CERT-HR Service Description

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

1. Document Information

1.1. Date of Last Update

This is version 2, published March 9 2023

1.2. Distribution List for Notifications

The current version of this profile is always available on:

```
https://hr.nl/security
```

CERT-HR has been registered by SURFcert (http://cert.surfnet.nl/). This registration is maintained by SURFcert. One of the requirements for registration is to keep this RFC-2350 up-to-date. CERT-HR supports that requirement. Any specific questions or remarks please address to the CERT-HR mail address.

1.3. Locations where this Document May Be Found

The current version of this profile is always available on:

```
https://hr.nl/security
```

2. Contact Information

2.1. Name of the Team

CERT-HR , the CSIRT or CERT team for the Hogeschool Rotterdam, The Netherlands.

2.2. Address

Hogeschool Rotterdam

CERT-HR

Faciliteiten en Informatietechnologie (FIT)

Blaak 555

3011 GB ROTTERDAM

The Netherlands

2.3. Time Zone

GMT+1 (GMT+2 with DST, according to EC rules)

2.4. Telephone Number

+31 (0)10 794 4141

2.5. Facsimile Number

+31 (0)10 794 4369

2.6. Other Telecommunication

Not available.

2.7. Electronic Mail Address

`cert@hr.nl`

2.8. Public Keys and Encryption Information

PGP is currently only on request supported for secure communication. A CERT-HR public PGP key is available on: `https://pgp.surfnet.nl`

```
UserID:         HR-CERT (CERT Team Hogeschool Rotterdam) <cert@hr.nl>

KeyID :         B9B5A2BD

Fingerprint:    38A3 1C2C 218C F384 D08E 25DC 967C 1D5A B9B5 A2BD
                2023-01-25T13:29:58Z
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGPRLtYBDACzHIchxTXIm+FjKAsMea/hv+yUpS/mRVzut7RoeVrAYqR2ygbl
s2MoShCTBHSWJ3NldPLv4DwLC3WIj1osi5TRVUDP9D6Pl8sfAXA/T5NNU/wnCj+h
KxVpGfyeWeT64LoK81n68SY38aSBGKV1ROp6YL0ZxPHOMRX/eFMfvm90flKO5z5V
wTvQ+FeWspiYO6d5M3b7RU0ncxbvenSK2gL5MAVWDA4lLEdSvf+cAtFNiE+vlAkP
Eae23U0WT20N9TNji1ghK/aeqsQ5qZIGSt0zz1boobIIwYh6Jg1NTkdb/c7KSt4T
cFYnpsnh064Et2Jr8eCJ/NS+qZz1ZGyeImyiEQQGKGwFGfgMAFwCwb+n1pth186+
w/AD9vRCqXaUArEoAH1tEJs63QrI7nCYtgBYBnXQ6gE//vj1IFGphMEro+8BJZTf
x0j9hYkPAcup8nxIRwfSY6kH5IDK6j5ZwnisYwVukzW/YhuIwM03X/JPNyceBvN8
+7J82G3Cc76xDY0AEQEAAbQrQ0VSVCBUZWFtIEhvZ2VzY2hvb2wgUm90dGVyZGFt
IDxjZXJ0QGhyLm5sPokB1AQTAQoAPhYhBDijHCwhjPOE0I4l3JZ8HVq5taK9BQJj
0S7WAhsDBQkDwmcABQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEJZ8HVq5taK9
TCAL/ieA8IPvcg5y+G1qB6gdAQeW2VoqLH7WNNAYk9UHlY2mCByUE73hDGGga17I
msK2avlZv/+7WqF4E613PMm5jhnKpPhR9iJVfwaBwsEesSXWR9OvU0NvnrOUJBuX
5QK6xcsH1cCVlNwvBDASE6hqNCJbJcgyFRFLNmeOVLtg75Lsaref4hWuKh2sPjO1
rRITbtgPl3GBlca/hygeBKPM7mP9bJQdOEMutjt0ugQdnDBWfV8S2PUhvrMj3cDi
IAPaQl80iguLDSKSR6LOIlL6SiFgrSQQybN8SCLQo1XXGkH7mj92e+CMj4rcZXUz
8Mv5sXXjp3tdfo+ELopxRgFyfsPqhEjva39DmFvMev1EZ2zP97wZqVFtl2JIiaOX
0BaE2EHzI37u299JmWZuTp8fBSrKibqueWDkw0UacwohHeEjhAM0+mk9b6ImSzRg
7zy+u7UlJDr28TC8SIqk2KSgmIIZAJnkeVihcnSmxsfEBaU7kKTN88xHdVJa8biH
dXIahbkBjQRj0S7WAQwAuiKFwnXm/8lL2KG3Gz9VXdtZCE3Y5WBbuGhWpWPU86xo
t/Rtzn49NDPPbXv0XNN6Nhsg8Wd2UhxpxBGd4Fe9EJ4qg0fZJ5M+paN68cCzGHgf
XXN9bk3q8c3S15OqDpwpcY/dSvQp/1Zp4rdMA6qZ+DGeyMQcSYWYWM/YyVWd564O
60GwVsAeCC/gIU+dd6BKOB70oi/GGSobloONX2KLmmClfYtwOt4GzcnlqAfsRHD6
1bh/Zo4xfVMI/TZRAOg+BtcF+5bwcTbyv+lv7eD5SbISa3mFgfG7g0zoqCNCnwMU
UIVqBQU6f8XynK6BYmiG4+nn+VOTOHAsix437DxQQvSLQYWP6LpHbnbOLwipCJn4
gi5QCZB4ZxjqBh7W7HIYa7Wn4gNYzqxyPmRJSMh/F41CVEqm7it0RZJlKt97Mfq7
9E4yDHNDnRgJ3eljtmgVSh4wDi4QP+qidpwHgShqgWFbnVVnjfY6NRVREkSceMwP
4SRoZhzCKMVGuz/DSBPtABEBAAGJAbwEGAEKACYWIQQ4oxwsIYzzhNCOJdyWfB1a
ubWivQUCY9Eu1gIbDAUJA8JnAAAKCRCWfB1aubWivfz1C/4sy0wvzBbMsGO7Lk3x
dXljG9D5RgVBEfabASB6E4WDYjRqj/p/zV8xBOMV+dNU2mZWFtlb7Ki3b0cmZzcv
ATGocootT/YkEe+SfSvxWeHUVy7p9iBPgKYEYQTkDM8ps02zq+t+LT+XVPGAqnxB
OnnE3/L7ZkjFtg8OKcEokqukWK5PmzcSAS9USXdrFcvlyePVdvkYD0wt8THLFiEO
a5fyLgyOUZuMo3OZ63RgC7O93RH1cNDIs+2iE+UmFw2WRotF+cRj+ktrjFgTaRLI
KSIFqMRgr88Ier0gQ8V2CKHd2yS6hcXKUsQwiqO8pXoh/RfW4E2qo6GO+bUXC8yT
hbei+xBNoTuj7yd7DKaf1R30NVVNDYUU+2XBoXiRCyKPPxJImq4mr56EdbIsRjwp
pPfYZzxjcJhkmJpPckjdgImLrEAcEg/r47hgXmKQxWo0vkR4sB8EDyUO2lxrzRou
ZP0pmS/zOoxWGo96e7i+DccSR/RsE7o7Vmibdm6Hjr2wkjQ=
=9eqm
-----END PGP PUBLIC KEY BLOCK-----
```

Please use this key to encrypt messages sent to CERT-HR. Sign your message using your own key please. It helps if that key is verifiable using the public keyservers.

CERT-HR can sign messages using its PGP key. Individual team members may also use S/MIME.

2.9. Team Members

CERT-HR team members are drawn from the ranks of Hogeschool Rotterdam ICT professionals, contact information about individual team members is confidential. Further details to be found at:

https://hr.nl/security

2.10. Other Information

See `https://hr.nl/security`

2.11. Points of Customer Contact

Normal cases: Use CERT-HR mail address.

Regular response hours (local time, save public holidays in The Netherlands):

Monday-Friday: 08:00 - 17:30

EMERGENCY cases:

Use CERT-HR phone number with back-up of mail address for all details (putting **EMERGENCY** in subject line is recommended). The CERT-HR phone number is available at regular response hours.

3. Charter

3.1. Mission Statement

CERT-HR's mission is to coordinate the resolution of IT security incidents related to the Hogeschool Rotterdam (HR) and to help prevent such incidents from occurring. For the world, CERT-HR is the interface with regards to IT security incident response. All IT security incidents (including abuse) related to Hogeschool Rotterdam can be reported to CERT-HR.

3.2. Constituency

Hogeschool Rotterdam and institutions connected to the HR network, with all related students and employees.

3.3. Sponsorship and/or Affiliation

CERT-HR is part of Hogeschool Rotterdam Department for Facilities and IT (*Faciliteiten en Informatietechnologie (FIT)*).

3.4. Authority

The goal of CERT-HR is organisation-wide prevention and, in the case of information security incidents, remediary action. CERT-HR is also involved in external security incidents impacting students and employees of HR in any way. In such cases, the services of SURFcert are used. SURFcert is the organization supporting Dutch higher education providers in information security (incidents) and connecting them with CSIRTs worldwide.

Among others, CERT-HR has the following responsibilities:

- Detecting and documenting all information security incidents, coordinating mitigation, and supervising the resolution of issues that led to an incident or have been caused by an incident (or providing support to those tasked with the above).
- Educating and supporting network-/system administrators, developers, and users in matters involving information security.

In fulfilling the duties above, CERT-HR is authorized to isolate systems and (sub)networks when necessary.

4. Policies

4.1. Types of Incidents and Level of Support

All incidents are considered normal priority unless they are labelled EMERGENCY. CERT-HR itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to CERT-HR as EMERGENCY, but it is up to CERT-HR 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-HR by default, regardless of its priority.

Information that is evidently very sensitive in nature is only communicated and stored in a secure environment, if preferably using encryption technologies.

When reporting an incident of very sensitive nature, please state so explicitly (e.g. by using the label VERY SENSITIVE or using the appropriate Traffic Light Protocol (TLP) code in the subject field of e-mail) and, if possible, use encryption.

CERT-HR will use the information you provide to help solve security incidents, as all CSIRTs do or should do. This means explicitly that the information will be distributed further only on a need-to-know basis (TLP:AMBER), and preferably in an anonymized fashion.

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

CERT-HR does not report incidents to law enforcement, unless required by Dutch law (e.g. in the case of felonies). Likewise, CERT-HR cooperates with law enforcement in the course of an official investigation only, meaning a court order must be present, AND in case a CERT-HR constituent requests that CERT-HR cooperates in an investigation or formal report. In the latter case, when a court order is absent, CERT-HR will only provide information on a need-to-know basis.

4.3. Communication and Authentication

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

5. Services

5.1. Incident Response

HR-CERT will assist system administrators in handling the technical and organisational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1. Incident Triage

Assessment of incident reports in terms of validity and impact on the rest of the organisation’s network, systems and constituents.

5.1.2. Incident Coordination

CERT-HR is tasked with technical analysis into the cause(s) of an incident, reporting to organizational management (and, where necessary: partner organisations, law enforcement, etc.), and coordinating with the internal crisis team and relevant system administrators during mitigation.

5.1.3. Incident Resolution

CERT-HR is responsible for technical analysis (triage), coordination and reporting of information security incidents concerning Hogeschool Rotterdam in any form. Incident resolution is the responsibility of the relevant administrators, internally and externally.

5.2. Proactive Activities

CERT-HR advises its constituency and the organisation about recent vulnerabilities, best practices and trends with regards to information security, and other matters in computer/network security. CERT-HR performs constant monitoring, and can start investigations based on data therein.

Roles listed above are consulting roles; CERT-HR is not responsible for implementation.

6. Incident Reporting Forms

No standard incident reporting form available. Please refer to section 2 for ways to contact Hogeschool Rotterdam in the case of an incident.

7. Disclaimers

A generic disclaimer stating confidentiality and *need to know*-status of specific information is available below. In due cases this disclaimer will be adopted according to the nature of the incident and persons/organizations involved.

-------------start generic disclaimer------------------

<addressee>,

You are receiving this information due to your involvement in an incident dealt with by CERT-HR (https://hr.nl/security). You must treat this information as strictly confidential. Copies of this information in your possession (electronic and/or hard copy) must be stored in a manner which is not accessible to unauthorised third parties. If it should be necessary to further distribute this information in the process of handling the incident involved, this should be done on an individual basis, making use of this disclaimer and with a copy being sent to CERT-HR (cert@hr.nl).

-------------end generic disclaimer------------------