

## Operational Framework GOVCERT.NL

Version 3 August 2011

### Introduction

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 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.

GOVCERT.NL is part of the Ministry of Security and Justice and consist of a general manager and 3 teams for incident response, expertise center and new services. National Coordinator for Counterterrorism and Security at the Ministry is commissioner for GOVCERT.NL.

This Framework describes GOVCERT.NL, its organization, and the basic operational policies. Specific procedures are detailed in separated documents.

GOVCERT.NL provides 4 basic services for the constituency:

- Incident Prevention (e.g. security advisories, alerts, training, exercises, ..)
- Incident Response (24x7 availability for incident reporting and coordination)
- Monitoring ( 12x7 active watch, network monitoring, ...)
- Knowledge Sharing (Best practices, factsheets, symposium, ...)

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

This document, called operational framework, brings together the agreed basic principles and conditions under which GOVCERT.NL operates.

### Goal and mission

GOVCERT.NL's vision and mission statement are defined in GOVCERT.NL's strategic plan and are reviewed annually as part of the planning and control cyclus of the Dutch government. A brief summary of the goal of GOVCERT.NL:

*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.*

## Membership

Membership of GOVCERT.NL is open to any government organization or private organization with a 100% public assignment (publicly funded). New members must apply to GOVCERT.NL and a mutual agreement must be signed. A membership fee is mandatory for all members except the central government departments, for which a government funded budget is available.

Some of the best practices and factsheets are also available for non-members via the website [www.govcert.nl](http://www.govcert.nl).

Alerting service Waarschuwingsdienst is free for all via the public website [www.waarschuwingsdienst.nl](http://www.waarschuwingsdienst.nl). Registration is needed if citizens want to receive risk alerts via e-mail or text messages. This is also free of charge.

## Services

Services of GOVCERT.NL are described in the *products and services catalog* and the conditions are set down in the *standard conditions*. A summary is published on the website [www.govcert.nl](http://www.govcert.nl):

*GOVCERT.NL focuses on four main areas: monitoring, knowledge exchange, prevention and incident handling.*

- *Monitoring consists of all activities aimed at providing a current and accurate picture of threats and vulnerabilities. GOVCERT.NL analyses open and closed sources 12/7 for new threats to ICT-systems and infrastructures and relevant developments. GOVCERT.NL has arrangements with CERTs across the globe to cover the other 12/7 in a follow the sun way. Automated sensor systems are developed and deployed to provide operational and tactical information on attacks.*
- *Knowledge exchange consists of acquiring and sharing the necessary knowledge to fulfill the main tasks. Knowledge exchange is aimed at strengthening the capabilities of the constituency and the CERT-community to prevent and respond to incidents. White papers and factsheets are published to share best practices and threat information. Tools built to facilitate GOVCERT.NL's processes are shared with the CERT-community to help set up and mature incident response organizations. Through ISACs GOVCERT.NL shares knowledge with organizations in the vital infrastructure in The Netherlands.*
- *Prevention and preparation consists of all activities aimed at reducing the probability or impact of an incident for the constituents. GOVCERT.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.*

*GOVCERT.NL provides alerts and practical advise to the public and small enterprises via the alerting service [Waarschuwingsdienst.nl](http://Waarschuwingsdienst.nl).*

- *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.*

*Within these areas, they offer a range of additional services:*

- *International exchange of knowledge: ICT security does not stop at the border. In order to keep up the quality of their services, GOVCERT.NL deems it important to co-operate and exchange information on an international level. That is why we are part of an extensive international network.*
- *Data bank: GOVCERT.NL is an information centre. It provides participants access to the knowledge and experience of their staff and constituency. Furthermore, they encourage the exchange of information among these organizations. Their data bank facilitates exchange by means of mailing lists, an archive of relevant documents and best practices.*
- *Forums: GOVCERT.NL organizes regular meetings to give participants and incident response teams in The Netherlands the opportunity to exchange knowledge and ideas on current affairs.*

## **National Partnerships**

In the national context, GOVCERT.NL works together with National Police (KLPD), Intelligence Service (AIVD), National Infrastructure against Cyber Crime (NICC), Dutch Telecom Authority (OPTA), Dutch internet service providers and other incident response teams in The Netherlands. GOVCERT.NL works together with the banking sector in handling phishing sites. Furthermore GOVCERT.NL participates in Information Sharing and Analysis Centers with organizations in the critical infrastructures.

## **International partnerships**

GOVCERT.NL is part of an extensive network of affiliated organizations, mainly other Computer Emergency Response Teams (CERTs). Since this network is a vital information hub, we find it is just as important to make our expertise available to other teams as it is to benefit from the knowledge of the international CERT community.

Our aim is to achieve maximum results with minimum means, and international collaboration is one way to realize this. That is why GOVCERT.NL encourages the development of shared standards and specialization in different areas. Our primary networks:

- EGC – European Governmental CERTs, in which GOVCERT.NL holds a prominent position
- FIRST – Forum of Incident Response and Security Teams, which consists of 150 CERTs worldwide

- TERENA – Trans-European Research and Education Networks Association, lobby of European national academic networks
- I4 – International Information Integrity Institute, a co-operative in the field of security, including private sector participants
- ISF – Information Security Forum, a co-operative in the field of security consisting of various international organizations

## Point of contact arrangements

The GOVCERT.NL point of contact arrangements have been established to provide a framework for sharing information about serious and time critical computer threats, vulnerabilities or incidents for the constituency.

At all times, urgent incident related can be shared with GOVCERT.NL via e-mail to [cert@govcert.nl](mailto:cert@govcert.nl). Other questions or information can be sent to [info@govcert.nl](mailto:info@govcert.nl).

Other relevant contact information are shared in the CIIP-directory, the RfC2350 info on [www.govcert.nl](http://www.govcert.nl) and the Trusted Introducer service of TERENA.

## Organization

The organization of GOVCERT.NL is defined in *Rapport inzake de organisatie en formatie van de GBO.Overheid*.

## Policies

GOVCERT.NL handling of information is subject to *Voorschrift Informatiebeveiliging Rijksdienst* and all correlated or more specific policies for Dutch Government. Additionally, GOVCERT.NL is subject to the information security policies of the Ministry of Internal Affairs and Kingdom Relationships and to more specific policies of GOVCERT.NL itself. The policies are part of the review and audit cycle of Dutch Government.

GOVCERT.NL has a press officer, to answer questions of media. The press officer of GOVCERT.NL operates within the PR-policies of the Ministry of Internal Affairs and Kingdom Relationships and Logius.

## Amendments to GOVCERT.NL operational framework

Amendments to this Operational Framework must be approved by the General Manager of GOVCERT.NL.