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

1. Document Information

1.1. Date of Last Update
This is version 2.1 of Jan 24, 2017.

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

2.2. Address
NCSC
PO Box 20301
2500 EH The Hague
The Netherlands

2.3. Time Zone
* CET, Central European Time
  (UTC+1, between last Sunday in October and last Sunday in March)
* CEST (also CET DST), Central European Summer Time
  (UTC+2, between last Sunday in March and last Sunday in October)

2.4. Telephone Number
+31 (0)70 751 55 75

2.5. Facsimile Number
None

2.6. Other Telecommunication
None

2.7. Electronic Mail Address
cert(at)ncsc.nl

2.8. Public Keys and Encryption Information
NCSC uses PGP for digital signatures and to receive encrypted information. 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/english/organisation/

2.11. Points of Customer Contact
In any case use NCSC-NL mail address, cert(at)ncsc.nl
Our regular response hours (local time) are everyday of the week from 07:00 - 22.00. 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. Public and private parties, acting within their statutory scope, collect information, knowledge and expertise in the National Cyber Security Centre, which will help improve understanding of developments, threats, and trends and help parties deal with incidents and make decisions in crises. The main tasks include:

- Coordination in case of ICT related incidents such as data leakage, computer viruses, hacking and vulnerabilities in applications and hardware;
- Proactive action to prevent ICT 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 central government organizations, private organization with a 100% public assignment (publicly funded) or organizations in the Dutch critical infrastructure.

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 ICT and internet related incidents and coordinates response to these incidents.

NCSC-NL is established on 1 January 2012 and incorporates the activities of GOVCERT.NL. GOVCERT.NL was established in 2002 as CERT-RO and operates to

deal with computer security problems and their prevention, within its constituency. CERT-RO has been renamed into GOVCERT.NL as of 01-02-2003.

NCSC-NL is part of the Ministry of Security and Justice and consists of a general manager and 3teams for incident response, knowledge services and organizational development. National Coordinator for Security and Counterterrorism (NCTV) at the Ministry is commissioner for NCSCNL.

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 depends on the type of the incident and the severity as determined by NCSC-NL staff.

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 en 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 ICT related incidents and consists of expertise, tools and other capabilities to act, analyze and communicate with stakeholders and media.

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

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, NCSC-NL assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.