**REGULAMIN**

**ŚWIADCZENIA OCHRONY**

**INFRASTRUKTURY ABONENTA PRZED ATAKAMI TYPU DDoS (Distributed Denial of Service) NA PUBLICZNIE DOSTĘPNEJ USŁUDZE TELEKOMUNIKACYJNEJ**

**dla Podmiotów realizujących zadania publiczne oraz Podmiotów istotnych z punktu widzenia bezpieczeństwa RP**

## § 1 Postanowienia wstępne

1. Niniejszy Regulamin świadczenia Ochrony Infrastruktury Abonenta przed Atakami DDoS publicznie dostępnej usługi telekomunikacyjnej dla Podmiotów realizujących zadania publiczne oraz Podmiotów istotnych z punktu widzenia bezpieczeństwa RP (dalej zwany "Regulaminem"), określa zasady świadczenia Ochrony 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 „NASK") z siedzibą w Warszawie, ul. Kolska 12, 01-045 Warszawa, wpisany 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 realizowanych przez siebie zadań.
4. Postanowienia Porozumienia oraz odrębnych regulaminów odmienne od postanowień zawartych w Regulaminie, znajdują pierwszeństwo przed postanowieniami Regulaminu.
5. NASK w ramach realizowanych zadań Ochrony 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 NASK;
    2) Ankieta techniczna – dokument stanowiący załącznik do Porozumienia, który Abonent zobowiązany jest dostarczyć NASK 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 Centrum Czyszczenia oraz Wariant ochrony anty-DDoS, który jest optymalny dla Abonenta;
    3) Aplikacje Abonenta – aplikacje internetowe Abonenta istotne z punktu widzenia zachowania ciągłości realizacji zadań publicznych lub zadań istotnych dla bezpieczeństwa RP (lub inne aplikacje internetowe Abonenta nie spełniające powyższego warunku o ile nie wykorzystują dodatkowych licencji, przy czym jedna licencja oznacza wykorzystanie jednego certyfikatu SSL powiązanego z jednym adresem IP), dostępne przez port https lub serwisy DNS wskazane w Ankiecie technicznej i objęte Ochroną anty-DDoS na mocy Porozumienia.

**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

Klasyfikacja: O (Wybrać: O, W, C, S)

4) Atak DDoS – wolumetryczny lub aplikacyjny atak typu DDoS (ang. Distributed Denial of Service) na Aplikacje Abonenta lub Infrastrukturę Sieciową Abonenta przeprowadzany w celu uniemożliwienia działania Abonenta poprzez zajęcie dostępnych zasobów lub pasma sieci internetowej;
5) Awaria - przerwa w świadczeniu Ochrony anty-DDoS lub obniżenie poziomu świadczenia Ochrony anty-DDoS w stosunku do poziomu deklarowanego przez NASK. Nie stanowi Awarii przerwa w realizacji Ochrony anty-DDoS lub obniżenie jakości Ochrony anty-DDoS związane z urządzeniami, elementami infrastruktury lub innymi zasobami należącymi do Abonenta;
6) Centrum Czyszczenia – infrastruktura służąca do czyszczenia ruchu kierowanego do Infrastruktury Abonenta z Ataków DDoS;
7) Centrum Kontaktu – wydzielona struktura NASK odpowiedzialna za bieżący kontakt z Abonentem, w tym za przyjmowanie Ankiety technicznej, przyjmowanie i obsługę Zgłoszeń Awarii i reklamacji lub informowanie o kwestiach technicznych dotyczących Ochrony anty-DDoS;
8) Czas Automatycznej Mitygacji/CAM – CAM mierzony jest dla Ochrony anty-DDoS w Wariancie I; oznacza czas pomiędzy automatycznym wykryciem Ataku DDoS, a przystąpieniem przez NASK do automatycznej Mitygacji Ataku DDoS;
9) Czas Reakcji na Atak/CRA – CRA mierzony jest dla Ochrony 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 przystąpieniem przez NASK do automatycznej Mitygacji Ataku DDoS lub 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 Ochrony anty-DDoS w Wariancie II lub Wariancie III obejmującym Infrastrukturę Sieciową Abonenta; oznacza czas pomiędzy przyjęciem przez NASK od Abonenta Zlecenia Mitygacji Ataku DDoS lub Zatwierdzenia do momentu przystąpienia przez NASK do Mitygacji Ataku DDoS;
11) Czas Zakończenia Mitygacji/CZM – CZM mierzony jest dla Ochrony 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;
14) 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;
15) Infrastruktura Sieciowa Abonenta - zbiór urządzeń oraz oprogramowania, które wchodzą w skład sieci informatycznej Abonenta, wskazane w Ankiecie technicznej i objęte Ochroną anty-DDoS na mocy Porozumienia;
16) Instruktaż – szkolenie zapewnione przez NASK na rzecz Abonenta, z zakresu Ochrony anty-DDoS oraz korzystania z Konta w Portalu Administracyjnym;
17) Konto – konto Abonenta w Portalu Administracyjnym powiązane z danym wariantem Ochrony;
18) Koordynator Ochrony Abonenta – osoba wskazana w Porozumieniu przez Abonenta, odpowiedzialna za obsługę Konta w Portalu Administracyjnym oraz nadzorowanie realizacji Ochrony po stronie Abonenta;
19) Mitygacja Ataku DDoS – działania podejmowane przez NASK, które mają na celu przekierowanie ruchu z Infrastruktury Abonenta do Centrum Czyszczenia i oczyszczenie ruchu Abonenta z Ataków DDoS;

Projekt finansowany ze środków Ministra Cyfryzacji

20) Obiekt – Aplikacje Abonenta, serwer DNS lub wskazana w ankiecie technicznej sieć/prefix, którego maska ma maksymalnie 24 bity, objęte Ochroną anty-DDoS;
21) Okno Serwisowe – okres, o którym zostanie powiadomiony Abonent, w którym mogą być wykonywane Prace Planowane;
22) Podmiot istotny z punktu widzenia bezpieczeństwa RP – podmiot wskazany do objęcia Ochroną anty-DDoS przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa;
23) 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);
24) Porozumienie – porozumienie o świadczenie Ochrony zawierane pomiędzy NASK i Abonentem w formie pisemnej, elektronicznej lub dokumentowej, w zależności od uzgodnienia pomiędzy stronami Porozumienia. Porozumienie określa m. in. okres świadczenia Ochrony dla Abonenta, Wariant Ochrony anty-DDoS oraz warunki i zasady rozwiązania Porozumienia. Porozumienie zawierane jest na czas określony;
25) Portal Administracyjny – system informatyczny udostępniony nieodpłatnie Abonentowi za pomocą środków komunikacji elektronicznej w celu realizacji Ochrony anty-DDoS;
26) Prace Planowane – prace konserwacyjne i modernizacyjne mogące skutkować przerwami w świadczeniu Ochrony;
27) Raport – wygenerowany w Koncie na Portalu Administracyjnym wykaz informacji z realizacji Ochrony anty-DDoS;
28) 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.);
29) SLA – gwarantowany poziom świadczonej Ochrony anty-DDoS;
30) Strony – NASK i Abonent;
31) Uprawniony Użytkownik – wyznaczona przez Abonenta osoba, uprawniona do obsługi Ataku DDoS po stronie Abonenta;
32) Ochrona anty-DDoS, Ochrona – nieodpłatna dla Abonenta Ochrona 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;
33) Wariant – zakres Ochrony anty-DDoS świadczonej przez NASK na rzecz Abonenta w zależności od Infrastruktury Abonenta objętej Ochroną anty-DDoS, tj. Aplikacji Abonenta lub Infrastruktury Sieciowej Abonenta;
34) Zadania – ochrona świadczona przez NASK na rzecz Abonenta na podstawie Porozumienia i Regulaminu, w szczególności Ochrona anty-DDoS; zakres zdefiniowany jest w § 3;
35) Zatwierdzenie – zatwierdzenie przez Abonenta Mitygacji Ataku DDoS, stosowane jest w Wariancie II i III Ochrony anty-DDoS w przypadku ataku DDoS dotyczącego Infrastruktury Sieciowej Abonenta;
36) Zdarzenie – każde wzmożenie ruchu w Infrastrukturze Abonenta mające cechy Ataku DDoS;
37) Zgłoszenie – dokument w formie elektronicznej, zawierający niezbędne informacje na temat Awarii;
38) Zlecenie Mitygacji – zgłoszenie Abonenta przeprowadzenia przez NASK Mitygacji Ataku DDoS; Zlecenie Mitygacji stosuje się w Wariancie II i III obejmującym Infrastrukturę Sieciową Abonenta Ochrony 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.

Projekt finansowany ze środków Ministra Cyfryzacji

## § 3 Zadania

1. NASK zobowiązany jest, pod warunkiem zawarcia Porozumienia i na zasadach w nim określonych, świadczyć nieodpłatnie na rzecz Abonenta:

   a. Ochronę anty-DDoS w jednym z Wariantów określonych w Porozumieniu;
   b. Prowadzenie Konta w Portalu Administracyjnym;
   c. Instruktaż.

2. NASK oświadcza, że:

   a. Zapewnia realizację Ochrony anty-DDoS przez podwykonawcę posiadającego aktualne poświadczenie certyfikacji ISO 27001;
   b. Ochrona anty-DDoS co do zasady jest świadczona w centrach danych znajdujących się na terenie Europejskiego Obszaru Gospodarczego;
   c. Ochrona anty-DDoS zapewnia geolokalizację adresów IP umożliwiającą blokadę ruchu przychodzącego z danego kraju bądź obszaru geograficznego;
   d. w ramach Ochrony anty-DDoS nie są zapewniane połączenia z numerami alarmowymi oraz nie są gromadzone informacje dotyczące lokalizacji telekomunikacyjnego urządzenia końcowego;
   e. Ochrona 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. Zadania mogą być wykonywane przy wykorzystaniu systemów teleinformatycznych NASK. Warunki korzystania z takich systemów teleinformatycznych mogą być uregulowane w odrębnych umowach.
4. NASK zapewnia Abonentowi dostęp do Raportów za pośrednictwem Konta w Portalu Administracyjnym. Raport zawiera w szczególności informacje na temat:

   a) Dla Wariantu I:
      i. liczby i kategorii Zdarzeń, w tym Ataków DDoS, które wystąpiły w okresie objętym Raportem;
      ii. statystyk związanych z ruchem do Aplikacji Abonenta.
   b) Dla wariantu II:
      i. statystyk związanych z ruchem do Infrastruktury Sieciowej Abonenta.
   c) Dla wariantu III:
      i. w zakresie o którym mowa w lit. a w odniesieniu do realizacji Ochrony anty-DDoS w obrębie Aplikacji Abonenta;
      ii. w zakresie o którym mowa w lit. b w odniesieniu do realizacji Ochorny anty-DDoS w obrębie Infrastruktury Sieciowej Abonenta.

## § 4 Zawarcie Porozumienia i rozpoczęcie świadczenia Ochrony anty-DDoS

1. W celu świadczenia Ochrony, Strony zawierają Porozumienie określające zasady jej świadczenia.

Projekt finansowany ze środków Ministra Cyfryzacji

2. NASK uzależnia zawarcie Porozumienia od przesłania przez Abonenta wypełnionej Ankiety technicznej, stanowiącej podstawę do kwalifikacji do objęcia Ochroną anty-DDoS oraz umożliwiającej wybór Wariantu Ochrony anty-DDoS oraz Centrum Czyszczenia.
3. Skutki złożenia przez Abonenta w Porozumieniu nieprawdziwych oświadczeń, zatajenia lub podania błędnych informacji wymaganych do zawarcia lub wykonywania Porozumienia obciążają Abonenta.
4. Ochrona 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 Ochrony anty-DDoS zgodnie z wytycznymi od NASK.

5. Termin realizacji czynności, o których mowa w ust. 4 lit. b i c powyżej, Strony określą w Porozumieniu.
6. NASK i Abonent potwierdzą uruchomienie Ochrony anty-DDoS w protokole zawierającym datę uruchomienia Ochrony anty-DDoS. NASK sporządza projekt protokołu uruchomienia Ochrony anty-DDoS i przekazuje go do Abonenta. Abonent jest zobowiązany dostarczyć NASK podpisany przez siebie protokół uruchomienia w terminie 3 Dni Roboczych od dnia przekazania mu przez NASK tego protokołu. Niedostarczenie podpisanego protokołu przez Abonenta w terminie 3 Dni Roboczych od przekazania mu protokołu uruchomienia Ochrony anty-DDoS, jest równoznaczne z podpisaniem protokołu przez Abonenta.

## § 5 Ochrona anty-DDoS

1. Ochrona 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 wnioskować o zmianę Wariantu. W takim przypadku Strony dokonują zmiany Porozumienia; § 4 Regulaminu stosuje się odpowiednio.
4. W ramach świadczenia Ochrony anty-DDoS NASK 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 NASK w wykonywaniu Ochrony;
   b. Informowania NASK o wszelkich okolicznościach mających wpływ na realizację Ochrony;
   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 NASK poprzez dostarczanie Abonentowi informacji o wykryciu Ataku DDoS. Za uruchomienie Ochrony lub Zlecenie Mitygacji odpowiada Abonent.

Projekt finansowany ze środków Ministra Cyfryzacji

6. Ochrona 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 NASK na podstawie pomiarów ruchu, a Ochrona 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; Ochrona anty-DDoS uruchamiana jest, po wykryciu Ataku DDoS przez Abonenta (na podstawie dostarczonych NASK próbek ruchu z Infrastruktury Sieciowej NASK dostarcza Abonentowi informacje o wykryciu ataku), po otrzymaniu przez NASK Zatwierdzenia; po uruchomieniu Ochrony 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. Włączenie ochrony w tym trybie może też zostać wykonane ręcznie przez Abonenta poprzez Panel Administracyjny.
      ii. w trybie automatycznym; Ochrona anty-DDoS uruchamiana jest w sposób automatyczny po wykryciu Ataku DDoS na podstawie dostarczonych NASK próbek ruchu z Infrastruktury Sieciowej Abonenta, po uruchomieniu Ochrony 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 Ochrony 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 NASK:

      i. NASK powiadamia Abonenta o Ataku DDoS;
      ii. Abonent dokonuje Zatwierdzenia, na podstawie którego NASK przeprowadza Mitygację Ataku DDoS lub samodzielnie włącza ochronę dla danego prefiksu poprzez Panel Administracyjny;
      iii. Abonent może dokonać Zlecenia Mitygacji, po samodzielnym wykryciu Ataku DDoS lub samodzielnie włączyć ochronę dla danego prefiksu poprzez Panel Administracyjny.

8. NASK zastrzega, że:

   a. nie gwarantuje oczyszczenia ruchu do 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.

Projekt finansowany ze środków Ministra Cyfryzacji

9. Abonent jest zobowiązany do poinformowania NASK z wyprzedzeniem minimum 2 tygodnie o planowanym, okresowym znacznym (powyżej 30%), zwiększeniu zapotrzebowania na zasoby Ochrony (tj. ilość chronionych aplikacji, ilość zapytań DNS, ilość zapytań do aplikacji) albo znaczącym (powyżej 30%), zwiększeniu ruchu w stosunku do wartości podanych w Porozumieniu.

**§ 6. Obsługa Zdarzeń, w tym Ataków DDoS**

1. W przypadku Zdarzenia, w szczególności podejrzenia Ataku DDoS, NASK:
   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;
   e. powiadamia Abonenta o zakończeniu Mitygacji.
2. Zdarzenia zostaną przyporządkowane przez NASK 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 NASK, 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

Projekt finansowany ze środków Ministra Cyfryzacji

zawarte w Infrastrukturze Abonenta. W takim przypadku NASK 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 NASK, 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 NASK o:

   a. Charakterze i rodzaju takiego przedsięwzięcia lub zadania;
   b. Planowanym okresie trwania takiego przedsięwzięcia lub zadania.

**§ 7. Dostęp do Konta w Portalu Administracyjnym**

1. W celu realizacji Ochrony anty-DDoS NASK zapewnia Abonentowi dostęp do Konta w Portalu Administracyjnym, na warunkach, o których mowa w ust. 6.
2. Konto w Portalu Administracyjnym umożliwia:

   a. w przypadku ochrony Aplikacji Abonenta – zarządzanie oraz monitorowanie Ochrony anty-DDoS;
   b. w przypadku ochrony Infrastruktury Sieciowej Abonenta – komunikację w zakresie realizacji Ochrony anty-DDoS;

3. W celu świadczenia Ochrony anty-DDoS w Wariancie I lub III w zakresie ochrony Aplikacji Abonenta, w przypadku zgłoszonej konieczności, możliwe będzie wgranie, poprzez Portal Administracyjny 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, NASK umożliwi, poprzez Portal Administracyjny wygenerowanie Uprawnionemu Użytkownikowi certyfikatu na potrzeby konkretnej Aplikacji Abonenta albo certyfikatu obsługującego wszystkie subdomeny Abonenta.
5. Generowanie certyfikatu w sposób wskazany w ust. 4 jest możliwe pod warunkiem przeprowadzenia przez NASK 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.
6. Zasady korzystania z Portalu Administracyjnego określają odrębne warunki właściwe dla udostępnionego Abonentowi Portalu Administracyjnego.

**§ 8. Instruktaż**

1. NASK przeprowadza Instruktaż na rzecz Uprawnionych Użytkowników.
2. Termin Instruktażu zostanie określony przez Strony.
3. Instruktaż obejmuje:

   a. Zasady działania Ochrony 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 Ochrony.

4. Nieprzystąpienie lub nieukończenie Instruktażu przez Uprawnionego Użytkownika uprawnia NASK do wstrzymania świadczenia Ochrony, bez ponoszenia z tego tytułu konsekwencji.
5. Instruktaż może być realizowany w formie wideokonferencji dla wielu podmiotów jednocześnie.

Projekt finansowany ze środków Ministra Cyfryzacji

## § 9 Zawieszenie świadczenia Ochrony

1. NASK może zawiesić świadczenie Ochrony, bez prawa Abonenta do odszkodowania, w następujących przypadkach:
   a. działania lub zaniechania Abonenta lub osoby, za której działanie lub zaniechanie Abonent ponosi odpowiedzialność, powodującego szkodę lub utrudniającego bądź uniemożliwiającego świadczenie lub korzystanie z Ochrony przez innych abonentów, NASK lub inne podmioty współpracujące z NASK (w tym działania mające na celu naruszenie bezpieczeństwa lub integralności sieci lub realizacji zadania);
   b. korzystania z Ochrony w sposób naruszający obowiązujące przepisy lub dobre obyczaje;
   c. podania przez Abonenta nieprawdziwych danych w Ankiecie technicznej, zatajenia lub podania błędnych informacji wymaganych do zawarcia lub wykonywania Zadania;
   d. nieumożliwienia lub utrudnienia NASK przez Abonenta monitorowania sposobu korzystania z Ochrony lub z Portalu Administracyjnego;
   e. naruszenia w inny sposób postanowień Regulaminu, Porozumienia lub innych warunków świadczenia Zadania.
2. Ponadto NASK ma prawo zawiesić świadczenie Ochrony 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. NASK utraci w całości lub części uprawnienia niezbędne do świadczenia Ochrony;
   c. z innych względów, w szczególności technicznych, NASK utraci możliwość świadczenia Ochrony;
   d. działania Abonenta stanowią nadużycie w komunikacji elektronicznej na podstawie art. 2 pkt 8 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. 1703 oraz z 2024 r. poz. 1222) rozumianej jako korzystanie z Ochrony telekomunikacyjnej lub korzystanie z urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, których celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu lub użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści dla podmiotu dopuszczającego się nadużycia w komunikacji elektronicznej, innej osoby fizycznej, osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej („Nadużycie w Komunikacji Elektronicznej").
3. NASK poinformuje Abonenta niezwłocznie o zawieszeniu Ochrony wraz z podaniem przyczyny zawieszenia określonej w ust. 1 lub 2.
4. Wznowienie świadczenia Ochrony następuje po ustaniu przyczyn zawieszenia.
5. W przypadku zawieszenia Ochrony na podstawie ust. 1, NASK może uzależnić wznowienie świadczenia Ochrony od pisemnego wniosku Abonenta.
6. Okresu zawieszenia świadczenia Ochrony nie uwzględnia się przy ustalaniu czasu dostępności Ochrony anty-DDoS.

## § 10 SLA

1. NASK deklaruje dostępność Ochrony anty-DDoS, rozumianej jako gotowość NASK do świadczenia Ochrony anty-DDoS, na poziomie 99% w roku świadczenia Ochrony anty-DDoS wskazanym w Porozumieniu.
2. Do czasu dostępności Ochrony anty-DDoS, o której mowa w ust. 1, nie wlicza się przerw spowodowanych Pracami Planowanymi oraz zawieszeniem Ochrony zgodnie z § 9 Regulaminu.
3. NASK będzie informować Abonenta o Pracach Planowanych prowadzonych w Oknie Serwisowym w formie pisemnej, telefonicznie lub pocztą elektroniczną z co najmniej 48-godzinnym

Projekt finansowany ze środków Ministra Cyfryzacji

wyprzedzeniem. NASK deklaruje świadczenie Ochrony 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 Ochrony anty-DDoS, bez uszczerbku dla skutków wynikających z bezwzględnie obowiązujących przepisów prawa.

4. W przypadku Wariantu I Ochrony anty-DDoS NASK deklaruje dochowanie następujących terminów:

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

5. W przypadku Wariantu II Ochrony anty-DDoS NASK 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 Ochrony anty-DDoS NASK deklaruje:
   a. dochowanie terminów określonych w ust.4 – w odniesieniu do Aplikacji Abonenta;
   b. dochowanie terminów określonych w ust. 5 – w odniesieniu do Infrastruktury Sieciowej Abonenta.
7. Celem usunięcia wątpliwości NASK potwierdza, że przyznana przez niego kategoria Zdarzenia, zgodnie z § 6 ust. 2 nie wpływa na terminy, o których mowa w ust. 4 i 5 powyżej.
8. NASK oświadcza, że wprowadził procedury mające na celu pomiar i organizację ruchu w elementach sieci telekomunikacyjnej NASK służącej świadczeniu Ochrony 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 oraz zarządzaniu transmisją danych oraz zarządzaniu infrastrukturą i urządzeniami służącymi do świadczenia Ochrony anty-DDoS. Wprowadzone przez NASK procedury mają na celu zachowanie jakości świadczonej Ochrony anty-DDoS.
9. W ramach SLA NASK zapewnia nadzór nad ciągłością i jakością świadczenia Ochrony anty-DDoS, w tym utrzymywanie ustalonych w Porozumieniu warunków technicznych Ochrony anty-DDoS, przyjmowanie Zgłoszeń oraz usuwanie Awarii. Szczegółowe warunki usuwania Awarii mogą być określone w Porozumieniu.
10. W przypadku przekroczenia przez NASK terminów wskazanych w ust. 4 i 5 Abonent zgłasza Awarię za pośrednictwem Centrum Kontaktu pod adresem addos_noc@nask.pl lub pod nr telefonu: +48 22 38 08 276
11. Abonent zobowiązany jest zgłosić Awarię do Centrum Kontaktu niezwłocznie po jej stwierdzeniu. Zgłoszenie Awarii powinno zawierać dane umożliwiające identyfikację Abonenta, wariant Ochrony 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 NASK w sprawach dotyczących usuwania Awarii powinien podawać numer Zgłoszenia.
14. NASK deklaruje usunięcie Awarii w terminie 2 Dni Roboczych od momentu Zgłoszenia.

Projekt finansowany ze środków Ministra Cyfryzacji

15. Abonent zobowiązany jest do współpracy z NASK podczas usuwania Awarii, o ile jest to niezbędne. W przypadku braku możliwości skontaktowania się z Abonentem przez co najmniej jedną godzinę, NASK może wstrzymać usuwanie Awarii. Momentem wstrzymania jest w takim przypadku godzina rozpoczęcia próby skontaktowania się z Abonentem. W takim przypadku NASK podejmuje próbę skontaktowania się z Abonentem, łącznie nie dłużej jednak niż przez 3 godziny. Jeżeli próba taka nie powiedzie się, Zgłoszenie zostaje zawieszone. Czas wstrzymania usuwania Awarii i zawieszenia Zgłoszenia nie wlicza się do czasu, o którym mowa powyżej.
16. Po usunięciu Awarii NASK 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, NASK zamyka Zgłoszenie bez potwierdzenia ze strony Abonenta.

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

1. Abonenci mogą składać NASK reklamacje dotyczące:
   a. niedotrzymania z winy NASK terminu uruchomienia Ochrony anty-DDoS, okresu świadczenia Ochrony,
   b. niewykonania lub nienależytego wykonania Ochrony, Regulaminu lub Porozumienia.
2. Celem usunięcia wątpliwości NASK potwierdza, że zgłoszenie dotyczące przekroczenia terminu wykonania Ochrony anty-DDoS realizowane jest w trybie wskazanym w § 10 SLA.
3. Abonent może złożyć reklamację w terminie 12 miesięcy od dnia, w którym zakończyła się przerwa w świadczeniu Ochrony, lub od dnia, w którym Ochrony zostały nienależycie wykonane lub miały być wykonane.
4. Reklamację złożoną po upływie terminu wskazanego w ust. 3 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 NASK 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 Ochrony – w przypadku reklamacji dotyczącej niedotrzymania z winy NASK terminu rozpoczęcia świadczenia Ochrony;
   f. sposób, w jaki ma zostać przekazana odpowiedź na reklamację;
   g. podpis Abonenta – w przypadku reklamacji złożonej w formie pisemnej.
6. W przypadku, gdy reklamacja złożona przez Abonenta ustnie albo w formie pisemnej osobiście podczas wizyty reklamującego jednostce obsługującej Abonentów nie spełnia warunków określonych w ust. 5, upoważniona osoba reprezentująca NASK, przyjmując reklamację jest obowiązana, o ile uzna, że jest to konieczne do prawidłowego rozpatrzenia reklamacji, do poinformowania Abonenta o konieczności jej niezwłocznego uzupełnienia z pouczeniem, że nieuzupełnienie reklamacji spowoduje pozostawienie reklamacji bez rozpoznania. Reklamację nieuzupełnioną pozostawia się bez rozpoznania.
7. W przypadku, gdy reklamacja złożona w inny sposób niż wskazany w ust. 6, nie spełnia warunków określonych w ust. 5, jednostka NASK rozpatrująca reklamację, o ile uzna, że jest to konieczne do

Projekt finansowany ze środków Ministra Cyfryzacji

prawidłowego rozpatrzenia reklamacji, niezwłocznie wzywa reklamującego do jej uzupełnienia, określając termin, nie krótszy niż 7 dni, i 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.

8. Reklamacja może być złożona:
   a. w formie pisemnej – osobiście podczas wizyty osoby reprezentującej Abonenta w jednostce NASK obsługującej Abonentów albo przesyłką pocztową w rozumieniu art. 3 pkt 21 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (t.j. Dz. U. z 2023 r., poz. 1640 z późn. zm.) na adres siedziby NASK-PIB, ul. Kolska 12, 01-045 Warszawa; z dopiskiem „Reklamacja ADDoS";
   b. ustnie – telefonicznie pod nr telefonu +48 22 38 08 276 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;

9. W przypadku złożenia reklamacji osobiście przez Abonenta (osobą uprawnioną do jego reprezentacji) w jednostce obsługującej Abonentów - ustnie albo w formie pisemnej, osoba przyjmująca reklamację ze strony NASK, niezwłocznie potwierdza przyjęcie reklamacji.
10. W przypadku złożenia reklamacji w formie pisemnej przesyłką pocztową, telefonicznie, albo elektronicznej wykorzystaniem środków komunikacji elektronicznej, NASK 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.
11. Potwierdzenie przyjęcia reklamacji wskazuje dzień złożenia oraz numer reklamacji, nazwę, adres i numer telefonu jednostki NASK rozpatrującej reklamację.
12. NASK jest zobowiązany do rozpatrzenia reklamacji w terminie do 30 dni od daty jej wniesienia. Jeżeli reklamacja nie zostanie rozpatrzona w terminie 30 dni od dnia jej złożenia, uważa się, że została ona uwzględniona. Przez rozpatrzenie reklamacji rozumie się wysłanie przed upływem tego terminu odpowiedzi zawierającej informacje o uwzględnieniu lub nieuwzględnieniu reklamacji wraz z uzasadnieniem.
13. Odpowiedź na reklamację zawiera:
   a. wskazanie jednostki NASK rozpatrującej reklamację;
   b. informację o dniu złożenia reklamacji;
   c. rozstrzygnięcie o uznaniu lub odmowie uznania reklamacji;
   d. dane identyfikujące upoważnionego pracownika reprezentującego NASK, z podaniem jego imienia, nazwiska oraz zajmowanego stanowiska;
   e. uzasadnienie;

14. W przypadku odmowy uznania reklamacji w całości lub części odpowiedź na reklamację:
   a. oprócz elementów wskazanych w ust. 13 lit. a – e powyżej zawiera uzasadnienie faktyczne i prawne, w szczególności w zakresie przyczyn nieuwzględnienia reklamacji;
   b. w przypadku, gdy jest udzielana na piśmie, powinna być doręczona przesyłką poleconą.

15. NASK potwierdza przyjęcie reklamacji na papierze oraz udziela odpowiedzi na reklamację zgodnie ze sposobem wskazanym przez Abonenta. Z wyjątkiem przypadków opisanych w punktach 16-17 poniżej, NASK potwierdza przyjęcie reklamacji na papierze.
16. Za zgodą Abonenta, wyrażoną w reklamacji, w Porozumieniu lub odrębnym oświadczeniu, NASK potwierdza przyjęcie reklamacji w formie elektronicznej na wskazany w tym celu adres poczty elektronicznej albo z wykorzystaniem innego, wskazanego przez Abonenta środka komunikacji elektronicznej.

Projekt finansowany ze środków Ministra Cyfryzacji

17. W przypadku złożenia reklamacji z wykorzystaniem środków komunikacji elektronicznej NASK potwierdza przyjęcie reklamacji w formie elektronicznej na wskazany w tym celu adres poczty elektronicznej albo z wykorzystaniem innego, wskazanego przez Abonenta środka komunikacji elektronicznej. Jeżeli Abonent nie wskaże adresu poczty elektronicznej albo innego środka komunikacji elektronicznej, NASK potwierdza przyjęcie reklamacji oraz udziela odpowiedzi na reklamację na adres poczty elektronicznej, z którego reklamacja została wysłana, albo z wykorzystaniem środka komunikacji elektronicznej użytego przez Abonenta do złożenia reklamacji.
18. NASK udziela odpowiedzi na reklamację zgodnie ze sposobem wskazanym przez Abonenta w reklamacji. W przypadku niewskazania przez Abonenta sposobu udzielenia odpowiedzi i nieuzupełnienia reklamacji w tym zakresie zgodnie z ust. 6 albo 7, NASK udzieli odpowiedzi na papierze, chyba że Abonent złożył reklamację za pomocą środków komunikacji elektronicznej – wówczas NASK udzieli odpowiedzi na reklamację na adres poczty elektronicznej, z którego reklamacja została wysłana, albo z wykorzystaniem środka komunikacji elektronicznej użytego przez Abonenta do złożenia reklamacji.
19. Posłużenie się innym środkiem komunikacji elektronicznej, o którym mowa w ust. 16, 17 i 18, jest dopuszczalne, jeżeli przekazane w ten sposób potwierdzenie przyjęcia reklamacji oraz odpowiedź na reklamację spełniają wymogi, o których mowa odpowiednio w ust. 11 oraz ust. 13 i ust. 14 lit. a), a postać i forma potwierdzenia przyjęcia reklamacji oraz odpowiedzi na reklamację umożliwia Abonentowi ich zapisanie, przechowywanie i odtwarzanie w zwykłym toku czynności.
20. Jeżeli wysłana przez NASK odpowiedź na reklamację nie została doręczona Abonentowi, NASK, na żądanie Abonenta wyrażone w sposób określony w ust. 8, niezwłocznie przekazuje ponownie tę odpowiedź, jej duplikat lub kopię.
21. Reklamujący, w porozumieniu z NASK, określa sposób, formę i postać w jakiej ponownie przekazywana odpowiedź na reklamację, jej duplikat lub kopia, o których mowa w ust. 20, ma zostać przekazana.
22. Na żądanie Abonenta, w przypadku odmowy uznania reklamacji w całości lub części, NASK ponownie przekazuje odpowiedź na reklamację, jej duplikat lub kopię przesyłką poleconą, bez względu na formę, w jakiej pierwotnie została wysłana odpowiedź na reklamację.
23. NASK 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.
24. Procedura zgłaszania Awarii wskazana w § 10 ust. 10 ma pierwszeństwo zastosowania względem procedury zgłoszenia reklamacji zawartej w niniejszym paragrafie, co znaczy, że powinna być stosowana w pierwszej kolejności.

## § 12 Odpowiedzialność

1. NASK ponosi odpowiedzialność z tytułu niewykonania lub nienależytego wykonania Ochrony na zasadach określonych w Porozumieniu i Regulaminie.
2. O ile nic innego nie wynika z Regulaminu lub Porozumienia NASK ponosi odpowiedzialność wyłącznie za staranne działanie i nie ponosi odpowiedzialności za rezultat, tj. skuteczność i przydatność dla Abonenta Ochrony anty-DDoS.
3. Abonent odpowiada za szkody NASK, spowodowane przez Abonenta.
4. NASK 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 Ochrony, jeśli nie jest to wynikiem działania NASK.
5. NASK nie ponosi odpowiedzialności za utratę danych Abonenta, jeśli utrata danych była spowodowana awarią urządzeń lub systemu teleinformatycznego, z których korzysta Abonent.
6. NASK nie odpowiada za szkodę wynikającą z niewykonania lub nienależytego wykonywania Ochrony, gdy ich niewykonanie lub nienależyte wykonanie jest następstwem:

Projekt finansowany ze środków Ministra Cyfryzacji

a. działania Siły Wyższej,
b. przyczyn dotyczących Abonenta lub osoby trzeciej,
c. zawieszenia świadczenia Ochrony uzgodnionego przez Abonenta i NASK lub wynikającego z Regulaminu lub Porozumienia,
d. naruszenia przez Abonenta postanowień Regulaminu lub Porozumienia;
e. zaprzestania świadczenia Ochrony, jeśli nastąpiło to z winy Abonenta lub z innych przyczyn niezależnych od NASK;
f. działania lub zaniechania Abonenta sprzecznego z przepisami powszechnie obowiązującego prawa.

7. Wyłączenie odpowiedzialności NASK na podstawie niniejszego paragrafu nie uchybia innym przesłankom wyłączenia odpowiedzialności określonym w Regulaminie, Porozumieniu lub przepisach prawa.
8. Ze względu na to, że Ochrona realizowana jest nieodpłatnie i Abonent nie jest płatnikiem opłat za realizowane zadanie Abonentowi nie przysługują żadne roszczenia odszkodowawcze z tytułu niewykonania lub nienależytego wykonania Ochrony, bez uszczerbku dla przypadków wynikających z Regulaminu i bezwzględnie obowiązujących przepisów prawa.
9. NASK przekazuje Abonentowi informacje o zagrożeniach związanych ze realizowaną Ochroną 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 Ochrony lub sieci telekomunikacyjnej NASK służącej świadczeniu Ochrony:

    a. podjęcia środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa i integralności Ochrony i sieci telekomunikacyjnej NASK służącej świadczeniu Ochrony oraz przekazu komunikatów w związku ze świadczoną Ochroną;
    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 realizowanego Zadania lub sieci telekomunikacyjnej NASK służącej świadczeniu Ochrony, 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 realizowanego Zadania oraz sieci telekomunikacyjnej NASK służącej świadczeniu Ochrony oraz przekazu komunikatów związanych z realizowanymi Zadaniami, w tym eliminacji przekazu komunikatu, który zagraża bezpieczeństwu Ochrony lub sieci telekomunikacyjnej NASK służącej świadczeniu Ochrony, oraz przerwania lub ograniczenia świadczenia Ochrony na zakończeniu sieci telekomunikacyjnej NASK służącej świadczeniu Ochrony, z którego następuje wysyłanie komunikatów zagrażających bezpieczeństwu Ochrony lub sieci telekomunikacyjnej NASK służącej świadczeniu Ochrony;
    e. niezwłocznego informowania Prezesa UKE o podjęciu środków mających na celu zapewnienie bezpieczeństwa i integralności Ochrony i sieci telekomunikacyjnej NASK służącej świadczeniu Ochrony oraz przekazu komunikatów związanych ze świadczoną Ochroną, jednak nie później niż w ciągu 24 godzin od ich podjęcia.

11. NASK rekomenduje Abonentowi standardowe zabezpieczenie urządzeń końcowych, dla których uruchomiona jest Ochrona anty-DDoS.

Projekt finansowany ze środków Ministra Cyfryzacji

## § 13 Poufność

1. NASK i Abonent zobowiązani są do zachowania poufności informacji uzyskanych na etapie przygotowania i realizacji Ochrony 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 NASK.
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. Abonent może udzielić na rzecz NASK referencji dotyczących Ochrony objętych Porozumieniem.

## § 14 Dane osobowe

1. NASK oświadcza, że świadczenie Ochrony 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. NASK oświadcza, że:
   a. świadczenie Ochrony anty-DDoS wiąże się z przetwarzaniem danych osobowych zawartych w Infrastrukturze Abonenta w trakcie ich przesyłu;
   b. NASK nie przetwarza danych osobowych zawartych w Infrastrukturze Abonenta w trakcie ich spoczynku.
3. Zasady przetwarzania przez NASK danych osobowych zawartych w Infrastrukturze Abonenta dla celów świadczenia Ochrony 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. Prawidłowa realizacja Ochrony może być zależna od dopełnienia przez Abonenta warunków wynikających z ustawy KSC, w tym dotyczącej zgłoszeń incydentów do odpowiedniego CSIRT. Niedopełnienie tych warunków może skutkować obniżeniem parametrów SLA, za co NASK 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. Regulamin w niniejszej treści wchodzi w życie od dnia 01.03.2026 roku.

Projekt finansowany ze środków Ministra Cyfryzacji