CERT-HKU

The following profile of CERT-HKU has been established in adherence to RFC-2350.

1. Document Information

1.1. Date of Last Update:

This version is last updated on 16-11-2022.
(updated URL under 2.10)

1.2. Distribution List for Notifications

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

1.3. Locations where this Document May Be Found

The current version of this profile is always available by means of the public website of HKU and file-share of the Network and Information department of HKU (NID-HKU) and is furthermore available on request. Email notifications are sent to all HKU security team members.

2. Contact Information

2.1. Name of the Team

Full name: Computer Emergency Response Team Hogeschool voor de Kunsten Utrecht
Short name: CERT-HKU

2.2. Address

NID – HKU
Oudenoord 700
3513 EX Utrecht
Netherlands

2.3 Time Zone

* CET, Central European Time
GMT+1 (GMT+2 with DST or Summer Time, which starts on the last Sunday in March and ends on the last Sunday in October)

2.4. Telephone Number

+31 (0)30-2091209

2.5. Facsimile Number

None

2.6. Other Telecommunication

None

2.7. Electronic Mail Address

cert@hku.nl
This address can be used to report all security incidents to which relate to the CERT-HKU constituency, including copyright issues, spam and abuse.

2.8. Public Keys and Encryption Information

A public PGP key is not yet available on the public key servers.
For highly sensitive/confidential information, contact CERT-HKU.

2.9. Team Members

No information is provided about the CERT-HKU teammembers in public

2.10. Other Information

General information about the HKU, Privacy, Security and the responsible disclosure information can be found on https://www.hku.nl/privacy-statement-en-disclaimer

2.11. Points of Customer Contact

In any case use cert@hku.nl mail address, cert(at)hku.nl
Our regular response hours (local time, save public holidays in The Netherlands) are everday of the week from 08:30 - 18.00.
Outside these hours the CERT team can be reached by the general email adress.

3. Charter

3.1. Mission Statement

The mission of CERT HKU is to resolve IT security incidents related to their constituency (see 3.2), and to prevent such incidents from occurring.

3.2. Constituency

HKU University of the Arts Utrecht and institutions connected to HKU network
Domein: hku.nl

3.3. Sponsorship and/or Affiliation

CERT-HKU is embededded in the Network and Information Services department of HKU (NID-HKU)

3.4. Authority

CERT-HKU coordinates and resolves security incidents on behalf of HKU and is expected to make operational recommendations in dealing with security incidents. Such recommendations can include for instance blocking addresses or networks. The implementation of such recommendations is a responsibility of Network and Information Department.

4. Policies

4.1. Types of Incidents and Level of Support

CERT-HKU handles various types of security incidents. The level of support depends on the type of the incident and the severity as determined by CERT-HKU staff.

4.2. Co-operation, Interaction and Disclosure of Information

All incoming information is handled confidentially by CERT-HKU, regardless of its priority.
Information that is evidently very sensitive in nature is only communicated en stored in a secure environment, if necessary using encryption technologies.
CERT-HKU will use the information you provide to help solve security incidents. Information will only be distributed further to other teams and members on a need-to-know base, and preferably in an anonymized fashion.

4.3. Communication and Authentication

The preferred method of communication is via e-mail. 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.

5. Services

5.1 Incident Response (Triage, Coordination and Resolution)

CERT-HKU is responsible for the coordination of security incidents involving their constituency (as defined in 3.2). CERT-HKU therefore handles both the triage and coordination aspects. Furthermore CERT-HKU supports responsible administrators with incident resolution within the constituency

5.2. Proactive Activities

Prevention and preparation consists of all activities aimed at reducing the probability or impact of an incident for the constituents. CERT-HKU provides the constituents with current information and advice on new threats, and attacks which may have impact on their operations and builds awareness and skills of employees.

6 Incident Reporting Forms

There are no special forms required to report an incident.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CERT-HKU assumes no responsibility for errors