

RFC 2350 – NonStop SOC sp. z o.o.

1. Informacje o niniejszym dokumencie

Niniejszy dokument zawiera opis NonStop SOC zgodnie z RFC 2350 („Oczekiwania dotyczące reagowania na incydenty związane z bezpieczeństwem komputerowym”).

Niniejszy dokument jest przeznaczony dla klientów, partnerów biznesowych oraz współpracujących zespołów ds. cyberbezpieczeństwa działających w ramach polskiego i europejskiego systemu cyberbezpieczeństwa.

Dokument zawiera zwięzły opis zakresu usług, zasad działania oraz kanałów komunikacji NonStop SOC jako komercyjnego Security Operations Center (SOC).

1.1 Data ostatniej aktualizacji

Wersja 1.0, opublikowana 7 października 2026 r.

1.2 Dystrybucja powiadomień

Powiadomienia o aktualizacjach niniejszego dokumentu mogą być przekazywane:

- wybranych klientów i partnerów oraz
- odpowiedniemu krajowemu organowi ds. cyberbezpieczeństwa
- opublikowane na stronie internetowej firmy.

1.3 Publikacja dokumentu

Aktualna wersja jest dostępna pod adresem:

<https://www.nonstopsoc.com.pl/nonstop-soc-rfc-2350/>

1.4 Uwierzytelnienie niniejszego dokumentu

Niniejszy dokument został podpisany cyfrowo przy użyciu klucza PGP. Odpowiedni klucz publiczny i powiązana suma kontrolna zostały opisane w sekcji 2.8.

2. Dane kontaktowe

2.1 Nazwa zespołu

NonStop SOC

2.2 Adres

NonStop SOC Sp. z o.o.
ul. Jutrzenki 116
02-230 Warszawa
Polska

2.3 Strefa czasowa

Czas środkowoeuropejski (CET) – UTC+1

Centrum-europejski czas letni (CEST) – UTC+2 zgodnie z przepisami UE
(od ostatniej niedzieli marca do ostatniej niedzieli października)

2.4 Numer telefonu

+48 22 570 13 91

2.5 Numer faksu

Brak faksu

2.6 Inne środki komunikacji

W zależności od ustaleń umownych NonStop SOC korzysta również z bezpiecznej komunikacji z klientami za pośrednictwem dedykowanego portalu klienta oraz bezpiecznych komunikatorów.

2.7 Adres e-mail

incydent@nonstopsoc.com.pl

2.8 Klucze publiczne i inne informacje dotyczące szyfrowania

NonStop SOC wykorzystuje OpenPGP w celu ochrony poufności i integralności wrażliwej korespondencji.

User ID: NonStop SOC incydent@nonstopsoc.com.pl

Key ID: C3FBDADBB02D48D3

Key type: RSA

Key size: 4096 bits

Expires: 2036-10-02

Fingerprint: 0E37 E858 3B56 6031 A341 D8B5 C3FB DADB B02D 48D3

Klucz jest dostępny pod adresem:

<https://www.nonstopsoc.com.pl/nonstop-soc-rfc-2350/>

Plik podpisu dokumentu: <https://www.nonstopsoc.com.pl/nonstop-soc-rfc-2350/>

2.9 Informacje dodatkowe

Ogólne informacje na temat NonStop SOC są dostępne pod adresem:
<https://nonstopsoc.com.pl>

2.10 Punkty kontaktowe dla klientów

Incydenty związane z bezpieczeństwem można zgłaszać za pomocą poczty elektronicznej na adres incydent@nonstopsoc.com.pl oraz za pośrednictwem portalu klienta udostępnionego klientom po podpisaniu umowy o świadczenie usług SOC.

W przypadku kontaktu poprzez e-mail zachęcamy do korzystania z szyfrowania z użyciem klucza PGP w celu zapewnienia integralności i poufności.

Kontakt ogólny lub zapytania można inicjować za pomocą formularza kontaktowego na stronie <https://www.nonstopsoc.com.pl/kontakt/>

Godziny pracy: NonStop SOC działa 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku (tryb 24x7)

3. Statut

3.1 Misja

Misją NonStop SOC jest ochrona systemów informatycznych i infrastruktury IT klientów poprzez ciągłe monitorowanie, szybką reakcję na incydenty oraz proaktywne zarządzanie zagrożeniami.

NonStop SOC świadczy wysokiej jakości usługi zarządzane w zakresie cyberbezpieczeństwa, wspierane przez doświadczonych specjalistów oraz zaawansowane technologie i platformy służące do gromadzenia i przetwarzania informacji o zagrożeniach.

3.2 Obszar działania

Baza klientów NonStop SOC obejmuje organizacje prywatne, publiczne, które zawarły umowy na świadczenie zarządzanych usług w zakresie cyberbezpieczeństwa (SOC).

Obejmuje to podmioty podlegające wymogom regulacyjnym wynikającym z:

- polskiej ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC),
- dyrektywy NIS2,
- przepisów branżowych dotyczących cyberbezpieczeństwa i ryzyka związanego z technologiami informacyjno-komunikacyjnymi (ICT),
- w przypadku klientów z sektora finansowego – ustawy o cyfrowej odporności operacyjnej (rozporządzenie (UE) 2022/2554 – DORA).

Obsługiwane przez nas organizacje działają w takich sektorach, jak produkcja, dystrybucja i transport, infrastruktura krytyczna, finanse, sektor publiczny – w tym opieka zdrowotna oraz telekomunikacja.

3.3 Powiązania organizacyjne

NonStop SOC sp. z o.o. jest wyspecjalizowanym podmiotem zajmującym się cyberbezpieczeństwem, działającym w ramach Grupy COMP.

3.4 Uprawnienia

NonStop SOC działa w imieniu swoich klientów w zakresie określonym w umowach oraz zgodnie z obowiązującym prawem.

NonStop SOC nie wykonuje żadnych uprawnień regulacyjnych, nadzorczych ani organów ścigania.

4. Zasady

4.1 Rodzaje incydentów i poziomy wsparcia

NonStop SOC zajmuje się incydentami związanymi z cyberbezpieczeństwem mającymi wpływ na środowiska klientów, w tym między innymi:

- infekcje złośliwym oprogramowaniem,
- nieuprawniony dostęp i włamania,
- phishing i inżynieria społeczna,
- ataki typu „odmowa usługi”,
- naruszenia bezpieczeństwa danych,
- naruszenia zasad bezpieczeństwa.

Priorytetyzacja incydentów, czasy reakcji oraz zasady eskalacji są określone w umowie o świadczenie usług zarządzanych SOC. W przypadku braku konkretnych postanowień umownych incydenty są rozpatrywane zgodnie ze standardowymi poziomami priorytetów.

4.2 Współpraca, interakcja i udostępnianie informacji

Wszelkie informacje dotyczące incydentów obsługiwanych przez NonStop SOC są traktowane jako poufne. Informacje są przekazywane za pośrednictwem bezpiecznych protokołów, w tym TLP.

Informacje mogą być udostępniane zaufanym podmiotom zewnętrznym (takim jak dostawcy technologii, operatorzy telekomunikacyjni lub zespoły CSIRT) wyłącznie w zakresie niezbędnym do wykonania zadania i wyłącznie w celu obsługi incyduentu lub złagodzenia jego skutków.

NonStop SOC nie powiadamia organów ścigania o incydentach, chyba że wyraźnie wymaga tego obowiązujące prawo. Współpraca z takimi organami odbywa się wyłącznie w ramach formalnych postępowań lub na wyraźną prośbę klienta, którego dotyczy incydent.

4.3 Komunikacja i uwierzytelnianie

NonStop wykorzystuje szyfrowanie GPG w celu ochrony poufności i integralności komunikacji. Wszelkie przekazywane dane wrażliwe powinny zostać odpowiednio zaszyfrowane przed przesłaniem.

Wiadomości dotyczące incydentów wysyłane przez personel NonStop SOC są podpisywane cyfrowo przy użyciu głównego klucza GPG organizacji (patrz sekcja 2.8) oraz szyfrowane, o ile zawierają treści wrażliwe lub poufne.

Zespół zastrzega sobie prawo do weryfikacji autentyczności i pochodzenia wszelkich otrzymanych informacji w zakresie dozwolonym przez obowiązujące przepisy prawa.

4.4 Ochrona danych osobowych (RODO)

NonStop SOC przetwarza dane osobowe wyłącznie w zakresie niezbędnym do świadczenia usług SOC oraz zgodnie z rozporządzeniem (UE) 2016/679 (RODO).

O ile w umowie nie określono inaczej, NonStop SOC pełni rolę podmiotu przetwarzającego dane w imieniu klienta, który jest administratorem danych.

Stosowane są zasady minimalizacji danych, ograniczonych okresów przechowywania oraz odpowiednich środków bezpieczeństwa. Szczegółowe warunki są określone w każdej umowie o przetwarzaniu danych (DPA).

5. Usługi

5.1 Reagowanie na incydenty

NonStop SOC wspiera organizacje w radzeniu sobie zarówno z technicznymi, jak i organizacyjnymi aspektami incydentów związanych z cyberbezpieczeństwem. Zakres usług obejmuje cały cykl reagowania na incydenty:

- Przygotowanie
- Wykrywanie i analiza
- Ograniczanie, eliminacja i przywracanie
- Analiza po incydencie i zalecenia

- Wsparcie regulacyjne (na żądanie) – dostarczanie danych faktycznych wymaganych przez klientów do ustawowych zgłoszeń incydentów (np. KSC, NIS2, DORA, RODO)

5.2 Działania proaktywne

NonStop SOC zwiększa odporność klientów dzięki proaktywnym usługom bezpieczeństwa, w tym:

- Monitorowanie bezpieczeństwa 24/7 (SOC)
- Koordynacja i automatyzacja bezpieczeństwa (SOAR) – automatyzacja działań reagowania w celu skrócenia średniego czasu reakcji
- Analiza zagrożeń i wykrywanie zagrożeń
- Testy penetracyjne i audyty bezpieczeństwa
- Zarządzanie lukami w zabezpieczeniach – terminowe powiadomienia o zagrożeniach istotnych dla środowisk klientów
- Szkolenia i doradztwo
- Wsparcie w zakresie zgodności z przepisami (KSC, NIS2, DORA, RODO)

6. Formularze zgłaszania incydentów

Nie jest wymagany żaden specjalny formularz zgłaszania incydentów.

Zachęcamy klientów do zgłaszania incydentów za pośrednictwem szyfrowanej poczty elektronicznej lub portalu klienta w przypadku podmiotów, które podpisały umowy na usługi zarządzane SOC.

7. Zastrzeżenia

NonStop SOC dokłada wszelkich starań, aby zapewnić dokładność i jakość dostarczanych informacji.

NonStop SOC nie ponosi odpowiedzialności za jakiegokolwiek błędy, pominięcia lub konsekwencje wynikające z wykorzystania informacji zawartych w niniejszym dokumencie.

8. Podpis PGP i weryfikacja autentyczności

Dokument NonStop SOC RFC2350 jest podpisany cyfrowo przy użyciu PGP.

Klucz publiczny PGP: <https://www.nonstopsoc.com.pl/nonstop-soc-rfc-2350/>

Odcisk klucza: 0E37 E858 3B56 6031 A341 D8B5 C3FB DADB B02D 48D3

Autentyczność dokumentu można zweryfikować za pomocą standardowych narzędzi Pong (np. GnuPG).