Windesheim CSIRT

Computer Security Incident Response Team

(RFC2350)

April 6, 2020

Description and mission statement of Windesheim CSIRT including all contact information

hogeschool Windesheim

Inhoudsopgave

1 Document information

1.1 Date of last Update

April 6, 2020

1.2 Distributionlist for notification

There is no active notification for updates.

1.3 Location where this document may be found

The most recent version of this CSIRT description document is available at:
URL: https://www.windesheim.com/disclaimer-and-security

A Dutch version is available at:
URL: https://www.windesheim.nl/disclaimer

Make sure you use the latest version.

2 Contact Information

2.1 Name of the team

Windesheim CSIRT : The Windesheim Computer Security Incident Response Team

2.2 Address

Visitors address
Windesheim CSIRT
Dienst bedrijfsvoering
IVT
Campus 2-6
8017 CA Zwolle
The Netherlands

Mail address
Windesheim CSIRT
Dienst Bedrijfsvoering
IVT
Postbus 10090
8000 GB Zwolle
The Netherlands

2.3 Time zone

Amsterdam (GMT +0100, en GMT +0200 from april till october)

2.4 Telephone Number

+31 88 469 90 70 (during office hours only)
Ask for the IVT Windesheim CSIRT.

2.5 Facsimile Number

2.6 Other telecommunication

2.7 E-mail address

CSIRT@windesheim.nl
security@windesheim.nl
abuse@windesheim.nl
cert@windesheim.nl

These mailboxes will be monitored by the employee on duty for the Windehein CSIRT.

2.8 Public Keys and other encryption information

2.9 Teammembers

The manager Infrastructure is in charge of the CSIRT team. Daily CSIRT services will be performed by members of the Infrastructure team who are also part of the CSIRT team. Other members of the CSIRT team are a legal advisor, a communication advisor and head of security.

2.10 Other information

2.11 Points of customer contact

The preferred method for contacting the Windesheim CSIRT is via e-mail CSIRT@windesheim.nl .This mailbox is monitored by the employee on duty. When you require immediate assistance please put “URGENT” in your subject line.

If it is not possible (or not advisable for security reasons) to use e-mail the Windesheim CSIRT can be reached by telephone during regular office hours. Please contact the Service Desk ICT tel +31 (0)88-4699070. They will forward the message or if confidentiality is an issue you may request that your call will be directly forwarded to the CSIRT officer on duty. In general CSIRT availability hours are also limited to regular office hours. (monday - friday 8.00 – 17.00).

3 Charter

3.1 Mission Statement

The purpose of the CSIRT is to coordinate the resolution of IT security incidents related to Windesheim and to help prevent such incidents from occurring by implementing proactive measures to reduce the risks of computer security incidents.

There are three areas of interest:
- Prevention
- Detection
- Correction

The Windesheim CSIRT focuses on (coordination) detection and correction and contributes to prevention through recommendations on possible vulnerabilities and threats.

Windesheim CSIRT monitors to detect security incidents and coordinates implementing a solution. It ensures the removal of the cause and recovery of the damage.

3.2 Constituency

The CSIRT Windesheim constituency are all Windesheim students en employees and is related to all ICT facilities offered by IVT.

However please note that, notwithstanding the above, CSIRT Windesheim services will be provided for Windesheim owned systems only.

3.3 Sponsorship and/or affiliation

CSIRT Windesheim is part of the university of applied sciences Windesheim. It is in close contact with SURFcert and different CSIRT teams within de Higher Education Community, united in SCIRT.

3.4 Authority

CSIRT Windesheim operates under auspices of, and with authority delegated by, the Manager IVT.
During the time of an incident the CSIRT team has full authority to take any action deemed necessary to minimize the impact of an incident.

When it comes to taking preventive measures to improve the security situation in the organization, there is a shared responsibility. In this case, the CSIRT team will make recommendations to improve the situation. The CSIRT is involved in the decision making process but does not decide on its own.

The CSIRT Windesheim expects to work cooperatively with system administrators and users at Windesheim, and will try to avoid an authoritarian attitude. However, should it be necessary the CSIRT will not fail to use the authority it has been granted.

All members of the CSIRT staff are employees of Windesheim, are bound to confidentiality, are familiar with and act according to the integrity code of practice for ICT workers.

They will also act in accordance with the current information security policies and regulations and the “ICT regulations for employees and students”.

Employees or students of Windesheim who would like to oppose the actions taken by the CSIRT should contact the Manager IVT.

4 Policies

4.1 Types of incidents and level of support

CSIRT Windesheim is authorized to address all types of computer security incidents which occur, or threaten to occur, at Windesheim.

The level of support given by the CSIRT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the CSIRT resources at the time, though in all cases some response will be made within one working day.

If an incident is to be treated with high priority, the reporter must label the incident as “URGENT”. The CSIRT team reserves the right to change priorities.

Reporters of vulnerabilities will receive a message that their report has been received, but no message whether and when the vulnerability concerned has been remedied, unless the report proceeds in accordance with the responsible disclosure procedure.

4.2 Cooperation, interaction and disclosure of information

All incoming information is considered confidential and will be dealt with accordingly by the CSIRT team.

CSIRT Windesheim will use the information provided to help solve security incidents. Information will be stored in a secure environment and will be distributed only on a need-to-know base, and if possible in an anonymized fashion.

CSIRT Windesheim cooperates with law enforcement in the course of an official investigation only, meaning a court order is present.

4.3 Communication and Authentication

For normal communication not containing sensitive information CSIRT Windesheim might use conventional methods like unencrypted e/mail. For secure communication PKI encrypted e-mail or telephone will be used. If it is necessary to authenticate a person before communicating, this can be done either through existing webs of trust or by other methods like call-back, mail-back or even face-to-face meeting if necessary.

Preferred method of communication is through e-mail.

5 Services

5.1 Incident Response

Windesheim CSIRT supports the handling of security incidents and takes care of both the technical and organizational aspects..

5.1.1 Incident Triage

5.1.2 Incident coordination

5.1.3 Incident Resolution

5.2 Proactive activities

CSIRT Windesheim pro-actively informs system administrators and functional management of recent vulnerabilities and trends in hacking/cracking and advises Windesheim on matters of computer and network security. In both these cases CSIRT Windesheim operates as a consultant and is not responsible for implementation.

It is responsible for monitoring the quality of the monitoring activities performed by the infrastructure team and initiates security audits on a regular base.

6 Incident Reporting forms

External: Not available.

For Windesheim students and employees through https://serviceplein.windesheim.nl

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 disclaimer>

You are receiving this information due to your involvement in an incident dealt with by CSIRT Windesheim. 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 unauthorized 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 CSIRT Windesheim.

<end disclaimer>