Universiteit Maastricht > RFC-2350 Print

RFC-2350

following profile of UM-CERT has been established in adherence to RFC-2350.

1. Document Information

1.1. Date of Last Update

This is version 4.0 of Jan 1th 2013.

1.2. Distribution List for Notifications

The current version of this profile is always available on:

http://www.maastrichtuniversity.nl/um-cert

UM-CERT members and UM LISO's (Local Information Security Officers) are actively notified of updates to this framework.

UM-CERT is affiliated with SURFcert (http://www.surfnet.nl/surfcert CSIRT SURFnet B.V.) which requires notification of updates also to SURFcert.

Members of UM-CERT participate in SCIRT (SURFnet Community of Incident Response Teams)

Any specific questions or remarks please address to the UM-CERT mail address.

1.3. Locations where this Document May Be Found

The current version of this profile is always available on:

http://www.maastrichtuniversity.nl/um-cert

2. Contact Information

2.1. Name of the Team

UM-CERT, the CSIRT or CERT team for the Universiteit Maastricht (UM), The Netherlands.

2.2. Address

Universiteit Maastricht
UM-CERT
ICTS
P.O.Box 616
NL - 6200 MD MAASTRICHT
The Netherlands

2.3. Time Zone

GMT+1 (GMT+2 with DST, according to EC rules)

2.4. Telephone Number

+31 (0)43 3885555

2.5. Facsimile Number

+31 (0)43 3885566

2.6. Other Telecommunication

Not available.

2.7. Electronic Mail Address

um-cert@maastrichtuniversity.nl

2.8. Public Keys and Encryption Information

PGP is supported for secure communication, but on request only.

An UM-CERT public PGP key is not yet available on the public keyservers.

On request PGP-communication can be established through the Chair of UM-Cert:

L.C. van den Heuvel (Bart.vandenHeuvel@maastrichtuniversity.nl)

Public PGP key to be found on:

- http://pgp.surfnet.nl:11371/
- http://keyserver.pgp.com

Fingerprint=4C16 AB53 D038 5201 9D39 B7CF E7AD 4906 5159 4489

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.0

mQGiBEAGwHoRBAD08SGt0Qd9veRO/KgItrxrJ2Ze+gk8lnDy8ZmluWe0QDp4MEGHlMmQI9Iu
C1eEpXhf+fdtxTV2aB7DKa0kjxPdf4QGEOvzA0v9zY7CKi0K9850uHpZBzK6gRAiR3nTLxJ3
384THDphSKDKEzzsFjxPw0imqHTC76y+GfeZWb1xVQCg/7/eKZNMR3xPxM5FP7nCFwzyhKsE
AO+c++6IytKcOIgdABZx1IEG/kzlEMDsdeW6WdeREq6m6JYmVn0bimVqJb9Cg8Ezr1z23wv9
md//BkbZELpxk+uPR78VA0kcvwCVSuUCo7d0z/MXmi4rDOg/6MXTFxdFGTVnlnKxkvBBllQP
xBmxSXW4DR/A7iT1k6gp7jUXZiQYBADUPJVMqqC7kfA2cxGGQSicU2GGKcVsSN6SAdcljNn9
36y3MKFcENPs4CiDs046J8tg3RiBsfN0Jo5DuCbqHid1aip6TLxCCaV5OZFDUoP+v/dIYKC4
3h+Ka2Koa/v92sUGJbXcZGwwQMvsXvWt40PS8d4bAp+vZEP1HZZfqR2K7rQAiE4EEBECAA4F
AkAGwHwHCwkIBwMCCgAKCRDnrUkGUVlEiSbLAKDXyRS3vtYWeXKpPnwZogiLR8g4HACfbhrl
LOgg9M1QPJh3PGcB3U8eVDa0K2xjdmRoZXV2ZWwgaG90bWFpbCA8bGN2ZGhldXZlbEBob3Rt
YWlsLmNvbT6IVAQQEQIAFAUCSm8D9AcLCQgHAwIKBRsDAAAAAAoJEOetSQZRWUSJPBAAoNh+
t/GdZ+FCZxn+0vyUKAeUc6e4AJ0dI9zKcBXmNHXVZwxFZZYBSeRcrLQ3TC5DLiB2YW4gZGVu
IEhldXZlbCA8QmFydC52YW5kZW5IZXV2ZWxAaWN0cy51bmltYWFzLm5sPohMBBARAgAMBQJA
atmjBQMJZ1MAAAoJENeMvOVmp0sxSKMAn3hbTg/kb4HZenqSFUE8LvJZBc9gAKDRFw+HVrZI
Lu08dc08k6s1zVymvYhMBBARAgAMBQJAatnhBQMJZ1MAAAoJEDHKw8xgZxokrokAnjxk7Amo
K8uGBvA+hf0vrq6INkJYAKCEvBUGbY1dL52Q2btBeKC8+i4QC4hXBBARAgAXBQJABsB6BwsJ
CAcDAgoCGQEFGwMAAAAACgkQ561JBlFZRIlIWACdFQ5MDS/YPsiV2tgmV7QUChR8uCoAoO9a
aOf0JY95S2vngypn/YxZQsFoiFcEEBECABcFAkpu/TkHCwkIBwMCCgIZAAUbAwAAAAAKCRDn
rUkGUVlEiWlAAKDxYT8a2RZYSbUcPPQ+kNqAihwHWQCfRuY2PhgBqHyz3/9Y5941YAy+ct20
P0JhcnQgdmFuIGRlbiBIZXV2ZWwgPGJhcnQudmFuZGVuaGV1dmVsQG1hYXN0cmljaHR1bml2
ZXJzaXR5Lm5sPohXBBARAgAXBQJKbv05BwsJCAcDAgoCGQEFGwMAAAAACgkQ561JBlFZRInK
cACeMBD+L7fJzxc+SsozuILsUcf+YtcAn1CJstogeUvZQTxXdHE4jZ+eGuvWtFVIZXV2ZWwg
QmFydCB2YW4gZGVuIChJQ1RTKSA8L289VU5JTUFBUy9vdT1VTklNQUFTL2NuPVJlY2lwaWVu
dHMvY249QmFydC52YW5kZW5IZXV2ZWw+iFQEEBECABQFAkIVu2gHCwkIBwMCCgUbAwAAAAAK
```

```
CRDnrUkGUVlEiYBTAJ9JMEkysPYTS6e0EDNqInSK71a6RQCeOT59dYTgimioSlgVfRdqqFIi
Aaq5AgwEQAbAehAIAPZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65Szgg2gGnVqMU6Y9AVfPQ
B8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09jdvOmeFXklnN/biudE/F/Ha8g8VH
MGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brwv0YAWCvl9Ij9WE5J280gtJ3kkQc2azNsOA1F
HQ98iLMcfFstjvbzySPAQ/ClWxiNjrtVjLhdONM0/XwXV0OjHRhs3jMhLLUq/zzhsSlAGBGN
fISnCnLWhsQDGcgHKXrKlQzZlp+r0ApQmwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7DVekyCzsA
AgIH+J/F6T35shpG2IkWB4j34Ry8awCMQlcoCdqQqzlebUltwBr0ocxC79tlb8+VWu2hZASQ
67NKTL3UFko3u+H8Omau4cw2efchwdaj7joPNqPQBWWR/tz1wj5L2nnS9R95ZSUKvW5zNyai
FMW3NtqkR0ZXw5UrYk1shaBKfy08uGPefi4sl+86PxP66Ee67ba0Dz3oqvcTuIfltl/xWsIX
jYi8XdCekTTuybk6J9n0ms+ykpPNTU4zafQVWIC+9i2zNAXW2lWEO/XisNweAOHLO969gcJo
UfrsXr+pXwwRZ51N6j2XAn0pRq9dXC1Cdj5FqRpTlXW849GokzFcI4mvqIhMBBgRAgAMBQJA
BsB6BRsMAAAAAAoJEOetSQZRWUSJuwIAn1IGesbMVKnIH5ZWf6knS4Lv1ZdZAKD3DMaH+Efs
h+sEnhlQCc/WODb3tw==
=AI6N
-----END PGP PUBLIC KEY BLOCK-----
```

Please use this key to encrypt messages sent to UM-CERT. Sign your message using your own key please – it helps if that key is verifiable using the public keyservers.

In the near future messages from UM-CERT will in due cases be signed using the UM-CERT key. Its credentials will then be available on the public keyservers.

2.9. Team Members

UM-CERT team members are drawn from the ranks of UM ICT professionals, contact information about individual team members is confidential. Chair and secretary are provided by ICTS, the UM computational/networking centre. Further details to be found at http://www.maastrichtuniversity.nl/um-cert .

2.10. Other Information

See http://www.maastrichtuniversity.nl/informationsecurity and http://www.maastrichtuniversity.nl/icts

2.11. Points of Customer Contact

Normal cases: Use UM-CERT mail address.

Regular response hours (local time, save public holidays in The Netherlands):

Monday-Friday: 08:00 – 17:00

EMERGENCY cases:

Use UM-CERT phone number with back-up of mail address for all details (putting EMERGENCY in subject line is recommended). The UM-CERT phone number is available at regular response hours. The duty-officer (not a UM-CERT team member) decides if UM-CERT will be involved directly or not.

3. Charter

3.1. Mission Statement

UM-CERT’s mission is to coordinate the resolution of IT security incidents related to the Universiteit Maastricht (UM), and to help prevent such incidents from occurring.

For the world, UM-CERT is the UM interface with regards to IT security incident response. All IT security incidents (including abuse) related to UM can be reported to UM-CERT.

3.2. Constituency

Universiteit Maastricht (UM) and institutions connected to UM’s network , with all related students, Alumni and employees.

3.3. Sponsorship and/or Affiliation

UM-CERT is part of UM operations.

3.4. Authority

UM-CERT coordinates security incidents on behalf of UM and has no authority reaching further than that. UM-CERT is however expected to make operational recommendations in the course of its work. Such recommendations can include for instance blocking addresses or networks. The implementation of such recommendations is not a responsibility of UM-CERT however, but solely of those to whom the recommendations were made.

4. Policies

4.1. Types of Incidents and Level of Support

All incidents are considered normal priority unless they are labeled EMERGENCY. UM-CERT itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to UM-CERT as EMERGENCY, but it is up to UM-CERT to decide whether or not to uphold that status.

4.2. Co-operation, Interaction and Disclosure of Information

ALL incoming information is handled confidentially by UM-CERT, 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. When reporting an incident of very sensitive nature, please state so explicitly (e.g. by using the label VERY SENSITIVE in the subject field of e-mail) and if possible use encryption as well.

UM-CERT will use the information you provide to help solve security incidents, as all CSIRTs do or should do. This means explicitly that the information will be distributed further only on a need-to-know base, and preferably in an anonymized fashion.

If you object to this default behavior of UM-CERT, please make explicit what UM-CERT can do with the information you provide. UM-CERT will adhere to your policy, but will also point out to you if that means that UM-CERT cannot act on the information provided.

UM-CERT does not report incidents to law enforcement, unless Dutch law requires so – as in the case of first-degree crime. Likewise, UM-CERT cooperates with law enforcement in the course of an official investigation only, meaning a court order is present, AND in case a UM-CERT constituent requests that UM-CERT cooperates in an investigation or formal report. In the latter case, when a court order is absent, UM-CERT will only provide information on a need-to-know base.

4.3. Communication and Authentication

See 2.8 above. Usage of PGP in all cases where sensitive information is involved is highly recommended.

5. Services

5.1. Incident Response

5.1.1. Incident Triage

5.1.2. Incident Coordination

5.1.3. Incident Resolution

UM-CERT is responsible for the coordination of security incidents somehow involving UM. UM-CERT therefore handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within UM and externally.

5.2. Proactive Activities

UM-CERT pro-actively advises its constituency with regards to recent vulnerabilities and trends in hacking/cracking.

UM-CERT advises UM on matters of computer and network security. It can do so pro-actively in urgent cases, or on request.

Both roles are roles of consultancy – UM-CERT is not responsible for implementation.

6. Incident Reporting Forms

Not available. Incidents are reported in UM’s central IT-Incident registration system .

7. Disclaimers

A generic disclaimer stating confidentiality and “need to know”-status of specific information is available below. In due cases this disclaimer will be adopted according to the nature of the incident and persons/organizations involved.

-------------start generic disclaimer-----------------

<addressee>,

You are receiving this information due to your involvement in an incident dealt with by UM-CERT (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.

-------------end generic disclaimer-----------------