CCoP - CSIRT Code of Practice – version 2.3 final draft

v2.3 final draft / 2005-2017

Andrew Cormack
Klaus-Peter Kossakowski
Miroslaw Maj
Dave Parker
Don Stikvoort

NOTE:
This final draft version 2.3 is an updated and improved instance of the TF-CSIRT approved version 2.1 of 2005.

This document is set up as a Code of Practice for cyber security teams (CSIRTs, SOCs, etc) and their team members in general.

Version 2.1 of this CCoP was adopted by the TF-CSIRT/TI Accredited Teams at their meeting on 15 September 2005 in Lisbon, Portugal, as a SHOULD criterion for accreditation. A SHOULD criterion 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, they acknowledge that they have read and understood this document and that their team members will comply with the MUST principles that are stated within it, and give proper attention to the SHOULD principles.

This final draft version 2.3 will be presented to the TF-CSIRT/TI Accredited Teams on 15 May 2017 and distributed on 16 May 2017 with a request for final comments. The consolidated version 3.0 will be sent to the Accredited Teams no later than 20 August 2017, and be voted on in the TF-CSIRT/TI meeting in Stockholm on 21-22 September 2017.

1. Definitions

1.1 "incident" should be read as "information/cyber/computer/network security incident".

1.2 "vulnerability" should be read as any error/bug/hole/insufficiency in computers (including network devices, handhelds, appliances, etc) or the applications running on them, that can be exploited, potentially leading to incidents.

1.3 "incident management" is used to identify the general incident related process, including all possible included or related services, ranging from preparation and preventive measures, via detection and analysis, to resolution and finally lessons learnt. On purpose the terms "security management" and "risk management" have been avoided since these are generalisations beyond the typical scope for teams dealing with incidents.

1.4 "CSIRT" (Computer Security Incident Response Team) is used to mean all sorts of cyber security teams tasked with one or more aspects of incident management, such as CERTs, incident handling teams, cyber defence capabilities, SOCs, national cyber security centres, and also including PSIRTs (product security teams dealing with vulnerabilities).

1.5 "the team": the subject CSIRT evaluating this Code of Practice is referred to as "the team".

1.6 "team members" are all persons working for the team in whatever capability (employed, freelancer, voluntarily, part time, external consultant, liaison from other organisation, …) and therefore processing sensitive information available to the team

1.7 MUST: this word, or the terms 'REQUIRED' or 'SHALL', mean that the definition is an absolute requirement of the specification. (literally adopted from RfC-2119)

1.8 SHOULD: this word, or the adjective 'RECOMMENDED', mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. (literally adopted from RfC-2119)

2. Starting Points

2.1 *MUST* The cooperation in the global CSIRT community operates on the basis of peer-to-peer relationships without cost recovery. Wherever such peer-to-peer relationships exist, the team is expected to react to incident reports and inquiries by peers with due care.

2.2 *MUST* When the team is a member of a national CSIRT cooperation, or of a transnational cooperation such as TF-CSIRT, APCERT or FIRST, or of any other CSIRT cooperation, all other members of those cooperations are regarded as peers in the sense of 2.1, with the exception of the case where a cooperation is explicitly based on different standards.

2.3 *SHOULD* Any CSIRT or party acting as such, beyond those referred to in 2.2, who sends an incident report or inquiry, is to be given the benefit of the doubt and treated as peer in the sense of 2.1, when both their identity and report or inquiry appear to be valid, with the exception of the case where the relationship between both is different and bound by agreement.

3. Legal Requirements

3.1 *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.

3.2 *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.

3.3 *SHOULD* In the event that requirement 3.1 leads to a conflict in itself as a result of contradicting legislation applicable to a specific event, the team will give precedence to those parts of the legislation that best reflect the team's professional assessment of how the matter at hand should be resolved.

4. The Team

4.1 *MUST* The team will, considering its stated services towards its constituency, take appropriate incident management action when it is notified of an incident in its constituency.

4.2 *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.

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

5. Team Members

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

5.2 *SHOULD* The team will on a regular basis engage its team 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.

6. Information Handling

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

6.2 *MUST* The team holding information valuable to other CSIRTs will give due 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.

6.3 *MUST* As a general rule, any disclosure of information to other CSIRTs 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.

6.4 *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.

7. Vulnerability Handling Requirements

The below requirements are only applicable when the team operates a vulnerability handling service.

7.1a *MUST* The team actively involved in vulnerability research and responsible disclosure will have documented procedures for the proper processing of such research and its results.

7. 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.

7.2 *SHOULD* The team will publish their responsible disclosure practice, or spread it on a need-to-know basis, and encourage the adoption and use thereof.

7.3 *MUST* When the team becomes aware of a particular vulnerability, from whatever source, the information will be handled as defined above under "Information Handling" and in accordance with the process documented under 7.1, throughout the entire research and disclosure process.

7.4 *MUST* Where appropriate, and considering the team's 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.

7.5 *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.

7.6 *SHOULD* Any public disclosure of what could be considered critical vulnerabilities should not only follow the guideline of 7.4, but also the team should seek to achieve a coordinated effort within the CSIRT community – and especially any such disclosure should be done as a concerted and synchronised effort.