TF-CSIRT
TRUSTED INTRODUCER

INVITATION PACKAGE
FOR
TI "ACCREDITED" STATUS

Version 3.1 – 1 July 2025

INDEX

1 ESSENTIALS 3

1.1 WHAT IS TI ACCREDITATION ALL ABOUT? 3
1.2 WHAT IS THE FIRST STEP IN THE TI ACCREDITATION PROCESS? 5
1.3 MOVE ON TOWARDS TI "ACCREDITED" STATUS 5
1.4 BEING AN "ACCREDITED" TEAM! 6

2 ACCREDITATION CANDIDATE STATUS 8

3 ACCREDITED STATUS 9

4 APPENDIX A: FORM TO ACCEPT THE INVITATION 11

5 APPENDIX B: INFORMATION TEMPLATE FOR "ACCREDITED" TEAMS 12

5.1 MANDATORY FIELDS DESCRIBING THE TEAM 13
5.2 OPTIONAL FIELDS DESCRIBING THE TEAM 17
5.3 SERVICE RELATED FIELDS USED INTERNALLY BY THE TI 19

6 APPENDIX C: CRITERIA FOR "ACCREDITED" STATUS 21

6.1 EXPLANATION AND GUIDANCE 21
6.2 LIST OF ALL MUST CRITERIA 21
6.3 LIST OF ALL SHOULD CRITERIA 22

7 APPENDIX D: STANDARD DEFINITIONS TAKEN FROM THE IETF APPROACH [RFC2119] 23

8 APPENDIX E: TI BACKGROUND 24

8.1 TI ENTITIES 24
8.2 TI STATUS: "LISTED", "ACCREDITATION CANDIDATE" AND "ACCREDITED" 25
8.3 VALIDATION OF INFORMATION 26

1 ESSENTIALS

Your team is invited to join the TI (=Trusted Introducer) Framework as "TI Accredited" team. This document describes all what you as invited team needs to know to acquire the "accredited" status, i.e. passing the accreditation process for your team. If you have any questions during the process, please direct them to:

E-mail address: ti@trusted-introducer.org

If you send e-mail to us, please make sure to include the ticket number send to you as part of the subject of our e-mail to you with your invitation. That way we can keep track of the progress and ensure a consistent view of your process.

To send confidential data encrypted to us use the following public key, available through the xxx TF-CSIRT web site as https://www.tf-csirt.org/xxx.asc:

```
User ID:       Trusted Introducer (TI) ** TICKET SYSTEM ** key
               <ti@trusted-introducer.org>
Key ID:        0xA778F9E1
Key type/size: DSA and Elgamal / 1024D/4096Elg
Fingerprint:   C5BB A470 AAD6 7013 2917  F1BF A648 80D2 A778 F9E1
```

The TI team has assigned two of its members—called "Primary" and "Secondary Introducer" – to oversee your accreditation process from beginning to end and assist you when you meet with problems. Most communication will be with your "primary Introducer" as we try to avoid hand-overs unless a longer absence requires such change. You reach both through the above service e-mail address – please do not use personal e-mail addresses for reasons of contingency for all official steps.

1.1 What is TI Accreditation all about?

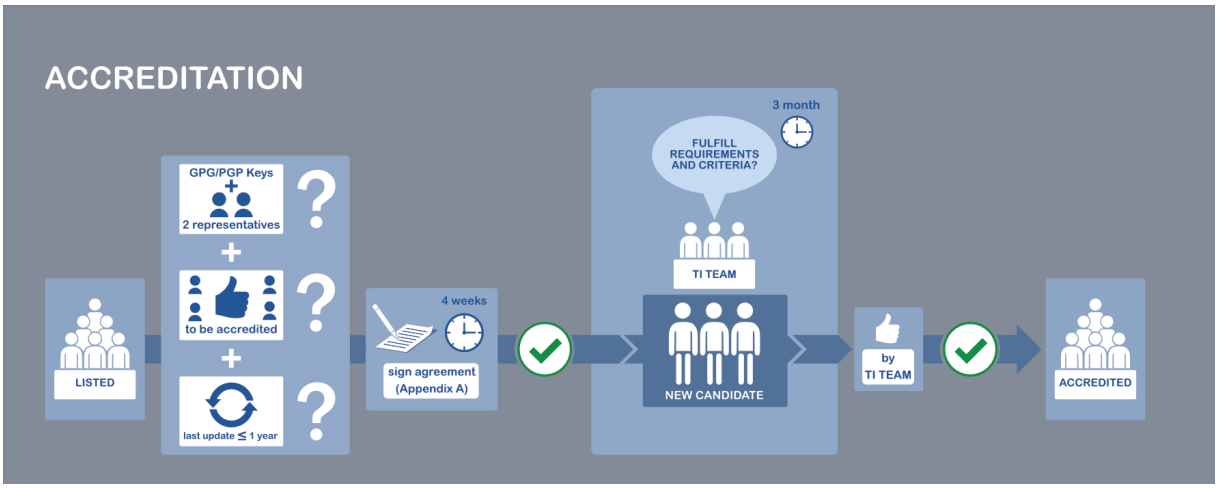
The TI Framework has been created based on an initiative of the European security and incident response team community in 2000. Such teams (or functions) within an organisation deal with all kinds of computer and network security incidents. They strive to prevent incidents from happening, help detecting attacks, support the mitigation of as well as the recovery from incidents, and coordinate all activities including the contact to external teams when they do occur.

The teams of our community cooperate worldwide to combat attacks on IT systems and infrastructures or other IT related crime. Starting from Europe the forum for such cooperation is called TF-CSIRT. To cooperate efficiently and swiftly when security incidents occur, a certain level of mutual trust is needed between teams. An important pre-requisite for mutual trust is shared operational knowledge about one another. But also some services, supporting such sharing as well as the coordination needs to be made available.

The TI accreditation service is meant to do just that: facilitate trust by formally accrediting teams that are ready to take that step. For a team to proceed from the status of "listed" to the status of "accredited" its organisation needs to go through a formalised accreditation scheme – the subject of this invitation package. Once "accredited" the team gains access to the "*full-members-only*" information: there they find the details about their fellow accredited and certified teams but also all listed teams. In addition, tailored value-added services towards the needs of cooperating teams are accessible: readily downloadable contact databases and GPG/PGP keyrings, access to secure discussion fora, registration of RIPE Database IRT objects, emergency alerting services based on communication means independent from the Internet and so on.

A crucial benefit that is part of the TI framework is maintenance: in a four-monthly cycle the actuality of data is verified with the accredited teams to prevent the information from going out-of-date and ensure, necessary updates are made in time. More background information about the TI can be found in Appendix E. Chapter 2 talks about issues related to being an "accreditation candidate" and activities during this phase, while Chapter 3 explains the details of being an "accredited team". You are formally advised to read that Chapter, which includes a description of the maintenance process as well as the fee structure applicable.

The TI framework is being further developed, as information and IT security plays an increasingly important role in today's networks, and indeed the world at large, and more severe demands are placed on teams involved worldwide. FIRST, the global meeting place of CERTs, has adopted part of the TI framework for their membership procedure. Meanwhile the TI teams are further improving the accreditation scheme and have added a certification status[1] as important step to improve its members quality and ability to perform their functions. And to make any such improvement measurable and visible to all others depending on such insights and knowledge.



[1] https://www.trusted-introducer.org/processes/certification.html

The overview (figure on the page before) illustrates the successful accreditation process, which we will describe in the following sections in more detail.

1.2 What is the first Step in the TI Accreditation Process?

The first step is to move your team from "listed" to "accreditation candidate" status. Your team already has acquired "listed" status, because that is a pre-requisite for being invited to the accreditation process.

Moving to "accreditation candidate" status is simple: just print out Appendix A, have it properly filled and signed (this proofs your team's approval and acceptance of the fee structure as well as the governing principles as laid out in this invitation), and send the original version to the TI service provider. Please either use fax or e-mail, but also send it by normal post, registered post is not needed.

Send your agreement by e-mail to **ti@trusted-introducer.org** , but only PGP-signed!

We appreciate the original by postal mail to:

Trusted Introducer
c/o DFN-CERT Services GmbH
Nagelsweg 41-45
20097 Hamburg / Germany

PLEASE NOTE:

This step must be completed within 28 days after receiving the invitation.[2]

If there should be any problem with the filled-out Appendix A the TI team will contact you to sort out any such issue. Once a properly signed Appendix A is available, the TI team sends out a formal "TI Accreditation Candidate Status Acknowledgement" by signed e-mail: that means your team is an "accreditation candidate" as of the date specified within the acknowledgement.

1.3 Move on towards TI "Accredited" Status

Moving to "accredited" status depends on your team's ability to provide the required set of information (see Appendix B) as well as responding to several requirements (see Appendix C). It is vital for the TI framework that all accredited teams understand, appreciate, and fulfil those requirements.

[2] Please note also: as a rule, an invitation package will be sent out to any team no more than twice every twelve (12) months.

As the TI Self-Service is readily available, the updates are made directly using it:

https://up.trusted-introducer.org

This step should be started within the first two (2) months of the "TI Accreditation Candidate Status Acknowledgement" date, as it is not that difficult to provide the information asked for. But to get the level of detail right and to be able to discuss issues in the submitted texts needs some time sometimes. Therefore, please don't try to submit everything on the last minute. This causes stress on all sides and might lead to an unsuccessful application, if the quality and extend of the text provided is simply not enough.

The TI team will review all updates your team have provided. One of the team will then discuss any issues arising out of this review. Once all issues have been satisfactorily met, the updates will be approved and made available on both the public TF-CSIRT web site and restricted part for *full-members-only*. Once all requirements are fulfilled and all data has been provided, the TI team sends out a formal "TI Accreditation Status Acknowledgement" by e-mail: that means your team is recognized as an "accredited team" as of the date of the acknowledgement.

The date of the "TI Accreditation Status Acknowledgement" must be within three (3) months of the "TI Accreditation Candidate Status Acknowledgement" date, unless the delay is caused by the TI due to additional checks or discussions. [3]

Your team will from then on be invoiced on an annual basis for maintenance of the "accredited" status by the OpenCSIRT Foundation (The Netherlands, the host of TF-CSIRT since 2022). The annual fees of EUR 1,200 (VAT might apply) are invoiced from September to August the following year. For the first year the invoice covers only the months, EUR 100 each, after the "TI Accreditation Status Acknowledgement" up until August. At the same time your team will also be invoiced for the one-off amount applicable to all accreditation candidates of EUR 800 (VAT might apply).

1.4 Being an "Accredited" Team!

From the moment of your team's accreditation, you can enjoy the value-added services that come with the "accredited" status. Most namely:

- Access to the *full-members-only* part of the TF-CSIRT web site, featuring in-depth operational data of all accredited teams; this access is provided on basis of X.509 certificates which are created by the TI team for the accredited team's representatives and all team members registered with the TI;

3 Please note: non-compliance to this deadline might cause an immediate fall back of your team to "listed" status, the invitation counting as a failed invitation.

- Access to the TI mailing lists open to accredited teams only, e.g. meant for discussion of open security issues within a trusted environment;
- Access to value-added information available only for accredited teams, like easily downloadable contact information (e.g. for PDA integration) and GPG/PGP key-rings;
- Registration of a so-called IRT object in the RIPE database corresponding with your team: the aim is a direct mapping between your constituency's IP number ranges and your team's contact data which can readily be accessed by any interested user through the Internet;
- GPG/PGP key-signing by the TI team of public keys of your team and its representatives;
- Access to the in-band and out-of-band alerting services – the in-band mechanism is a re-encrypting e-mail list that supports both X.509 and GPG/PGP simultaneously, whereas the out-of-band mechanism records voice messages and uses SMS and/or telephone calls with the recorded messages to spread alerts in case the Internet is unavailable or unreliable;
- Access to TI meetings adjacent to TF-CSIRT meetings restricted to members of accredited teams, TI Associates, the TI team and the TF-CSIRT Steering Committee (TF-CSIRT SC, the group that oversees the operation of the TI service) only;

To keep your team's information current and actual, every four (4) month you will be prompted to update the information. If there are no changes, your team's representative will still need to acknowledge that fact. This is part of the TI processes called "Maintenance".

2 ACCREDITATION CANDIDATE STATUS

From the moment on that your team – because of a correctly filed Appendix A – has received a formal "TI Accreditation Candidate Status Acknowledgement", the team is considered as "accreditation candidate". The only goal of that status is to move to "accredited" status, as follows:

- The change to "accreditation candidate" status is reflected on the TI public website.
- Your team will be charged the one-time accreditation fee, regardless of whether your team will succeed in acquiring accreditation or not.
- Within three (3) months from the Acknowledgement date, your team must provide the information as described in Appendix B and to meet the accreditation criteria as defined in Appendix C. How to meet those criteria is described below.
- In addition, relevant public keys need to be submitted also, i.e. your team's GPG/PGP key and those of your team's representatives.
- Your team will need to meet all MUST criteria as laid out in Appendix C. The TI team strongly advocates taking into consideration the SHOULD criteria at the same time. To document the current status, your team needs to fill out Appendix C, which is meant to summarize your position with regards to all criteria.
- The "accreditation candidate" status of your team provides the TI team with the right to publish the information it receives from your team on its restricted web site, which is only open to accredited teams as well as the TI Associates, TI team and the TF-CSIRT SC.
- Within two (2) months from the Acknowledgement date, your team should start to provide the required information.
- The TI team will gauge the material you sent in. Once all requirements are met, your team will receive a "TI Accreditation Status Acknowledgement" which means the transition to "accredited" status.
- If the material is not sufficient or if there are open questions, you will get a request for additional information. Please react to any such request as soon as possible as the timeslot (3 months) available to reach the "accredited" status does not change.
- If "accredited" status has not been reached within the allowed time frame, your team automatically falls back to "listed" status and the invitation expires.

3 ACCREDITED STATUS

From the moment that your team has properly documented that it meets the accreditation criteria – by means of correctly filed Appendices B and C – and has received a formal "TI Accreditation Status Acknowledgement", the team is publicly considered as being "accredited". The following then applies:

- The change to "accredited" status is reflected on the TF-CSIRT web site.
- The "accredited" status of your team provides the TI team with the right to update the information about your team on its restricted web site, which is only open to accredited teams as well as the TI Associates, TF-CSIRT SC and the TI team.
- The information about your team contained in Appendix B and C marked for PUBLIC release and your completed RFC 2350 will be provided on the TI public website.
- An invoice will be issued once a team is recognized as "accredited" by the TI team.
  - Your team will be charged an annual fee for a 12 month period starting on 1 September each year.
  - The first invoice will cover the month from acquiring "accredited" status until the next annual fee cycle starts (1 September each year). The charge will be proportional.
  - The fee is non-refundable, also if the team would lose its "accredited" status at some point in time.
  - The fee MUST be paid within two (2) months of the invoice being sent. Otherwise, the "accredited" status will be suspended or even revoked if no explanation is given.
- Your team will receive information about how to access the TI "members only" website which also contains specific services tailored towards accredited teams like a downloadable database of all "listed" and "accredited" teams. The designated e-mail address provided by your team will be subscribed to a restricted mailing list of all accredited teams. An IRT object will be generated for your team in the RIPE database, with automatic maintenance through the TI process, if you request its creation.
- Your team will be reminded of the necessary maintenance if needed. Maintenance of the information about your team is essential. If your team fails to uphold that maintenance, it will fall back to "listed" status, because the maintenance is one of the MUST criteria for accredited teams. More in detail the following rules apply with regards to maintenance activities:

- Your team MUST inform the TI team about any change that relates to contact or public key information or changes that impact its establishment (like constituency or fundamental organisational changes) within two (2) weeks and provide the appropriate corrections to the Appendix B form and/or RFC 2350.
- All other changes to the information provided by means of Appendices B and C MUST be passed on to the TI within four (4) months – preferably sooner. This includes information about new GPG/PGP keys.
- Your team MUST reply to requests by the TI team regarding the status of the information your team has provided.
- At least every four (4) months the information available about accredited teams MUST be verified. The success of this practice depends on the joint effort of your team and the TI. If no status updates are received by the TI for four consecutive months, the TI will send out a message requesting an acknowledgement, that the current set of available information is still correct. Two (2) more reminders of this will be sent, if no answer follows, within two (2) months of the first reminder.
- If your team does verifiable not comply with the above rules the TI team will give your team formal notice (by signed e-mail and written letter) that your accredited status will be suspended (revoked in case of non-payment of the annual fee) within two (2) months. If your team still fails to comply within this time period, your accredited status will be suspended, or, in case of non-payment of the annual fee, the accredited status will be removed.
- If an accredited team is suspended, the TI team will inform all other teams and update the TF-CSIRT web site accordingly, both public and *full-members-only*. Following a suspension, the TF-CSIRT SC, assisted by the TI team, will then decide whether to lift the suspension and if so when, or whether your team's accredited status should be revoked. Revoked teams can either go back to "listed" status, or be removed from the TI database entirely, decided by the TF-CSIRT SC.
- If an urgent situation, not covered by any of the above rules, occurs that could impact the accredited status of your team, the TF-CSIRT SC can take actions like making enquiries or direct the TI team to interact with your team, if necessary, also by conducting a site visit. The TF-CSIRT SC can take appropriate actions including the revocation of the accredited status, based on their assessment of the overall situation.

4 APPENDIX A: FORM TO ACCEPT THE INVITATION

The form required will be send to any applying team by email as PDF!

5 APPENDIX B: INFORMATION TEMPLATE FOR "ACCREDITED" TEAMS

The set of information a team needs to provide to acquire "accredited" status – and that it needs to maintain after that – consists of three parts:

1. **Mandatory** fields describing the team;
2. **Optional** fields describing the team; and
3. **Service-related** fields used internally by the TI team.

In case the team has already a filled-out RFC 2350 many requested information might be already available. In such case instead of copying the relevant copy simply sending in the RFC is usually sufficient.

The complete set of information of part 1 and 2 will be published on the *full-members-only* TF-CSIRT web site. A subset of both parts will be published on the *public* web site. The following labels are used to make that explicit:

- **PUBLIC:** this information will be published on the *public* TF-CSIRT web site. The whole world can potentially access and read this.
- **SECURE:** this information will only be published on the *full-members-only* TF-CSIRT web site. It is therefore only available to accredited teams.
- **TI INTERNAL:** this information will only be used to provide TI services. It is therefore not directly available to accredited teams (like SMS numbers for the alerting service) but might become visible indirectly (like bounces caused by mailer problems).
- **MIXED:** Indicates that the corresponding section contains both PUBLIC as well as SECURE or TI INTERNAL fields as indicated.

In case you don't want a sensitive piece of information (for example an emergency contact number) to be published on the *public* TF-CSIRT web site, you might indicate this accordingly. Also, if you would like to have different information published on the *public* and the *full-members-only* TF-CSIRT web site, you might indicate this for the applicable fields. Another set of information for which such considerations might apply is the IRT object, which contains e-mail addresses and telephone numbers. If in doubt, contact your primary introducer and discuss this with him.

Note on GPG/PGP and X.509: anywhere where a GPG key is requested, this of course can also be a PGP key as GPG is functionally equivalent to PGP. It cannot be an X.509 certificate for now. X.509 is wholly different from GPG/PGP and is not used much yet by teams for external communication. For internal use within organisations and teams, X.509 is well suited, but not at this moment for inter-team communication as the installed base simply is not sufficient for that.

Regarding the standards for using GPG/PGP keys, the TI highly recommends the following:

- Crypto algorithm: RSA, Elgamal or DH/DSS
- Key length: at least 2048 bits

This recommendation is not a MUST but highly recommended – also the TI will only sign keys corresponding with these minimum demands.

In all cases make sure that a team's or team member's "from" e-mail address is contained in either the primary user id of the corresponding GPG/PGP key, or in an additional user id (which can be added afterwards as well). This is for example needed to get subscribed on the TI's encrypted mailing list. Also, the GPG/PGP key must be at least self-signed.

5.1 Mandatory Fields describing the Team

Name of the Team PUBLIC

- Short team name or acronym used
- Official team name
- Host organisation of which the team is a part of
- Country the team is located in (list multiple countries if needed)
- Date of establishment

Constituency PUBLIC

- Type of constituency: [CHOSE ONE OR MORE OF] research-or-educational / government / military / national / financial-organisation / other-commercial-organisation / non-commercial-organisation / ISP-customers / commercial-customers / OTHER (EXPLAIN).
- Description of constituency: verbal description explaining the formal and informal constituencies and the exact relationship, especially if more than one type of constituency is listed above.
- Internet domain, AS numbers and/or IP (and IPv6 if applicable) address information defining the constituency and its networks.
- All countries in which constituency members are located in

Contact Information PUBLIC

- Regular telephone number (country code, telephone number, time zone)
- Emergency telephone number (country code, telephone number, time zone)
- Facsimile number (country code, telefax number, time zone)
- Other telecommunication facilities (if applicable)
- Postal address of team
- E-mail address of team and associated GPG/PGP key, e-mail address MUST be present in a user-id of it
- Public web page(s) if available

Business Hours MIXED

- Description of business hours PUBLIC
- Procedure for contacting the team outside business hours SECURE

Team Representative(s) SECURE

Please note: Two representatives can be registered – however also all team members SHOULD be registered to get access to the services and to complement the information about your team (see 5.2 Optional Fields).

- Name of primary person representing the team (mandatory)
  - Regular telephone number (country code, telephone number, time zone)
  - Mobile telephone number (country code, telephone number, time zone)
  - Facsimile number (country code, telefax number, time zone)
  - Other telecommunication facilities (if applicable)
  - Postal address if different from team
  - E-mail address and associated GPG/PGP key, e-mail address MUST be present in a user-id of it
- Name of secondary person representing team (optional, but recommended)
  - Regular telephone number (country code, telephone number, time zone)
  - Mobile telephone number (country code, telephone number, time zone)
  - Facsimile number (country code, telefax number, time zone)
  - Other telecommunication facilities (if applicable)

- Postal address if different from team
- E-mail address and associated GPG/PGP key, e-mail address MUST be present in a user-id of it

Policies SECURE

- Specify how incoming information is "tagged" or "classified" or "sorted" to differentiate between various information sources and priorities?
- Specify how information is handled, especially with regards to restricting access and protecting its confidentiality once received by your team? Are there legal considerations to take into account with regards to the information handling?
- What considerations are adopted for the disclosure of information ("when what?"), especially incident related information passed on to other teams or to sites?
- Specify any special legal considerations to take into account with regards to the handling and disclosure of information.
- Specify any special legal considerations to take into account with regards to the use of cryptography (based on e.g. GPG/PGP or X.509) in the handling of information. This specification must include possible legal boundary conditions as key escrow or enforceability of weak cryptographic technologies.

RFC 2350 PUBLIC

- The information beyond is usually contained in the filled-out RFC 2350, in which case submitting this document will be enough to satisfy the need for this information.
- URL of the published RFC 2350
- Date of last update and version number (if applicable)
- Distribution mechanisms for notifications about updates

Membership of Professional Team / Security Organisations MIXED

- Does your team participate in TF-CSIRT and if yes, since what year? SECURE
- Is your team a member of FIRST and if yes, since what year? PUBLIC
- Is your team member of a national CERT cooperation or community and if yes, since what year? PUBLIC
- Specify other CERT or security organisations where your team (or your host organisation) is a member of and if yes, since what year? SECURE

Services provided to the Constituency SECURE

If you provide services not listed below – or if you believe, that the terms chosen do not fit clearly to your services – please describe those services in free text format!

These services are not yet aligned with the CSIRT Services Framework currently developed by experts within the FIRST context. We will start supporting this framework with the upcoming v 2.0 version!

- Specify available reactive services, using the following list (or adding to it):
  - alerts and warnings
  - artifact analysis
  - artifact response
  - artifact response coordination
  - forensic analysis
  - incident analysis
  - incident response
  - incident response support
  - incident response on-site
  - incident response coordination
  - vulnerability analysis
  - vulnerability response
  - vulnerability response coordination
- Specify available proactive services, using the following list (or adding to it):
  - announcements
  - configuration and maintenance of security tools, applications and infrastructures
  - development of security tools
  - intrusion detection services
  - security audits or assessments
  - security-related information dissemination
  - technology watch

- Trend and neighbourhood watch

- Specify security quality management services, using the following list (or adding to it):
  - awareness building
  - business continuity and disaster recovery planning
  - education/training
  - product evaluation or certification
  - risk analysis
  - security consulting

5.2 Optional Fields describing the Team

Contact Persons for Constituency SECURE

- Person representing the Constituency
  - Organisation
  - E-mail address

Contact Persons for Host Organisation SECURE

- Person representing the Host Organisation
  - Organisation
  - E-mail address

Team Members SECURE

- For each member of your team that shall receive an X.509 user certificate for accessing TI services, please provide
  - Full name
  - E-mail address
  - If applicable provide associated GPG/PGP keys as well. (e-mail address MUST be present in a user-id of the individual keys)

Tools and Expertise SECURE

Please note: The two first bullets are about the IM process only. It can vary from software like AIRT or RTIR (the next question asks for the software details of that) and how they are used unto the simple use of logbooks, spreadsheets, and human written e-mail as well as exchange formats.

- Specify your team's Incident Management process tool (workflow, reporting interfaces, exchange formats, contact person).
- Specify your team's Incident Management related software (name, last update, version, URL, license, description, contact person)
- Specify (special/specific) expertise of your team on TCP/IP and/or other Networks
- Specify (special/specific) expertise of your team on System Platforms
- Specify (special/specific) expertise of your team on Operating Systems
- Specify (special/specific) expertise of your team on Specific Software Packages (e.g. SAP)

Team / Process Information SECURE

- Specify any relevant team or host organisation accreditations or certifications, like ISO 27001, ISO 9000, etcetera. Explain where needed.
- Specify relevant team projects (name, goal, time-period, partners, contact person): **note** that the goal here is not to provide detail but to enable other teams to see what your team is up to – this serves as aid for more effective collaboration and sharing.
- Specify your team's reporting structure (type of reports, target audience(s), frequency).

Team / Staff Information SECURE

- Specify the team members required or recommended relevant education levels (examples: TRANSITS, SANS, CERT/CC trainings for CERT/technical expertise)

Please note: You can also state your team's policy here in that regard like the goals that are set. That might be easier to maintain than any representation of an actual situation.

- Specify your team's headcount (normal and backup).

Please note: This is the number of people involved in the team operational business. "Normal" is the standard category – "backup" implies all people that are not part of your team's operation normally but could be utilized e.g. in cases of emergency.

- Specify your team's work force in terms of FTE (full time equivalent) both for "normal" and "backup"

Please note: The number of FTE is smaller than or equal to the headcount by definition. A team might have a headcount of 7 (part time staff) with a budgeted or estimated workload of 2.5 FTE for instance.

Information Resources SECURE

- If your team provide additional information resources (for example AnonFTP servers, specific web pages with tools) that are accessible for TI Accredited and Certified teams, please add:
  - URL of the service
  - Description
  - Process to get access

IRT Object related Information PUBLIC

- If a IRT object shall be created, all information might be taken from the above set of fields about the team.
- In case specific information shall be used for the IRT object, this will need to be listed.

5.3 Service-related Fields used internally by the TI

Encrypted TI Accredited Teams Mailing List TI INTERNAL

- Designated e-mail address for subscription to mailing lists for TI accredited teams only, used for alerts, announcements and discussion
  - Associated GPG/PGP key, e-mail address MUST be present in a user-id of the GPG/PGP key.

Encrypted TI Accredited Team Reps Mailing List TI INTERNAL

Note: The information for this mailing list – encrypted and only for team representatives – is taken from the already provided data for the team representative.

Outband Alerting System TI INTERNAL

Please note: In time of a real Internet crisis an out-of-band – phone, not Internet based – alerting system is available. More than one contact can be provided. All

registered contacts will receive an SMS and/or a telephone call in case of an alert. For telephone calls a PIN must be provided by the called person for authentication purposes.

For each contact you need to register the following information:

- number to send SMS to or to call out to
- type of contact:
  - SMS: an SMS will be sent to the given number
  - phone: a call will be made to it
  - mobile: both, SMS and phone, will be triggered
- time zone information including DST
  - time period (from / to) in 24h notation (for example 09:00 for 9am and 15:00 for 3pm) in which alerts should be communicated to the given point of contact
  - coverage: weekday (Mo-Fr) or all (Mo-Su)

Billing Information TI INTERNAL

- Postal address for invoices (if different from team's postal address)

Please note: The billing address used will contain the name of the team representative, the short team's name and the team address otherwise.

- Reference field for billing (if applicable)

Please note: The reference field is an additional line of information for the invoice and can contain e.g. an internal reference or purchase order number, or any other codeword or personal name as required by your organisation. If no information is provided, this field will be left empty.

- VAT number of the legal organisation

Please note: If no VAT number is assigned (i.e. for Government agencies) please write "N/A".

6 APPENDIX C: CRITERIA FOR "ACCREDITED" STATUS

6.1 Explanation and Guidance

An "accredited" team MUST or 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 D.
- If you do NOT (yet) fully support a MUST criterion: 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 with the TI Team.
- If you do not support a SHOULD criteria, put down "not supported". It would be helpful if you explain what is missing or needed. Indicate planned support.

6.2 List of all MUST Criteria

- Teams MUST be described by qualitative and a minimum number of quantitative values as per Appendix B and ensure that these descriptions continue to match reality.
- Teams MUST cooperate with the publication of all delivered data on the TF-CSIRT *full-members-only* website. Access is restricted to "accredited" teams (including all certified teams), TI Associates, the TI team and the TF-CSIRT SC.
- Teams MUST cooperate with the publication of the essentials of their contact information – meaning all items marked PUBLIC in Appendix B – on the TF-CSIRT public website (https://www.tf-csirt.org/trusted-introducer/).
- Teams MUST register two team representatives.
- Teams MUST present at least their external services, if any, to the outside world as per RFC 2350,[4] including a specification of quantitative values and ensure that these descriptions continue to match reality, including indicated service levels.
- Teams MUST actively support the TI requirement to keep the information provided to the TI team up to date, that is to ensure its actuality and usability.

4 https://www.ietf.org/rfc/rfc2350.txt

- Teams MUST support question-and-answer sessions per e-mail or on the phone with the TI team to discuss issues or questions arising with regards to the provided information, its authenticity or its actuality.
- Teams MUST pay the fees established for acquiring and maintaining "accredited" status.
- Teams MUST support (not financially) a site visit if the TI team or the TF-CSIRT SC 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 team member conducting the site visit.
- Teams MUST recognise and support the "Information Sharing Traffic Light Protocol"[5] as ratified by the TI Accredited Teams.
- Teams 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. Teams MUST describe their policy in that respect and are urgently advised in this regard to establish a secure communications scheme based on GPG/PGP and/or X.509.
- Teams MUST actively support the signing of their team and representatives GPG/PGP keys, during TI/TF-CSIRT meetings and other occasions, by the TI team.

6.3 List of all SHOULD Criteria

- Teams SHOULD regularly attend TI and TF-CSIRT meetings.
- Teams SHOULD comply with the "CSIRT Code of Practice"[6] as ratified by the TI Accredited Teams.
- Teams SHOULD use the "SIM3 Maturity Model"[7] as a starting point for self-assessments or audits of their services.
- Teams SHOULD respond to TI reaction tests to demonstrate that they can be reached via their official contacts.

5 https://www.trusted-introducer.org/ISTLP.pdf
6 https://www.trusted-introducer.org/CCoPv21.pdf
7 https://www.trusted-introducer.org/SIM3-Reference-Model.pdf

7 APPENDIX D: 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.

8 APPENDIX E: TI BACKGROUND

This background information about the TI service and its processes is offered as additional information. There is no formal requirement to read this appendix, but it might be useful, if you are not yet familiar with the TI services and its framework.

8.1 TI Entities

The following entities are of interest within the TI framework:

- **TF-CSIRT Community:**[8] Formally the group of full members of TF-CSIRT (TI Accredited and Certified teams and members of those teams), individual members (TI Associates), TF-CSIRT SC members as well as the TI team. Informally also the teams which are TI Listed are included.
- **TI Associates:** Individual members of TF-CSIRT whose experience and/or skills can be of clear benefit to the TI Community, but who are not member of an TI Accredited team (anymore) and thus cannot contribute through their team.
- **(the) TI** or **TI Team:** The group of people operating the TI services, maintaining the TI part of the TF-CSIRT web site (https://www.tf-csirt.org/trusted-introducer/), and maintain the TI Directory.
- **Primary and Secondary Introducer:** A member of the TI team who monitors your accreditation process from beginning to end and assists you during this phase. The "Secondary" is acting as backup. While routine tasks like answering basic e-mail questions or handling acknowledgements are handled in shifts by TI team members, the "Primary" introducers provide you with continuity and a personal touch.
- **GÉANT:** The "Trusted Introducer" service originated in September 2000 from cooperation activities between CERTs and security teams that were organized by TERENA. It's successor GÉANT (www.geant.org) continued to act as the legal and financial home of the TF-CSIRT until August 2022.
- **OpenCSIRT Foundation:** Since September 2022 the foundation is the legal host of all TF-CSIRT activities including the TI services and TRANSITS as well as organizing the Community meetings and elections. RIPE NCC and GÉANT have agreed to join the foundation as founding fathers to support it in the long-term.

  In addition to support the TF-CSIRT activities the foundation will continue to maintain, promote and further develop the SIM3 standard for all kind of cyber security teams, most namely CSIRTs, SOCs, ISACs and PSIRTs.

[8] Sometimes this community is also called „TI Community", but as TI is a service of TF-CSIRT there is basically no difference.

- **TF-CSIRT Steering Committee (TF-CSIRT SC):** The TF-CSIRT SC reviews the operation of the TI team and addresses all special issues that might result from its operation as well as any question that is not addressed by the operational framework. The TF-CSIRT SC performs the following tasks:
  - Support and foster the acceptance and recognition of the TI service.
  - Oversee and change policies and framework, in close cooperation with the TF-CSIRT Community.
  - Review the TI service, including the review of tri-annual reports issued by the TI team.
  - Handle specific inquiries about the functioning of the TI service, which are related to the strategical perspective represented by the TF-CSIRT SC.
  - Decide about any issues that are outside existing TI policies, like making exceptions to the defined rules for status change (towards "accredited" status, or fall-back to "listed" status), deciding on a site visit to clarify issues that could not be handled otherwise, handling objections from the TF-CSIRT Community regarding listing and accreditations, etcetera.

  The TF-CSIRT SC has the right to review the archive maintained by the TI team at any time to clarify any inquiries concerning the TI service directed to the TF-CSIRT SC and to enable an overall review of the TI service.

  The chair of the TF-CSIRT SC is elected by full-members of TF-CSIRT.
- **TI Operator / Service Provider:** The OpenCSIRT Foundation operates the TI service based on a mixture of external service providers and own staff members.

8.2 TI Status: "Listed", "Accreditation Candidate" and "Accredited"

As you received this invitation, your team already has acquired the "listed" status, meaning its general information is already present in the TI Directory on the public TF-CSIRT web site (https://www.tf-csirt.org/trusted-introducer/). This invitation is aimed at your reaching out for "accredited" status, thereby passing the intermediate "accreditation candidate" status.

The various statuses are characterised as follows:

- **Listed:** Information about the team is available indicating that the team's service or operation is within the scope of the TI framework. This information is preferably provided by the team itself but can also be harvested from other sources (news spread within the community, public directories).

- **Accreditation Candidate:** Temporary intermediate phase for teams acquiring "accredited" status, with only two possible outcomes: formal accreditation if the team formally meets the defined criteria within the specified period or fall back to "listed" status when it does not.
- **Accredited:** Detailed operational information about the team is available, obtained from individuals representing its organisation, thus ensuring authenticity and correctness. The team participates in the international community of CERTs and security teams and maintains the actuality of the information it had provided.

8.3 Validation of Information

To acquire "accredited" status a team must provide a useful, but limited, amount of operational information. The TI accreditation process focuses primarily on the team's statements on those criteria that the TI will use to gauge its operational status and standing. Statements can be provided in various forms, as filled-out form, as answers to additional questions, etcetera. Any such statement has three properties the TI framework depends on and needs to be recognized here:

- **Authenticity:** This means that the TI team can be sure that the statement came from the team and/or its parent organisation. This includes the integrity of the information of course: if the integrity is not assured then it is not authentic in any case.
- **Actuality:** The statement reflects the current state of affairs, and not one of a past no longer applicable. Actuality can only be achieved when statements are maintained: *maintenance* and *actuality* are two sides of the same coin.
- **Correctness:** This requires that the statements are more than just authentic and actual: they are met by reality. This can only be checked by – essentially – performance or quality measurements of a team's ability and performance. Within the certification available to accredited teams correctness of information is of critical importance.

The TI accreditation process concentrates on the *authenticity* and *actuality* properties of team statements alone: to check *correctness* is now part of the certification processes within the TI framework, for which you might apply once being accredited.

To ensure[9] the *authenticity* of information coming from "accredited" teams or "accreditation candidates", verification of the source of information is essential. One of

[9] „Ensuring" is to be understood as in statistics, i.e. if something is ensured, there is a high probability – definition of „high" deducible from the context – that it is in fact true: in matters of security there is no such thing as absolute certainty.

the following two procedures are considered necessary and sufficient as verification method of the TI process:

- Direct (eye) contact is established with an individual from the team and/or its parent organisation who can prove the facts about the team and its operation. At least the personal ID is checked, and the individual can prove his/her right to represent the team and/or its parent organisation.
- Indirect (cyber) contact is established with an individual from the team and/or its parent organisation who can prove the facts about the team. Such contacts are secured with strong cryptography, and the identity of the individual must be linked to a cryptographic key that has been certified including a check of the personal ID. The individual can prove his/her right to represent the team and/or its parent organisation.

To ensure the *actuality* of information, all full-member teams (TI Accredited and Certified) are expected to keep the information they provided up-to-data. To help them meet that goal, the TI team entertains a four (4) monthly maintenance cycle, prompting all teams which have not been updated for four months. Also, any changes that the TI team happens to notice by itself, are fed back to the related teams for validation, thus again prompting an update to the information set, like expired GPG/PGP keys or email bounces.