RFC 2350

1. Document information 2
   1.1 Date last updated 2
   1.2 Document location 2
   1.3 Reliability of the document 2
2. Contact information 2
   2.1 Team name 2
   2.2 Team address 2
   2.3 Time zone 2
   2.4 Telephone number 2
   2.5 Mailbox address 2
   2.6 Public keys and other encryption information 2
   2.7 Team members 2
   2.8 Customer contact points 3
3. Statute 3
   3.1 Mission 3
   3.2 Area of operation 3
   3.3 Funding and Affiliations 3
   3.4 Enshrinement 3
4. Policies 3
   4.1 Incident types and level of support 3
   4.2 Collaboration, Interaction and Disclosure of Information 3
   4.3 Communication and authentication 4
5. Services 4
   5.1 Reactive Services 4
   5.2 Proactive Services 4
6. Incident reporting forms 4
7. Disclaimers 5

1. Document information

This document provides information about the Flowberg IT SOC computer security incident response team.

1.1 Date last updated

Version: 1.1 as of July 3, 2023

1.2 Document location

The current version of the document is available in:

PL version – https://flowbergit.pl/cyberbezpieczenstwo/soc/

ENG version – https://flowbergit.pl/cyberbezpieczenstwo/soc/

1.3 Reliability of the document

This document was signed using FlowbergIT CEO's electronic signature.

2. Contact information

2.1 Team name

Flowberg IT SOC

2.2 Team address

FlowbergIT Sp. z o. o.
Security Operations Center
Borowska street 283b
50-556 Wrocław
Poland

2.3 Time zone

Central European Time UTC+1.

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

2.4 Telephone number

+48 71 728 10 80

2.5 Mailbox address

Please send notifications, incident reports and operational issues to: soc@flowbergit.pl

Please send queries regarding the offer, scope of services provided and business issues to biuro@flowbergit.pl

2.6 Public keys and other encryption information

We use PGP encryption technology to protect your confidential data.

Public Key: 0535E92182D5C22669A97E6A25AC42757E9C1733
Author: Flowberg IT Security Operations Center (soc@flowbergit.pl)

The public key can be found at: https://flowbergit.pl/cyberbezpieczenstwo/soc/

2.7 Team members

The Flowberg IT SOC team members are strongly committed to 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 our competences.

2.8 Customer contact points

The preferred method of contacting Flowberg IT SOC is e-mail.

3. Statute

3.1 Mission

The mission of Flowberg IT SOC is to maintain IT security at the highest level.

3.2 Area of operation

The area of operation of Flowberg IT SOC includes all users of Flowberg IT systems and clients from the public and private sectors.

3.3 Funding and Affiliations

Flowberg IT SOC is an internal unit of Flowberg IT Sp. z o. o. and it is financed by Flowberg IT Sp. z o.o. acting within its structure.

3.4 Enshrinement

Flowberg IT SOC operates under the auspices and authorization of the management of Flowberg IT Sp. z o. o.

Flowberg IT SOC operates on the basis of internal regulations, terms of contracts with clients, legal provisions and adopted standards and principles.

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 based on contract provisions. Any change in priority is decided by the Flowberg IT SOC team.

4.2 Collaboration, Interaction and Disclosure of Information

All information regarding incident handling is treated as confidential. We recommend that when reporting incidents and providing confidential information, you use PGP encryption or alternatively establish another secure communication channel with Flowberg IT SOC.

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

Information provided to Flowberg IT SOC may be forwarded to interested parties, such as other CSIRT/CERT teams, owners or administrators of affected assets, on a need-to-know basis, except for incident handling purposes (to the extent necessary to identify and mitigate the threat).

Flowberg IT SOC does not independently report incidents to law enforcement authorities, unless required by law. However, in case of proceedings conducted by authorized bodies, we may provide information at their request.

Flowberg IT SOC does not independently report incidents to law enforcement authorities, unless required by law. However, in case of proceedings conducted by authorized bodies, we may provide information at their request.

4.3 Communication and authentication

Flowberg IT SOC secures sensitive information in accordance with applicable laws and internal policies.

In particular, we respect the confidentiality markings defined by the authors of the information submitted to Flowberg IT SOC.

For low-sensitivity information, you can contact Flowberg IT SOC via unencrypted email or telephone. All sensitive information that is transmitted should be encrypted.

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

5. Services

Flowberg IT offers its clients, 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 field of cybersecurity.

5.1 Reactive Services

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

5.2 Proactive Services

- support in creating a security development strategy
- implementing security solutions
- maintaining and developing security solutions
- warnings about new vulnerabilities and threats
- vulnerability tests
- building security awareness

6. Incident reporting forms

Incidents should be reported by e-mail to SOC@flowbergit.pl, preferably encrypted with our PGP public key.

When contacting Flowberg IT SOC, please provide the following information:

1. Contact and organizational information - name and surname of the person, name and address of the organization, e-mail address, telephone number,
2. Type and brief summary of the incident/event,
3. Source of the event/incident - in what system it was observed, source and destination public IP addresses, etc.,

4. Affected entities or systems
5. Estimated impact - e.g. loss of service availability),
6. Additional information and observations that led to the detection of the incident - scan results (if any), log extract showing the issue, etc.

If you forward a suspicious email, please ensure all headers, body and attachments are included.

7. Disclaimers

Although we take every care in preparing information, notices and warnings, Flowberg IT SOC is not liable for errors or omissions or for damages resulting from the use of the information contained therein.