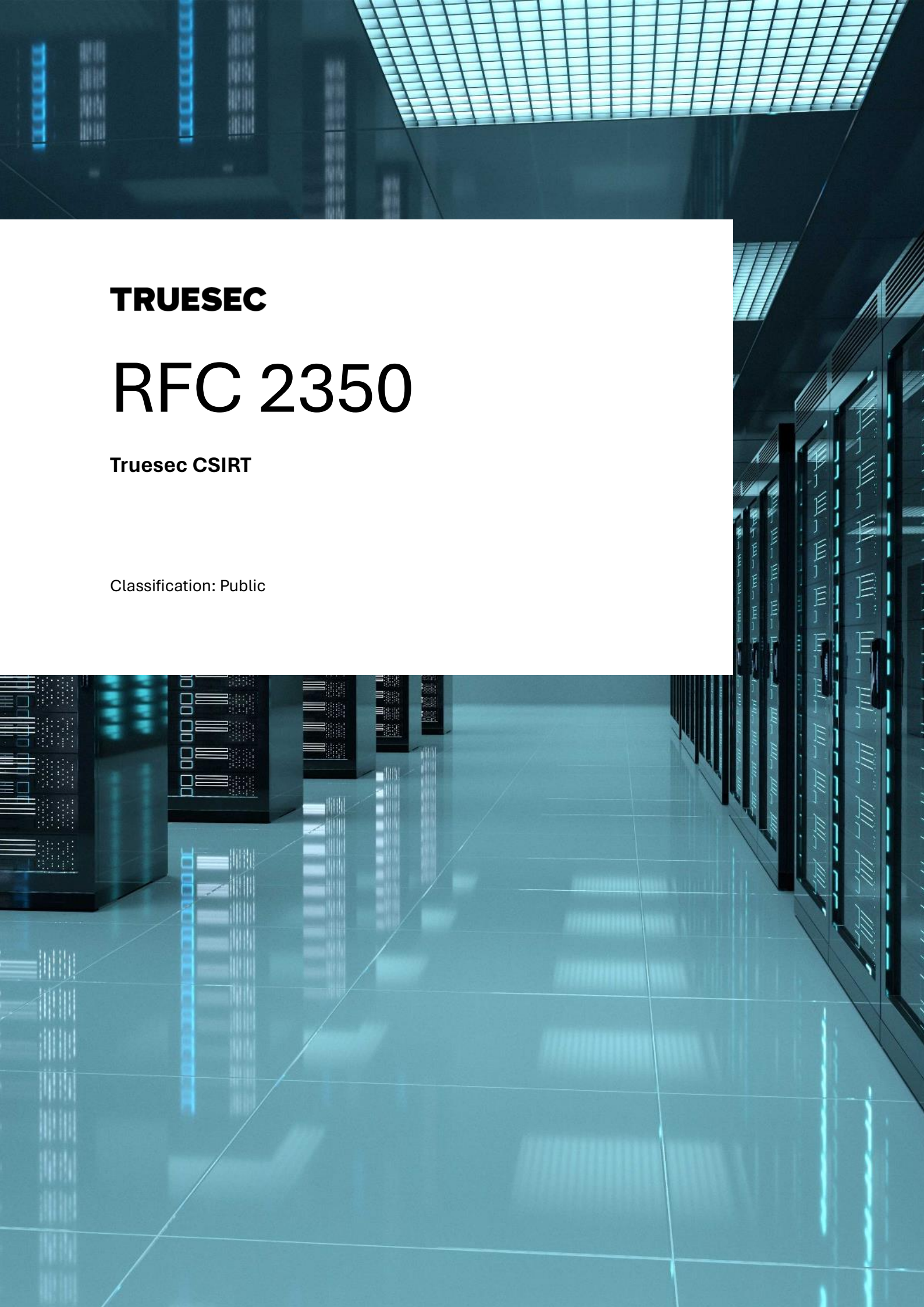


TRUESEC

RFC 2350

Truesec CSIRT

Classification: Public

1. Document Information

1.1. Date of last update

This document was last updated on 2023-12-13.

The following Table presents the revision and changes.

Date	Version	Comment
2022-04-01	1.0	Initial document
2022-04-26	1.1	Content edits
2022-06-02	1.2	TI status changed to “Accredited”
2023-12-13	1.3	TI status changed to “Certified”. Content updates.

1.2. Distribution list for information

The latest version of this document can be found on the location specified in 1.3.

Please direct any question to csirt[@]truesec.se.

1.3. Locations where this document may be found

The latest version of this document is available at
https://files.truesec.com/hubfs/PDF/RFC2350.pdf

2. Contact information

2.1. Name of the team

Full Name: Truesec CSIRT

2.2. Address

Main postal address: Truesec CSIRT, Luntmakargatan 18, 111 37 Stockholm, Sweden

2.3. Time zone

Truesec CSIRT operates in the time zone Europe/Stockholm.

The time is defined as CET (without DST) and is at UTC+0100 between the last Sunday of October and the last Sunday of March. Between the last Sunday of March and the last Sunday of October, the time zone is CEST (with DST) and is at UTC+0200.

2.4. Telephone numbers

Main number (24/7): +46 81 00010.

Emergency number: +46 81 07200

2.5. Facsimile number

Truesec CSIRT does not use fax.

2.6. Other telecommunications

Additional channels such as Teams and Signal are available for communications between Truesec CSIRT and its constituency.

2.7. Electronic mail address

Truesec CSIRT may be reached at csirt[@]truesec.com.

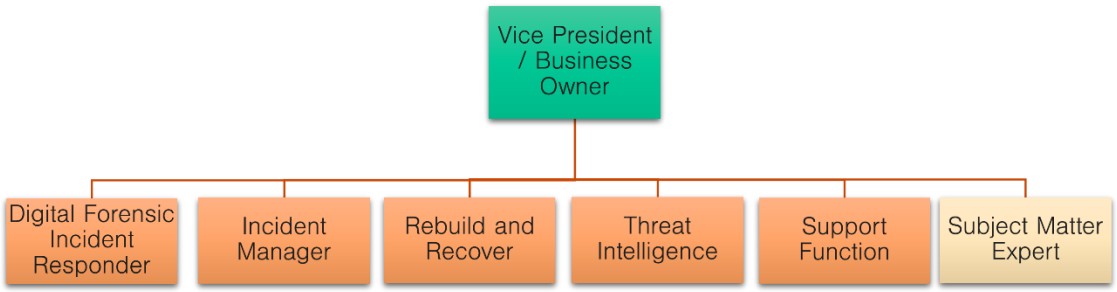
2.8. Public key and encryption

The Truesec CSIRT's PGP public key for the address csirt[@]truesec.com is available on the team's web page, https://www.truesec.com/csirt/team-pgp-key. It is used to digitally sign or encrypt communications. We recommend that parties communicating with the CSIRT use PGP as well.

2.9. Team members

First contact should always be made with the team key if using PGP (recommended). The Truesec CSIRT's PGP team key location is shown under 2.8 above.

The CSIRT is organized in the following way.



2.10. Other information

See our webpage https://www.truesec.com/csirt.

- Truesec CSIRT is a Trusted Introducer Certified team
- Truesec CSIRT is a full member of FIRST
- Truesec CSIRT is a member of Swedish CERT-forum

2.11. Points of Customer Contact

Unless a specific client point of contact has been provided, general cases may be reported through the CSIRT email address or via the phone numbers.

3. Charter

3.1. Mission Statement

Truesec CSIRT's missions are:

- to prevent cybercrime and minimize its impact when it happens
- to help its constituency prepare for cyber incidents through awareness and exercises
- to help its constituency respond to, and recover from cyber incident
- to help its constituency identify potentially adverse or harmful items and activities
- to help its constituency identify and prosecute adverse cyber actors that have caused harm
- to exchange relevant information with law enforcement agencies and national CSIRTs/CERTs in order to raise cyber security, and to help these same parties identify and prosecute adverse cyber actors that threaten national or international security

3.2. Constituency

Truesec CSIRT's constituency is made of:

- the members of the Truesec group
- the customers that have contracted Truesec CSIRT to be their dedicated CSIRT
- the customers of the Truesec Detect (SOC) that have opted in to having their incidents handled by Truesec CSIRT
- the customers that have contracted Truesec CSIRT to assist with an incident

Given the nature of the work, the exact identity of said customers is kept confidential.

3.3. Sponsorship organization and affiliation

Truesec CSIRT is a part of Truesec AB. It operates with the authority delegated by Truesec AB and by the members of its constituency through contractual relationships.

3.4. Authority

Truesec CSIRT operates under the supervision of its constituents' respective management team. Truesec CSIRT is expected to make operational recommendations in the interest of each of its constituents, however Truesec CSIRT neither implements nor bears responsibility for the implementation of the recommendation or lack thereof.

In the cases where our mandate includes intervention, Truesec CSIRT will operate within the boundaries of the powers granted contractually. These actions are performed under the responsibility of the Customer's management team.

4. Policies

4.1. Types of Incidents and Level of Support

All incidents are considered as normal priority unless stated otherwise. Truesec CSIRT may, based on the circumstances and contract, raise, or lower the priority of the incident. A customer may set a priority to an incident, however Truesec CSIRT has the authority to change this priority after the initial assessment.

4.2. Co-operation, Interaction and Disclosure of Information

Truesec CSIRT handles all information received confidentially, regardless of its priority. When communicating sensitive information, please include the word SENSITIVE in the subject line of the email and use encryption. Furthermore, Truesec CSIRT uses and honors the TLP value set. All Information received without a TLP[1] value is automatically assigned a value of "TLP:AMBER."

Truesec CSIRT routinely communicates with other CSIRT, especially with national CSIRTs such as CERT-SE, officially registered to Trusted Introducer or FIRST members. These communications may include the exchange of anonymized information related to incidents, such as indicators of compromise.

Unless required by law or by the customer, Truesec CSIRT does not report incidents to law enforcement. Similarly, Truesec CSIRT will cooperate with law enforcement only if either obligated by law or permitted by the customer. However, if national security or the physical integrity of people is in jeopardy, Truesec CSIRT may communicate with agencies such as SÄPO or Europol.

Truesec CSIRT will notify the relevant vendors of previously unknown vulnerabilities discovered during incident responses and will handle the disclosure in accordance with its vulnerability disclosure policy.

Lastly, designated members of the Truesec CSIRT may communicate with the press. Although no specific case will be discussed without the affected party's expressed and written consent, Truesec CSIRT may comment on cyber security matters.

4.3. Communication and authentication

Truesec CSIRT uses PGP for its email communications: messages that do not require confidentiality shall be signed with the sender's key, messages requiring confidentiality or having sensitive content shall be encrypted. This latter requires that Truesec CSIRT have received the partners' public keys, ideally at the beginning of the contracted service. The location of Truesec CSIRT's PGP key is indicated under 2.8 above.

As an alternative, Truesec CSIRT may use Office365 encryption to communicate with its constituency.

[1] https://www.first.org/tlp/

Voice communications shall happen only when the identity of the interlocutor may safely be established, for example using a phone number that has been received in person or provided in the service contract. Communications regarding ongoing incident shall be carried preferentially in person, if not possible over Signal using a video conference so the identity of participants may be established.

5. Services

5.1. Incident response

Truesec CSIRT provides incident response services such as triage, forensics, recovery and incident management. Broadly speaking, Truesec CSIRT's services cover the containment, eradication, recovery and lessons learnt phases of incidents response. This includes the analysis, communication, coordination and support required for each phase.

5.1.1. Incident Triage

All incidents go through Truesec CSIRT's triage phase to determine whether the incident actually happened and its potential extent.

5.1.2. Incident Coordination

5.1.3. Incident Management

When mandated, Truesec CSIRT will manage the incident response, that is that one of Truesec CSIRT's Incident Managers will lead the response activities and personnel assigned to the incident, including members of the Truesec CSIRT, members of the extended Truesec CSIRT, the customer personnel assigned to the incident, and third parties.

This includes managing the communications between the different response teams, the customer management team, the customer personnel, third parties, and possible law enforcement agencies. The communications are done on a need-to-know basis.

5.1.4. Incident Resolution

Truesec CSIRT's incident response includes the search for the root cause of the incident (patient "0", initial vector of compromise, ...), the tactics, techniques, and procedures (TTP) a threat actor used, the determination of the population of machines compromised or accessed, the threat actor's intent and all information relevant for the containment and eradication.

Once the intent and the full extent of the incident are known, Truesec CSIRT will perform all the tasks related to the complete removal of the threat actor, its tools, and accesses from the environment (eradication) and will proceed with helping the client to recover from the incident.

5.1.5. Threat Hunting

When indicators of compromise related to incident with the potential for a critical impact are received either from an external party or through Truesec CSIRT's investigations and responses, Truesec CSIRT will proactively engage in threat hunts for its constituency, wherever possible, unless specifically excluded in the contract.

5.1.6. Digital Forensics

Truesec CSIRT performs digital forensics analyses on computers, mobile devices such as phones and tablets, and removable media. This may be in support of an active incident, to understand the causes of a resolved incident, in support of a criminal or civil court case, in HR and internal matters, or when instructed by a LEA.

5.1.7. Threat Intelligence

Truesec CSIRT will research threats in order to assist an incident response, a digital forensic analysis or a threat hunt.

5.1.8. Expert witness

If required, Truesec CSIRT's expert witness will testify in court on digital forensics examinations related to an Incident Response Truesec CSIRT performed.

The collection of evidence is performed during the response as part of the routine process.

5.1.9. "Lessons learned" debriefing

At the conclusion of an incident, Truesec CSIRT may, at the request of the affected party or parties, organize a debriefing session on the "lessons learned": Truesec CSIRT will present the items noticed during the incident response process that have hindered or prevented a speedier resolution. This debriefing aims at improving the handling of future, similar incidents.

5.2. Proactive services

In order to raise awareness on cyber security and to identify potential items a threat actor may leverage, the Truesec CSIRT engages in proactive cyber security activities, meaning activities that do not respond to an incident or a specific request from a member of its constituency. These include:

- the organization of cyber security awareness via email, social media, and web communications
- the information on existing cyber security events, recent vulnerabilities and recommendations issued by official bodies and agencies
- the identification of exposed services ("open ports") on the publicly accessible subnets assigned to its constituency
- the provision on security recommendations, either generic or specific to a customer

Truesec CSIRT is not responsible for the implementation of measures.

6. Incident Reporting Form

There is no form for reporting. Incidents should be reported using the communication channels presented under 2 above.

7. Disclaimers

This document does not constitute a contract between Truesec CSIRT and its constituency and should be interpreted as presenting and explaining the roles and tasks of Truesec CSIRT. As such, Truesec CSIRT assumes no liability nor obligation as arising from the provision herein.

8. Abbreviations

Abbreviation	Definition
CERT	Computer Emergency Response Team
CEST	Central European Summer Time
CET	Central European Time
CSIRT	Computer Security Incident Response Team
DST	Daylight Saving Time
LEA	Law Enforcement Agency
SÄPO	Säkerhetspolisen, the Swedish Security Service
TA	Threat Actor