Hanzehogeschool
Groningen
University of Applied Sciences

Hanze-CSIRT

Service Description

(RFC-2350)

share your talent. move the world.

TLP	[TLP: WHITE] TLP: WHITE information may be distributed without restriction, subject to copyright controls
Version	2.1
Date	11-3-2021
Author	Arjen Sterenborg – Security Officer

Table of contents

1. About this document

Foreword: This document describes the Hanze-CSIRT services in compliance with the RFC 2350 document. RFC 2350 is an IETF Best Current Practice available at: https://www.ietf.org/rfc/rfc2350.txt

1.1. Date of last update

This is version 2.1, published March 11, 2021.

1.2. Distribution List for Notifications

There is no Distribution List, or other dissemination mechanism to inform of changes made to this document.

1.3. Locations where this document may be found

The current version of this document is available on the Hanzehogeschool Groningen (Hanze) public website, at the following location:
https://www.hanze.nl/nld/organisatie/stafbureau/informatisering/beveiliging-privacy/melden/meldpunt-datalekken-beveiligingsincidenten

1.4. Authenticating this document

Currently, no PGP-signed version of this document is available.

2. Contact information

2.1. Name of the Team

Short name: Hanze-CSIRT

Full name: Hanzehogeschool Groningen - Computer Security Incident Response Team

Hanze-CSIRT is the CERT or CSIRT team for Hanzehogeschool Groningen in The Netherlands

2.2. Address

Hanzehogeschool Groningen
Hanze-CSIRT
Zernikeplein 11
9747 AS Groningen

2.3. Time Zone

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

Hanze-CSIRT does not have a direct telephone number. You can contact the IT Supportdesk (050 595 4566) and they can redirect your call.

2.5. Facsimile Number

Not available

2.6. Other Telecommunication

Not Available

2.7. Electronic Mail Address

You can contact Hanze-CSIRT on the following mail address: csirt@org.hanze.nl
This address can be used to report all security incidents which relate to the **Hanze-CSIRT** constituency, including copyright issues, spam and abuse.

2.8. Public Keys and Encryption Information

Only PGP is currently supported for secure communication.

The Hanze-CSIRT public PGP key is available on the public keyservers.

Its key-id is 0xc4f42511cf1bb6bc and its fingerprint is

675C F256 A61C C653 B853 DB10 C4F4 2511 CF1B B6BC.

Please use this key to encrypt messages sent to Hanze-CSIRT. Sign your message using your own key please – it helps if that key is verifiable using the public keyservers.

Messages from Hanze-CSIRT will in due cases be signed using the same Hanze-CSIRT key. Its credentials can be checked by you on the public keyservers.

2.9. Team Members

The team members are drawn from the ranks of Hanze ICT professionals. No further information is provided about the Hanze-CSIRT team members in public.

2.10. Other information

No further information available

2.11. Point of Customer Contact

Normal cases: use Hanze-CSIRT mail address.
Normal response hours: Monday-Friday, 09:00-17:00 (except public holidays in The Netherlands).
Emergency cases: send e-mail with EMERGENCY in the subject line.

3. Charter

3.1. Mission Statement

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

3.2. Constituency

Hanzehogeschool Groningen, with all its organizations, employees and students.

3.3. Sponsorship and/or Affiliation

Hanze-CSIRT is part of the Hanzehogeschool Groningen

3.4. Authority

Hanze-CSIRT coordinates security incidents on behalf of their constituency and has no authority reaching further than that. Hanze-CSIRT is however expected to make operational recommendations in the course of their work. Such recommendations can include but are not limited to blocking accounts, addresses or networks. The implementation of such recommendations is not a responsibility of the team, but solely of those to whom the recommendations were made.

4. Policies

4.1. Type of Incidents and Level of Support

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

Information that is evidently very sensitive in nature is only communicated in an encrypted fashion. 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.

Hanze-CSIRT 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 base, and in an anonymized fashion.

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

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

4.3. Communication and Authentication

See 2.8 above. Usage of PGP in all cases where sensitive information is involved is highly recommended. In cases where there is doubt about the authenticity of information or its source, **Hanze-CSIRT** reserves the right to authenticate this by any (legal) means.

5. Services

5.1. Incident Response (Triage, Coordination and Resolution)

Hanze-CSIRT is responsible for the coordination of security incidents somehow involving their constituency (as defined in 3.2). **Hanze-CSIRT** therefore handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency – however **Hanze-CSIRT** will offer support and advice on request.

5.2. Proactive Activities

HANZE-CSIRT pro-actively advises their constituency in regard to recent vulnerabilities and trends in hacking/cracking.
HANZE-CSIRT advises **Hanzehogeschool Groningen** on matters of computer and network security. It can do so pro-actively in urgent cases, or on request.
Both roles are roles of consultancy: **Hanze-CSIRT** is not responsible for implementation.

6. Incident Reporting Forms

Not available.

7. Disclaimers

Not available