This profile of CERT-UT is established according to RFC-2350.

1. Document Information

1.1. Date of Last Update

December 6, 2016

1.2. Distribution List for Notifications

1.3. Locations where this Document May Be Found

The current version of this profile is always available on https://www.utwente.nl/nl/cyber-safety/cybersafety-map/.

2. Contact Information

2.1. Name of the Team

CERT-UT is the Computer Emergency Response Team of the University of Twente

2.2. Address

University of Twente
Secretariaat LISA
T.a.v. CERT-UT
P.O Box 217
NL – 7500 AH Enschede
The Netherlands

2.3. Time Zone

CERT-UT lives in timezone ‘Europe/Amsterdam’ which means CET (UTC+1) in winter and CEST (UTC+2) in the summer.

2.4. Telephone Number

During business hours CERT-UT is reachable at +31(0)53 – 489 13 13. If the phone isn’t answered and the message involves an emergency you can contact the ICT Servicedesk at +31(0)53 – 489 55 77.

Outside these hours contact by phone is not yet possible.

2.5. Other Telecommunication

Not available.

2.6. Electronic Mail Address

cert@utwente.nl

2.7. Public Keys and Encryption Information

PGP is currently only supported on request.

2.8. Team Members

CERT-UT is led by two Security Managers, Peter Peters and Marc Berenschot.
No public information is provided about other CERT-UT team members.

2.9. Other Information

- See the University webpages https://www.utwente.nl/
- See the cyber safety website https://www.utwente.nl/cyber-safety/
- CERT-UT is registered by SURFcert, see https://www.surf.nl/diensten-en-producten/surfcert/index.html

2.10. Points of Customer Contact

Regular cases: use CERT-UT e-mail address.
Regular response hours: Monday - Friday, 08:00 - 17:00 (except public holidays in the Netherlands).

EMERGENCY cases:
Send an e-mail with EMERGENCY in the subject line.
The CERT-UT phone number is not available outside the regular response hours.
Emergency response hours: Monday - Friday, 17:00 -22:00
Saturday, Sunday, public holidays. 08:00 - 22:00

3. Charter

3.1. Mission Statement

The Computer Emergency Response Team of the University consists of IT professionals from LISA. They investigate all reports in the field of security and privacy and engage the necessary (technical) specialists to solve the report. When a report has a privacy aspect, it works directly with the FG team. Incidents relating to employees' workplaces or devices are picked up by the LISA ICT service desk. For reports about workplaces or devices of students, there is close contact between CERT-UT and the SNT helpdesk.

3.2. Constituency

The constituency for CERT-UT is the University of Twente, it’s related institutions and associations as well as other organizations connected to the University’s network.
Systems, networks, applications and data part of the University’s computing and communication infrastructure, including those managed by third parties and third-party infrastructure managed by the University.

3.3. Sponsorship and/or Affiliation

CERT-UT is part of LISA, the Library, IT Services & Archive department at the University.

3.4. Authority

CERT-UT has the authority to order a system to be disconnected from the network pending investigation of a reported problem.
CERT-UT has the authority to order any other measure deemed fit to resolve an ongoing security problem.

4. Policies

4.1. Types of Incidents and Level of Support

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

CERT-UT will usually respond within one working day. If CERT-UT acknowledges an EMERGENCY a response will be send within 8 hours.
Data breaches are in itself considered an EMERGENCY and will be handled accordingly.
When information regarding a possible vulnerability, which creates an opportunity for future incidents, is received, CERT-UT may decide to act upon this information.

4.2. Co-operation, Interaction and Disclosure of Information

ALL incoming information is handled confidentially by CERT-UT, regardless of its priority.

Information that is evidently sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies. When reporting an incident of sensitive nature, please state so explicitly, e.g. by using the label SENSITIVE in the subject field of the e-mail.

CERT-UT supports the Information Sharing Traffic Light Protocol (ISTLP – see https://www.first.org/tlp).

Unless otherwise noted CERT-UT considers every information it receives as TLP:AMBER. It is often necessary to share information, on a need-to-know base with relevant parties, be it internal administrators or external suppliers. Information is preferably shared in an anonymised fashion.

If you object to this default behavior of CERT-UT, please make explicit what CERT-UT can do with the information you provide. CERT-UT will adhere to your policy, but will also point out to you if that means that CERT-UT cannot act on the information provided.

CERT-UT does not report incidents to law enforcement, unless national law requires so. Likewise, CERT-UT only cooperates with law enforcement EITHER in the course of an official investigation – meaning that a court order is present – OR in the case where a constituent requests that CERT-UT cooperates in an investigation.

CERT-UT might interact about incidents with upstream CSIRT’s, such as the SURFnet CERT team SURFcert, and possibly with CSIRT’s of other Universities who might be affected by the incident.

CERT-UT does not deal with the press directly. All press enquiries will have to go through the communications office of the University of Twente.

4.3. Communication and Authentication

See 2.7 above. Usage of PGP/GnuPG in all cases where sensitive information is involved is highly recommended.

5. Services

5.1. Incident Response

5.1.1. Incident Triage

Incident triage is handled by CERT-UT.

5.1.2. Incident Coordination

Incident coordination is handled by CERT-UT.
Coordination of high profile incidents, based on judgement bij CERT-UT, can be done by the IT Security Managers of the University.

5.1.3. Incident Containment

Incident containment is left to the responsible administrator within the University and externally. If containment is urgent CERT-UT can decide to handle containment itself.

5.1.4. Incident Resolution

Incident resolution is left to the responsible administrators within the University and externally. CERT-UT will offer support and advice both requested and unrequested.

5.2. Proactive Activities

CERT-UT pro-actively advises their constituency in regard to recent vulnerabilities and trends in attacks.

CERT-UT advises the University on matters of computer and network security. It can do so unrequested and requested.

Both roles are roles of consultancy: CERT-UT is not responsible for implementation.

6. Incident reporting Forms

CERT-UT does not use incident reporting forms.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CERT-UT assumes no responsibility for errors or omissions, of for damages resulting from the use of the information contained within. CERT-UT also assumes no responsibility for any actions it has taken or did not take in the cause of its duty.