CCoP - CSIRT Code of Practice – *approved* version 2.1

v2.1/ Approved Version 15 September 2005

Andrew Cormack
Miroslaw Maj
Dave Parker
Don Stikvoort

NOTE:
This version 2.1 is an approved instance of "work in progress". More CSIRT service areas may be covered in later versions. It is however approved and useable in its current form – though not claiming completeness.

This document is set up as a Code of Practice for CSIRTs *and their members* in general.

This CCoP was adopted by the TI Accredited Teams at their Lisbon meeting on 15 September 2005, as a SHOULD criterium for accreditation. A SHOULD criterium is highly recommended to follow, but not obligatory. Every team specifies whether they chose to comply, or not – and they can change this choice along the way.

If and when an accredited team complies with this CCoP, then they acknowledge that they have read and understood this document and that their teams will comply with the MUST principles that are stated within it, and give proper attention to the SHOULD principles.

0. Definitions

0.1 "the team": the subject CSIRT evaluating this Code of Practice is referred to as "the team" below

0.2 "incident" should be read below as "computer/network security incident"

0.3 "incident management" is used below to identify the general CSIRT process, including all possible included or related services, ranging from pro-active auditing to repression – on purpose the terms "security management" and "risk management" are avoided since these are generalisations beyond the typical CSIRT scope

0.4 MUST below means: an absolute requirement – note that in some cases the MUST statement is conditioned by elements in the requirement

0.5 SHOULD below means: a strong recommendation, but not a MUST

1. Legal Requirements

1.1 *MUST* The team and its members are expected to comply with the legal requirements of their individual countries at all times whilst dealing with incident

management matters. [Where there is any conflict, this article always takes precedence over other principles stated in this document.]

1.2 *SHOULD* The team and its members will, to the best of their abilities, take into consideration the legal requirements of other countries when their activities have a cross-border component.

1.3 *SHOULD* In the event that requirement 1.1 leads to a conflict in itself as a result of contradicting legislation applicable to a specific event, the team will give precendence to those parts of the legislation that best reflect the team's professional assessment of how the matter at hand should be resolved.

2. The Team

2.1 *MUST* The team will, considering its own operational requirements, alert those sufficiently trusted peer CSIRTs, Vendors and organisations whose operations, or whose constituencies, are likely to be significantly affected by an event or omission known to the team.

2.2 *SHOULD* The team will in its operations act in such a way that it sets an example of responsible Internet and security behaviour.

3. Team Members

3.1 *MUST* The team will ensure that all of its members receive a paper and electronic copy of this document, and will ensure that they have read and understood it.

3.2 *SHOULD* The team will on a regular basis engage its members in discussions on the issues touched by this document – this to help ensure that the team members appreciate the issues at hand and are equipped to act accordingly.

4. Information Handling

4.1 *MUST* The team receiving or holding information, regardless of the subject matter, that may affect either another CSIRT team's constituency, the community of CSIRTs as a whole, or indeed the security of the Internet or users thereof, will handle this information responsibly and protect it against inadvertent disclosure to unauthorised parties.

4.2 *MUST* The team holding information valuable to other CSIRTs or Vendor Teams will give ample consideration to disclosing the information to the appropriate party, at the earliest opportunity, taking into consideration their own organisational

responsibilities and security requirements. Third party requirements, e.g. those of Vendors, for any disclosure or non-disclosure of the information will be acknowledged.

4.3 *MUST* As a general rule, any disclosure of information to other CSIRTs, Vendor Teams or other organisations, is done on a need-to-know basis, while protecting stakeholders in an incident as much as possible without turning the incident information into void information, not useable for incident handling by the receiving party.

4.4 *MUST* The security of the methods of storing and transmitting information inside or outside the team, will be appropriate to its sensitivity. In general this means that sensitive information will be kept and sent only in encrypted formats or over secure channels – this explicitly includes back-ups of sensitive information.

5. Service specific requirements

The below requirements only are applicable when the team offers the service involved.

5.1 Incident Handling

5.1.1 *MUST* Articles 2.1 and 4.* apply.

5.2 Vulnerability Handling

5.2.1a *MUST* The team actively involved in vulnerability research and disclosure processes will have documented procedures for the proper processing of such research and its results.

5.2.1b *SHOULD* Where appropriate, such procedures will be available for review both by Vendors, trusted peer CSIRTs, or – when appropriate – the CSIRT community as a whole.

5.2.2 *MUST* When the team becomes aware of a particular IT related vulnerability, from whatever source, the information will be handled as defined above under "Information Handling" and in accordance with the process documented under 5.2.1, throughout the entire research and disclosure process.

5.2.3 *MUST* Where appropriate, and considering the team's own security requirements, the details of the vulnerability and any associated research will be provided to the relevant vendor(s) for assessment and remediation at the earliest opportunity.

5.2.4 *SHOULD* The vendor(s) will be given every reasonable opportunity, consistent with the CSIRT's defined procedures, to complete their remediation processes relating to the vulnerability before any public disclosure by the team.