21 NOVEMBER 2022

Declaration
RFC 2350 | wersja 1.0

Smartech IT Sp. z o.o.
ul. Irysowa 1
55-040 Bielany Wrocławskie
NIP: 8961562660

tel. **+48 71 727 71 00, www.smartech-it.eu**

Table of Contents

1. Obtaining the Document

This document provides information about the SmartSOC Computer Security Incident Response Team (CSIRT) in a format appropriate to RFC 2350.

1.1 Date of last update

Version 1.0 from 21 November 2022

1.2 Distribution list

Not applicable.

1.3 Location of the document

Up-to-date version of the document is available at:
https://smartech-it.eu/rfc/

1.4 Document authentication

The document has been signed using the PGP key.
The document credential can be verified by the SmartechIT's PGP key published in section 2.8 of the document.

2. Contact Information

2.1 Team name

SmartSOC – Smart Security Operations Center

2.2 Address

Smartech IT Sp. z o.o.
SmartSOC
Irysowa 1
55-040 Bielany Wrocławskie
Polska

2.3 Time zone

Central European Time UTC+1
Summer Central European Time UTC+2 (from the last Sunday of March to the last Sunday of October).

2.4 Telephone numbe

+48 71 727 71 00

2.5 Facsimile number

Not applicable.

2.6 Other communication

Not applicable.

2.7 Electronic mail address

Questions regarding the offer, the scope of services provided and business issues should be sent to: sekretariat@smartech-IT.eu
Direct contact with the team is possible after receiving the individual address of the team member, which can be obtained by contacting the following address: sekretariat@smartech-IT.eu

2.8 Public keys and other encryption information

In order to protect any sensitive information, we use PGP encryption.
E-mail: sekretariat@smartech-IT.eu
Fingerprint: 580F DC39 D897 8034 6B48 B191 6A07 FA4C 0FA7 36E2
The key is published on the website: https://smartech-it.eu/kontakt/

2.9 Team members

The SmartSOC team consists of young people, whose passion is to deepen their knowledge and skills in the field of cybersecurity. Our goal is to use our resources to effectively raise awareness and cybersecurity quality through constant monitoring and quick response to detected incidents, conducting penetration tests and threat analysis. We are interested in supporting enterprises and

administration in building secure data processing environments both from the technological side and properly informed employees

2.10 Other information

Additional information available at: https://smartech-it.eu

2.11 Additional Contact Info

The SmartSOC team works around the clock. The preferred method of contacting SmartSOC is email, we recommend using PGP to ensure integrity and confidentiality.
Standard customer service hours are 9:00-16:00 Monday to Friday excluding holidays.

3. Charter

3.1 Mission Statement

Our mission is to assure our customers that their valuable assets maintain their confidentiality, are integrated and available when they are needed. The goal is to maintain the highest satisfaction of our customers, which we measure with their good opinions about our cybersecurity services.

3.2 Constituency

The scope of SmartSOC's activity includes clients from the private and public sectors, with whom Smartech IT Sp. z.o.o. has concluded an agreement in the field of support in monitoring, detecting and responding to computer security incidents as well as constant raising of employee awareness at customers' premises.

3.3 Sponsoring Organization / Affiliation

SmartSOC operates within Smartech IT Sp. z o.o.

3.4 Authority

SmartSOC operates within the organizational structure of Smartech IT Sp. z.o.o. with the authorization of the management and on the basis of agreements with customers of Smartech IT Sp. z.o.o. and on the terms resulting from these agreements.

4. Policies

4.1 Types of Incidents and Level of Support

All incidents are automatically prioritized by the Smartech IT system in terms of threat level: small, medium and high. Before starting operations, the SmartSOC team conducts an analysis of each incident and verifies the classification based on the terms of the contract concluded with the client.

4.2 Co-operation, Interaction and Disclosure of Information

Smartech IT declares that all incident handling information is considered confidential and secured by NDAs

Information from customers is processed in a secure environment, in special cases is also encrypted. When reporting an incident and providing confidential information, we recommend to use encryption or contact Smartech IT to determine another secure communication channel.

Information provided to Smartech IT may be transferred to trusted entities (such as internet service provider, other CERT teams) for the necessary knowledge and solely for the purpose of handling incidents. Smartech IT does not report incidents to law enforcement agencies unless required by national law. Smartech IT cooperates with law enforcement agencies only during the official investigation.

4.3 Communication and Authentication

To ensure the confidentiality and integrity of communications, Smartech IT uses PGP encryption. All sensitive information that is transmitted should be encrypted. Incident messages sent by Smartech IT staff are signed with our main PGP key (see section 2.8) and encrypted when they contain sensitive information.
Smartech IT reserves the right to verify the authenticity of the information or its source to the extent permitted by law.

5. Services

5.1 Incident response

Smartech IT supports organizations in handling incidents related to ICT security, both in the technical and organizational aspect. Smartech IT capabilities cover the entire incident response process:

- preparation
- detection and analysis
- restrictions, elimination and restoration
- drawing conclusions, analyzing the collected evidence and recommendations.

5.2 Proactive Activities

Smartech IT makes every effort to increase resistance to security incidents and limit their impact. Smartech IT experts help organizations develop awareness about cyber threats, how to protect themselves against them and how to respond to them by conducting specialized training for company employees, managers and executives, as well as participating in and organizing conferences in the field of cybersecurity.

We conduct an ongoing analysis of our clients' security in order to optimize our activities and effectively increase the level of security. Analyses are carried out on the basis of penetration tests, audits and customer logs.
A detailed description of these services together with other information is available on the Smartech IT website: https://smart-soc.com

5.3 Incident reporting forms

There are no special forms for reporting incidents to Smartech IT.

5.4 Disclaimers

Every precaution will be taken during the preparation of any information, notifications and alerts. Smartech IT is not responsible for errors, omissions or for damages resulting from the use of the information contained in this document.