CERT@tue

Established according to RFC-2350

1. **Document Information**

   1.1. Date of last update
   This is version 1.8 of 30-01-2024

   1.2. Distribution list for notifications
   Any specific questions or remarks please address to the CERT@tue.nl mail address.

   1.3. Locations where this document may be found
   The current version of this profile is always available on:
   https://www.tue.nl/en/our-university/about-the-university/support-services/library-and-information-services/ict-security

2. **Contact Information**

   2.1. Name of the team
   CERT@tue, the CSIRT or CERT team for the Eindhoven University of Technology (TU/e), The Netherlands.

   2.2. Address
   CERT@tue
   Library and Information Services
   PO Box 513
   5600 MB Eindhoven
   The Netherlands

   2.3. Time zone
   GMT+1 (GMT+2 with DST, according to EC rules)

   2.4. Telephone number
   +31 (0)40 247 5678 (during office hours only)

   2.5. Facsimile number
   Not available.

   2.6. Other telecommunication
   Not available.

   2.7. Electronic mail address
   CERT@tue.nl

2.8. Public keys and encryption information

CERT@tue uses PGP for secure communication.
We generate a new key once a year for the email address CERT@tue.nl

Key information:

Name	Eindhoven University of Technology - CERT (2024) <cert@tue.nl>
ID	0xE01C3D0C
Fingerprint	984E 8890 322B AE18 3EA7 2FEB 899C EEE9 E01C 3D0C
Valid until	2025-01-30

https://pgp.surfnet.nl/pks/lookup?op=get&search=0x899ceee9e01c3d0c

2.9. Team members

CERT@tue team members are drawn from the ranks of the Operational Security Team (OST) of the University.

2.10. Other information

See https://www.tue.nl/en/our-university/about-the-university/support-services/library-and-information-services/ict-security

CERT@tue is registered by SURFcert, see https://wiki.surfnet.nl/display/CSIRTs

2.11. Points of customer contact

Normal cases:
Use CERT@tue e-mail address.
Business hours response only: 08:30-16:00 local time on Monday-Friday save public holidays in The Netherlands.

Emergency cases:
Use CERT@tue phone number with back-up of e-mail address for all details (putting EMERGENCY in subject line is recommended). The CERT@tue phone number is available during office hours.

3. Charter

3.1. Mission statement

CERT@tue ’s mission is to coordinate the resolution of IT security incidents related to the Eindhoven University of Technology, and to help prevent such incidents from occurring.

For the world, CERT@tue is the TU/e interface with regards to IT security incident response. All IT security incidents (including abuse) related to TU/e can be reported to CERT@tue.

3.2. Constituency

Technische Universiteit Eindhoven (TU/e) or Eindhoven University of Technology, with all its organizations, employees and students.

3.3. Sponsorship and/or affiliation

CERT@tue is part of TU/e operations.

3.4. Authority

CERT@tue coordinates security incidents on behalf of TU/e and has no authority reaching further than that. CERT@tue is however expected to make operational recommendations in the course of its work. Such recommendations can include binding advice to block accounts, addresses or networks.
CERT@tue can obtain private contact information for individual employees or students without consultation with CVB, HRM or ESA during a critical incident.
CERT@tue can communicate directly to individual employees or students.

4. Policies

4.1. Types of incidents and level of support

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

4.2. Co-operation, interaction and disclosure of information

All incoming information is handled confidentially by CERT@tue , regardless of its priority.

Information that is evidently very sensitive in nature is only communicated in an encrypted fashion (see 2.8 above). When reporting an incident of very sensitive nature, please state so explicitly (e.g. by using the label VERY SENSITIVE in the subject field of e-mail) and use encryption as well.

CERT@tue will use the information you provide to help solve security incidents, as all CSIRTs should do. This means explicitly that the information will be distributed further only on a need-to-know base, and in an anonymized fashion.

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

CERT@tue does not report incidents to law enforcement, unless Dutch law requires so – as in the case of first-degree crime. Likewise, CERT@tue cooperates with law enforcement in the course of an official investigation only, meaning a court order is present, and in case a CERT@tue constituent requests that CERT@tue cooperates in an investigation. In the latter case, when a court order is absent, CERT@tue will only provide information on a need-to-know base.

4.3. Communication and authentication

See 2.8 above. Usage of encryption in all cases where sensitive information is involved is highly recommended.

4.4 Responsible disclosure

CERT@tue follows the guidelines outlined in our Responsible Disclosure Policy.
Responsible_Disclosure_Policy.pdf (tue.nl)

5. Services

5.1. Incident Response (Registration, Coordination, Triage, Resolution)

CERT@tue is responsible for the registration and coordination of information security incidents somehow involving their constituency (as defined in 3.2) . CERT@tue therefore handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency. CERT@tue will offer support and advice on request.

6. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CERT@tue assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.