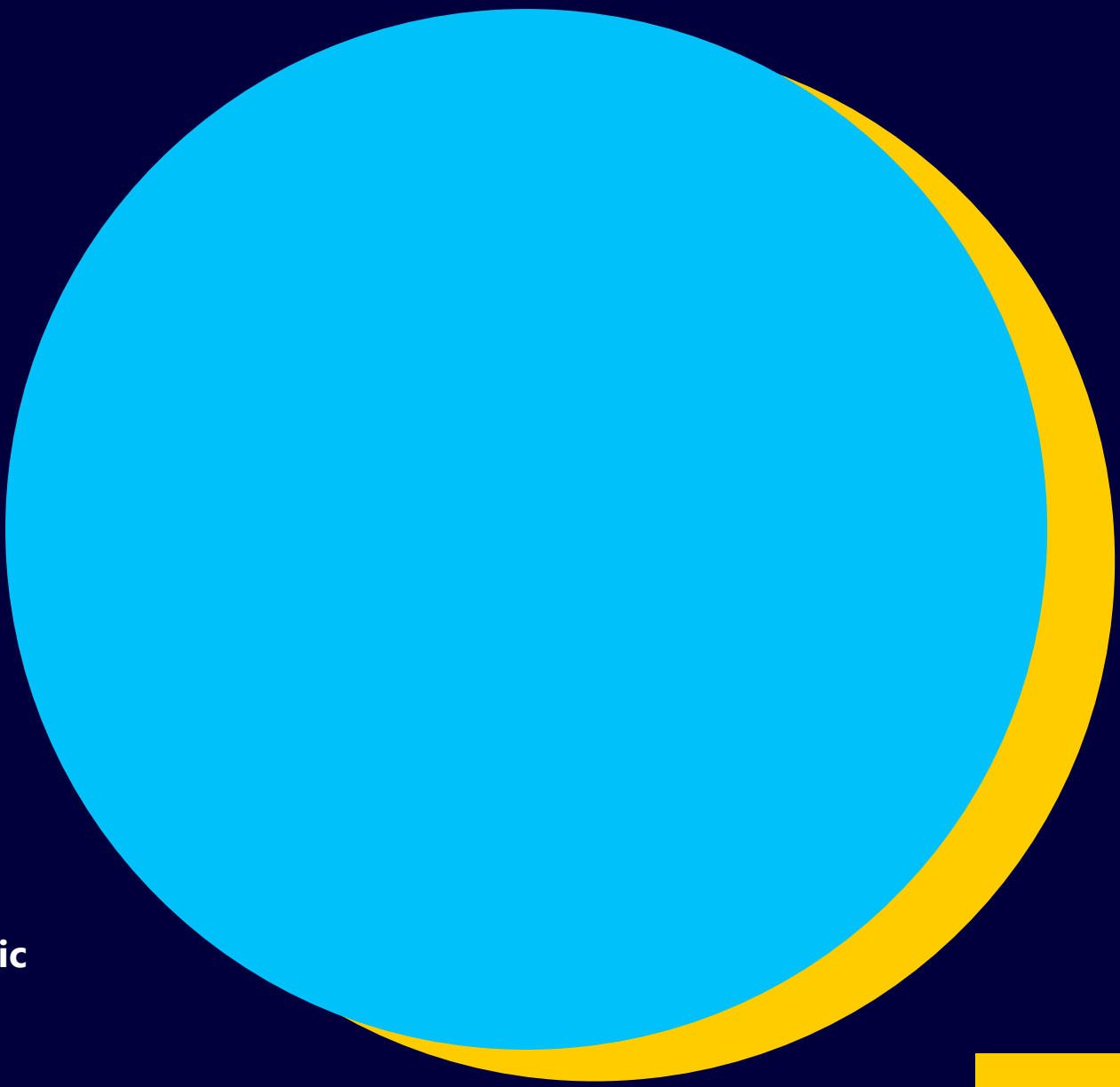
Swiss Post Cybersecurity

CSIRT Service Description

RFC-2350



Public

swisspost-cybersecurity.ch

CSIRT
Service Description
RFC-2350

Document issued:

01.08.2025

Prepared for: Everyone

Classification: PUBLIC

Statement of Confidentiality

This document is public and does not contain any confidential data.

Author:

Greg Divorne

Head of CSIRT

Template version:

AA-0

Index

1. Introduction

This document contains a description of Swiss Post Cybersecurity SA CSIRT (SPCS CSIRT) as implemented by RFC 2350. It provides information about CSIRT (SWISS POST CYBERSECURITY SA), as channels of communication, roles, responsibilities, and the services offered.

SPCS is the official acronym to represent Swiss Post Cybersecurity SA

1.1 Date of last update

Version 4, created on 2025-08-01

1.2 Distribution list for notifications

There is no distribution list for notifications. This document is kept up to date at the location specified in **1.3**. Should you have any questions regarding updates, please contact the CSIRT (SWISS POST CYBERSECURITY SA) email address.

1.3 Locations where this document may be found

The current and latest version of this document is available from SPCS' website from this URL: https://www.swisspost-cybersecurity.ch/solutions-csirt

1.4 Authenticating this document

This document has been signed with the PGP key of CSIRT (SWISS POST CYBERSECURITY SA).

The signature is available from SPCS' website, from this URL: https://www.swisspost-cybersecurity.ch/hubfs/csirt/SPCS_CSIRT_0xFC83178A_public.asc

1.5 Document identification

- Title: CSIRT_SWISSPOST-CYBERSECURITY_SERVICE-DESCRIPTION_RFC-2350
- Version: 4
- Document Date: 2025-08-01
- Expiration: This document is valid until superseded by a more recent version

2. CONTACT INFORMATION

This section describes how to contact CSIRT (SWISS POST CYBERSECURITY SA) for Switzerland and Luxembourg.

2.1 Name of the team

- Full name: SWISS POST CYBERSECURITY SA CSIRT
- Short name: SPCS CSIRT

2.2 Address

Switzerland:

Swiss Post Cybersecurity SA

Rue de Lausanne 35A

1110 Morges

Switzerland

Luxembourg:

SPCS Lux SA

9 Rue du Laboratoire

1911 Luxembourg

Luxembourg

2.3 Time zone

GMT+1 (with Daylight Saving Time or Summertime, which starts on the last Sunday in March and ends on the last Sunday in October). Also known as CET/CEST.

2.4 Telephone number

Switzerland:

Tel: +41 21 519 05 01

Luxembourg:

Tel: +352 20 30 15 86

2.5 Facsimile number

None available

2.6 Electronic mail address

If you need to notify us about an information security incident, please contact us at: csirt@swisspost-cybersecurity.ch

2.7 Public Keys and Encryption Information

PGP/GnuPG is supported to secure communication.

Consequently, the CSIRT (SWISS POST CYBERSECURITY SA) has a PGP key:

- KeyID: 3FA0 FAA0 FC83 178A
- Fingerprint: 22BABC3D7337A650530027263FA0FAA0FC83178A

The PGP key is available from SPCS' website, from this URL: https://www.swisspost-cybersecurity.ch/hubfs/csirt/SPCS_CSIRT_0xFC83178A_public.asc

The key shall be used whenever information related to security incident, must be sent to CSIRT (SWISS POST CYBERSECURITY SA) in a secure manner.

- Please use this key to encrypt messages that you send to CSIRT (SWISS POST CYBERSECURITY SA)
- When required CSIRT (SWISS POST CYBERSECURITY SA) will sign messages.
- When required, sign your messages using your own key please. It helps when that key is verifiable (for instance, using the public key servers).

2.8 Team members

CSIRT (SWISS POST CYBERSECURITY SA) "Head of" is Greg DIVORNE, the technical lead is Antony ANCELIN.

The team consists of IT security specialists with broad skills in defensive and offensive security.

2.9 Other information

General information about CSIRT (SWISS POST CYBERSECURITY SA) can be found at the following URL:

https://www.swisspost-cybersecurity.ch/solutions-csirt

2.10 Point of customer contact

The preferred method to contact CSIRT (SWISS POST CYBERSECURITY SA) is to send an email to the following address: csirt@swisspost-cybersecurity.ch

3. CHARTER

This section describes CSIRT (SWISS POST CYBERSECURITY SA)'s mandate.

3.1 Mission statement

CSIRT (SWISS POST CYBERSECURITY SA) is a private CSIRT team delivering security services, mainly in Switzerland and Luxembourg.

Its main purpose is to assist its customer community:

- First, in evaluating customer capacity to suffer a possible security breach and recover from it efficiently.
- Second, implementing proactive measures to reduce the risks of computer security incidents.
- And third, in responding to such incidents whenever they occur.

CSIRT (SWISS POST CYBERSECURITY SA)'s **mission** is to support its customer community to protect themselves against both

The **scope** of CSIRT (SWISS POST CYBERSECURITY SA) activities cover prevention, detection, response, and support on recovery.

CSIRT (SWISS POST CYBERSECURITY SA) oversees digital forensics and incident response (DFIR) activities.

CSIRT (SWISS POST CYBERSECURITY SA) are driven by several **key values**:

- CSIRT (SWISS POST CYBERSECURITY SA) strives to act according to the highest standards of ethics, integrity, honesty and professionalism.
- CSIRT (SWISS POST CYBERSECURITY SA) is committed to deliver a high-quality service to its constituency.
- CSIRT (SWISS POST CYBERSECURITY SA) will ensure to respond to security incidents as efficiently as possible.
- CSIRT (SWISS POST CYBERSECURITY SA) will ease the exchange of good practices between constituents and with peers, on a need-to-know basis.

3.2 Constituency

CSIRT (SWISS POST CYBERSECURITY SA)'s primary constituency is composed of all the elements of SWISS POST CYBERSECURITY SA Information system composed of:

- Users
- Systems
- Applications
- Networks

However, CSIRT (SWISS POST CYBERSECURITY SA)'s services are also delivered to a secondary constituency.

As a commercial CSIRT, the CSIRT (SWISS POST CYBERSECURITY SA)'s also provides services to its customers base, who subscribed a "Incident Response" support contract.

Current customers who are in Switzerland or Luxembourg are found among:

- Private sector organizations
- Public sector bodies
- Commercial bodies

3.3 Sponsoring Organization / Affiliation

CSIRT (SWISS POST CYBERSECURITY SA) is a private CSIRT. It is owned and operated by SPCS.

It maintains relationships with various CSIRTs in Switzerland and Luxembourg.

CSIRT (SWISS POST CYBERSECURITY SA) is officially member of FIRST since 19 December 2018.

https://www.first.org/members/teams/spcs_csirt

CSIRT (SWISS POST CYBERSECURITY SA) is officially Accredited of TF-CSIRT (Trusted Introducer) since 10 May 2024.

https://www.trusted-introducer.org/directory/teams/spcs-csirt-ch.html

3.4. Authority

CSIRT (SWISS POST CYBERSECURITY SA) coordinates security incidents on behalf of its constituency, and only at its constituents' request. Consequently, CSIRT (SWISS POST CYBERSECURITY SA) operates under the endorsement, guidance and authority delegated by its constituents.

CSIRT (SWISS POST CYBERSECURITY SA) primarily acts as an advisor regarding local security teams and is expected to make operational recommendations. Therefore, CSIRT (SWISS POST CYBERSECURITY SA) may not have any specific authority to require specific actions.

The implementation of such recommendations is not a responsibility of CSIRT (SWISS POST CYBERSECURITY SA), but solely of those to whom the recommendations were made.

4. POLICIES

4.1 Types of Incidents and Level of Support

CSIRT (SWISS POST CYBERSECURITY SA) addresses all types of computer security incidents (cyber-attacks) which occur, or threaten to occur, in its constituency (see 3.2).

The level of support given by CSIRT (SWISS POST CYBERSECURITY SA) will vary depending on the type and severity of the incident or issue, its potential or assessed impact, the type of constituent, the size of the user community affected, and CSIRT (SWISS POST CYBERSECURITY SA)'s resources at the time. Depending on the security incident's type, CSIRT (SWISS POST CYBERSECURITY SA) will gradually roll out its services which include incident response and digital forensics.

Note that no direct support will be given to end users. They are expected to contact their internal IT department. The CSIRT (SWISS POST CYBERSECURITY SA) will support the latter people.

4.2 Co-operation, Interaction and Disclosure of Information

CSIRT (SWISS POST CYBERSECURITY SA) considers the importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar bodies, and with other organizations, which may aid to deliver its services, or which provide benefits to CSIRT (SWISS POST CYBERSECURITY SA)'s constituency.

Consequently, CSIRT (SWISS POST CYBERSECURITY SA) exchanges all necessary information with affected parties, as well as with other CSIRTs, on a need-to-know basis.

However, neither personal nor overhead data are exchanged unless explicitly authorized. Moreover, CSIRT (SWISS POST CYBERSECURITY SA) will protect the privacy of its customers/constituents, and therefore (under normal circumstances) pass on information in an anonymized way only (unless other contractual agreements apply). All incoming information is handled confidentially by CSIRT (SWISS POST CYBERSECURITY SA), regardless of its priority.

All sensible data (such as personal data, system configurations, known vulnerabilities with their locations) are stored in a secure environment, and are encrypted if they must be transmitted over unsecured environment as stated below.

CSIRT (SWISS POST CYBERSECURITY SA) supports the Information Sharing Traffic Light Protocol version 2.0 (see https://www.first.org/tlp/). Information that comes in with the tags CLEAR, GREEN, AMBER or RED will be handled appropriately.

CSIRT (SWISS POST CYBERSECURITY SA) operates within the current Swiss and Luxembourgish legal framework.

4.3 Communication and Authentication

CSIRT (SWISS POST CYBERSECURITY SA) protects sensitive information in accordance with relevant Swiss and European regulations and policies within Swiss and the EU. CSIRT (SWISS POST CYBERSECURITY SA) respects the sensitivity markings allocated by originators of information communicated to CSIRT (SWISS POST CYBERSECURITY SA) ("originator control").

CSIRT (SWISS POST CYBERSECURITY SA) also recognizes and supports the FIRST TLP (Traffic Light Protocol) version 2.0.

Communication security (which includes both encryption and authentication) is achieved using PGP primarily or any other agreed means, depending on the sensitivity level and context.

In CSIRT (SWISS POST CYBERSECURITY SA)'s context of operations, the following communication security levels may be encountered:

- Telephones will be considered sufficiently secure to be used, in view of the types of information that CSIRT (SWISS POST CYBERSECURITY SA) deals with.
- Unencrypted email will not be considered particularly secure but will be enough for the transmission of low sensitivity data.
- If it is necessary to send highly sensitive data by email, encryption (preferably PGP) will be used (See **2.7**). Network file transfers will be like email for these purposes: sensitive data should be encrypted for transmission. Regarding our SOC's customers, file transfer using the "file sharing" functionality of our portal remains a possibility.

5. SERVICES

This section describes CSIRT (SWISS POST CYBERSECURITY SA)'s services.

5.1 Announcements

CSIRT (SWISS POST CYBERSECURITY SA) may provide information on the threat landscape, published vulnerabilities, new attack tools or artefacts and security measures.

5.2 Alerts and Warnings

CSIRT (SWISS POST CYBERSECURITY SA) distribute information on cyberattacks, disruptions, security vulnerabilities, intrusion alerts, malware, and provides recommendations to tackle the issue within its constituency. Alerts and warnings may be passed on to other CERTs, CSIRTs, SOCs and similar bodies if deemed necessary or useful to them on a need-to-know basis.

CSIRT (SWISS POST CYBERSECURITY SA) is not responsible for the implementation of its recommendations. Incident resolution is usually left to the responsible administrators within the constituency. However, CSIRT (SWISS POST CYBERSECURITY SA) will offer support and advice on request.

5.3 Pre-emptive Security Controls

CSIRT (SWISS POST CYBERSECURITY SA) performs pre-emptive security controls to detect potential breaches or vulnerabilities and misconfigurations that may be leveraged in cyberattacks. The security controls also check the compliance level of various systems and applications with the security policies.

CSIRT (SWISS POST CYBERSECURITY SA) handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency. However, CSIRT (SWISS POST CYBERSECURITY SA) will offer support and advice on request.

5.4 Digital Forensics and Incident Response (Triage, Coordination and Resolution)

CSIRT (SWISS POST CYBERSECURITY SA) performs incident response for its constituency (as defined in 3.2).

CSIRT (SWISS POST CYBERSECURITY SA) handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency. However, CSIRT (SWISS POST CYBERSECURITY SA) will offer support and advice on request.

CSIRT (SWISS POST CYBERSECURITY SA) will assist IT Security team in handling the technical and organizational aspects of incidents. It will aid or advice with respect to the following aspects of incident management:

Incident Triage:

- Investigating whether indeed an incident occurred
- Determining the extent of the incident

Incident Coordination:

- Determining the initial cause of the incident (vulnerability exploited)
- Performing acquisition and Digital Forensics whenever necessary (including hard drive and memory forensics)
- Facilitating contact with Security Contacts and/or appropriate law enforcement officials, if necessary
- Making reports to other CSIRTs, CERTs, SOC (if applicable)

Incident Resolution:

- Providing guidance and support to fix the vulnerability
- Providing support in securing the system from the effects of the incident
- Evaluating whether certain actions are likely to reap results in proportion to their cost and risk
- Collecting evidence where criminal prosecution, or disciplinary action, is contemplated

5.5 Development of Security Tools

CSIRT (SWISS POST CYBERSECURITY SA) internally develops security tools for its own use, to improve its services and support its activities as needed.

5.6 INCIDENT REPORTING FORMS

No local form has been developed to report incidents to CSIRT (SWISS POST CYBERSECURITY SA).

In case of emergency or crisis, please provide CSIRT (SWISS POST CYBERSECURITY SA) at least the following information:

- Contact details and organizational name, including address and telephone number.
- Date and time when the incident started.
- Date and time when the incident was detected.
- Incident description.
- Affected assets, impact.
- Actions taken so far.
- Expectations or priorities.