NORCERT PROFILE

Established according to RFC-2350

1. Document Information

1.1. Date of Last Update

This is version 1.0 of 2015-06-24

1.2. Distribution List for Notifications

This profile is kept up-to-date on the location specified in 1.3 . E-mail notification of updates are sent to:

- ➜ All NorCERT members and partners
- ➜ The Trusted Introducer for CERTs in Europe (see https://www.trusted-introducer.org/)

Any questions about updates please address to the NorCERT e-mail address: **post@cert.no**

1.3. Locations Where This Document May Be Found

The current version of this profile is always available on:

https://www.nsm.stat.no/norcert

Postboks 814
1306 Sandvika

02497 (operations)
67 86 40 00 (switchboard

post@cert.no
norcert@cert.no

2. Contact Information

2.1. Name of the Team

Full name: **Norwegian Computer Emergency Response Team**

Short name: **NorCERT**

NorCERT is the National CERT in Norway. NorCERT is the coordinating body for all major Cyber security incidents related to Norway. The constituency is all parts of Critical National Information Infrastructure (CNII) in Norway.

2.2. Address

Norwegian National Security Authority (NSM)
NorCERT
P. O. Box 814
1306 Sandvika
Norway

2.3. Time Zone

- ➜ CET, Central European Time
- ➜ CEST, Central European Summer Time (UTC+2 between the last Sunday in March and the last Sunday in October)

2.4. Telephone Number

+47 23 31 07 50

2.5. Facsimile Number

+47 23 09 25 88 Note: this is not a secure fax.

2.6. Other Telecommunication

Not available.

2.7. Electronic Mail Address

E-mail: post@cert.no

Incidents e-mail: norcert@cert.no

2.8. Public Keys and Encryption Information

PGP/Gnu-PG is supported for secure communication.

The current NorCERT team-key can be found on
https://www.nsm.stat.no/tjenester/handtering/kontakt-operasjonssenteret/
and is also present on the public keyservers.

Please use this key when you want/need to encrypt messages that you send to NorCERT. When due, NorCERT will sign messages using the same key.

When due, sign your messages using your own key please - it helps when that key is verifiable using the public keyservers.

PGP Fingerprint: 216C 1DA6 FB74 91C7 1268 FCD0 3FEB 3674 8258 8811

2.9. Team Members

No information is provided about the NorCERT team members in public.

2.10. Other Information

- ➜ See the NorCERT web page
- ➜ NorCERT is accredited by the Trusted Introducer for CERTs in Europe, see https://www.trusted-introducer.org/teams/country_AS.html
- ➜ NorCERT is described in the RIPE whois database by means of an IRT-object, see http://www.db.ripe.net/whois and search for "-B IRT-NorCERT

2.11. Points of Customer Contact

General information: **post@cert.no**

Regular response hours: Monday-Friday, 08:00-16:00 (except public holidays in Norway).

EMERGENCIES / INCIDENTS (24/7):

Send e-mail with EMERGENCY in the subject line to **norcert@cert.no** and call the 24/7 Emergency phone: **+47 23 31 07 50**

3. Charter

3.1. Mission Statement

NorCERT coordinates preventative work and response to severe ICT-incidents related to Norway.

NorCERT detects and alerts on serious attacks, threats and vulnerabilities related to critical ICT-systems in Norway, and coordinates an efficient and timely response. NorCERT is the National Point of Contact for operational cyber security and incident handling.

3.2. Constituency

NorCERT's constituency consists of all organizations with critical functions for the Norwegian society, in both the public and the private sector.

3.3. Sponsorship and/or Affiliation

NorCERT is part of the Norwegian National Security Authority (NSM): https://www.nsm.stat.no/om-nsm/english/

3.4. Authority

NorCERT's main purpose is the coordination of incident response. As such, NorCERT advises constituents and have no authority to demand certain actions.

4. Policies

4.1. Types of Incidents and Level of Support

All incidents are considered normal priority unless they are labelled EMERGENCY. NorCERT itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to NorCERT as EMERGENCY, but it is up to NorCERT to decide whether or not to uphold that status.

4.2. Co-operation, Interaction and Disclosure of Information

NorCERT handles all incoming information confidentially, regardless of its priority.

When reporting an incident of sensitive nature, please state so explicitly, e.g. by using the label SENSITIVE in the subject field of e-mail, and if possible using encryption as well.

NorCERT supports the Information **Sharing Traffic Light Protocol** (ISTLP – see https://www.trusted-introducer.org/links/ISTLP-v1.1-approved.pdf) - information that comes in with the tags WHITE, GREEN, AMBER or RED is handled appropriately.

NorCERT will use the information you provide to help solve security incidents, as all CERTs do, and in accordance to ISTLP. Information will only be distributed further to other parties on a need-to-know base, and preferably in an anonymised form.

NorCERT operates under the restrictions imposed by Norwegian laws.

4.3. Communication and Authentication

See 2.8 above.

For unclassified information sharing, NorCERT recommends the use of PGP/GnuPG, both for signing and encryption.

5. Services

5.1. Reactive Services (Incident Response, Triage, Coordination and Resolution)

NorCERT is responsible for coordinating the handling of serious cyber security incidents related to Norway. As such, NorCERT is involved with both triage and coordination processes (hereunder time critical information sharing both in and outside Norway).

Incident resolution is the formal responsibility of the owners of the ICT-systems affected but NorCERT offers support and advice on a request basis.

5.2. Proactive Activities

NorCERT proactively advises their constituency in regard to recent vulnerabilities and trends.

Reports are produced on a regular basis on both classified and unclassified level.

NorCERT shares updated IDS-signatures to the national NorCERT sensors (called Warning system for critical infrastructure). These sensors are deployed within the constituency.

5.3. Artifact handling

NorCERT do malware analysis and store all artifacts in a house developed database called NAAS.

5.4. Security quality management

NorCERT arranges courses and exercises related to incident response on a regular basis for the constituency.

NorCERT is involved in supporting different organizations in rising awareness related to computer security and information assurance.

6. Incident reporting Forms

Not available. Preferably report in plain text using e-mail, fax or phone.

7. Disclaimers

While every precaution is taken in the preparation of information, notifications and alerts, NorCERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.