Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

RFC-2350

The following profile of NCSC-NL has been established in adherence to RFC-2350.

01-07-2026

Veilig vooruit in een digitaal weerbaar Nederland

Contents

1. Document Information 3

1.1. Date of Last Update 3
1.2. Distribution List for Notifications 3
1.3. Locations where this Document May Be Found 3

2. Contact Information 4

2.1. Name of the Team 4
2.2. Address 4
2.3. Time Zone 4
2.4. Telephone Number 4
2.5. Facsimile Number 4
2.6. Other Telecommunication 4
2.7. Electronic Mail Address 4
2.8. Public Keys and Encryption Information 4
2.9. Team Members 4
2.10. Other Information 5
2.11. Points of Customer Contact 5

3. Charter 6

3.1. Mission Statement 6
3.2. Constituency 6
3.3. Sponsorship and/or Affiliation 6
3.4. Authority 7

4. Policies 8

4.1. Types of Incidents and Level of Support 8
4.2. Co-operation, Interaction and Disclosure of Information 8
4.3. Communication and Authentication 8

5. Services 9

5.1. Incident Response 9
5.1.1. Incident Triage 9
5.1.2. Incident Coordination 9
5.1.3. Incident Resolution 9
5.2. Proactive Activities 9

6. Incident Reporting Forms 10
7. Disclaimers 11

1. Document Information

1.1. Date of Last Update

This is version 1.0 of July, 2026.

1.2. Distribution List for Notifications

Changes to this document are not distributed by a mailing list. Any specific questions or remarks please address to the NCSC-NL mail address.

1.3. Locations where this Document May Be Found

The current version of this profile is always available on:
https://www.ncsc.nl/organisatie/operational-framework.html

2. Contact Information

2.1. Name of the Team

Nationaal Cyber Security Centrum (National Cyber Security Centre)

2.2. Address

NCSC
PO Box 117
2501 CC The Hague
The Netherlands

2.3. Time Zone

- CET, Central European Time (also known as Middle European Time) (UTC+01:00, between last Sunday in October and last Sunday in March)
- CEST (sometimes referred also as CEDT), Central European Summer Time (UTC+02:00, between last Sunday in March and last Sunday in October)

2.4. Telephone Number

The general telephone number during office hours: (070) 751 55 55
The 24/7 emergency telephone number for incidents: +31 (0)70 751 55 75

2.5. Facsimile Number

None

2.6. Other Telecommunication

None

2.7. Electronic Mail Address

For general matters: info(at)ncsc.nl
For incidents: cert(at)ncsc.nl

2.8. Public Keys and Encryption Information

NCSC-NL uses PGP for digital signatures and to receive encrypted information. Every calender year a new team key will be generated. The key is available on public PGP/GPG keyservers and at:
https://www.ncsc.nl/english/organisation/contact/pgp-key.html

2.9. Team Members

A full list of NCSC-NL team members is not publicly available. Team members will identify themselves to the reporting party with their full name in an official communication regarding an incident.

2.10. Other Information

General information about the National Cyber Security Centre in English is available at:
https://www.ncsc.nl/en

2.11. Points of Customer Contact

In any case use NCSC-NL mail address, info(at)ncsc.nl. In case of an incident cert(at)ncsc.nl.
Our regular response hours (local time) are everyday of the week from 07:30 – 21:30. Outside these hours the Duty Officer is available for incidents and can be reached at +31 (0)70 751 55 75

3. Charter

3.1. Mission Statement

NCSC-NL's vision and mission statement are defined in the National Cyber Security Strategy of The Netherlands. The operations are detailed in the NCSC-NL's strategic plan and are reviewed annually as part of the planning and control cycle of the Dutch government. A brief summary of the goal of NCSC-NL:

NCSC-NL is the National Cyber Security Centre in The Netherlands. The NCSC, acting within it's statutory scope, collects information, knowledge and expertise, which will help improve understanding of developments, cyberthreats, incidents and vulnerabilities, monitor and analyse such threats, signals trends and help parties deal with incidentmanagement and make decisions in crises. The main tasks include:

- Coordination in case of network and information systems related incidents such as malware spreading, cyberthreats and vulnerabilities in applications and hardware;
- Proactive action to prevent network and information systems related incidents or to prepare for such incidents and reduce the impact.

3.2. Constituency

The constituency of NCSC-NL in the Netherlands consists of organizations covered by the Dutch Cybersecurity Act (Cbw) implementing the NIS2 Directive. These entities have both obligations, such as incident reporting and duty of care, and rights, including access to NCSC-NL assistance.
Following the integration with the Digital Trust Center (DTC), NCSC-NL also serves SMEs. Non-NIS2 SMEs may report incidents voluntarily but are not subject to mandatory obligations and are generally not entitled to the same level of assistance.

3.3. Sponsorship and/or Affiliation

The National Cyber Security Centre of The Netherlands (NCSC-NL) is the center for expertise on cyber security and incident response of the Dutch government. It is aimed at preventing network and information systems related incidents and coordinates response to these incidents.
As from January 1, 2019, NCSC-NL is no longer part of the National Coordinator for Security and Counterterrorism (NCTV), but became a separate agency under the Ministry of Justice and Security.
As from July 1, 2026 NCSC-NL consists of a general director and four separate directorates, focused on;
1. Strategy, Governance and Internal Operations;
2. Digital Resilience Collaboration;
3. Prevention and Intervention;
4. Digital, Tech and Data.

3.4. Authority

The main purpose in incident handling is the coordination of incident response. As such, we advise constituents and have no authority to demand certain actions.

4. Policies

4.1. Types of Incidents and Level of Support

NCSC-NL handles various types of security incidents. The level of support is determined case-by-case by NCSC-NL, based on factors such as the type of incident and severity.

4.2. Co-operation, Interaction and Disclosure of Information

All incoming information is handled confidentially by NCSC-NL, regardless of its priority. Information that is evidently very sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies.
NCSC-NL 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.
NCSC-NL understands the Traffic Light Protocol (TLP) for sharing sensitive information.

4.3. Communication and Authentication

The preferred method of communication is via e-mail. When the content is sensitive enough or requires authentication, the NCSC-NL PGP key is used for signing e-mail messages. All sensitive communication to NCSC-NL should be encrypted against the team's PGP key.

5. Services

Incident response provides 24/7 availability to coordinate recovery from all types of network and information systems related incidents and consists of expertise, tools and other capabilities to act, analyze and communicate with stakeholders and media.

5.1. Incident Response

5.1.1. Incident Triage

- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.

5.1.2. Incident Coordination

- Determining the initial cause of the incident.
- Facilitating contact with other sites which may be involved.
- Communicate with stakeholders and media

5.1.3. Incident Resolution

- Providing advice to the reporting party that will help removing the vulnerabilities that caused the incident and securing the systems from the effects of the incidents.
- Evaluating which actions are most suitable to provide desired results regarding the incident resolution.
- Provide assistance in evidence collection and data interpretation when needed.

5.2. Proactive Activities

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

6. Incident Reporting Forms

Incident melden | NCSC

7. Disclaimers

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

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ ncsc_nl

juli 2026