SURFcert Reports: Operational Framework SURFcert

Updated -8-4-2015

Author/Source	: Wim Biemolt / SURFnet BV	Index	:	R-92-01
Distribution	: SURFnet Constituency	Page	:	1
Classification	: External	Version	:	4
Subject	: Operational Framework SURFcert	Date	:	08 april 2015

1. INTRODUCTION

The (Dutch) SURFnet Computer Emergency Response Team (SURFcert) was established and operates to deal with computer security problems and their prevention, within its constituency.

SURFcert was earlier known as CERT-NL (1992-2003) and SURFnet-CERT (2004-2007) before it was finally renamed in 2007.

SURFcert consists of a Kernel of Members, and a Chairman.

This Framework describes SURFcert, its organization, and the basic operational policies. The FIRST Operational Framework served as one of the leading documents [FIRST]. Specific procedures are detailed in separated documents.

The field of security can be divided into three main topics:

- prevention
- repression
- correction

SURFcert will concentrate mainly on the repression and correction topics. By means of general education, SURFcert will give preventing recommendations concerning vulnerabilities.

This Framework does not contain the names of people for the functions mentioned. This information is available as an annex to this document, also containing contact information.

2. DEFINITIONS

SURFnet bv:	The company responsible for the computer network (called SURFnet) for research and higher education in the Netherlands, located in Utrecht.
SURFnet:	The computer network for research and higher education.
SURFnet Connected Institution:	Institution or person, having a valid use agreement with SURFnet bv.
SURFcert	The Dutch Computer Emergency Response Team, coordinated by SURFnet bv.
Chairman:	This person chairs the SURFcert. The SURFcert Chairman is participating in FIRST.
Member:	A person inside the SURFcert Kernel, appointed by the SURFnet bv management.
Kernel:	SURFcert is operated by the Kernel. The Kernel consists of the Chairman and the Members.
Secretariat:	The Secretariat of SURFcert is operated by the secretariat of SURFnet bv.
Site Security Contact:	The person responsible for the computer cq. network security within the SURFnet Connected Institution. Abbreviated to SSC.
Constituency:	The SURFcert Constituency are those sites who are connected to SURFnet.
Incident:	An event that has actual or potentially adverse effects on computer or network operations resulting in fraud, waste, or abuse; compromise of information; or loss or damage of property of information. Examples include penetration of a computer system, exploitation of technical vulnerabilities, or introduction of computer viruses or other forms of malicious software.
FIRST:	The Forum on Incident Response and Security Teams, the parent CERT organization.

3. PURPOSE and GOALS OF SURFcert

The primary purpose of SURFcert is to provide a mechanism for institutions within the Netherlands, connected to SURFnet, to deal with computer security problems and their prevention.

The goals of SURFcert are:

- To handle security incidents and solve security problems (assist where necessary).
- To educate in a general sense (give general recommendations to system managers and users, by means of information distribution).

4. SURFcert Kernel and SSCs

4.1 SURFcert Kernel

The Kernel will consist of one chairman and a number of Members. Members are employed by their individual organizations. Those organisations will receive reimbursement for the work a Member is doing for SURFcert. Members are obliged to maintain a log book on all their work carried out on behalf of SURFcert, for the purpose of gathering detailed information on security incidents.

The minimum number of Members in the Kernel is initially set to 5, the maximum number of members is yet to be determined. The Kernel will remain as small as possible, to keep it manageable.

New, possible Members, could be asked for a screening by the Ministry of Internal Affairs (Ministerie van Binnenlandse Zaken) when nominated. In case of a negative advice from the AIVD (the Dutch General Intelligence and Security Service) the nomination can be revoked.

Membership of the Kernel can be voluntary terminated at any time the Member may wish to leave the Kernel. Participation may be revoked for non- compliance with this Operational Framework, lack of cooperation, or failure to contribute to the purpose and goals of SURFcert by the SURFnet bv management, after having heard the Kernel for advice.

4.2 Site Security Contact

Each institution within the constituency of SURFcert already has an "Instellings Coordinator" (English: Technical Site Coordinator), whose name, address, telephone number, email address and FAX number are registered by the SURFnet Secretariat.

Each Site Security Contact can have one or more backups. A department (e.g., the operations group of a computing center) can not be a Site Security Contact, it should be a real person. The emergency phone within an institution may be operated by a group of persons. The number of backups to the SSC should not be larger than 3, to keep it manageable.

5. GENERAL COORDINATION AND ORGANIZATION

The general coordination of SURFcert will be provided by the SURFnet bv management. The Secretariat will carry out the administrative work for SURFcert. The Kernel consists of one Chairman and several Members. The Chairman acts as an advisor to the SURFnet bv management.

The Chairman shall be responsible for general operating policy, procedure, and related matters affecting SURFcert as a whole. The Chairman is working with SURFnet bv and is appointed by the SURFnet bv management.

Membership of the Kernel is on a personal basis and can last as long as the Member:

- does not voluntary terminates his or her membership

or

- is not revoked.

A Member is always working within an institution belonging to the Constituency of SURFcert.

The Kernel can establish Ad Hoc Committees, if and when necessary. These Ad Hoc Committees will always be devoted to computer cq. network security. Its chairman, membership and operating procedures will be decided on during a Kernel meeting. An Ad Hoc Committee can exist of Members and external experts. Ad Hoc Committees are responsible towards the Kernel. The outcome of an Ad Hoc Committee has the status of a recommendation towards the Kernel.

6. INFORMATION GATHERING AND DISTRIBUTION

The Chairman will be on all email distribution lists for security related information and will forward it to the appropriate lists. Several email distribution lists will be maintained by the Chairman:

cert-kernel	Chair and Members of Kernel
cert-sep	Site Security Contacts and teams

Furthermore, the email address "cert" has been created (cert@surfnet.nl) to reach SURFcert by email. Email send to cert@surfnet.nl will be reacted upon within 24 hours of receipt.

7. CONTACTING SURFcert and TECHNICAL PROVISIONS

SURFcert will be reachable using:

- telephone,
- email,
- snailmail

from every individual inside or outside The Netherlands. The Chairman is responsible for maintaining excellent reachability and for advertising the various ways to contact SURFcert.

There is a three stage priority level defined, with communication means attached to it:

- Normal priority: The preferred way of communicating with SURFcert will be either using email or using snailmail. Response to messages entering through this preferred way will be within 24 hours of receipt.
- High priority: During office hours (09:00 hrs - 17:00 hrs) on working days telephone calls can be placed to the SURFnet HelpDesk. The HelpDeskers will have full instruction on how to deal with these high priority SURFcert calls. This instruction includes the immediate forwarding of such a call to the Chairman or to a Member.
- Extremely high priority: In order to maintain a 7 * 24 reachability of SURFcert for severe incidents a special telephone number will be used, which will be known amongst the Members, the Site Security Contacts and the other FIRST Member CERTs. This telephone number will be routed to a Member, who will function as the entry point for extremely high priority problems. Any misuse of the "extremely high priority" status will be seriously dealt with within Kernel and the SURFnet bv management.

8. FUNDING

SURFnet bv will fund the work of the Secretariat and will fund the technical provisions needed in order to gain and maintain maximum reachability.

All expenses will be carried by the individual Member, whose institution will receive a contracted reimbursement.

9. OPERATIONAL ACTIVITIES AND POLICIES

9.1 Information classification

All SURFcert information and communications shall be provided security protection appropriate to the nature and sensitivity of the information involved. Therefore SURFcert uses three classes of information classification:

- INTERNAL CLASSIFIED
  This type of information will be disclosed within the Kernel. This type of information will also be disclosed to SURFnet bv management and among other FIRST Member CERTs on a need-to-know basis.
- INTERNAL UNCLASSIFIED
  This type of information may be disclosed within the Kernel, to the SURFnet bv management and to the Site Security Contacts and to other FIRST Member CERTs.
- EXTERNAL
  This type of information may be disclosed to the public and will therefore be impersonalised.

All Members must adhere to the information classification type specified by the originating source (the originating source is the Kernel person revealing the information to the entire Kernel). Each message (email, fax or snailmail) should always have a clearly stated originating source. Only the origination source may alter the information classification. Information without an information classification is considered to have the INTERNAL CLASSIFIED information classification.

The above means that information disclosed to any Kernel person will be disclosed inside the entire Kernel. This information however will always be handled INTERAL CLASSIFIED, unless otherwise stated.

The Members are employed and funded by their parent organizations. The SURFcert is an organization strictly for the purpose as listed in Chapter 2 of this Framework. SURFcert is not a legal entity.

Communication between Members and a Member and an SSC may be in Dutch. However, English is preferred in order to make communication to the FIRST and Member CERTs fast and easy.

9.2 Meetings

At least six times a year the Kernel will meet. One of these meetings will be shortly after the FIRST meeting in order to have a fast information dissemination from the FIRST meeting. Other meetings will be organized on appropriate occasions.

10. HANDLING OF SECURITY INCIDENTS

During the starting phase of SURFcert much effort will be put into the writing of "Security Incident Procedures". These Procedures will be as much in line with the procedures other FIRST Member CERTs may have as much as possible.

In these Procedures the following items will at least be covered:

- The liaison to the SURFnet Beheer Partners (SURFnet Operations Centers).
- What is requested from the SURFnet Beheer Partners.
- When and how to disconnect from the network.

11. AMENDMENTS TO SURFcert OPERATIONAL FRAMEWORK

Amendments to this Operational Framework must be approved by the SURFnet bv management, after having heard the SURFcert Kernel for advice.

BIBLIOGRAPHY

[FIRST] FIRST Operational Framework, FIRST, 1991.

SURFcert is the Computer Emergency Response Team for SURFnet customers. SURFnet is the Dutch network for educational, research and related institutes. SURFcert is a Full Member of the Forum of Incident Response and Security Teams (FIRST).

All SURFcert material is available under:

http://cert.surfnet.nl/

In case of computer or network security problems please contact your local CERT/security-team or SURFcert (if your institute is NOT a SURFnet customer please address the appropriate (local) CERT/security-team).

SURFcert is one/two hour(s) ahead of UTC (GMT) in summer/winter,
i.e. UTC+0100 in summer and UTC+0200 in winter (DST).

Email: cert@surfnet.nl
Phone: +31 88 7873000
Snailmail: SURFnet bv
Attn. SURFcert
P.O. Box 19035
NL - 3501 DA UTRECHT
The Netherlands

A 7 * 24 hours phone number is available to SURFnet SSC's and FIRST members on request.