SIRT / SOC Description for SOC24.PL

[TLP:CLEAR]

1. About this Document

This document describes SOC24.PL in accordance with RFC 2350 ("Expectations for Computer Security Incident Response").

It is intended for customers, business partners, and cooperating security teams operating within the Polish and European cybersecurity
ecosystem.

The purpose of this document is to provide a clear and transparent description of the scope of services, operational principles, and communication channels of SOC24.PL as a commercial Security Operations Center.

1.1 Date of Last Update

Version 4.00 – published on 19 March 2026

1.2 Distribution List for Notifications

Information about updates to this document may be provided to:
- Trusted Introducer (ti@trusted-introducer.org)
- Selected customers and partners via contractual communication channels

1.3 Locations where this Document May Be Found

The current and authoritative version of this document is available at:
https://www.nomios.pl/soc24-rfc-2350

1.4 Authenticating this Document

This document is digitally signed using the SOC24.PL PGP key.
The corresponding public key is described in section 2.8.

2. Contact Information

2.1 Name of the Team

SOC24.PL

2.2 Address

NOMIOS Poland Sp. z o.o.
ul. Puławska 537
02-844 Warsaw
Poland

2.3 Time Zone

Central European Time (CET, UTC+1)
Central European Summer Time (CEST, UTC+2)

2.4 Telephone Number
+48 22 460 07 85

2.5 Facsimile Number
Not applicable

2.6 Other Telecommunication
Depending on contractual arrangements, SOC24.PL also uses secure communication with customers via a dedicated customer portal and Microsoft Teams.

2.7 Electronic Mail Address
Primary operational contact:
soc@soc24.pl

2.8 Public Keys and Other Encryption Information
SOC24.PL uses OpenPGP to protect the confidentiality and integrity of sensitive communications.

User ID: SOC24 <soc@soc24.pl>
Key ID: 6D5056E6
Key type: EdDSA (25519)
Fingerprint:
4073 F86E 09CF 0D09 A49C D271 1993 1641 6D50 56E6
Expiration date: 27 December 2026

The public key is available at:
https://www.nomios.pl/soc24-publicpgpkey

2.9 Other Information
General information about SOC24.PL and its services is available at:
https://www.nomios.pl/soc24

2.10 Points of Customer Contact
SOC24.PL accepts incident reports via e-mail at soc@soc24.pl and via the customer portal provided to contracted customers.
Initial contact with SOC24.PL may be initiated via the contact form available at: https://www.nomios.pl/kontakt/.

SOC24.PL operates 24 hours a day, 7 days a week, 365 days a year (24/7/365).

3. Charter

3.1 Mission Statement
The mission of SOC24.PL is to protect constituent environments through
continuous monitoring, rapid incident response, and proactive threat management.

SOC24.PL delivers high-quality cybersecurity operations supported by experienced specialists, advanced automation, and actionable threat intelligence.

3.2 Constituency
The constituency of SOC24.PL consists of private, public, and governmental organisations that have contracted SOC24.PL Security Operations Center services.

This includes entities subject to regulatory requirements under:
- the Polish Act on the National Cybersecurity System (KSC),
- the NIS2 Directive,
- sector-specific cybersecurity and ICT risk regulations,
- and, for financial-sector customers, the Digital Operational Resilience Act (Regulation (EU) 2022/2554 – DORA).

Organisations served operate across sectors such as finance, insurance, telecommunications, and critical infrastructure.

3.3 Sponsorship and Affiliation
SOC24.PL operates as part of NOMIOS Poland Sp. z o.o. and the Nomios Group.

3.4 Authority
SOC24.PL acts on behalf of its customers within the scope defined by contractual agreements and applicable law.
SOC24.PL does not exercise regulatory, supervisory, or law-enforcement
authority.

4. Policies

4.1 Types of Incidents and Level of Support
SOC24.PL handles cybersecurity incidents affecting customer environments, including, but not limited to:
- malware infections,
- unauthorised access and intrusions,
- phishing and social engineering,
- denial-of-service attacks,
- data breaches,
- violations of security policies.

Incident prioritisation, response time, and escalation rules are defined contractually. In the absence of specific contractual provisions, incidents are handled with standard priority.

4.2 Cooperation, Interaction and Disclosure of Information
All incident-related information handled by SOC24.PL is treated as confidential.

Information sharing follows the Traffic Light Protocol (TLP).
Information may be shared with trusted third parties (such as vendors,
telecommunications providers, or other CSIRTs) strictly on a need-to-know basis and solely for the purpose of incident handling or mitigation.

SOC24.PL does not notify law enforcement authorities unless:
- required by applicable law, or
- explicitly requested or authorised by the customer.

4.3 Communication and Authentication
OpenPGP is used to protect the confidentiality and integrity of sensitive communications.

Customers are encouraged to encrypt incident-related information. SOC24.PL reserves the right to verify the authenticity of information
and its source, within the limits permitted by law.

4.4 Data Protection (GDPR)
SOC24.PL processes personal data only as necessary for the provision of SOC/CSIRT services and in accordance with Regulation (EU) 2016/679 (GDPR).
Unless otherwise contractually defined, SOC24.PL acts as a data processor on behalf of the customer as data controller.
Data minimisation, limited retention, and appropriate safeguards apply. Detailed terms are defined in the applicable contract and/or Data Processing Agreement (DPA).

5. Services

5.1 Incident Response
SOC24.PL supports organisations in handling both the technical and organisational aspects of cybersecurity incidents.

Capabilities cover the full incident response lifecycle:
- Preparation – playbook development, runbook maintenance, SOAR automation
- Detection and Analysis – continuous monitoring, alert triage, threat correlation
- Containment, Eradication and Recovery – automated and manual response
  actions, coordination with customer teams
- Post-Incident – lessons learned, evidence analysis, recommendations,
  and reporting
- 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
SOC24.PL enhances customer resilience through proactive security services, including:
- Threat Intelligence – production and delivery of tactical, operational, and strategic intelligence
- Detection Engineering – development and tuning of detection rules and correlation logic

- Threat Hunting – hypothesis-driven investigations of previously
  undetected threats
- Security Orchestration and Automation (SOAR) – automation of
response
  actions to reduce mean time to respond
- Vulnerability and Advisory Notifications – timely alerts on
threats
  relevant to customer environments
- Compliance enablement (KSC, NIS2, DORA, GDPR) – advisory and
technical
  support for aligning detections, retention, and audit trails with
  regulatory expectations, without assuming regulatory roles

6. Incident Reporting

No dedicated incident reporting form is required.
Customers are encouraged to report incidents via encrypted e-mail or the customer portal.

7. Disclaimer

SOC24.PL makes reasonable efforts to ensure the accuracy and quality of
information provided.
SOC24.PL assumes no liability for errors, omissions, or consequences arising from the use of information contained in this document.

8. PGP Signature and Authenticity Verification

The SOC24.PL RFC2350 document is digitally signed using PGP.
Public PGP key:
https://www.nomios.pl/soc24-publicpgpkey
Key fingerprint:
4073 F86E 09CF 0D09 A49C D271 1993 1641 6D50 56E6
Document authenticity can be verified using standard OpenPGP tools (e.g., GnuPG).