CERT Stockholm RFC 2350

Version 1.0 – 2025-10-28

1 Document Information

This document contains a description of the computer security incident response (CSIRT) function of CERT Stockholm in accordance with RFC 2350[1]. It provides basic information regarding CERT Stockholm, its channels of communication, and its roles and responsibilities.

1.1 Date of Last Update

Version 1.3 as of October 1, 2025

1.2 Locations where this Document may Be Found

The current version of this profile is available at https://stokab.se/det-har-ar-stokab/vilka-vi-ar/st-erik-kommunikation-ab

2 Contact Information

2.1 Team name

CERT Stockholm

2.2 Address

2.2.1 Mailing Address

S:t Erik Kommunikation AB
Att: CERT Stockholm
Box 711
120 02 ÅRSTA
SWEDEN

2.2.2 Visiting Address

S:t Erik Kommunikation AB
Att: CERT Stockholm
Pastellvägen 6 p4
121 36 JOHANNESHOV
SWEDEN

[1] https://www.ietf.org/rfc/rfc2350.txt

2.3 Time zone

CET/CEST, Central European Time/Central European Summer Time, UTC+0100/UTC+0200

2.4 Telephone number

+46 8 508 304 40

2.5 Electronic mail address

cert@stockholm.se

This address can be used to report all IT security incidents which relate to CERT Stockholm's constituency, see 3.2.

2.6 Public keys and encryption

If there is a need for communication within the city of a more sensitive nature, it is recommended to use the City of Stockholm's secure messaging service[2]. Currently, CERT Stockholm does not support any encryption.

2.7 Team members

CERT Stockholm is staffed by S:t Erik Kommunikation AB. A specific list is not provided in this document.

2.8 Operating Hours

CERT Stockholm's hours of operation are generally restricted to regular business hours, except public holidays.

Monday to Thursday 08:00-16:45
Friday 08:00-16:15

[2] https://start.stockholm/om-webbplatsen/personuppgifter-och-dataskydd/sakra-meddelanden/

3 Charter

3.1 Mission Statement

CERT Stockholm’s objective is to enhance the City of Stockholm's ability to prevent, detect and manage IT security incidents. The City of Stockholm refers to the municipality as a whole.

In order to prevent, detect, and mitigate incidents or risks that arise within the IT delivery of the municipality, a collaboration across organizational, contractual and technical boundaries is required between affected key suppliers, departments and companies. For that purpose, CERT Stockholm is responsible for the task of coordinating and managing IT security incidents within the city.

3.2 Constituency

The City of Stockholm's departments, companies, foundations, key suppliers, and all things concerning the complete IT delivery.

3.3 Sponsoring Organization / Affiliation

CERT Stockholm is commissioned by the City Executive Office with the unit for Protective- and Information Security within the Security Division as client representative, and S:t Erik Kommunikation AB as supplier of the CERT Stockholm function.

3.4 Authority

CERT Stockholm shall not operationally take responsibility for technical measures for an affected operation in the city, but CERT Stockholm is responsible for advising, coordinating and collecting and distributing verified information.

4 Policies

4.1 Types of Incidents and Level of Support

CERT Stockholm delivers services according to a written agreement between the City of Stockholm and S:t Erik Kommunikation AB.

4.2 Co-operation, Interaction and Disclosure of Information

CERT Stockholm uses information provided to us to further the city's ability to prevent, detect and manage IT security incidents. This means that by default the information may be distributed further to the appropriate stakeholders.

Information shared with CERT Stockholm information is handled with in accordance with the City of Stockholm's information handling policy and Swedish law.

Personal data is processed in accordance with the City of Stockholm's data protection privacy policy.

CERT Stockholm supports the Traffic Light Protocol (TLP, see https://www.first.org/tlp). Information shared with the tags TLP:CLEAR, TLP:GREEN, TLP:AMBER, TLP:AMBER+STRICT or TLP:RED will be handled appropriately.

4.3 Communication and Authentication

See 2.6 above.

5 Services

CERT Stockholm offers services within the FIRST Services Framework:

- Information Security Incident Management
- Vulnerability Management
- Situational Awareness
- Knowledge Transfer

5.1 Incident Management

CERT Stockholm provides incident response coordination of security incidents somehow involving their constituency (as defined in 3.2), such as, but not limited to:

- Crisis management support and advisories
- Information sharing, proxying and anonymisation
- Communication, contact and collaboration networks
- Situational awareness

The responsibility to design, deploy and operate the systems and services in a secure manner and resolve incidents remains at all times on the owners of the said systems and services. Incident resolution is left at the discretion of the involved constituents. CERT Stockholm will offer support and advice upon request.

5.2 Proactive Activities

CERT Stockholm participates in information sharing and awareness building activities, advises their constituency in regard to recent vulnerabilities and on matters of computer- and network security. CERT Stockholm is not responsible for mitigative implementation or security updates, which is always left at the discretion of the constituents.

6 Incident Reporting Forms

Not available. Whenever possible, please report in plain text using e-mail (see 2.5).

7 Disclaimers

None.