eduCSC-NO RFC 2350 profile

1 Document Information

This document is compliant with RFC 2350.

1.1 Date of Last Update

This is version 2.0, 2023-03-28.

1.2 Distribution List for Notifications

This profile is kept up-to-date on the location specified in section 1.3.
E-mail notifications of updates are sent to the Trusted Introducer for CERTs in Europe (see https://www.trusted-introducer.org/).

1.3 Locations where this Document may be found

The current version of this profile is available at https://sikt.no/abuse.

2 Contact Information

2.1 Name of the Team

Cyber security centre for research and education (eduCSC-NO).

2.2 Postal Address

eduCSC
Sikt
PO box 5782 Torgarden
NO-7437 Trondheim
Norway

2.3 Time Zone

Nominally CET (UTC +1), CEST (UTC +2) during daylight saving time.

2.4 Telephone Number

+47 73984040

2.5 Facsimile Number

Not applicable

2.6 Other Telecommunication

Not applicable

2.7 Electronic Mail Address

Main e-mail address for all communication: cert@educsc.sikt.no.

2.8 Public Keys and Encryption Information

Please encrypt any sensitive information with the eduCSC team key.
The current key can be found at https://sikt.no/abuse

Please sign your messages using your own key, which should be verifiable through public key servers.

2.9 Team Members

This information is available only to TI accredited teams, see https://tiw.trusted-introducer.org/directory/teams/educsc-no-no.html

2.10 Other Information

eduCSC-NO is certified by the Trusted Introducer for CERTs in Europe, see https://www.trusted-introducer.org/directory/teams/educsc-no-no.html for details.

eduCSC-NO is a member of the Forum of Incident Response and Security Teams (FIRST), see https://www.first.org/members/teams/educsc-no for details.

3 Points of Customer Contact

E-mail is the preferred method for contacting eduCSC-NO.

- E-mail address: cert@educsc.sikt.no.
- Telephone during business hours (08:00–15:30 CET/CEST Monday–Friday): +47 73984040
- Telephone for time-critical emergencies outside business hours: +47 73984040 and press “1”.

4 Charter

4.1 Mission Statement

The purpose of eduCSC-NO is to prevent and minimize damage from IT security related incidents in the Norwegian research and higher education sector.
eduCSC-NO shall assist technical staff that are responsible for maintenance or development of networks, infrastructure, and information systems – at Sikt and Sikt’s customers – in the prevention, detection, and handling of security incidents.
eduCSC-NO is given the authority to independently implement necessary precautions to protect network, infrastructure, and IT resources in conjunction with IT security incidents.

4.2 Constituency

Sikt is the Norwegian NREN (national research and education network), and the services of eduCSC-NO are available to all of Sikt's customers.

4.3 Sponsorship and/or Affiliation

eduCSC-NO is part of Sikt and financed through Sikt's budget with additional proceeds coming from customer subscriptions.

4.4 Authority

If activities on a customer's internal network constitute a problem for Sikt or other parties, eduCSC-NO has the authority to take relevant countermeasures. In particular, eduCSC-NO may block individual hosts or the organization's entire network from accessing the Internet.

5 Policies

5.1 Types of Incidents and Level of Support

All incidents are initially considered normal priority. eduCSC-NO will assess incidents based on severity and impact on the constituency.

5.2 Co-operation, Interaction and Disclosure of Information

Classification
Sensitive information encompasses sensitive personal data, as defined by relevant privacy legislation, and business confidential information. All information related to security incidents is considered sensitive, unless all concerned parties specifically state otherwise.
Non-sensitive information consists of publicly available (open) information.

Information handling
Sensitive information is stored and communicated securely. Sensitive information brought to the team's knowledge may be distributed amongst the eduCSC-NO team members. Members of eduCSC-NO are subject to explicit non-disclosure agreements regarding all sensitive information.

Information disclosure
In order to investigate and resolve security incidents, incident related information may be released to appropriate parties on a strictly need-to-know basis, and preferably anonymized. Non-sensitive information may be distributed to the general public on a need-to-know basis.

Legal considerations
Sikt is not subject to the Norwegian Telecommunications Act which states that logs should be handed over to the authorities on request, without any prior court order. However, eduCSC-NO will in general cooperate with law enforcement authorities during investigation of possible criminal activity relevant to our constituency, and providing e.g. event and system logs. Sensitive information can be handed over

to relevant authorities following a court order.

Traffic Light Protocol (TLP)

eduCSC-NO supports the Traffic Light Protocol v2.0, and all labelled information will be handled in accordance with https://www.first.org/tlp.

5.3 Communication and Authentication

See 2.8 above.

eduCSC-NO uses PGP/GPG to ensure the confidentiality and integrity of sensitive information. Normally, all information provided by eduCSC-NO is digitally signed with the team key, and sensitive information is encrypted. It is highly recommended to use PGP/GPG in all cases where sensitive information is involved. Norwegian authorities do not enforce restrictions on key sizes or the use of cryptography, and there are no key escrow requirements.

6 Services

6.1 Incident Response

eduCSC-NO can assist system administrators in handling the technical and organizational aspects of computer security incidents.

6.1.1 Incident Triage

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

6.1.2 Incident Coordination

- Establish and maintain dialogue with afflicted customer organizations, normally through their incident response team or other security contact.
- Correlate indicators from detection vectors with other central or customer-specific information sources.
- Contact other members of the constituency that may be involved in the incident or exposed to the particular threat.
- Compose announcements to end users, if applicable.
- Share information with other CSIRTs, if applicable.
- Contribute to determining the initial cause of the incident.

6.1.3 Incident Resolution

- For incidents occurring at customer organizations, eduCSC-NO typically assumes an advisory role.
- For internal incidents, the following relevant steps are taken:
  - Remove the vulnerability.
  - Secure the system from the effects of the incident.
  - Collect evidence after the fact, if applicable.
  - Take appropriate countermeasures to protect against recurring incidents.
  - Wrap-up, lessons learned.

6.2 Proactive Activities

- eduCSC-NO maintains security mailing lists, including:
  - sikkerhetsvarsel@lister.sikt.no is open to customer organizations. Only information labelled as TLP:CLEAR is shared.
  - irt-varsel@lister.sikt.no is a closed list only for customer incident response teams that have signed a TLP agreement with eduCSC. Any TLP labelled information may be shared, including TLP:RED.
- Configuration and maintenance of security-related tools, applications, and infrastructure.
- Non-intrusive monitoring of network traffic for indications of misuse.

Please send incident reports to cert@educsc.sikt.no. Encrypting sensitive information is highly encouraged.

7 Disclaimers

None.