

RFC 2350 – NonStop SOC sp. z o.o.

1. About this Document

This document contains a description of the NonStop SOC in accordance with RFC 2350 ("Expectations for Computer Security Incident Response").

This document is intended for customers, business partners and cooperating cybersecurity teams operating within the Polish and European cybersecurity framework.

It provides a clear and transparent description of the scope of services, operational principles, and communication channels of NonStop SOC as a commercial Security Operations Center.

1.1 Date of Last Update

Version 1.0, published on October 7, 2026

1.2 Distribution List for Notifications

Updates notifications to this document may be provided to:

- selected clients and partners and
- appropriate national cyber security entity
- published on the company website.

1.3 Locations Where this Document May Be Found

The current version is available at:

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

1.4 Authenticating this Document

This document has been signed digitally using a PGP key. The corresponding public key and related checksum is described in section 2.8.

2. Contact Information

2.1 Name of the Team

NonStop SOC

2.2 Address

NonStop SOC Sp. z o.o.

116 Jutrzenki Str.

02-230 Warsaw

Poland

2.3 Time Zone

Central European Time (CET) - UTC+1

Central European Summer Time (CEST) - UTC+2 according to EU regulations

2.4 Telephone Number

+48 22 570 13 91

2.5 Facsimile Number

No fax available

2.6 Other Telecommunications

Depending on contractual arrangements, NonStop SOC also uses secure communication with customers via a dedicated customer portal and secure communicators.

2.7 Electronic Mail Address

incydent@nonstopsoc.com.pl

2.8 Public Keys and Other Encryption Information

NonStop SOC uses OpenPGP to protect the confidentiality and integrity of sensitive communications.

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

Key is available at: <https://www.nonstopsoc.com.pl/en/nonstop-soc-rfc-2350/>

Document signature file: <https://www.nonstopsoc.com.pl/en/nonstop-soc-rfc-2350/>

2.9 Other Information

General information about NonStop SOC is available at:
<https://www.nonstopsoc.com.pl/en/homepage-en/>

2.10 Points of Customer Contact

Security incidents may be reported using the e-mail at incydent@nonstopsoc.com.pl and via customer portal provided to contractual customers.

In the case of contact via e-mail, we encourage you to use PGP encryption to ensure integrity and confidentiality.

Initial contact with NonStop SOC may be initiated using contact form available at: <https://www.nonstopsoc.com.pl/en/contact/>

Operating hours: NonStop SOC operates 24 hours a day, 7 days a week, 365 days a year (24x7 mode)

3. Charter

3.1 Mission Statement

NonStop SOC's mission is to protect clients' information systems and IT infrastructure through continuous monitoring, rapid incident response and proactive threat management.

NonStop SOC provides high-quality managed cybersecurity services, supported by experienced specialists, advanced technologies and platforms that collect and process information on threats.

3.2 Constituency

NonStop SOC's client base comprises private, public organisations that have entered into contracts for the provision of managed cybersecurity services (SOC).

This includes entities subject to regulatory requirements arising from:

- the Polish Act on the National Cybersecurity System (KSC),
- the NIS2 Directive,
- sector-specific regulations concerning cybersecurity and risks associated with information and communications technology (ICT),
- in the case of clients from the financial sector – the Act on Digital Operational Resilience (Regulation (EU) 2022/2554 – DORA).

The organisations we serve operate in sectors such as manufacturing, distribution and transport, critical infrastructure, finance, public sector – including healthcare – and telecommunications.

3.3 Sponsoring Organization / Affiliation

NonStop SOC sp. z o.o. is a specialized cybersecurity entity that operates as part of the COMP Group.

3.4 Authority

NonStop SOC acts on behalf of its clients within the scope specified in the contracts and in accordance with applicable law.

NonStop SOC does not exercise any regulatory, supervisory or law enforcement powers.

4. Policies

4.1 Types of Incidents and Levels of Support

NonStop SOC handles cybersecurity incidents affecting customers' environments, including, amongst others:

- malware infections,
- unauthorised access and intrusions,
- phishing and social engineering,
- denial-of-service attacks,
- data breaches,
- security policy breaches.

Incident prioritisation, response times and escalation policies are set out in the SOC managed services agreement. In the absence of specific contractual provisions, incidents are handled according to standard priority levels.

4.2 Cooperation, Interaction, and Disclosure of Information

All information relating to incidents handled by NonStop SOC is treated as confidential. Information is shared via secure protocols, including TLP.

Information may be shared with trusted third parties (such as technology providers, telecoms operators or CSIRT teams) only to the extent necessary to carry out the task and solely for the purpose of handling the incident or mitigating its impact.

NonStop SOC does not notify law enforcement authorities of incidents unless explicitly required by applicable law. Cooperation with such agencies takes place only within the scope of formal proceedings or at the express request of the affected client.

4.3 Communication and Authentication

NonStop utilizes GPG encryption to protect the confidentiality and integrity of communications. Any sensitive data submitted should be properly encrypted before transmission.

Incident-related messages from NonStop SOC personnel are digitally signed using the organization's primary GPG key (refer to section

2.8), and are encrypted whenever they include sensitive or confidential content.

The team retains the right to validate the authenticity and origin of any received information, within the scope permitted by applicable laws.

4.4 Data Protection (GDPR)

NonStop SOC processes personal data only to the extent necessary to provide SOC services and in accordance with Regulation (EU) 2016/679 (GDPR).

Unless otherwise specified in the contract, NonStop SOC acts as a data processor on behalf of the client, who is the data controller.

The principles of data minimisation, limited retention periods and appropriate security measures are applied. The detailed terms and conditions are set out in each Data Processing Agreement (DPA).

5. Services

5.1 Incident Response

NonStop SOC supports organisations in handling both the technical and organisational aspects of cybersecurity incidents. Capabilities cover the full incident response lifecycle:

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-Incident Analysis and Recommendations
- Regulatory support (on request) – provision of factual data required by customers for statutory incident notifications (e.g. KSC, NIS2, DORA, GDPR)

5.2 Proactive Activities

NonStop SOC enhances customer resilience through proactive security services, including:

- 24/7 Security Monitoring (SOC)
- Security Orchestration and Automation (SOAR) – automation of response actions to reduce mean time to respond
- Threat Intelligence and Threat Hunting
- Penetration Testing and Security Audits

- Vulnerability management - timely alerts on threats relevant to customer environments
- Training and Consultancy
- Compliance enablement (KSC, NIS2, DORA, GDPR)

6. Incident Reporting Forms

No special incident reporting form is required.

We encourage customers to report incidents via encrypted email or through the customer portal for those who have signed contracts for SOC-managed services.

7. Disclaimers

NonStop SOC makes every effort to ensure the accuracy and quality of the information provided.

NonStop SOC accepts no liability for any errors, omissions or consequences arising from the use of the information contained in this document.

8. PGP Signature and Authenticity Verification

The NonStop SOC RFC2350 document is digitally signed using PGP.

Public PGP key: <https://www.nonstopsoc.com.pl/en/nonstop-soc-rfc-2350/>

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

Document authenticity can be verified using standard OpenPGP tools (e.g., GnuPG).