



**Appendix A :**  
**Standard definitions taken from the IETF approach [RFC2119]**

**MUST**

This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

**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.

## Appendix B : Information Template for “accredited” CSIRTs

**\*\*\* NOTE: please use the ASCII/text form B/D provided separately for filling out – not this form \*\*\***

The set of information a CSIRT needs to provide to acquire “accredited” status (and that it needs to maintain after that, in cooperation with the TI), consists of three parts:

- a mandatory part related to the CSIRT itself,
- an optional part related to the CSIRT itself
- a mandatory part related to the task of the TI.

The complete set of information will be published on the *restricted* TI web site, only for “accredited” CSIRTs to behold, and is marked ACCR below. Any exceptions to this rule are clearly marked below as:

- HIDDEN: these will not be published anywhere and stay within the TI (e.g. invoice address), or:
- PUBLIC: the sub-set of information that will be published on the *public* TI web site.

**\*\*\* NOTE: please use the ASCII/text form B/D provided separately for filling out – not this form \*\*\***

### Mandatory Fields describing the CSIRT

<b>CSIRT Name</b>	<b>PUBLIC</b>
-------------------	---------------

Official CSIRT name  
 Short CSIRT name (Acronym)  
 Host organisation (if the CSIRT is decentralised, list all host organisations)  
 Country the CSIRT is located in (if multiple offices exist, list all countries)  
 Date of establishment

<b>Constituency</b>	<b>PUBLIC</b>
---------------------	---------------

Type of constituency (vendor customer base, internal to host organization, ISP customer base, ...)  
 Description of constituency  
 Internet domain, AS numbers and/or IP address information describing the constituency  
 All countries in which constituency members are located in

<b>CSIRT Contact Information</b>	<b>PUBLIC</b>
----------------------------------	---------------

Regular telephone number (country code, telephone number, timezone)  
 Emergency telephone number (country code, telephone number, timezone)  
 Email address  
 Facsimile number (country code, telefax number)  
 Other telecommunication facilities  
 Postal address

<b>TI Specific Information</b>	<b>HIDDEN</b>
--------------------------------	---------------

E-mail address for subscription to ti-accr-teams mailing list (containing all accredited CSIRTs, meant for discussion on structural issues and for TI info dissemination)

Billing address for invoicing accredited CSIRTs (and accreditation candidates)  
 VAT number of your organisation if applicable

<b>Business Hours</b>	mixed :
Description of business hours	PUBLIC
Procedures for contacting the CSIRTs outside business hours	ACCR
<b>CSIRT Representatives</b>	ACCR
Name of primary person representing the CSIRT & Contact information	
Name of secondary person representing the CSIRT & Contact information (only two representatives can be administered in the database – however an unlimited amount of team members can be registered: see below)	
<b>References</b>	ACCR
Track record of working relationships with other CSIRTs	
<b>Services</b>	ACCR
[The following lists of services are only meant as examples.] Specify available reactive services, using the following list (or adding to it):	
<ul style="list-style-type: none"> <li>- vulnerability analysis</li> <li>- critter analysis</li> <li>- forensic analysis</li> <li>- incident response</li> <li>- incident response support</li> <li>- incident response coordination</li> <li>- vulnerability response coordination</li> </ul>	
Specify available proactive services, using the following list (or adding to it):	
<ul style="list-style-type: none"> <li>- announcements (intrusion and vulnerability warnings and advisories)</li> <li>- technology and trend watch</li> <li>- security audit and neighbourhood watch</li> <li>- configuration/maintenance of security tools</li> <li>- development of security tools</li> <li>- provision of intrusion detection services</li> </ul>	
Specify security quality management services, using the following list (or adding to it):	
<ul style="list-style-type: none"> <li>- risk analysis</li> <li>- business continuity planning</li> <li>- security consulting</li> <li>- awareness building and training</li> <li>- product evaluation</li> </ul>	
<b>Information handling policy</b>	ACCR
How is incoming information “tagged” or “classified”?	
How is information handled, especially with regards to exclusivity?	
What considerations are adopted for the disclosure of information (“when what?”), especially incident related information passed on to other CSIRTs or to sites?	
Are there legal considerations to take into account with regards to the information handling?	

<b>Cryptography</b>	mixed :
Policy on use of cryptography to shield confidentiality and integrity in archives and/or in datacommunication, especially e-mail. This policy must include possible legal boundary conditions as key escrow or enforceability of decryption in case of lawsuits.	ACCR
If encrypted e-mail is possible, then at least provide:	
▪ PGP <sup>1</sup> key of CSIRT Representative;	ACCR
▪ PGP "CSIRT" and / or "master" keys if applicable;	PUBLIC
▪ Provision of X.509 certificates (for S/MIME, etc.) is optional	PUBLIC
<b>FIRST Membership</b>	PUBLIC
Membership status (No member / FIRST Member/ FIRST Liaison)	
In case of Member or Liaison : date of member/liaisonship approval	

## Optional Fields describing the CSIRT

<b>CSIRT Members</b>	ACCR
Names, contact information and PGP keys / X.509 certificates of other CSIRT members	
<b>Technical Expertise</b>	ACCR
Operating Systems	
System Platforms	
Networks	
<b>Contact Information for Constituency / Host Organization</b>	ACCR
Contact information for person/organization representing the constituency	
Contact information for person representing the host organization	
<b>PGP Key Revocation Certificates</b>	ACCR
Key Revocation Certificates for previously distributed PGP keys	
<b>Information Server</b>	mixed :
Public WWW server	PUBLIC
Other WWW server	ACCR
Mailing lists	ACCR
(Anon)FTP server	ACCR
NetNews	ACCR

**\*\*\* NOTE: please use the ASCII/text form B/D provided separately for filling out – not this form \*\*\***

<sup>1</sup> For all practical considerations PGP/GpG is the established standard for providing confidential and authentic communication within the CSIRT community.

## Appendix C: Form to accept the invitation to acquire TI “accredited” status

CSIRT Acronym or Name : \_\_\_\_\_

We hereby declare that we accept the invitation to acquire “accredited” status as laid out in the "Invitation Package for TI “accredited” Status" (in short: Invitation Package) v3.0 of 01 January 2005 as sent to us by the Trusted Introducer (in short: TI), and that we support the criteria, procedure and timeline set out in the Invitation Package.

More specifically, we:

- declare that we are prepared to meet and maintain the „MUST“ criteria for “accredited” status laid out in Invitation Package Appendix D;
- commit ourselves to file completed Appendices B and D of the Invitation Package to the TI within 2 months;
- agree to the publication of various data, as specified in the Invitation Package, provided by us to the TI on the public and restricted TI websites (note on privacy: personal data will not appear on the public website; on the restricted website only as far as the CSIRT has specified them);
- commit ourselves to pay a one-off amount of € 900 to TERENA to cover the cost of the application for “accredited” status (if your organisation is a TERENA member a discount arrangement may apply here);
- declare that we have taken note of, and intend to pay, the yearly fee that is due to TERENA if and when we obtain “accredited” status

City, Date: \_\_\_\_\_

Representative of  
CSIRT: \_\_\_\_\_

Signature: \_\_\_\_\_

## Appendix D: Criteria for “Accredited” Status

An “accredited” CSIRT MUST/SHOULD meet the below criteria.

- The MUSTS are criteria which have to be met to successfully pass the accreditation process and to acquire/maintain the “accredited” status.
- The SHOULDs are strong recommendations, not obligations.
- MUST and SHOULD are defined according to IETF standards, see Appendix A.

Describe in as few words as possible your support of the various accreditation criteria.

- If you support a MUST criterion, just put down : “supported”.
- If you do NOT (yet) fully support a MUST criteria, put down : “not (fully) supported (yet)”, **and explain what you do not support (yet) and why, and when you plan to support it.** Support of the MUST criteria is obligatory to acquire “accredited” status, so any non-support of such criteria must be cleared as soon as possible between CSIRT and TI.
- If you support a SHOULD criteria, put down “supported”. You may like to add a short note of explanation, if not covered by Appendix B. If you have filled out RFC-2350, please send it along with Appendix D, or write down its URL below.
- If you do not support a SHOULD criteria, put down “not supported”. If you plan to support it in time, please add a short note explaining what and when.

**Please be as concise as possible.**

1. CSIRTs MUST be described by qualitative and a minimum level of quantitative values (basic set of information and services offered) as per Appendix B.

YOUR SUPPORT: ...

CSIRTs MUST cooperate with the publication of the delivered data on the TI **restricted-access** website. Access is restricted to “accredited” CSIRTs, the TI and the TI Review Board.

YOUR SUPPORT: ...

2. CSIRTs MUST cooperate with the publication of the essentials of their contact information – meaning the items marked PUBLIC in Appendix B – on the TI **public** website (<http://www.trusted-introducer.org/>).

YOUR SUPPORT: ...

3. CSIRTs SHOULD comply with the [CSIRT Code of Practice] as ratified by the TI Accredited Teams.

YOUR SUPPORT: ...

4. CSIRTs MUST comply with the [CSIRT Code of Practice] if they support compliance here. If your CSIRT does not support the Code of practice, the statement is NOT APPLICABLE.

YOUR SUPPORT: ...

5. CSIRTs SHOULD present their service to the outside world as per [RFC 2350], including a specification of quantitative values (advanced set of information).

YOUR SUPPORT: ...

6. CSIRTs MUST adhere to their description as per [RFC 2350] including all service level statements therein – if such a description is existent. This statement is NOT APPLICABLE if your CSIRT does not have such a description.

YOUR SUPPORT: ...

7. CSIRTs MUST actively support the TI requirement to keep the information they provided to TI up-to-date, that is to ensure the *actuality* of the sent-in templates etc. This criteria of *actuality* maintenance also applies to SHOULD criteria.

YOUR SUPPORT: ...

8. CSIRTs MUST handle all sensitive or private information sent to them – including all incident related information - in a secure and protective way (subject to local law), internally but also when sending it out again. CSIRTs MUST describe their modus operandi in that respect, by filling out the “Information Handling Policy” field of Appendix B. CSIRTs are advised to establish a secure communications scheme based on PGP/GpG and/or S/MIME in order to help meet this goal.

YOUR SUPPORT: ...

9. CSIRTs MUST support question-and-answer sessions (per e-mail in principle) with the TI to clear problems or questions arising with regards to the provided information, its *authenticity* or its *actuality*.

YOUR SUPPORT: ...

10. CSIRTs MUST support (not financially) a site visit if the TI concludes that a site visit is necessary. Site visits are last-resort possibilities if question-and-answer sessions fail or when other pressing reasons exist – but a site visit can also be invited. Observations made during the site visit bearing a relation to the criteria described here, will be objectively logged by the TI.

YOUR SUPPORT: ...

11. CSIRTs SHOULD regularly attend FIRST conferences, TF-CSIRT meetings and other TI supported CSIRT meetings.

YOUR SUPPORT: ...

12. CSIRTs MUST pay the fees established for acquiring and maintaining “accredited” status as set by TERENA.

YOUR SUPPORT: ...