UM-CERT
Revised description/organisation of CSIRT UM

Date 1st version	**Registration number**	**Author**	**Change management**
31 October 2005	ICTS/IS-2006-00128	Bart van den Heuvel	CISO (Bart van den Heuvel)

Status: DEFINITIVE

Distribution of document	Draft: ICTS, DO-ICT, LO-L, Decision-making: Executive Board Definitive: http://www.maastrichtuniversity.nl/informationsecurity and http://www.maastrichtuniversity.nl/um-cert

Version	**Date**	**Description of change**
1.0	November 1994	Foundation documents for CERT-RL: Electronically available as scanned document: IS-2005-00217. This document is replaced in its entirety by the new one.
2.0	4 July 2006	New structure and new name (UM), update MAASnet rules and regulations, changes to information security organisation, CSIRT-standards etc.
2.1	1 January 2013	Actualization of addresses, phone-numbers, layout etc.

UM-CERT
Operational model for a CSIRT

Contents

UM-CERT
Operational model for a CSIRT

1. Introduction

This document describes the operational model for UM-CERT: the Computer Security Incident Response Team of Universiteit Maastricht. UM-CERT is more than just a new name for the CERT-RL team, which has been in existence since 1994. It stands for a new organisational model, focused on current developments in the area of information security incidents and in the area of the ICT and information security organisation for UM.
This document describes the objective, tasks, powers, responsibilities and position of UM-CERT within the organisation. In addition, the primary operational activities and reachability of UM-CERT are further fleshed out. In large part, these are based on existing operational procedures and the internal UM organisation as well as models of (inter)nationally comparable institutions.
UM-CERT focuses primarily on the coordination of various activities following up on information security incidents: corrective measures and, when necessary, collecting evidence, measures to limit further damage, and communication and information in that regard.

2. Background

CERT and CSIRT

Since the mid-1990s, the fast pace of international developments with regard to research networks and the Internet has been accompanied by a rise in the number of information security incidents and related threats. Organisations with links to the Internet therefore found themselves in need of an effective internal organisation in order to counter the threat of security incidents.
The name originally given to such an internal organisation was ‘Computer Emergency Response Team’: ‘CERT’. However, ‘CERT’ is a registered trademark of MIT in Boston, which means that this acronym can no longer be used on its own outside MIT. The internationally accepted name is now ‘Computer Security Incident Response Team’: CSIRT. For historical reasons, many CSIRT organisations have retained the acronym CERT in their name, which explains the name ‘UM-CERT’.
In 1998, the international RFC2350 standard was established with the aim of introducing some degree of uniformity regarding CSIRTs. An RFC-2350 description is also available for UM-CERT at: HTTP://www.maastrichtuniversity.nl/um-cert.

From CERT-RL to UM-CERT: the CSIRT of Universiteit Maastricht

In 1994, SURFnet took on the task of establishing a CSIRT (or CERT as it was then still called) in the Netherlands: CERT-NL. Following this, the Rijksuniversiteit Limburg, currently Universiteit Maastricht, established its own CERT in November 1994: CERT-RL[1].

Particularly during the first years of CERT-RL’s existence, the number of incidents which occurred was rather limited with a relatively modest impact on the university's operations. However, many of the individual incidents represented a new kind of problem, which meant that a great deal of time and discussion was necessary within CERT-RL to deal with them.

[1] CERT-RL was established by the then ‘steering committee on security’, which in terms of composition was comparable to the present Coordinating Directors’ Board (CBB). The original document, ‘CERT-RL; operational model computer emergency response team Rijksuniversiteit Limburg’, dated November 1994, is available in the ICTS digital archive under number IS-2005-00217.

Since 2000, as the frequency of Internet use increased, the number of incidents has risen steeply, but the nature of the incidents involved had an increasingly standardised fingerprint, and their impact was still relatively limited. Between 2000 and 2003, most of the incidents were dealt with by the ICTS (ICT Service Centre) operational department: the systems and networks teams, with a shift to standard actions by the Service Desk.

In 2002, however, two things happened: several serious incidents took place, and UM management recognised that Information Security could no longer be approached in an incident-driven fashion but had to be anchored within the framework of institutional policy and the organisation of information flows at UM. A start was made in that regard in 2002, which led to the establishment of a formal Information Security policy[2], the formal appointment of a policy officer for information security[3] and the launch of a UM-wide information security programme in the autumn of 2002. It was also recognised that CERT-RL needed a major update. As incidents were being dealt with relatively easily in terms of operations, it was decided not to give priority to this at the time. In 2002, the name was simply changed to UM-CERT, and a reference to the existing CERT was also included in the "MAASnet UM USAGE AND MANAGEMENT CONDITIONS" (Version 1, authorised on 6 May 2002).

The most important reasons for taking action now to redefine the nature of UM-CERT as a CSIRT for UM are:

- Anchoring the system within the information security organisation
- Dividing tasks and responsibilities based on the type of incident:
  - Standard incidents (Service Desk)
  - More complex incidents with greater impact (ad hoc team)
  - Specific incidents involving confidentiality, the law etc. (CISO)
- Modifying the team's composition to take into account modified tasks, responsibilities and profile, linkage of systems and networks etc.:
  - More attention on collecting evidence (forensic investigation)
  - Profile based on expertise rather than on target group (geographic)
  - Multidisciplinary ad hoc teams for each (non-standard) incident
- Compliance with (inter)national standards.

[2] Documents related to information security policy, the organizational model and the supplementary house rules and policies which have been adopted in the meantime can be found on the website: http://www.maastrichtuniversity.nl/informationsecurity.

[3] The policy officer for information security is referred to as: "Central Information Security Officer" or CISO.

3. Objective and target group

The primary objective of UM-CERT is to provide a platform which enables UM to respond effectively to information security incidents – proactively, during or immediately after an incident is discovered, as well as in a preventive fashion. Activities are not only corrective in nature but may sometimes also focus on the collection of evidence. UM-CERT's target group is Universiteit Maastricht as well as all other persons and bodies connected to the MAASnet institutional network.
Although UM-CERT's primary focus is on the central UM infrastructure and thereby the continuity of operational activities, the activities also include all workstations, users and information (systems) which utilise UM facilities in any way whatsoever.

4. Tasks, powers and responsibilities

The primary task of UM-CERT is ensuring the operational continuity of a central coordination point and associated background organisation for dealing with and preventing computer and network security incidents (in short: security incidents) involving its target group. To coordinate matters outside the framework of its immediate target group, UM-CERT works closely together with SURFnet-CERT, the national umbrella organisation within SURFnet. UM-CERT's responsibilities include:

- Dealing with security incidents as they occur in accordance with relevant procedures within ICTS;
- Analysing and, if necessary, proactively distributing incoming security recommendations of general interest (such as the security advisories of SURFnet-CERT or government warning services) and making them available in a centralised fashion;
- Whenever necessary, coordinating actions to be taken in case of security incidents;
- Actually (helping in) resolving security problems by:
    - Analysis and documentation of the problem
    - Cleaning out compromised systems
    - Protecting or isolating compromised (sub)systems
    - Collecting evidence
- Educating system and network managers and computer users by providing relevant information;
- (Providing advice with regard to) developing and distributing supporting materials.

Generally speaking, the members of UM-CERT will be able to carry out their tasks within the framework of normal daily UM operations and usually also within the framework of their own position in the organisation, while taking into account the generally accepted procedures, consultative structures, line responsibilities and mandates. This also means that the necessary powers are either assigned on an individual basis and/or specifically authorised beforehand and that the associated responsibilities have been set down.

UM-CERT can provide recommendations regarding the desired or necessary modifications in implementations, configurations etc. The actual implementation of these recommendations is part of the regular job responsibilities of the central and decentralised managers and line management. These modifications therefore also need to be introduced into the procedures set out for the unit involved in terms of incident, change and problem management.

In addition, the merits of UM-CERT include the power – if there are adequate security-based reasons for doing so – to take the following actions whenever appropriate without consulting end users, ICT managers or responsible line officials:

- excluding systems and users from the network;
- disconnecting or isolating (sub)systems or network components;
- recording and authenticating traffic data and other data;
- ensuring safekeeping and authentication of systems owned by UM.

UM-CERT must register these actions and communicate them to the managers or users involved, while taking into account the relevant provisions set down in article 5 of the MAASnet Acceptable Use Policy; this is necessary to allow justification of the procedure followed after the fact.

All permanent members of UM-CERT must sign a written document confirming that they will comply with the Integrity and Behaviour Code for ICT staff at UM. The registration process involved here is the responsibility of the ICTS Director, in accordance with his[4] mandate, on behalf of the Executive Board. If members of UM-CERT call on the help of third parties, they must inform the third parties that the Integrity and Behaviour Code for ICT staff at UM serves as a set of compulsory work instructions for all activities carried out under the responsibility of UM-CERT.

5. Position and anchoring within the UM organisation

UM-CERT is part of the UM information security organisation[5]. UM-CERT is accountable to the portfolio holder for operations within the Executive Board; the strategic policy framework of UM-CERT is part of the agenda of the Coordinating Directors' Board (*CBB*).

Tactical and operational matters concerning UM-CERT will be dealt with by the Consultation Body for Information Security (‘*DO-IS*’)[6].
In case of calamities, UM-CERT has direct access to the responsible portfolio holder and thereby the highest administrative level within the university.

Within the information security organisation, a conscious decision was also taken to include the UM-CERT chairpersonship as part of the job description of the CISO (see footnote 3) in order to ensure a permanent link between UM policy in the area of information security and the operational activities with regard to incident management.

Within the framework of day-to-day affairs, UM-CERT’s activities fall under the responsibility of the ICTS director in accordance with the UM regulations on mandates.
The members of UM-CERT continue their regular work activities at their UM units. They carry out their UM-CERT activities as a recognised additional work activity, which receives the highest possible priority (comparable to emergency assistance such as first aid, fire

[4] In this document, the term ‘he/him/his’ is a gender-neutral description that includes ‘she/her’.
[5] Adopted in 2002: see http://www.maastrichtuniversity.nl/informationsecurity.
[6] At the time of adoption of this document by the Executive Board, the tasks of DO-IS are being handled by the Consultation Body for ICT (‘DO-ICT’).

fighting etc.). In other words, if the conditions warrant it, they will immediately make time for all necessary and relevant activities within the framework of UM-CERT. When acting in their role as UM-CERT members, they are therefore directly accountable in the hierarchy to (the relevant portfolio holder of) the Executive Board, with the director of ICTS being the only authorised representative responsible.

The UM-CERT reports periodically to the portfolio holder of the Executive Board via an annual report. In addition, UM-CERT can also report to the DO-IS about its activities and findings on a regular basis.

6. External coordination and contacts

Hundreds of CSIRTs are active on a global level. Nearly 200 of the large and/or umbrella type of CSIRTs are members of FIRST (Forum on Incident and Response Security Teams), which is aimed at providing the member CSIRTs with a platform for ensuring fast, easy and reliable mutual communication.
SURFnet-CERT operates on a national level as a CSIRT for the SURF target group, and is therefore intended to serve as a platform for information exchange on security incidents for all institutions connected to SURFnet. SURFnet-CERT is a member of FIRST and, on a national level, works together primarily with the Dutch government CSIRT: GOVCERT.NL

UM-CERT positions itself as a local CSIRT within SURFnet. The above can be schematically summarised as follows:

FIRST	global level (association of CSIRTs)
↓ ↑	
SURFnet-CERT	umbrella level (CSIRT for SURF target group)
↓ ↑	
UM-CERT	institutional level (CSIRT for UM)

UM-CERT has registered a Security Entry Point (SEP)[7] with SURFnet. SURFnet-CERT differentiates three lines of communication within the SEP registration:

- The Site Security Contact (SSC), for primarily organisational matters;
- The Security Entry Point (SEP), for all incident-related matters;
- An e-mail address for the Security Advisories.

[7] SURFnet-CERT uses a Security Entry Point (SEP) registration, which includes information that should not be allowed to become generally available (such as emergency and private telephone numbers). The SEP registration information is available only on the UM-CERT intranet.

7. Team composition

In addition to the chairperson, UM-CERT consists of five core members, selected on the basis of a primary focus on the central infrastructure, and a maximum of five additional members selected for their specific expertise. The Executive Board has set out the following combinations of necessary expertise for the core members and the expert members:

CORE MEMBERS:

- Chairperson, also SSC for SURFnet: CISO;
- Incident manager, also responsible for SURFnet SEP: Service Desk team leader;
- Expert in the area of Concern Information systems;
- System manager for Central Server systems;
- Network manager;
- Expert in the standardisation of workstation operating systems (standard desktop).

EXPERT MEMBERS:

- Technical (operating) systems specialist for central server systems;
- Technical network specialist;
- Technical (operating) systems specialist standard desktop;
- Technical (operating) systems specialist for decentralised server systems;
- Technical (operating) systems specialist for decentralised workstations.

A UM-CERT member is appointed by the Director of ICTS, in accordance with the UM regulations on mandates, on the basis of specific expertise in the above areas of attention Membership is accepted on a voluntary basis, to the extent that such is not implicitly linked to the actual position of the candidate. In light of the common university interest involved, the administrative unit do not receive compensation for membership activities (comparable to in-house emergency assistants). For the individual UM-CERT members, the normal schemes for overtime compensation and leave compensation apply.

A UM-CERT member can be removed from his position by the ICTS Director at any time. UM-CERT members take on the obligation of maintaining a logbook, in which they record all the activities carried out for UM-CERT.

If so desired, UM-CERT can put together an ad hoc committee to focus on a specific, urgent security problem. External experts can be members of such an ad hoc committee. Committee members must comply with the “Integrity and Behaviour Code for ICT staff at UM” and other UM-CERT guidelines and work procedures. A conclusion reached by the ad hoc committee will be viewed as a recommendation presented to the UM-CERT core members.

8. Contacting UM-CERT

Easy reachability is a basic condition for ensuring effective performance of UM-CERT. UM-CERT can be reached as follows:

- Internal e-mail: **UM-CERT-L@maastrichtuniversity.nl**
- Alternative external e-mail: UM-CERT@maastrichtuniversity.nl
- ICTS Service Desk telephone: +31 (0)43-3885555 during opening hours see http://www.maastrichtuniversity.nl/icts
- Fax: +31 (0)43-3885566
- Post: c/o ICT Service Centre, P.O. Box 616, 6200 MD Maastricht, Netherlands

Three priority levels have been defined for reporting security incidents and for contacting UM-CERT in general, each of which is linked to a specific technical communication resource or procedure.

Normal priority

Communication regarding security incidents with normal priority is preferably done via e-mail. Generally speaking, UM-CERT will respond within 24 hours after receiving such e-mail messages.

High priority

During the opening hours of the ICTS Service Desk, UM-CERT can be contacted by telephone for high-priority security incidents. The Service Desk has been given instructions on how to deal with such reports; directly putting through the call to a UM-CERT member is part of these instructions.
An emergency phone number is available at the ICTS Service Desk for UM-CERT members, the Executive Board portfolio holder, the ICTS Director and SURFnet-CERT. In addition, the UM persons involved have each other's private and mobile phone numbers.

Very high priority

As yet, UM-CERT is not directly available outside regular ICTS Service Desk opening hours or during collective leave days and recognised holidays. In case of serious security incidents outside office hours, the UM-CERT members can only be called in via the mediation of line management.

9. Communication and classification

All UM-CERT information and communication is archived and made available, taking into account the origin and confidentiality of the information involved. To this end, UM-CERT applies three levels of classification:

INTERNAL CLASSIFIED INFORMATION:

UM-CERT will make internal information available only for UM-CERT members, the Executive Board portfolio holder and the ICTS Director via a protected Electronic Community: "UM_CERT". Examples include private and mobile phone numbers, the updated

list of CERT members, confidential documents which have not yet been released for general use, etc.
All other forms of mutual communication will take place via e-mail. As soon as technological options are available for user-friendly and location/computer-independent encryption technology, such technology will be used for confidential e-mails.
Internal information, such as reports/minutes of UM-CERT meetings, can also be made available on a 'need to know' basis to persons outside UM-CERT.
In those cases where internal classified information is communicated outside the framework of UM-CERT and top management, such information will be accompanied by a disclaimer explaining the confidentiality and "need to know" status.

EXTERNAL CLASSIFIED INFORMATION:

This involves information which is exchanged with the individual external CSIRTs, the SURFnet Site Security Contacts and the internal (information) security officers at UM (DO-IS, DO-ICT and FD/AVM). With all these groups, (implicit) agreements are in place to the effect that each group will treat information from the other groups confidentially and that such information will be made available to other parties only on a "need to know" basis.
Communication generally takes place via e-mail.
In the above cases, any information supplied will also be accompanied by a disclaimer explaining the confidentiality and "need to know" status.
Any relevant associated files are stored in the Electronic Community as internal confidential files, as such files do not generally include a disclaimer in the file itself.

NON-CLASSIFIED PUBLIC INFORMATION:

UM-CERT will publish public information which specifically relates to UM-CERT on the website http://www.maastrichtuniversity.nl/um-cert .
In accordance with ICTS operational procedures, derived information (for example security advisories) will be published on existing specific support pages, such as the LO-Portal, and/or will be sent to existing specific mailing lists, such as UM-LO-L, by e-mail.

10. Internal operational procedures

The activities carried out by UM-CERT are generally incident-driven. Depending on the nature and impact of the incident, these activities are partly implemented outside normal UM office hours during times when line management is not normally available. This means that such activities cannot be carried out pursuant to strict formal procedures and a pragmatic approach will be employed. UM-CERT members will act in accordance with the work instructions below. Whenever necessary, some of the steps listed in these instructions will have to be carried out as soon as possible after the incident has taken place.

1. As soon as an incident is received by a UM-CERT member, based on that member's UM-CERT membership, feedback will be given to the person reporting the incident that:
    a. the incident will be dealt with within the framework of UM-CERT as of that moment. Continue on to step 2.
    b. the incident must be reported in accordance with normal incident procedures (generally to ICTS). The report is registered as "not justified", and the case is closed.

2. Relevant actions will be taken (depending on one's own judgment, immediately or not) in accordance with the objective, tasks and powers of UM-CERT.
3. A brief summary of the actions taken will be recorded, including:
    a. Date and time;
    b. UM-CERT members, line management and, when relevant, third parties involved;
    c. Nature of the action taken (collecting information, exchanging information, modifying configuration etc.).
4. The incident is reported to the ICTS Service Desk if that has not yet been done.
5. The incident is communicated via UM-CERT-L if that has not yet been done.
6. Working and communication agreements are made with at least one other UM-CERT member and/or with line management, in accordance with the following order of priority:
    a. UM-CERT member;
    b. ICTS Director;
    c. Executive Board portfolio holder;
    d. Own line manager;
    e. Line management of administrative unit involved, if relevant.
7. Depending on the nature and impact of the incident, the UM-CERT members and line management involved at that point in time decide to inform and/or involve the other parties in the order listed above.
8. The follow-up activities demanded by the incident are carried out and registered.
9. The incident is registered in accordance with the following guidelines:
    a. Standard, non-classified: within ICTS incident registration;
    b. UM Internal classified:
        - minimally anonymous and, if necessary, stripped of other information on nature and impact within ICTS incident registration;
        - other information within UM-CERT community, with ICTS ticket number as reference.
        - if necessary, copies of information and loggings will be stored in the confidential ICTS archive with the highest level of confidentiality after being initialled by the persons dealing with them and scanned for inclusion in the ICTS document registration system.

The UM-CERT members meet at least four times a year. The minutes of these meetings will be provided to the ICTS Director and the Executive Board portfolio holder. In addition, (parts of) these minutes may be communicated on a “need to know” basis in accordance with the guidelines in chapter 9.

APPENDIX 1: Proposal for team composition

CONFIDENTIAL!!!

(stored on the protected section of the UM-CERT community)

APPENDIX 2: Internal contact details and SEP registration for SURFnet(-CERT)

CONFIDENTIAL!!!

======= SEP registration Universiteit Maastricht ===========
The SEP is formed by our ICTS Service Desk.
The alarm number listed is our INTERNAL EMERGENCY NUMBER and should therefore be used only for real emergencies; it may NEVER BE COMMUNICATED to other relations. For other relations and for more normal operational matters, the following phone numbers apply (in addition to e-mail):
Service Desk: +31 (0)43-3885555
Secretariat: +31 (0)43-3885511
(1) name of institution: Universiteit Maastricht
(2) abbreviation of the SEP: UM-CERT
(3) e-mail address: Servicedesk-ICTS@maastrichtuniversity.nl
(4) advisory e-mail address: Servicedesk-ICTS@maastrichtuniversity.nl
(5) telephone number (during office hours): +31 (0)43-3885555
(6) emergency number:
during "Service Desk" hours: **CONFIDENTIAL**
24/7 (still under discussion): for the time being **CONFIDENTIAL** (mobile number CISO)
(7) fax number: +31 (0)43-3885566
(8) postal address: Universiteit Maastricht
Attn: UM-CERT, Bart van den Heuvel, ICTS
P.O.Box 616
6200 MD MAASTRICHT

SSC: 1) Bart van den Heuvel: Bart.vandenHeuvel@maastrichtuniversity.nl
Telephone: +31 (0)43-3885526 / 3885511
Fax: +31 (0)43-3885566
2) Jo Weijers: J.Weijers@maastrichtuniversity.nl
Telephone: +31 (0)43-3885504 / 3885511
Fax: +31 (0)43-3885566

For the sake of completeness:
For reporting incidents of abuse, the following address is also available:
abuse@maastrichtuniversity.nl (the Service Desk)
UM-CERT can be contacted via:
UM-CERT@maastrichtuniversity.nl (a mailing list)
======= End of SEP registration Universiteit Maastricht ===========

Internal numbers still need to be filled in on the protected section of the UM-CERT community.

APPENDIX 3: Disclaimer

If necessary, UM-CERT makes use of disclaimers, in accordance with the guidelines presented in chapter 9, to ensure the confidentiality of information. In some cases, a disclaimer will have to be adapted to specific situations (e.g. when naming specific addressees) and be presented in Dutch and/or English.
Several standard disclaimers will be placed on the protected section of the UM-CERT community.

The general template for disclaimers is:

<Addressee>,

You are receiving this information due to your involvement in an incident dealt with by UM-CERT (http://www.maastrichtuniversity.nl/um-cert). You must treat this information as strictly confidential. Copies of this information in your possession (electronic and/or hard copy) must be stored in a manner which is not accessible to unauthorised third parties. If it should be necessary to further distribute this information in the process of handling the incident involved, this should be done on an individual basis, making use of this disclaimer and with a copy being sent to UM-CERT.

APPENDIX 4: Line management UM-CERT members

CONFIDENTIAL!!!

(available in the protected section of the UM-CERT community)