CSIRT Description for **RTFS.PL**

1. About this document

This document contains a description of RTFS.PL according to RFC 2350. It provides basic information about the CERT, the ways it can be contacted, describes its responsibilities and the services offered.

1.1 Date of Last Update

This is version 1.0, published on 18 July 2022.

1.2 Distribution List for Notifications

This profile is kept up-to-date on the location specified in 1.3.

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available at RTFS.PL website at: https://rtfs.pl/rfc2350.pdf

Signature for this document is available at:
https://rtfs.pl/rfc2350.pdf.sig

Please make sure you are using the latest version.

1.4 Authenticating this Document

This document has been signed with a PGP key and its authenticity can be verified using RTFS.PL SOC key as published in 2.8.

2. Contact Information

2.1 Name of the Team

Full name: RTFS.PL SOC
Short name: RTFS.PL

The name RTFS comes from the first letters of the names of the founding companies — RED TEAM[1] Sp. z o.o. and ForSec SA. For this reason, the RTFS team can sometimes be referred to as **R**ED **T**EAM **F**OR**S**EC.

2.2 Address

RTFS Sp. z o.o.
al. Korfantego 138
40-156 Katowice
Poland

[1] https://redteam.pl

2.3 Time Zone

Europe/Warsaw
Central European Summer Time (CEST) – UTC +2
Central European Time (CET) – UTC +1

2.4 Telephone Number

Unavailable as initial contact method.

2.5 Facsimile Number

Fax is not available.

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

soc@rtfs.pl

2.8 Public Keys and Other Encryption Information

```
User ID:      RTFS SOC <soc@rtfs.pl>
Fingerprint:  D23F F012 444E FBB6 9198  8A93 43A6 1A6B EDB2 AFD9
```

This key can be retrieved from directory servers or directly from RTFS.PL website:
https://rtfs.pl/pgp/soc-rtfs-pl.asc

2.9 Team Members

No information is provided about the RTFS.PL team members in public.

2.10 Other Information

General information about RTFS.PL cyber security services can be found at:
https://rtfs.pl

2.11 Points of Customer Contact

The preferred method for contacting RTFS.PL SOC is e-mail soc@rtfs.pl

3. Charter

3.1 Mission Statement

RTFS.PL is a private company providing professional cyber security services, which includes i.a. digital forensics, incident response (DFIR) and IT Expert Witness opinions. RTFS.PL delivers CSIRT and SOC services to private and government organizations.

RTFS.PL in accordance with Polish law can cooperate with law enforcement agencies and the judiciary as an IT Expert Witness. Therefore can secure digital evidence, perform analyzes and opinions for criminal proceedings in the case of cyber crime.

3.2 Constituency

Our constituency consists of the organization who signed an agreement to use our incident response services.

3.3 Sponsorship and/or Affiliation

RTFS.PL is a private, self-funded company run by a partnership of two companies —
RED TEAM Sp. z o.o. and ForSec SA.

3.4 Authority

RTFS.PL handles and coordinates incidents on behalf of its customers and is bound by contractual terms.

4. Policies

4.1 Types of Incidents and Level of Support

All incidents are considered normal priority unless they are labeled otherwise.

4.2 Co-operation, Interaction and Disclosure of Information

ALL incoming information is handled confidentially by RTFS.PL, regardless of its priority.

RTFS.PL respects EthicsfIRST[2] and supports the Information Sharing Traffic Light Protocol[3] (ISTLP, TLP) – information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

4.3 Communication and Authentication

Usage of PGP in all cases where sensitive information is involved is highly recommended. RTFS.PL SOC PGP key is provided in 2.8.

[2] https://ethicsfirst.org
[3] https://www.trusted-introducer.org/ISTLPv11.pdf

5. Services

RTFS.PL offers a wide range of cyber security services.
Detailed descriptions are available on RTFS.PL websites:
https://rtfs.pl

5.1 Incident Response

RTFS.PL offers incident response and digital forensics services which includes but are not limited to securing evidence and forensics analysis after security incidents.

5.2 Proactive Activities

RTFS.PL provides various CSIRT and SOC services such as threat hunting and threat intelligence.

6. Incident Reporting Forms

There are no specific forms developed for reporting incidents to RTFS.PL SOC.
Incidents should be reported to the e-mail address provided in 2.7.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, RTFS.PL assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.