji Ataku DDoS lub
   b. w przypadku braku zgody Abonenta na automatyczną Mitygację Ataku DDoS - powiadomieniem Abonenta o Ataku DDoS w celu Zatwierdzenia;
10. **Czas Reakcji na Zlecenie Mitygacji lub Zatwierdzenie/CRZ** – CRZ mierzony jest dla Usługi anty-DDoS w Wariancie II lub Wariancie III obejmującym Infrastrukturę Sieciową Abonenta; oznacza czas pomiędzy przyjęciem przez Wykonawcę od Abonenta Zlecenia Mitygacji Ataku DDoS lub Zatwierdzenia do momentu przystąpienia przez Wykonawcę do Mitygacji Ataku DDoS;
11. **Czas Zakończenia Mitygacji/CZM** – CZM mierzony jest dla Usługi anty-DDoS we wszystkich Wariantach, oznacza czas pomiędzy zakończeniem Ataku DDoS, a przywróceniem ruchu do stanu sprzed Ataku DDoS; Mitygacja Ataku DDoS uważana jest za zakończoną w momencie zakończenia Ataku DDoS lub, w przypadku Ataku DDoS na Infrastrukturę Sieciową Abonenta, po upływie dodatkowego czasu Mitygacji, który określony jest wstępnie na 72 godziny;
12. **Dzień Roboczy** – każdy dzień tygodnia z wyjątkiem sobót i dni wolnych od pracy na podstawie przepisów powszechnie obowiązującego prawa w Rzeczpospolitej Polskiej; 13) Godziny Robocze - 8.00 – 17.00 w Dni Robocze;
13. **Infrastruktura Abonenta** – Aplikacje Abonenta oraz Infrastruktura Sieciowa Abonenta; ilekroć w postanowieniu Regulaminu mowa o Infrastrukturze Abonenta oznacza to, że ma ono zastosowanie zarówno do Aplikacji Abonenta jak i Infrastruktury Sieciowej Abonenta;
14. **Infrastruktura Sieciowa Abonenta** - zbiór urządzeń oraz oprogramowania, które wchodzą w skład sieci informatycznej Abonenta, wskazane w Ankiecie technicznej i objęte Usługą anty-DDoS na mocy Porozumienia;
15. **Instruktaż** – szkolenie zapewnione przez Wykonawcę na rzecz Abonenta, z zakresu Usługi anty-DDoS oraz korzystania z Konta w Portalu Administracyjnym;
16. **Konto** – konto Abonenta w Portalu Administracyjnym;
17. **Koordynator Usługi Abonenta** – osoba wskazana w Porozumieniu przez Abonenta, odpowiedzialna za obsługę Konta w Portalu Administracyjnym oraz nadzorowanie realizacji Usług po stronie Abonenta;
18. **Mitygacja Ataku DDoS** – działania podejmowane przez Wykonawcę, które mają na celu przekierowanie ruchu z Infrastruktury Abonenta do Centrum Czyszczenia i oczyszczenie ruchu Abonenta z Ataków DDoS;
19. **Obiekt** – sieć/prefix objęty Usługą anty-DDoS, którego maska ma maksymalnie 24 bity lub serwis umieszczony w publicznej sieci Internet;
20. **Okno Serwisowe** – okres, o którym zostanie powiadomiony Abonent, w którym mogą być wykonywane Prace Planowane;
21. **Podmiot istotny z punktu widzenia bezpieczeństwa RP** – podmiot wskazany do objęcia Usługą anty-DDoS przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa;
22. **Podmiot realizujący zadania publiczne** – podmiot na który na podstawie ustawy lub innych aktów prawnych nałożony został obowiązek realizacji zadań służących zaspokojeniu zbiorowych potrzeb ludności (zadań publicznych);
23. **Porozumienie** – porozumienie o świadczenie Usług zawierane pomiędzy NASK i Abonentem w formie pisemnej, elektronicznej lub dokumentowej, w zależności od uzgodnienia pomiędzy stronami Porozumienia. Porozumienie określa m. in. okres świadczenia Usług dla Abonenta, Wariant Usługi anty-DDoS oraz warunki i zasady rozwiązania Porozumienia. Porozumienie zawierane jest na czas określony;
24. **Portal Administracyjny** – system informatyczny Wykonawcy udostępniony nieodpłatnie Abonentowi za pomocą środków komunikacji elektronicznej w celu realizacji Usługi anty-DDoS;
25. **Prace Planowane** – prace konserwacyjne i modernizacyjne mogące skutkować przerwami w świadczeniu Usług;
26. **Raport** – wygenerowany automatycznie w Koncie na Portalu Administracyjnym wykaz informacji z realizacji Usługi antyDDoS przez Wykonawcę;
27. **Siła Wyższa** – zdarzenie zewnętrzne, niezależne od Stron, które ma charakter nadzwyczajny i któremu nie można zapobiec nawet przy dołożeniu należytej staranności (np. katastrofalne działanie przyrody, wojna, rozruchy itp.);
28. **SLA** - gwarantowany przez Wykonawcę poziom świadczonej Usługi anty-DDoS;
29. **Strony** – Wykonawca i Abonent;
30. **Uprawniony Użytkownik** – wyznaczona przez Abonenta osoba, uprawniona do obsługi Ataku DDoS po stronie Abonenta;
31. **Usługa anty-DDoS** – nieodpłatna dla Abonenta usługa polegająca na ochronie Infrastruktury Abonenta, w określonym przez Strony w Porozumieniu Wariancie, przed Atakami DDoS, świadczona przez NASK na podstawie Porozumienia, finansowana ze środków dotacji celowej udzielonej ze środków ministra właściwego do spraw cyfryzacji, w ramach realizowanego przez NASK zadania publicznego;

Projekt finansowany ze środków Ministra Cyfryzacji

32. **Usługi** – usługi świadczone przez Wykonawcę na rzecz Abonenta na podstawie Porozumienia i Regulaminu, w szczególności Usługa anty-DDoS; Usługi zdefiniowane są w § 3 Regulaminu;
33. **Wariant** – zakres Usługi anty-DDoS świadczonej przez Wykonawcę na rzecz Abonenta w zależności od Infrastruktury Abonenta objętej Usługą anty-DDoS, tj. Aplikacji Abonenta lub Infrastruktury Sieciowej Abonenta;
34. **Wykonawca** – NASK;
35. **Zatwierdzenie** – zatwierdzenie przez Abonenta Mitygacji Ataku DDoS, stosowane jest w Wariancie II i III Usługi anty-DDoS w przypadku ataku DDoS dotyczącego Infrastruktury Sieciowej Abonenta;
36. **Zdarzenie** – każde wzmożenie ruchu w Infrastrukturze Abonenta mające cechy Ataku DDoS. 38) Zgłoszenie – dokument w formie elektronicznej, zawierający niezbędne informacje na temat Awarii;
37. **Zlecenie Mitygacji** – zgłoszenie Abonenta przeprowadzenia przez NASK Mitygacji Ataku DDoS; Zlecenie Mitygacji stosuje się w Wariancie II i III obejmującym Infrastrukturę Sieciową Abonenta Usługi anty-DDoS;

2. Pojęcia, które występują w, Porozumieniu, w tym również w załącznikach do Porozumienia, a nie zostały zdefiniowane powyżej, lecz posiadają swe definicje w Porozumieniu, w tym również w załącznikach do Porozumienia lub przepisach prawa, mają znaczenie tam zdefiniowane.

## § 3

## Usługi

1. Wykonawca zobowiązany jest, pod warunkiem zawarcia Porozumienia i na zasadach w nim określonych, świadczyć nieodpłatnie na rzecz Abonenta:
   a. Usługę anty-DDoS w jednym z Wariantów określonych w Porozumieniu;
   b. Usługę prowadzenia Konta w Portalu Administracyjnym;
   c. Usługę Instruktażu.
2. Wykonawca oświadcza, że:
   a. Zapewnia realizację Usługi anty-DDoS przez podwykonawcę posiadającego aktualne poświadczenie certyfikacji ISO 27001;
   b. Usługa anty-DDoS co do zasady jest świadczona w centrach danych znajdujących się na terenie Europejskiego Obszaru Gospodarczego;
   c. Usługa anty-DDoS zapewnia geolokalizację adresów IP umożliwiającą blokadę ruchu przychodzącego z danego kraju bądź obszaru geograficznego;
   d. w ramach Usługi anty-DDoS nie są zapewniane połączenia z numerami alarmowymi oraz nie są gromadzone informacje dotyczące lokalizacji telekomunikacyjnego urządzenia końcowego;
   e. Usługa anty-DDoS ma minimalny wpływ na ruch w Infrastrukturze Abonenta (bardzo niewielkie prawdopodobieństwo tzw. false positives, tj. potencjalnej możliwości blokady i zakłócenia prawidłowego ruchu w Infrastrukturze Abonenta w przypadku braku wystąpienia Ataku DDoS, z możliwością przerwania Mitygacji nieprawidłowo wykrytego Ataku DDoS).
3. Usługi mogą być wykonywane przy wykorzystaniu systemów teleinformatycznych NASK. Warunki korzystania z takich systemów teleinformatycznych mogą być uregulowane w odrębnych umowach.
4. Wykonawca zapewnia Abonentowi możliwość generowania Raportu za pośrednictwem Konta w Portalu Administracyjnym z częstotliwością raz w tygodniu. Raport zawiera w szczególności informacje na temat:
   a. liczby i kategorii Zdarzeń, w tym Ataków DDoS, które wystąpiły w poprzednim okresie objętym Raportem;
   b. statystyki związane z ruchem do Infrastruktury Abonenta.

## § 4

## Zawarcie Porozumienia i rozpoczęcie świadczenia Usługi anty-DDoS

1. W celu świadczenia Usług, Strony zawierają Porozumienie określające zasady świadczenia tych Usług.
2. Wykonawca uzależnia zawarcie Porozumienia od przesłania przez Abonenta wypełnionej Ankiety technicznej, stanowiącej podstawę do kwalifikacji do objęcia Usługą anty-DDoS oraz umożliwiającej wybór Wariantu Usługi anty-DDoS.
3. Skutki złożenia przez Abonenta w Porozumieniu nieprawdziwych oświadczeń, zatajenia lub podania błędnych informacji wymaganych do zawarcia lub wykonywania Porozumienia obciążają Abonenta.
4. Usługa anty-DDoS może być uruchomiona po:
   a. Wyznaczeniu przez Abonenta Uprawnionych Użytkowników stosownie do § 6 ust. 6 Regulaminu;
   b. Utworzeniu Konta w Portalu Administracyjnym;
   c. Przygotowaniu przez Abonenta Infrastruktury Abonenta do świadczenia Usługi anty-DDoS.
5. Termin realizacji Usług, o których mowa w ust. 6 lit. b i c powyżej, Strony określą w Porozumieniu.

Projekt finansowany ze środków Ministra Cyfryzacji

6. Wykonawca i Abonent potwierdzą uruchomienie Usługi anty-DDoS w protokole zawierającym datę uruchomienia Usługi anty-DDoS. Wykonawca sporządza projekt protokołu uruchomienia Usługi anty-DDoS i przekazuje go do Abonenta. Abonent jest zobowiązany dostarczyć Wykonawcy podpisany przez siebie protokół uruchomienia Usługi anty-DDoS w terminie 3 Dni Roboczych od dnia przekazania mu przez Wykonawcę tego protokołu. Niedostarczenie podpisanego protokołu przez Abonenta w terminie 3 Dni Roboczych od przekazania mu protokołu uruchomienia Usługi anty-DDoS, jest równoznaczne z podpisaniem protokołu przez Abonenta.

## § 5

## Usługa anty-DDoS

1. Usługa anty-DDoS obejmuje jeden z następujących Wariantów, określony przez Strony w Porozumieniu:
   a. Wariant I: ochronę Aplikacji Abonenta;
   b. Wariant II: ochronę Infrastruktury Sieciowej Abonenta;
   c. Wariant III: ochronę zarówno Aplikacji Abonenta jak i Infrastruktury Sieciowej Abonenta.
2. Ilekroć w Regulaminie mowa jest o prawach i obowiązkach Stron bez określenia Wariantu lub jego zakresu, oznacza to, że w tym zakresie Regulamin zastosowanie ma do każdego Wariantu.
3. W przypadku zmian w Infrastrukturze Abonenta w toku obowiązywania Porozumienia, Abonent może dokonać zmiany Wariantu. W takim przypadku Strony dokonują zmiany Porozumienia; § 4 Regulaminu stosuje się odpowiednio.
4. W ramach świadczenia Usługi anty-DDoS Wykonawca zobowiązany jest do:
   a. monitorowania ruchu w Infrastrukturze Abonenta w celu wykrycia Ataków DDoS;
   b. przeprowadzenia Mitygacji Ataków DDoS;
   c. przekierowania oczyszczonego ruchu do Infrastruktury Abonenta.
5. Abonent zobowiązany jest do:
   a. Współdziałania z Wykonawcą w wykonywaniu Usług;
   b. Informowania Wykonawcy o wszelkich okolicznościach mających wpływ na realizację Usług;
   c. W przypadku Wariantu II i III w zakresie Infrastruktury Sieciowej Abonenta w przypadku braku zgody na automatyczną Mitygację Ataków DDoS - monitorowania Infrastruktury Sieciowej Abonenta w celu wykrycia Ataków DDoS. Monitorowanie Infrastruktury Sieciowej Abonenta może być wspomagane przez Wykonawcę poprzez dostarczanie Abonentowi informacji o wykryciu Ataku DDoS.
6. Usługa anty-DDoS, w zależności od Wariantu, świadczona jest w następujących trybach:
   a. Dla Wariantu I – w trybie ciągłym; w takim przypadku ruch w Aplikacjach Abonenta na stałe jest przekierowany do Centrum Czyszczenia. Ataki DDoS są automatycznie wykrywane przez Wykonawcę na podstawie pomiarów ruchu, a Usługa antyDDoS jest uruchamiana bez dodatkowego żądania Abonenta. Po wykonaniu Mitygacji Ataku DDoS oczyszczony ruch przesyłany jest do urządzenia na którym znajdują się Aplikacje Abonenta;
   b. Dla Wariantu II:
      i. w trybie na żądanie; Usługa anty-DDoS uruchamiana jest, po wykryciu Ataku DDoS przez Abonenta (na podstawie dostarczonych Wykonawcy próbek ruchu z Infrastruktury Sieciowej Wykonawca dostarcza Abonentowi informacje o wykryciu ataku), po otrzymaniu przez Wykonawcę Zatwierdzenia; po uruchomieniu Usługi anty-DDoS ruch z Infrastruktury Sieciowej przekierowany jest do Centrum Czyszczenia. Po wykonaniu Mitygacji Ataku DDoS, oczyszczony ruch zostaje zwrotnie przesłany do Infrastruktury Sieciowej Abonenta.

      ii. w trybie automatycznym; Usługa anty-DDoS uruchamiana jest w sposób automatyczny po wykryciu Ataku DDoS na podstawie dostarczonych Wykonawcy próbek ruchu z Infrastruktury Sieciowej Abonenta, po uruchomieniu Usługi anty-DDoS ruch z Infrastruktury Sieciowej przekierowany jest do Centrum Czyszczenia. Po wykonaniu Mitygacji Ataku DDoS, oczyszczony ruch zostaje zwrotnie przesłany do Infrastruktury Sieciowej Abonenta. Abonent ma możliwość uruchomienia Usługi anty DDoS w trybie wskazanym w pkt i powyżej.

   c. Dla Wariantu III – w trybie obejmującym:
      i. tryb ciągły, o którym mowa w lit. a w odniesieniu do Aplikacji Abonenta;
      ii. tryb na żądanie lub automatyczny, o których mowa odpowiednio w lit. b, w odniesieniu do Infrastruktury Sieciowej.
7. W przypadku Wariantu II i III w zakresie dotyczącym Infrastruktury Sieciowej Abonenta:
   a. Abonent może w Porozumieniu wyrazić zgodę na automatyczną Mitygację Ataku DDoS;
   b. Abonent może w Porozumieniu nie wyrazić zgody na automatyczną Mitygację Ataku DDoS, wówczas w przypadku wykrycia Ataku DDoS przez Wykonawcę:
      i. Wykonawca powiadamia Abonenta o Ataku DDoS;

      ii. Abonent dokonuje Zatwierdzenia na podstawie którego NASK przeprowadza Mitygację Ataku DDoS;

Projekt finansowany ze środków Ministra Cyfryzacji

c. Abonent może dokonać Zlecenia Mitygacji, po samodzielnym wykryciu Ataku DDoS.

8. Szczegółowy opis Usługi anty-DDoS zawiera załącznik nr 1 do Regulaminu.
9. Wykonawca zastrzega, że:
   a. nie gwarantuje oczyszczenia Infrastruktury Abonenta z każdego Ataku DDoS, deklarując wyłącznie podejmowanie, w dobrej wierze, działań w celu Mitygacji Ataków DDoS, a w razie braku możliwości Mitygacji Ataku DDoS - współpracę z Abonentem w celu określenia sposobu zapobieżenia skutkom Ataku DDoS;
   b. nie gwarantuje, że Mitygacja Ataku DDoS nie będzie prowadzić do zakłócenia działalności Abonenta, przy czym w takim przypadku Abonentowi przysługują uprawnienia określone w§ 6 ust. 7 Regulaminu.

## § 6.

## Obsługa Zdarzeń, w tym Ataków DDoS

1. W przypadku Zdarzenia, w szczególności podejrzenia Ataku DDoS, Wykonawca:
   a. powiadamia Abonenta o Zdarzeniu;
   b. weryfikuje ruch w Infrastrukturze Abonenta w celu potwierdzenia Ataku DDoS;
   c. powiadamia Abonenta o kategorii Zdarzenia, przy czym obowiązek ten nie istnieje w przypadku kategorii INFORMACYJNEJ/ Severity Low, o której mowa w ust. 2 poniżej;
   d. w przypadku potwierdzenia Ataku DDoS - podejmuje czynności mające na celu Mitygację Ataku DDoS w zależności od Wariantu:
      i w sposób automatyczny, przekazując powiadomienie automatycznego uruchomienia Mitygacji Ataku DDoS lub;
      ii po uzyskaniu Zatwierdzenia;
      iii po otrzymaniu Zlecenia Mitygacji;
   c. powiadamia Abonenta o zakończeniu Mitygacji.
2. Zdarzenia zostaną przyporządkowane przez Wykonawcę do jednej z niżej opisanych kategorii:

| Kategoria Zdarzenia | Opis Zdarzenia |
|---|---|
| KRYTYCZNE/ Severity High | Atak DDoS |
| INFORMACYJNE/ Severity Low | Fałszywy alarm albo anomalia w ruchu lub nagły wzrost ruchu wynikający z innych przyczyn niż Atak DDoS |

3. Obsługa Ataków DDoS realizowana jest przez następujące kanały komunikacji:
   a. Powiadomienie o Zdarzeniu i powiadomienie o kategorii Zdarzenia – telefon, poczta elektroniczna;
   b. Potwierdzenie automatycznego uruchomienia Mitygacji Ataku DDoS – poczta elektroniczna;
   c. Zatwierdzenie – poczta elektroniczna lub telefon;
   d. Zlecenie Mitygacji lub Zlecenie przerwania Mitygacji Ataku DDoS – poczta elektroniczna lub telefon;
   e. Powiadomienie o zakończeniu Mitygacji Ataku DDoS - poczta elektroniczna;
   f. Eskalacja w przypadku braku kontaktu poprzez pocztę elektroniczną lub telefon, w przypadkach, o których mowa w lit. b-e – SMS na numer wskazany przez Abonenta;
   g. W innych przypadkach określonych w Regulaminie – poczta elektroniczna.
4. Adresy poczty elektronicznej oraz numery telefonów Stron, o których mowa w ust. 3, wskazane są w Porozumieniu.
5. Obsługa Ataku DDoS realizowana jest po stronie Abonenta wyłącznie przez Uprawnionych Użytkowników.
6. Abonent wskaże Wykonawcy, w Porozumieniu Uprawnionych Użytkowników. Abonent może w każdym czasie zmienić Uprawnionych Użytkowników w sposób określony w Porozumieniu.
7. Abonent uprawniony jest, na swoje ryzyko, do zlecenia przerwania Mitygacji Ataku DDoS, jeżeli ma ona lub może mieć negatywny wpływ na wykonywane przez Abonenta zadania lub zasoby zawarte w Infrastrukturze Abonenta. W takim przypadku Wykonawca zobowiązany jest do przerwania Mitygacji Ataku DDoS w terminie 15 minut od momentu otrzymania zlecenia przerwania Mitygacji Ataku DDoS od Abonenta.
8. Abonent zobowiązany jest do poinformowania Wykonawcy, z wyprzedzeniem wynoszącym co najmniej 3 (trzy) Dni Robocze, o planowanym przez niego przedsięwzięciu lub realizacji zadania, które może spowodować znaczne przekroczenie poziomu deklarowanego w Ankiecie technicznej ruchu w Infrastrukturze Abonenta. W takim przypadku Abonent informuje Wykonawcę o:
   a. Charakterze i rodzaju takiego przedsięwzięcia lub zadania;
   b. Planowanym okresie trwania takiego przedsięwzięcia lub zadania.

Projekt finansowany ze środków Ministra Cyfryzacji

**§ 7.**

**Usługa Konta w Portalu Administracyjnym**

1. W celu realizacji Usługi anty-DDoS Wykonawca zapewnia Abonentowi dostęp do Konta w Portalu Administracyjnym.
2. Konto w Portalu Administracyjnym umożliwia:
   a. w przypadku ochrony Aplikacji Abonenta – zarządzanie oraz monitorowanie Usługi anty-DDoS;
   b. w przypadku ochrony Infrastruktury Sieciowej Abonenta – komunikację w zakresie realizacji Usługi anty-DDoS;
3. W celu świadczenia Usługi anty-DDoS w Wariancie I lub III w zakresie ochrony Aplikacji Abonenta, Portal Administracyjny umożliwia wgranie prywatnego klucza wygenerowanego na potrzeby posiadanego własnego certyfikatu SSL/TLS.
4. Jeżeli Abonent nie wyraża zgody na udostępnienie prywatnego klucza, zgodnie z ust. 3 powyżej, Wykonawca umożliwi, poprzez Portal Administracyjny wygenerowanie Uprawnionemu Użytkownikowi certyfikatu na potrzeby konkretnej Aplikacji albo certyfikatu obsługującego wszystkie subdomeny Abonenta.
5. Generowanie certyfikatu w sposób wskazany w ust. 4 jest możliwe pod warunkiem przeprowadzenia przez Wykonawcę walidacji posiadania przez Abonenta uprawnień do posługiwania się takim certyfikatem, na co Abonent wyraża zgodę. Walidacja taka wymaga od Abonenta możliwości konfiguracji danych w systemach DNS Abonenta.

**§ 8.**

**Usługa Instruktażu**

1. Wykonawca świadczy Usługę Instruktażu na rzecz Uprawnionych Użytkowników.
2. Termin Instruktażu zostanie określony przez Strony.
3. Instruktaż obejmuje:
   a. Zasady działania Usługi anty-DDoS,
   b. Zasady obsługi Konta w Portalu Administracyjnym;
   c. Zasady obsługi Ataków DDoS, w szczególności z uwzględnieniem praw i obowiązków Abonenta;
   d. Zasady współdziałania Abonenta w zakresie realizacji Usług.
4. Nieprzystąpienie lub nieukończenie Instruktażu przez Uprawnionego Użytkownika uprawnia Wykonawcę do wstrzymania świadczenia Usług, bez ponoszenia z tego tytułu konsekwencji.

**§ 9**

**Zawieszenie świadczenia Usług**

1. Wykonawca może zawiesić świadczenie Usług, bez prawa Abonenta do odszkodowania, w następujących przypadkach:
   1) działania lub zaniechania Abonenta lub osoby, za której działanie lub zaniechanie Abonent ponosi odpowiedzialność, powodującego szkodę lub utrudniającego bądź uniemożliwiającego świadczenie lub korzystanie z Usług przez innych abonentów, Wykonawcę lub inne podmioty współpracujące z Wykonawcą (w tym działania mające na celu naruszenie bezpieczeństwa lub integralności sieci lub usług);
   2) korzystania z Usług w sposób naruszający obowiązujące przepisy lub dobre obyczaje;
   3) podania przez Abonenta nieprawdziwych danych w Ankiecie technicznej, zatajenia lub podania błędnych informacji wymaganych do zawarcia lub wykonywania Usług;
   4) nieumożliwienia lub utrudnienia Wykonawcy przez Abonenta skontrolowania sposobu korzystania z Usług lub stanu i sposobu korzystania z Konta w Portalu Administracyjnym;
   5) naruszenia w inny sposób postanowień Regulaminu, Porozumienia lub innych warunków świadczenia Usług.
2. Ponadto Wykonawca ma prawo zawiesić świadczenie Usług Abonentowi, jeżeli:
   a. żądanie takie zgłoszą właściwe organy, w szczególności wykonujące zadania i obowiązki na rzecz obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego;
   b. Wykonawca utraci w całości lub części uprawnienia niezbędne do świadczenia Usług;
   c. z innych względów, w szczególności technicznych, Wykonawca utraci możliwość świadczenia Usług.
3. Wykonawca poinformuje Abonenta niezwłocznie o zawieszeniu Usług wraz z podaniem przyczyny zawieszenia określonej w ust. 1 lub 2.
4. Wznowienie świadczenia Usługi następuje po ustaniu przyczyn zawieszenia.
5. W przypadku zawieszenia Usługi na podstawie ust. 1, Wykonawca może uzależnić wznowienie świadczenia Usługi od pisemnego wniosku Abonenta.
6. Okresu zawieszenia świadczenia Usługi nie uwzględnia się przy ustalaniu czasu dostępności Usługi anty-DDoS.

Projekt finansowany ze środków Ministra Cyfryzacji

**§ 10**

**SLA**

1. Wykonawca deklaruje dostępność Usługi anty-DDoS, rozumianej jako gotowość Wykonawcy do świadczenia Usługi anty-DDoS, na poziomie 99,9% w okresie świadczenia Usługi anty-DDoS wskazanym w Porozumieniu.
2. Do czasu dostępności Usługi anty-DDoS, o której mowa w ust. 1, nie wlicza się przerw spowodowanych Pracami Planowanymi oraz zawieszeniem Usług zgodnie z § 9.
3. Wykonawca będzie informować Abonenta o Pracach Planowanych prowadzonych w Oknie Serwisowym w formie pisemnej, telefonicznie, pocztą elektroniczną z co najmniej 48-godzinnym wyprzedzeniem. Wykonawca deklaruje świadczenie Usługi antyDDoS z zachowaniem terminów określonych w niniejszym paragrafie. Abonent przyjmuje do wiadomości, że Zgłoszenie Awarii w ramach SLA stanowi jedyne zadośćuczynienie z powodu przekroczenia terminów realizacji Usługi anty-DDoS, bez uszczerbku dla skutków wynikających z bezwzględnie obowiązujących przepisów prawa.
4. W przypadku Wariantu I Usługi anty-DDoS Wykonawca deklaruje dochowanie następujących terminów:

| | |
|---|---|
| Czas Automatycznej Mitygacji | 5 sekund |

5. W przypadku Wariantu II Usługi anty-DDoS Wykonawca deklaruje dochowanie następujących terminów:

| | |
|---|---|
| Czas Reakcji na Atak | 15 minut |
| Czas Reakcji na Zlecenie Mitygacji lub Zatwierdzenie | 15 minut |
| Czas Zakończenia Mitygacji | Od 15 minut do 72 godzin – zależne od decyzji Abonenta |

6. W przypadku Wariantu III Usługi anty-DDoS Wykonawca deklaruje:
   a. dochowanie terminów określonych w ust. 5 – w odniesieniu do Aplikacji Abonenta;
   b. dochowanie terminów określonych w ust. 6 – w odniesieniu do Infrastruktury Sieciowej Abonenta.
7. Celem usunięcia wątpliwości Wykonawca potwierdza, że przyznana przez Wykonawcę kategoria Zdarzenia, zgodnie z § 6 ust. 2 nie wpływa na terminy, o których mowa w ust. 5 i 6 powyżej.
8. NASK oświadcza, że wprowadził procedury mające na celu pomiar i organizację ruchu w elementach sieci telekomunikacyjnej NASK służącej świadczeniu Usługi anty-DDoS, aby zapobiec osiągnięciu lub przekroczeniu pojemności łącza, w szczególności polegające na stałym monitorowaniu obciążenia sieci w charakterystycznych jej punktach lub na styku z sieciami innych operatorów, we współpracy z podwykonawcami Usługi anty-DDoS oraz zarządzaniu transmisją danych oraz zarządzaniu infrastrukturą i urządzeniami służącymi do świadczenia Usługi anty-DDoS. Wprowadzone przez NASK procedury mają na celu zachowanie jakości świadczonej Usługi anty-DDoS.
9. W ramach SLA Wykonawca zapewnia nadzór nad ciągłością i jakością świadczenia Usługi anty-DDoS, w tym utrzymywanie ustalonych w Porozumieniu warunków technicznych Usługi anty-DDoS, przyjmowanie Zgłoszeń oraz usuwanie Awarii. Szczegółowe warunki usuwania Awarii mogą być określone w Porozumieniu.
10. W przypadku przekroczenia przez Wykonawcę terminów wskazanych w ust. 5 i 6 Abonent zgłasza Awarię za pośrednictwem Centrum Kontaktu pod adresem addos_noc@nask.pl
11. Abonent zobowiązany jest zgłosić Awarię do Centrum Kontaktu niezwłocznie po jej stwierdzeniu. Zgłoszenie Awarii powinno zawierać dane umożliwiające identyfikację Abonenta, Usługi anty-DDoS, opis Awarii oraz numer Porozumienia.
12. Przyjmujący informację o Awarii tworzy Zgłoszenie i na żądanie podaje jego numer osobie zgłaszającej Awarię.
13. Abonent podczas kontaktów z Wykonawcą w sprawach dotyczących usuwania Awarii powinien podawać numer Zgłoszenia.
14. Wykonawca deklaruje usunięcie Awarii w terminie 2 Dni Roboczych od momentu Zgłoszenia.
15. Abonent zobowiązany jest do współpracy z Wykonawcą podczas usuwania Awarii, o ile jest to niezbędne. W przypadku braku możliwości skontaktowania się z Abonentem przez co najmniej godzinę, Wykonawca może wstrzymać usuwanie Awarii. Momentem wstrzymania jest w takim przypadku godzina rozpoczęcia prób skontaktowania się z Abonentem. W takim przypadku Wykonawca podejmuje próbę skontaktowania się z Abonentem, łącznie nie dłużej jednak niż przez 3 godziny. Jeżeli próba taka powiedzie się, Zgłoszenie zostaje zawieszone. Czas wstrzymania usuwania Awarii i zawieszenia Zgłoszenia nie wlicza się do czasu, o którym mowa w ust. 15.
16. Po usunięciu Awarii Wykonawca kontaktuje się z Abonentem w celu potwierdzenia usunięcia Awarii. Abonent potwierdza usunięcie Awarii, co skutkuje zamknięciem Zgłoszenia. W przypadku braku odpowiedzi Abonenta, braku możliwości skontaktowania się Abonentem lub bezzasadnej odmowy potwierdzenia przez Abonenta usunięcia Awarii, Wykonawca zamyka Zgłoszenie bez potwierdzenia ze strony Abonenta.

Projekt finansowany ze środków Ministra Cyfryzacji

**§ 11**

**Zasady, tryb i terminy składania oraz rozpatrywania reklamacji**

1. Abonenci mogą składać Wykonawcy reklamacje dotyczące:
   a. niedotrzymania z winy Wykonawcy terminu uruchomienia Usługi anty-DDoS, okresu świadczenia Usług,
   b. niewykonania lub nienależytego wykonania Usług, Regulaminu lub Porozumienia.
2. Celem usunięcia wątpliwości Wykonawca potwierdza, że zgłoszenie dotyczące przekroczenia terminu wykonania Usługi anty-DDoS realizowane jest w trybie wskazanym w § 10 SLA.
3. Abonent może złożyć reklamację w terminie 7 Dni Roboczych, od dnia w którym zakończyła się przerwa w świadczeniu Usług, lub od dnia, w którym Usługi zostały nienależycie wykonane lub miały być wykonane.
4. Reklamację złożoną po upływie terminu wskazanego w ust. 2 pozostawia się bez rozpoznania, o czym Centrum Kontaktu niezwłocznie powiadamia reklamującego Abonenta.
5. Reklamacja powinna zawierać:
   a. nazwę oraz adres Abonenta, a także dane niezbędne do kontaktu zwrotnego, w tym imię i nazwisko osoby składającej reklamację oraz jej funkcję; dane osobowe osoby składającej reklamację są przetwarzane przez Wykonawcę zgodnie z obowiązującymi przepisami; Informacja dotycząca przetwarzania danych osobowych jest przekazywana Abonentowi;
   b. przedmiot reklamacji;
   c. przedstawienie okoliczności uzasadniających reklamację;
   d. numer Porozumienia łączącego NASK i Abonenta;
   e. datę zawarcia Porozumienia i określony w niej termin rozpoczęcia świadczenia Usług – w przypadku reklamacji dotyczącej niedotrzymania z winy Wykonawcy terminu rozpoczęcia świadczenia Usług;
   f. podpis Abonenta – w przypadku reklamacji złożonej w formie pisemnej.
6. W przypadku, gdy reklamacja złożona przez Abonenta w sposób wskazany w ust. 1-5, nie spełnia warunków określonych w ust. 5, Wykonawca wzywa do jej uzupełnienia w terminie nie krótszym niż 7 dni wskazując zakres tego uzupełnienia, z pouczeniem, że nieuzupełnienie reklamacji w określonym terminie spowoduje pozostawienie reklamacji bez rozpoznania. Po bezskutecznym upływie wyznaczonego terminu, reklamację pozostawia się bez rozpoznania.
7. Reklamacja może być złożona:
   a. w formie pisemnej – przesyłką pocztową w rozumieniu art. 3 pkt 21 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (t.j. Dz. U. z 2022 r., poz. 896 z późn. zm.) na adres siedziby NASK-PIB, ul. Kolska 12 01-045 Warszawa; z dopiskiem „Reklamacja ADDoS";
   b. ustnie – telefonicznie albo osobiście do protokołu podczas wizyty reklamującego w jednostce obsługującej Abonenta;
   c. w formie elektronicznej - drogą poczty elektronicznej, na adres Centrum Kontaktu: addos_noc@nask.pl.
8. W przypadku złożenia reklamacji w formie pisemnej, albo w formie elektronicznej, Wykonawca w terminie 14 dni od dnia złożenia reklamacji potwierdza jej przyjęcie. Powyższego postanowienia nie stosuje się w przypadku udzielenia odpowiedzi na reklamację w terminie 14 dni od dnia jej złożenia.
9. Potwierdzenie przyjęcia reklamacji wskazuje dzień złożenia oraz numer reklamacji.
10. Wykonawca jest zobowiązany do rozpatrzenia reklamacji w terminie do 30 dni od daty jej wniesienia.
11. Odpowiedź na reklamację zawiera:
   a. wskazanie Wykonawcy rozpatrującego reklamację;
   b. informację o dniu złożenia reklamacji;
   c. rozstrzygnięcie o uznaniu lub odmowie uznania reklamacji;
   d. dane identyfikujące upoważnionego pracownika reprezentującego Wykonawcę, z podaniem jego imienia, nazwiska oraz zajmowanego stanowiska.
12. W przypadku odmowy uznania reklamacji w całości lub części odpowiedź na reklamację:
   a. zawiera uzasadnienie faktyczne;
   b. powinna zostać doręczona reklamującemu w tej samej formie, w której została doręczona, z uwzględnieniem możliwości doręczenia drogą elektroniczną na wniosek reklamującego w każdym przypadku.
13. Odpowiedź na reklamację jest każdorazowo doręczana reklamującemu w formie, w której została złożona, z uwzględnieniem możliwości doręczenia drogą elektroniczną na wniosek reklamującego w każdym przypadku. Wniosek powinien zostać złożony wraz z reklamacją lub w toku rozpatrywania reklamacji.
14. Jeżeli wysłana przez Wykonawcę odpowiedź na reklamację nie została doręczona Abonentowi, Wykonawca, na żądanie Abonenta wyrażone w sposób określony w ust. 6, niezwłocznie przekazuje ponownie tę odpowiedź, jej duplikat lub kopię.
15. Reklamujący, określa sposób w jakiej odpowiedź na reklamację, jej duplikat lub kopia, o których mowa w ust. 14, ma zostać przekazana wraz z reklamacją lub w toku rozpatrywania reklamacji.

Projekt finansowany ze środków Ministra Cyfryzacji

16. Na żądanie Abonenta, w przypadku odmowy uznania reklamacji w całości lub części, Wykonawca ponownie przekazuje odpowiedź na reklamację, jej duplikat lub kopię w formie wskazanej w ust. 13.
17. Wykonawca nie jest obowiązany do ponownego przekazania reklamującemu odpowiedzi na reklamację, jej duplikatu lub kopii, jeżeli z okoliczności danej sprawy jednoznacznie wynika, że odpowiedź na reklamację została doręczona reklamującemu.

## § 12

## Odpowiedzialność

1. Wykonawca ponosi odpowiedzialność z tytułu niewykonania lub nienależytego wykonania Usług na zasadach określonych w Porozumieniu i Regulaminie.
2. O ile nic innego nie wynika z Regulaminu lub Porozumienia Wykonawca ponosi odpowiedzialność wyłącznie za staranne działanie i nie ponosi odpowiedzialności za rezultat, tj. skuteczność i przydatność dla Abonenta Usług, w szczególności Usługi anty-DDoS.
3. Abonent odpowiada za szkody Wykonawcy, spowodowane przez Abonenta.
4. Wykonawca nie ponosi odpowiedzialności za problemy techniczne lub ograniczenia występujące w urządzeniach lub systemach teleinformatycznych, z których korzysta Abonent lub upoważniony przez niego użytkownik, które uniemożliwiają prawidłowe korzystanie z Usług jeśli nie jest to wynikiem działania Wykonawcy.
5. Wykonawca nie ponosi odpowiedzialności za utratę danych Abonenta, jeśli utrata danych była spowodowana awarią urządzeń lub systemu teleinformatycznego, z których korzysta Abonent.
6. Wykonawca nie odpowiada za szkodę wynikającą z niewykonania lub nienależytego wykonywania Usług, gdy ich niewykonanie lub nienależyte wykonanie jest następstwem:
   1) działania Siły Wyższej,
   2) przyczyn dotyczących Abonenta lub osoby trzeciej,
   3) zawieszenia świadczenia Usług uzgodnionego przez Abonenta i Wykonawcę lub wynikającego z Regulaminu lub Porozumienia,
   4) naruszenia przez Abonenta postanowień Regulaminu lub Porozumienia;
   5) zaprzestania świadczenia Usług, jeśli nastąpiło to z winy Abonenta lub przyczyn niezależnych od Wykonawcy;
   6) działania lub zaniechania Abonenta sprzecznego z przepisami powszechnie obowiązującego prawa.

7. Wyłączenie odpowiedzialności Wykonawcy na podstawie niniejszego paragrafu nie uchybia innym przesłankom wyłączenia odpowiedzialności określonym w Regulaminie, Porozumieniu lub przepisach prawa.
8. Ze względu na to, że Usługi świadczone są nieodpłatnie i Abonent nie jest płatnikiem opłat za Usługi, Abonentowi nie przysługują żadne roszczenia odszkodowawcze z tytułu niewykonania lub nienależytego wykonania Usług, bez uszczerbku dla przypadków wynikających z Regulaminu i bezwzględnie obowiązujących przepisów prawa.
9. NASK przekazuje Abonentowi informacje o zagrożeniach związanych ze świadczonymi Usługami, w tym o sposobach ochrony bezpieczeństwa, prywatności i danych osobowych za pośrednictwem swojej strony internetowej i poczty elektronicznej.
10. NASK jest uprawniony do następujących działań w związku z przypadkami naruszenia bezpieczeństwa lub integralności Usług lub sieci telekomunikacyjnej NASK służącej świadczeniu Usług:
    a. podjęcia środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa i integralności Usług i sieci telekomunikacyjnej NASK służącej świadczeniu Usług oraz przekazu komunikatów w związku ze świadczonymi Usługami;
    b. informowania użytkowników o wystąpieniu szczególnego ryzyka naruszenia bezpieczeństwa sieci wymagającego podjęcia środków wykraczających poza środki techniczne i organizacyjne podjęte przez NASK, a także o istniejących możliwościach zapewnienia bezpieczeństwa;
    c. niezwłocznego informowania Prezesa UKE o naruszeniu bezpieczeństwa lub integralności Usług lub sieci telekomunikacyjnej NASK służącej świadczeniu Usług, które miało istotny wpływ na ich funkcjonowanie, o podjętych działaniach zapobiegawczych i środkach naprawczych oraz podjętych przez NASK działaniach;
    d. podjęcia proporcjonalnych i uzasadnionych środków mających na celu zapewnienie bezpieczeństwa i integralności Usług oraz sieci telekomunikacyjnej NASK służącej świadczeniu Usług oraz przekazu komunikatów związanych ze świadczonymi Usługami, w tym eliminacji przekazu komunikatu, który zagraża bezpieczeństwu Usług lub sieci telekomunikacyjnej NASK służącej świadczeniu Usług, oraz przerwania lub ograniczenia świadczenia Usług na zakończeniu sieci telekomunikacyjnej NASK służącej świadczeniu Usług, z którego następuje wysyłanie komunikatów zagrażających bezpieczeństwu Usług lub sieci telekomunikacyjnej NASK służącej świadczeniu Usług;
    e. niezwłocznego informowania Prezesa UKE o podjęciu środków mających na celu zapewnienie bezpieczeństwa i integralności Usług i sieci telekomunikacyjnej NASK służącej świadczeniu Usług oraz przekazu komunikatów związanych ze świadczonymi Usługami, jednak nie później niż w ciągu 24 godzin od ich podjęcia.

Projekt finansowany ze środków Ministra Cyfryzacji

11. Wykonawca rekomenduje Abonentowi standardowe zabezpieczenie urządzeń końcowych, dla których uruchomiona jest Usługa antyDDoS.

**§ 13**

**Poufność**

1. Wykonawca i Abonent zobowiązani są do zachowania poufności informacji uzyskanych na etapie przygotowania i realizacji Usług w okresie jej świadczenia wskazanym w Porozumieniu.
2. Wszelkie informacje, o których mowa w ust. 1, mogą być udzielane osobom trzecim tylko w przypadkach przewidzianych prawem lub za porozumieniem Abonenta i Wykonawcy.
3. Informacje dotyczące faktu zawarcia Porozumienia ze wskazaniem jego Stron oraz przedmiotu nie są poufne i mogą być wykorzystane przez Strony poprzez umieszczanie ich w materiałach marketingowych i na stronie internetowej.

**§ 14**

**Dane osobowe**

1. Wykonawca oświadcza, że świadczenie Usług nastąpi zgodnie z rozporządzeniem 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).
2. Wykonawca oświadcza, że:
    a. świadczenie Usługi anty-DDoS wiąże się z przetwarzaniem danych osobowych zawartych w Infrastrukturze Abonenta w trakcie ich przesyłu;
    b. Wykonawca nie przetwarza danych osobowych zawartych w Infrastrukturze Abonenta w trakcie ich spoczynku.
3. Zasady przetwarzania przez Wykonawcę danych osobowych zawartych w Infrastrukturze Abonenta dla celów świadczenia Usługi anty-DDoS określa odrębna umowa.

**§ 15**

**Postanowienia końcowe**

1. W sprawach nieuregulowanych postanowieniami Porozumienia, Regulaminu oraz dla ich interpretacji i wykonania mają zastosowanie przepisy prawa polskiego.
2. Porozumienie sporządzane jest w języku polskim, a w przypadku sporządzenia egzemplarza Porozumienia również w innym języku, wersją wiążącą Porozumienia jest wersja w języku polskim.
3. Abonent obowiązany jest do niezwłocznego informowania NASK o wszelkich zmianach dotyczących jego statusu prawnego oraz danych, których ujawnienie wymagane jest przy zawarciu Porozumienia. W przypadku niedopełnienia powyższego obowiązku, wszelką korespondencję oraz inne formy kontaktu skierowane przez NASK do Abonenta na dotychczasowy adres lub inne dotychczasowe dane uważa się za prawidłowo dokonane.
4. Prawidłowe świadczenie Usługi może być zależne od dopełnienia przez Abonenta warunków wynikających z ustawy KSC, w tym dotyczącej zgłoszeń incydentów do odpowiedniego CSIRT. Nie dopełnienie tych warunków może skutkować obniżeniem parametrów SLA, za co Wykonawca nie ponosi odpowiedzialności.
5. Odpowiedzialność NASK za szkody Abonenta, spowodowane brakiem możliwości skontaktowania się z Abonentem lub wyznaczoną przez niego osobą, jest wyłączona.
6. Abonent nie może przenieść praw lub obowiązków wynikających z Porozumienia na stronę trzecią bez pisemnej zgody NASK.
7. Wszelkie spory pomiędzy Stronami powinny zostać rozwiązane w drodze polubownej, a w przypadku braku możliwości rozstrzygnięcia sporu w sposób polubowny, strony poddadzą spór pod rozstrzygnięcie sądu powszechnego właściwego dla siedziby NASK.
8. Aktualna wersja Regulaminu jest publikowana na stronie internetowej NASK.
9. Załącznik do Regulaminu stanowiący jego integralną część
    1) Załącznik nr 1 - szczegółowy opis Usługi anty-DDoS;
10. Regulamin w niniejszej treści wchodzi w życie z dniem [*] 2023 roku (*z chwilą zatwierdzenia poprzez opatrzenie kwalifikowanym podpisem elektronicznym)

Projekt finansowany ze środków Ministra Cyfryzacji