SUNET CERT RFC 2350 PROFILE

1. DOCUMENT INFORMATION

This document complies with RFC 2350.

1.1. Date of Last Update
This is version 1.3.1 as of April 26, 2024.

1.2. Distribution List for Notifications
This profile is kept up-to-date in the location specified in section 1.3.
E-mail notification of updates are sent to SUNET CERT management and investigators.
Please send any questions about updates to the SUNET CERT team e-mail address: cert@cert.sunet.se.

1.3. Locations where this Document May Be Found
The current version of this profile is always available at https://www.sunet.se/sunet-cert-rfc-2350-profile

---

2. CONTACT INFORMATION

2.1. Name of the Team
Full name: SUNET CERT Computer Emergency Response Team.
Short name: SUNET CERT

2.2. Addresses
2.2.1 Mail address
SUNET CERT
c/o Sunet/NUNOC
Tulegatan 11, 3tr
S-113 53 Stockholm, Sweden

2.2.2 Visiting address
SUNET CERT
Tulegatan 11, 3tr
Stockholm, Sweden

2.3. Time Zone
Central European Time, CET, UTC+1
Central European Summer Time, CEST, UTC+2 in summer time (last Sunday of March to last Sunday of October)

2.4. Telephone Number
SUNET CERT telephone number: +46 8 20 78 60

2.6. Other Telecommunication
Not applicable.

2.7. Electronic Mail Address
Please send incident reports that relate to SUNET, including copyright issues, spam and abuse to abuse@cert.sunet.se. Non-incident related mail should be addressed to cert@cert.sunet.se.

2.8. Public Keys and Encryption Information
Please encrypt any sensitive e-mail with the SUNET CERT PGP key with:

```
PGP keyid 0x3ACFD1F0 and
PGP fingerprint 9CBF AF18 D1E1 AF31 76E7 4C3E 2F23 CB19 3ACF D1F0
```

and send it to cert@cert.sunet.se.
Please sign messages using a key that is verifiable using the public keyservers. Because all SUNET CERT investigators can read mail encrypted with the cert@cert.sunet.se key, individuals can use it if they cannot find a key for a specific SUNET CERT team member.

2.9. Team Members
No public information is provided about SUNET CERT team members.

2.10. Other Information
Further information about the SUNET CERT can be found at http://www.sunet.se/cert.
SUNET CERT is listed by the Trusted Introducer (TI) for CERTs in Europe and has been registred as ”TI Accredidited CERT” since 14 May 2002; see https://www.trusted-introducer.org/teams/sunet-cert.html for details. SUNET CERT is a member of Forum for Incident Response and Security Teams (FIRST); see http://www.first.org/members/teams/sunet-cert for details.

2.11. Points of Customer Contact
The preferred method for contacting SUNET CERT is e-mail.

- For general inquiries, please send e-mail to: cert@cert.sunet.se.
- For abuse or security issues, please use abuse@cert.sunet.se.
- For network, server, or service issues, please use cert@cert.sunet.se.

- In an emergency, contact SUNET CERT on +46 8 20 78 60.

SUNET CERT's hours of operation are generally restricted to regular business hours, or 08:00 to 17:00 Monday to Friday except public holidays.
If the emergency phone at SUNET is occupied, calls are automatically redirected to a 247 telephone answering service.

---

3. CHARTER

3.1. Mission Statement

The SUNET CERT mission is to coordinate and inform about IT-security related issues for all SUNET's customers.
SUNET CERT also establishes and maintain networks with other CSIRT:s in Sweden and abroad and participate in national and international organizations for CERT cooperation. It's also the mission for SUNET CERT to monitor that all organisations are acting in compliance with the SUNET IT-security policy.

3.2. Constituency
SUNET customers which connected with SUNET. The corresponding AS-numbers are:
AS1653 and sub-AS (2831-2835,2837-2846,3224,5601,8748,8973,9088,12384,15980,16251,25072,41001,42307,43018,43665,43844,48514,207113)

3.3. Sponsoring Organisation / Affiliation
SUNET CERT operates with the authority delegated by SUNET.

3.4. Authority
SUNET CERT operates under the auspices of the SUNET members and the supervision of the SUNET management.
Should circumstances warrant it, the SUNET CERT will appeal to the NORDUNET NOC excert its authority.

---

4. POLICIES

4.1. Types of Incidents and Level of Support
Incidents are classified as Critical (response time 8 hours), Major (response time next business day, Minor (response time 3 business day) or Low (response time 5 business day).

4.2. Co-operation, Interaction, and Disclosure of Information
All incoming information is handled confidentially by SUNET CERT and in accordance with Swedish Law.
When reporting an incident of sensitive nature, please state so explicitly by using an appropriate label in the Subject field (for example, SENSITIVE, EMERGENCY, etc.) and if possible, use encryption as well.
SUNET CERT supports the Information Sharing Traffic Light Protocol (ISTLP; see https://www.trusted-introducer.org/links/ISTLP-v1.1-approved.pdf); information that arrives with the tags WHITE, GREEN, AMBER, or RED will be handled appropriately.

4.3. Communication and Authentication
See section 2.8; usage of PGP in all cases where sensitive information is involved is highly recommended.

---

5. SERVICES

5.1. Incident Response (Triage, Coordination, and Resolution)
SUNET CERT offers the services:

- IT security incident analysis (triage, information collection and coordination.)
- Vulnerability detection and scanning.
- Awareness building through reach out, workshops and community gatherings.
- Crisis exercises

---

6. INCIDENT REPORTING FORMS

Not available; please report using e-mail. When reporting an incident of sensitive nature use encrypted e-mail.

---

7. DISCLAIMERS

None.

Revision

1.3.1 2024-04-26 Updated: 2.11 and 4.1 /MT

1.3.0 2023-05-08: Deletede facsimile number. 3.1 Mission updated. 5.1 Services updated. /MT