

RFC-2350

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

1. Document Information

1.1. Date of Last Update

This is version 1.0 of Oct 25 2010.

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 GOVCERT.NL mail address.

1.3. Locations where this Document May Be Found

The current version of this profile is always available on:

<http://www.govcert.nl/organisatie/Operational+framework>

2. Contact Information

2.1. Name of the Team

GOVCERT.NL is the Computer Emergency Response Team for the Dutch Government.

2.2. Address

GOVCERT.NL

PO Box Postbus 117

2501 CC 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)70 888 75 75

2.5. Facsimile Number

+31 (0)70 888 75 50

2.6. Other Telecommunication

None

2.7. Electronic Mail Address

cert(at)govcert.nl

2.8. Public Keys and Encryption Information

GOVCERT.NL uses PGP for digital signatures and to receive encrypted information. The key is available on public PGP/GPG key servers and at <http://www.govcert.nl/render.html?it=43>. Information about the key:

Key-ID: 0xC3D62A13

Fingerprint: D9FD 6FED 14C3 754A C8D6 600A FF3B E8D4 C3D6 2A13

2.9. Team Members

A full list of GOVCERT.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 GOVCERT.NL in English is available at <http://www.govcert.nl/render.html?it=41>

2.11. Points of Customer Contact

In any case use GOVCERT mail address, [cert\(at\)govcert.nl](mailto:cert(at)govcert.nl)

Our regular response hours (local time, save public holidays in The Netherlands) are everyday of the week from 09:00 - 21.00.

Outside these hours the Duty Officer is available for incidents and can be reached at +31 (70) 888 75 75

3. Charter

3.1. Mission Statement

GOVCERT.NL is the Computer Emergency Response Team for the Dutch Government. Since 2002 they support the government in preventing and dealing with ICT related security incidents. Our 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 (Dutch) Government Computer Emergency Response Team (GOVCERT.NL) is the computer incident response team of the Dutch government. It is aimed at preventing ICT and internet related incidents and coordinates response to these incidents.

GOVCERT.NL also operates the public alerting service Waarschuwingsdienst.nl, aimed at small businesses and public.

3.3. Sponsorship and/or Affiliation

GOVCERT.NL is part of the Ministry of Internal Affairs and Kingdom Relationship and consist of a general manager and 3 teams for incident response, expertise center and new services. Directorate General DRI at the Ministry is commissioner for GOVCERT.NL.

3.4. Authority

GOVCERT.NL's 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

GOVCERT.NL handles various types of security incidents. The level of support depends on the type of the incident and the severity as determined by GOVCERT.NL staff.

4.2. Co-operation, Interaction and Disclosure of Information

All incoming information is handled confidentially by GOVCERT.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.

GOVCERT.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.

GOVCERT.NL understands the Traffic Light Protocol (TLP) for classifying 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 GOVCERT.NL PGP key is used for signing e-mail messages. All sensitive communication to GOVCERT.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, analyse 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

GOVCERT.NL informs their constituency with advisories, factsheets and whitepapers to prevent ICT related incidents or to prepare for such incidents and reduce the impact.

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