netia.pl t +48 22 352 20 00 Netia SA, 464 Puławska St.
f +48 22 330 23 23 02-884 Warsaw

RFC 2350

Version: 1.0

9 June 2022

TLP:WHITE | PUBLIC

TLP:WHITE information can be freely distributed.

NETIA SOC

1 About the document

This document contains information about the Netia SOC Computer Security Incident Response Team (CSIRT) in a format compliant with RFC 2350.

1.1 Last update date

Version: 1.0 of 9 June 2022.

1.2 Notification distribution list

Not applicable

1.3 Locations where you can find this document

The current version of the document is published at:

https://www.netia.pl/pl/csirt/rfc - Polish language version,

https://www.netia.pl/en/csirt/rfc - English language version

1.4 Authentication of this document

The document was signed with a PGP key belonging to Netia SOC. The signature can be found at:

https://www.netia.pl/en/csirt/rfc

2 Contact information

2.1 Team name

Netia SOC

2.2 Address

Netia S.A.
Netia SOC
13 Poleczki St.
02-822 Warsaw
Poland

2.3 Time zone

Central European Time UTC+1

Central European Summer Time UTC+2 (from the last Sunday in March to the last Sunday in October)

2.4 Telephone number

+48 22 352 25 55

2.5 Fax number

Unavailable.

2.6 Other communication

Unavailable.

2.7 Email address

Notifications, incident reports and operational issues should be sent to csirt@netia.pl

Questions regarding the offer, the scope of services provided and business issues should be sent to biznes@netia.pl

2.8 Public keys and other encryption information

In order to protect sensitive information, we use PGP encryption.

```
Email: csirt@netia.pl
```

```
Key fingerprint: 2777 F603 4CCF 1596 A22A FBFF DE20 21B7 2A76 31D1
```

The public key is published at https://www.netia.pl/en/csirt/rfc

2.9 Team members

The Netia SOC team consists of people strongly involved in the idea of promoting awareness in the area of cybersecurity. We constantly monitor activity in the digital space, observe the market of ICT security solutions and technologies, and improve competences.

2.10 Other information

Additional information can be found at https://www.netia.pl/en/csirt/rfc

2.11 Customer Contact Points

The preferred method of contacting Netia SOC is email. We recommend using PGP to ensure integrity and confidentiality.

Standard ticket processing hours are 9:00 am – 5:00 pm Monday through Friday excluding holidays. However, the Netia SOC team works around the clock and in urgent matters it is possible to contact us outside the above indicated hours.

3 Statute

3.1 Mission

The mission of Netia SOC is to support both entities from the Netia Group and Netia business customers in responding to and handling computer security incidents.

Netia SOC provides cybersecurity services to private customers and public entities.

3.2 Area of activity

The area of Netia SOC's activity includes the following Netia Group companies:

- Netia S.A.
- TK Telekom Sp. z o.o.

and customers from the private and public sectors, with whom Netia S.A. has concluded an agreement in the field of support in responding to computer security incidents.

3.3 Sponsorship and affiliation

Netia SOC operates within Netia S.A.

3.4 Authorization

Netia SOC operates under the auspices and authorization of the management of Netia S.A.

In addition, Netia SOC operates on the basis of agreements with business customers of Netia S.A. and on the terms resulting therefrom.

4 Policies

4.1 Incident types and level of support

The default priority for all reported incidents is normal priority. A different classification may apply on the basis of the provisions of agreements. The possible change of priority is decided by the Netia SOC team.

4.2 Collaboration, interaction and disclosure of information

All incident handling information is treated as confidential. When reporting incidents and providing confidential information, we recommend using PGP encryption or possibly establishing another secure communication channel with Netia SOC.

Netia SOC declares full support for Information Sharing Traffic Light Protocol (FIRST TLP v1.0, https://www.trusted-introducer.org/ISTLP.pdf). Information sent and marked in accordance with the ISTLP will be processed in an appropriate manner.

The information provided to Netia SOC may be forwarded to interested parties, such as other CSIRTs/CERTs, owners or administrators of the resources affected by the incident, on a “necessary knowledge” basis, exclusion for incident handling (to the extent necessary to identify and mitigate the threat).

Netia SOC does not independently report incidents to law enforcement agencies, unless it results from legal provisions. However, in the case of proceedings conducted by authorized authorities, we may provide information at their request.

4.3 Communication and authentication

Netia SOC secures sensitive information in accordance with relevant legal provisions and internal rules.

In particular, we respect the confidentiality flags defined by the authors of the information provided to Netia SOC.

For low-sensitivity information, it is possible to contact Netia SOC via unencrypted email or by phone, but in order to ensure the confidentiality and integrity of the communication, we recommend using PGP/GPG (see section 2.8). All sensitive information that is transmitted should be encrypted.

In order to verify the authenticity of the information received or its source, or to authenticate the contact person, it is possible to use publicly available sources of information such as the WHOIS database, social networking sites or registers. In justified cases, this can be done through a telephone confirmation or a meeting.

5 Services

Netia offers its customer, among others, Security Operations Center (SOC), services in the as-a-service model, including incident response services. In addition, we provide a number of professional services in the area of cybersecurity. Detailed information can be found at https://www.netia.pl/en/csirt/rfc

5.1 Incident response

- analysis of events in SIEM systems
- analysis and qualification of suspected incidents
- incident handling
- vulnerability handling
- IoC (Indication of Compromise) analysis

5.2 Proactive activities

- support in creating a security development strategy
- implementation of security solutions
- maintenance and development of security solutions
- warnings about new vulnerabilities and threats
- susceptibility tests
- building security awareness

6 Incident reporting forms

Incidents should be reported via email sent to csirt@netia.pl, preferably encrypted with our public PGP key.

When contacting Netia SOC, please provide the following information:

1. Contact and organizational information — person's name, organization name and address, email address, phone number,
2. Type and brief summary of the incident/event,
3. Event/incident source – in which system it was observed, public source and destination IP addresses, etc.,
4. Affected entities or systems,
5. Estimated impact, e.g., loss of availability of services),
6. Additional information and observations that led to the detection of the incident — scan results (if any), log extract showing the problem, etc.

If you forward a suspicious email, please make sure that all headers, content and attachments are included.

7 Reservations

Although we take every precaution to prepare information, notifications and warnings, Netia SOC is not responsible for errors or omissions, nor for damages resulting from the use of the information contained therein.