RFC2350 for OsloMet CSIRT

OsloMet CSIRT

2025-11-28

1 Document Information

This document is compliant with RFC 2350.

1.1 Date of Last Update

This is version 1.1, 2025-11-28.

1.2 Distribution List for Notifications

This profile is kept up-to-date on the location specified in section 1.3.

1.3 Locations where this Document may be found

The current version of this profile is available at https://oslomet.no/.well-known/rfc2350.pdf

2 Contact Information

2.1 Name of the Team

OsloMet Computer Security Incident Response Team - OsloMet CSIRT

2.2 Postal Address

```
Sikkerhet
c/o Avdeling for IKT
OsloMet – storbyuniversitetet
Postboks 4, St. Olavs plass
N-0130 Oslo
Norway
```

2.3 Time Zone

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

2.4 Telephone Number

+47 67 23 50 00

2.5 Facsimile Number

Not applicable

2.6 Other Telecommunication

Not applicable

2.7 Electronic Mail Address

The e-mail address for all communication: csirt@oslomet.no

2.8 Public Keys and Encryption Information

Please encrypt any sensitive information with the csirt@oslomet.no team key.
The current key can be found at https://oslomet.no/.well-known/pgp-key.txt
Please sign your messages using your own key, which should be verifiable through public key servers.

2.9 Team Members

This information is not available.

2.10 Other Information

OsloMet CSIRT reports to eduCSC-NO (Norwegian Cyber Security Centre for Research and Education), see https://sikt.no/en/tjenester/cyber-security-center

2.11 Availability

OsloMet CSIRT is available during normal business hours (08:00–16:00 CET/CEST), Monday to Friday. Outside these hours, response may be delayed.

3 Points of Customer Contact

E-mail is the preferred method for contacting OsloMet CSIRT.
E-mail address: csirt@oslomet.no

3.2 Reporting Incidents

Security incidents should be reported via email to csirt@oslomet.no. Please include relevant logs, timestamps, timezone, and a description of the issue.

4 Charter

4.1 Mission Statement

The purpose of the OsloMet CSIRT is to ensure an effective and coordinated response to IT security incidents at OsloMet. The CSIRT will help limit the extent of the damage from the incidents, restore operations and prevent similar incidents from occurring in the future.

4.2 Constituency

OsloMet CSIRT is the Computer Incident Response Team for Oslo Metropolitian University - see: https://www.oslomet.no/en The team reports to eduCSC-NO, see https://sikt.no/en/tjenester/cyber-security-center

4.3 Sponsorship and/or Affiliation

OsloMet CSIRT is a part of the ICT Department at Oslo Metropolitan University

4.4 Authority

OsloMet CSIRT:

- handles incidents concerning OsloMet's network resources, both on-premises and in the cloud
- has the mandate to take necessary actions when required
- coordinates with eduCSC-NO as its sectoral response environment (SRM)

5 Policies

5.1 Types of Incidents and Level of Support

All incidents are initially considered normal priority. OsloMet CSIRT will assess incidents based on severity and impact on the constituency.

5.2 Cooperation, Interaction, and Disclosure of Information

Classification

- **Sensitive information**: Personal data and business-confidential information.
- **Non-sensitive information**: Publicly available data.

Handling

Sensitive information is stored and communicated securely. All team members are bound by confidentiality agreements.

Disclosure

Information is shared only on a need-to-know basis, preferably anonymized. Non-sensitive information may be shared publicly when appropriate.

Legal Considerations

OsloMet is not subject to the Norwegian Telecommunications Act. However, OsloMet CSIRT cooperates with law enforcement in cases of suspected criminal activity. Sensitive information may be disclosed upon court order.

Traffic Light Protocol (TLP)

OsloMet CSIRT supports TLP v2.0: https://www.first.org/tlp

6 Services

6.1.1 Incident Triage

- **Identification** – Determine whether an incident occurred
- **Scope** – Assess the extent of the incident
- **Resolution** – Collaborate with service owners

- **Post-incident** – Analysis and reporting

6.1.2 Incident Coordination

- Dialogue with affected parties
- Correlate indicators
- Inform end users
- Share with other CSIRTs, CERTs and eduCSC-NO
- Contribute to root cause analysis

6.1.3 Incident Resolution

For major incidents:

- Remove vulnerabilities
- Secure systems
- Collect evidence
- Implement countermeasures
- Share lessons learned internally and externally

7 Version History

Version	Date	Description
1.0	2025-09-30	Initial publication
1.1	2025-11-28	Typos corrected