

ANNEX A: MODEL FOR THE REQUEST FOR THE RELEASE OF FUNDS

Annexes:

Summary of checks performed by relevant authorities on the steps for which funding is requested, including weaknesses identified and any corrective actions taken.

Fiche to be used for each step:

The step under review	National and governmental CERTs are operational and reach at least 'accredited' status on TF CSIRT Trusted Introducer.
Baseline	Based on the Law on Cybersecurity adopted by the Kosova Assmebly last year, the Cybersecurity Agency- CSA (as a Cybersecurity National Competent Authority defined in NIS) is in the process of being established (the first call for applications to be published in June 2024). The National CERT will be integrated into the CSA as National Centre for Prevention and Response to Cyber Incident (NCPRCI) department. Based on the organizational chart approved by the PM, the NCPRCI department will have 12 staff. The Government CERT will be part of the Agency for Information Society (AIS). The new organizational chart of AIS is being drafted and will be approved by the end of Q3-2024.
Deadline of the step	June 2026
Actual results	The national CERT (KOS-CERT) has maintained Accredited status within the TF-CSIRT Trusted Introducer framework since 3 July 2017, demonstrating continuous compliance with the Trusted Introducer requirements related to incident response, information sharing and international cooperation. The accreditation process has been completed following all the required steps. An initial application request was submitted, followed by the completion and submission of Appendix A (signed and officially registered). Subsequently, Appendices B & C were completed and returned to the accreditation body. All required documentation has been submitted, and the accreditation procedure has been finalized in line with the prescribed process. GovCERT (XK) has been operational and listed in the TF-CSIRT Trusted Introducer directory since 16 July 2025. During the reporting period, GovCERT initiated and continued the activities required under the TF-CSIRT Trusted Introducer accreditation process. These activities include the preparation and submission of the application for accreditation, completion and submission of the required Trusted Introducer documentation (Appendix A and Appendix B & C), review and alignment of operational procedures with the Trusted Introducer requirements, and continued cooperation with the Trusted Introducer

	accreditation team throughout the accreditation process. In 2025, Kosovo further strengthened its national CSIRT capacities through the certification of two Open CSIRT Foundation Certified SIM3 Auditors, increasing national expertise in CSIRT maturity assessments and supporting the continuous improvement of CSIRT capabilities in accordance with internationally recognised best practices. As of June 2026, KOS-CERT fulfils the accreditation requirement of this reform step by maintaining Accredited status within the TF-CSIRT Trusted Introducer framework. GovCERT (XK) is operational and continues implementing the remaining activities required to complete the Trusted Introducer accreditation process. Moreover, the verification was performed through a review of the TF-CSIRT Trusted Introducer directory, verification of the accreditation status of KOS-CERT and the operational status of GovCERT (XK), as well as an assessment of the supporting documentation related to the Trusted Introducer accreditation process. The supporting documentation reviewed included the Trusted Introducer application, the completed Appendix A and Appendix B & C forms, and the Trusted Introducer accreditation certificate issued to KOS-CERT. The review confirmed that KOS-CERT maintains Accredited status within the TF-CSIRT Trusted Introducer framework. It also confirmed that GovCERT (XK) is operational and listed in the Trusted Introducer directory while continuing the activities required to achieve Accredited status. Furthermore, the review confirmed that Kosovo strengthened its national CSIRT capabilities through the certification of two Open CSIRT Foundation Certified SIM3 Auditors in 2025, contributing to enhanced national expertise in CSIRT maturity assessments and alignment with internationally recognised best practices.
Evidence provided	1. Accreditation information of KOS-CERT in TF-CSIRT Trusted Introducer Directory https://tf-csirt.org/trusted-introducer/directory/teams/kos-cert/ 2. Status of GovCERT (XK) in TF-CSIRT Trusted Introducer Directory https://www.trusted-introducer.org/trusted-introducer/directory/teams/govcert-xk/ 3. Trusted Introducer Accreditation Certificate of KOS-CERT. 4. Initial application submitted to the Trusted Introducer. 5. Trusted Introducer Appendix A (template) 6. Trusted Introducer Appendix B & C (template) 7. Open CSIRT Foundation – Certified SIM3 Auditors (Kosovo)

	https://opencsirt.org/csirt-maturity/certified-auditors/
Checks performed in the verification of the step and related findings	During verification of the step, all available and possible evidence has been collected and reviewed. The evidence has been listed down in the checklist on the conducted verification, and all documents supporting the verification have been properly stored (in order to ensure audit trail). The following checks were conducted: • All available documentation in line with the level of the achievement (as attached to this report) has been reviewed to verify the current stage of the reform step; • Compliance with the descriptive part of the reform step from the Commission Implementing Decision has been verified to the maximum possible extent and scope (as evidenced by the documentation available); • The attached documentation can confirm non-fulfilment of the reform step, as presented in this report; The results of the checks indicate that the reform step has not been fully fulfilled by the end of the reporting period (June 2026). As soon as the information is received by the Implementing units on the complete achievement and fulfilment of the reform step, the checks will be re-performed and repeated to verify the underlying completion / fulfilment.
Compliance with general principles and DNSH principle	The implementation of the steps does not contravene the general principles outlined in Article 4 and 11(4) of Regulation (EU) 2024/1449 and Article 3 of the Facility Agreement. The implementation of the steps does not contravene the 'Do No Significant Harm' (DNSH) principle.
Double funding	No financial contributions from third parties have been identified in support of the implementation of this reform step.
Clear conclusion on the achievement of the step	The step is partially fulfilled. KOS-CERT fully complies with the accreditation requirement by maintaining Accredited status within the TF-CSIRT Trusted Introducer framework. GovCERT (XK) is operational and continues implementing the remaining activities required to obtain Accredited status. Kosovo has also strengthened its national CSIRT capacities through the certification of two Open CSIRT Foundation Certified SIM3 Auditors, supporting continuous organisational maturity and alignment with internationally recognised CSIRT standards.

ANNEX A: MODEL FOR THE REQUEST FOR THE RELEASE OF FUNDS

Annexes:

Summary of checks performed by relevant authorities on the steps for which funding is requested, including weaknesses identified and any corrective actions taken.

Fiche to be used for each step:

The step under review	National and governmental CERTs are operational and reach at least 'accredited' status on TF CSIRT Trusted Introducer.
Baseline	Based on the Law on Cybersecurity adopted by the Kosova Assmebly last year, the Cybersecurity Agency- CSA (as a Cybersecurity National Competent Authority defined in NIS) is in the process of being established (the first call for applications to be published in June 2024). The National CERT will be integrated into the CSA as National Centre for Prevention and Response to Cyber Incident (NCPRCI) department. Based on the organizational chart approved by the PM, the NCPRCI department will have 12 staff. The Government CERT will be part of the Agency for Information Society (AIS). The new organizational chart of AIS is being drafted and will be approved by the end of Q3-2024.
Deadline of the step	June 2026
Actual results	The national CERT (KOS-CERT) has maintained Accredited status within the TF-CSIRT Trusted Introducer framework since 3 July 2017, demonstrating continuous compliance with the Trusted Introducer requirements related to incident response, information sharing and international cooperation. The accreditation process has been completed following all the required steps. An initial application request was submitted, followed by the completion and submission of Appendix A (signed and officially registered). Subsequently, Appendices B & C were completed and returned to the accreditation body. All required documentation has been submitted, and the accreditation procedure has been finalized in line with the prescribed process. GovCERT (XK) has been operational and listed in the TF-CSIRT Trusted Introducer directory since 16 July 2025. During the reporting period, GovCERT initiated and continued the activities required under the TF-CSIRT Trusted Introducer accreditation process. These activities include the preparation and submission of the application for accreditation, completion and submission of the required Trusted Introducer documentation (Appendix A and Appendix B & C), review and alignment of operational procedures with the Trusted Introducer requirements, and continued cooperation with the Trusted Introducer

	accreditation team throughout the accreditation process. In 2025, Kosovo further strengthened its national CSIRT capacities through the certification of two Open CSIRT Foundation Certified SIM3 Auditors, increasing national expertise in CSIRT maturity assessments and supporting the continuous improvement of CSIRT capabilities in accordance with internationally recognised best practices. As of June 2026, KOS-CERT fulfils the accreditation requirement of this reform step by maintaining Accredited status within the TF-CSIRT Trusted Introducer framework. GovCERT (XK) is operational and continues implementing the remaining activities required to complete the Trusted Introducer accreditation process.
Evidence provided	1.Accreditation information of KOS-CERT in TF-CSIRT Trusted Introducer Directory https://tf-csirt.org/trusted-introducer/directory/teams/kos-cert/ 2.Status of GovCERT (XK) in TF-CSIRT Trusted Introducer Directory https://www.trusted-introducer.org/trusted-introducer/directory/teams/govcert-xk/ 3.Trusted Introducer Accreditation Certificate of KOS-CERT. 4.Initial application submitted to the Trusted Introducer. 5.Trusted Introducer Appendix A (template) 6.Trusted Introducer Appendix B & C (template) 7.Open CSIRT Foundation – Certified SIM3 Auditors (Kosovo) https://opencsirt.org/csirt-maturity/certified-auditors/
Checks performed in the verification of the step and related findings	The verification was performed through a review of the TF-CSIRT Trusted Introducer directory, verification of the accreditation status of KOS-CERT and the operational status of GovCERT (XK), as well as an assessment of the supporting documentation related to the Trusted Introducer accreditation process. The supporting documentation reviewed included the Trusted Introducer application, the completed Appendix A and Appendix B & C forms, and the Trusted Introducer accreditation certificate issued to KOS-CERT. The review confirmed that KOS-CERT maintains Accredited status within the TF-CSIRT Trusted Introducer framework. It also confirmed that GovCERT (XK) is operational and listed in the Trusted Introducer directory while continuing the activities required to achieve Accredited status. Furthermore, the review confirmed that Kosovo strengthened its national CSIRT capabilities through the certification of two Open CSIRT Foundation Certified SIM3 Auditors in 2025, contributing to enhanced national expertise in

	CSIRT maturity assessments and alignment with internationally recognised best practices.
Compliance with general principles and DNSH principle	The implementation of the steps does not contravene the general principles outlined in Article 4 and 11(4) of Regulation (EU) 2024/1449 and Article 3 of the Facility Agreement. The implementation of the steps does not contravene the ‘Do No Significant Harm’ (DNSH) principle.
Double funding	No financial contributions from third parties have been identified in support of the implementation of this reform step.
Clear conclusion on the achievement of the step	The step is partially fulfilled. KOS-CERT fully complies with the accreditation requirement by maintaining Accredited status within the TF-CSIRT Trusted Introducer framework. GovCERT (XK) is operational and continues implementing the remaining activities required to obtain Accredited status. Kosovo has also strengthened its national CSIRT capacities through the certification of two Open CSIRT Foundation Certified SIM3 Auditors, supporting continuous organisational maturity and alignment with internationally recognised CSIRT standards.

Membership Certificate

KOS-CERT

has been accredited by
TF-CSIRT Trusted Introducer since

3 July 2017

valid for

2026

on behalf of
Trusted Introducer



Dr. Klaus-Peter Kossakowski
TI Service Manager

on behalf of
TF-CSIRT



Věra Mikušová
TF-CSIRT Chair



From Shpend Lutfiu

To ti@trusted-introducer.org

2/8/2017, 10:04 AM

Subject **Request for Accreditation - KOS-CERT**

Dear Sir/Madam,

Now that KOS-CERT is listed Team we want to begin the process of accreditation so we kindly ask you if you can send us the "invitation package" materials needed to prepare for this process also the email contact where we can address the questions we may have regarding accreditation issue.

Best regards,



Shpend Lutfiu

Zyrtar i Lartë për Siguri të Rrjetave
High Officer for Network Security

Njësia Nacionale për Siguri Kibernetike/KOS-CERT

National CyberSecurity Unit /KOS-CERT

Autoriteti Rregullator i Komunikimeve Elektronike dhe Postare / ARKEP

Regulatory Authority of Electronic and Postal Communications / RAEPC

Adresa: Rruga "Bedri Pejani" Nr.23, 10000 Prishtinë-Kosovë

Tel: +381 (0)38 200 28563

Tel mob: +377 44 986 677

Web site: <https://www.kos-cert.org>

E-mail: shpend.lutfiu@kos-cert.org

PGP/GPG Key ID: 0x4F9A9DF9

Fingerprint: 5E3C 72CC B690 D421 115A 9C27 37CB 994E 4F9A 9DF9

🌱 ju lutem keni parasysh ruajtjen e ambientit para se te shtypni kete e-mail

🌱 please consider the environment before printing this e-mail

Important: This e-mail and any attachment(s) are intended for the addressees above named only and may be confidential. If you are not an addressee please notify me immediately. You must not copy or disclose the contents to any third party. Internet e-mail is not a fully secure communications medium. Please take this into account when sending e-mail to me. Any attachment(s) to this e-mail are believed to be free from virus, but it is the responsibility of the recipient to make all the necessary virus checks.



4 APPENDIX A: FORM TO ACCEPT THE INVITATION TO ACQUIRE TI “ACCREDITED” STATUS

Team 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” Version 2.3 – 09 January 2017 (in short: Invitation Package) as sent to us by the Trusted Introducer service provider (in short: TI), and that we support the criteria, procedures 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 C;*
- *commit **ourselves** to file completed appendices B and C of the Invitation Package to the TI within two (2) months;*
- *agree to the publication of various data, as specified in the Invitation Package, on the public and restricted TI web sites (note on privacy: personal data will appear on the public web site if marked as “public”);*
- *commit **ourselves** to pay a one-off amount of EUR 800 to GÉANT (formerly TERENA) to cover the cost of the application for “accredited” status (VAT might apply);*
- *declare that we have taken note of, and intend to pay, the annual fee of EUR 1,200 (VAT might apply) that is due to GÉANT (formerly TERENA) if and when we obtain “accredited” status.*

City, Country, Date: _____

Name of Representative: _____

Signature: _____



INFORMATION TO OBTAIN TI "ACCREDITED" STATUS

Team Name:

INDEX

5	APPENDIX B:	
	INFORMATION TEMPLATE FOR "ACCREDITED" TEAMS.....	3
5.1	Mandatory Fields describing the Team.....	4
5.2	Optional Fields describing the Team.....	7
5.3	Service related Fields used internally by the TI.....	9
6	APPENDIX C:	
	CRITERIA FOR "ACCREDITED" STATUS.....	11
6.1	Explanation and Guidance.....	11
6.2	List of all Criteria.....	11

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 *members-only* TI 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* TI web site. The whole world can potentially access and read this.
- **SECURE:** this information will only be published on the *members-only* TI 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* TI web site, you might indicate this accordingly. Also if you would like to have different information published on the *public* and the *members-only* TI 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 can not 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: [CHOOSE 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 it's networks.
- All countries in which constituency members are located in

Contact Information PUBLIC

- Regular telephone number (country code, telephone number, timezone)
- Emergency telephone number (country code, telephone number, timezone)
- Facsimile number (country code, telefax number, timezone)
- Other telecommunication facilities (if applicable)
- Postal address of team
- E-mail address of team
 - 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, timezone)
 - Mobil telephone number (country code, telephone number, timezone)
 - Facsimile number (country code, telefax number, timezone)
 - Other telecommunication facilities (if applicable)
 - Postal address if different from team
- E-mail address
 - 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, timezone)
 - Mobil telephone number (country code, telephone number, timezone)
 - Facsimile number (country code, telefax number, timezone)
 - Other telecommunication facilities (if applicable)
 - Postal address if different from team
 - E-mail address
 - 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 it's 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! | |
| ■ 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)

- 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 others 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)

Transit I – Training/Workshop

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" imply 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:
 - phone:
 - mobil: 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 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 **SHOULD**S are strong recommendations, not obligations.
- **MUST** and **SHOULD** are defined according to IETF standards, see Appendix D.

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

- 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 your team and the TI Personal Introducer.
- If you support a **SHOULD** criteria, put down "supported".
- If you do not support a **SHOULD** criteria, put down "not supported". Explain if needed or indicate planned support.

6.2 List of all Criteria

1. 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.

YOUR SUPPORT:

2. Teams **MUST** cooperate with the publication of all delivered data on the TI **members-only** website. Access is restricted to "accredited" teams (including all certified teams), TI Associates, the TI team and the TF-CSIRT SC.

YOUR SUPPORT:

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

YOUR SUPPORT:



4. Teams **MUST** register two team representatives.

YOUR SUPPORT:

5. Teams **MUST** present at least their external services, if any, to the outside world as per RFC 2350,¹ including a specification of quantitative values and ensure that these descriptions continue to match reality, including indicated service levels.

YOUR SUPPORT:

6. 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.

YOUR SUPPORT:

7. 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.

YOUR SUPPORT:

8. 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.

YOUR SUPPORT:

9. Teams **MUST** recognise and support the "Information Sharing Traffic Light Protocol"² as ratified by the TI Accredited Teams.

YOUR SUPPORT:

10. 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.

YOUR SUPPORT:

¹<http://www.ietf.org/rfc/rfc2350.txt>

²<https://www.trusted-introducer.org/ISTLPv11.pdf>



11. Teams SHOULD actively support the signing of their team and representatives GPG/PGP keys, during TI/TF-CSIRT meetings and other occasions, by the TI team.

YOUR SUPPORT:

12. Teams SHOULD regularly attend TI and TF-CSIRT meetings.

YOUR SUPPORT:

Explanation: It depends from RAEPC annual budget allocated by the Government.

13. Teams SHOULD comply with the "CSIRT Code of Practice"³ as ratified by the TI Accredited Teams.

YOUR SUPPORT:

14. Teams SHOULD use the "SIM3 Maturity Model"⁴ as a starting point for self-assessments or audits of their services.

YOUR SUPPORT:

Explanation: Planned to be adopted after reviewed by legal Department.

15. Teams MUST pay the fees established for acquiring and maintaining "accredited" status as set by GÉANT (formerly TERENA).

YOUR SUPPORT:

16. Teams SHOULD respond to TI reaction tests to demonstrate that they can be reached via their official contacts.

YOUR SUPPORT:

³<https://www.trusted-introducer.org/CCoPv21.pdf>

⁴<https://www.trusted-introducer.org/SIM3-Reference-Model.pdf>