ETIS - THE COMMUNITY OF TELECOM PROFESSIONALS

ETIS CERT-SOC Working Group Guidelines

Version: v1.0

5th September 2022

etis

1. Definitions

Within these Guidelines, the following terms with capital letters have the following meaning as defined below.

Attendee: A Member, a Central Office Representative or a Participating Guest taking part to a Working Group Activity (the notion of "Attendee" therefore excludes any "Visiting Guest");

Guidelines: The present guidelines;

Information: Any information (of whatever nature, age and form or format) that is exchanged and shared among Attendees within the framework of the Working Group Activities. It includes information, which is received in writing, electronically, or orally, offline, and online. Types of Information include, but are not limited to best practices, challenges and use-cases, trends and strategic topics, benchmarking, surveys, KPIs, working papers, discussion reports, feedback from peers on questions related to their experience in a particular area. Topics include, but are not limited to information about cybersecurity, cybersecurity incidents, data leaks, cyber security situational awareness, cyber threats and vulnerabilities, cyber threat indicators of compromise/attack, security vulnerabilities, alerts, attack actors or campaigns, mitigation measures, best practices, observations and opinions about any of these topics, identity of Attendees, date of activities, specific contributions or topics discussed…); cooperation; overall security of the telco infrastructure; threat intelligence sharing (most recent threats, intelligence, practical use cases, MISP); incident handling and management (responsibilities, processes, documenting, learnings, incident response); vulnerability and risk management (most recent trends, challenges and threats, risks, opportunities, priorities); governance (position in the organizational structure, team structure, allocation of responsibilities and resources, talent acquisition); internal and external security and protection (data, devices, infrastructure protection, awareness, education);

Member: An individual coming from a Partner who became member of the Working Group pursuant to art. 4.1 of the Guidelines;

Visiting Guest: An individual invited to a Working Group Activity according to art. 4.5 of the Guidelines;

Participating Guest: An individual invited to a Working Group Activity according to art. 4.4 of the Guidelines;

Partner: A "Partner" as defined in art. 1 of the ETIS' Regulations;

Recipient: An Attendee who has access to Information in the framework of the Working Group Activities;

Source: An Attendee who first discloses any particular Information in the framework of the Working Group Activities;

Third Party: A person who is not an Attendee, Member, Central Office Representative or Participating Guest (including, but not limited to Visiting Guests, journalists, media…);

Working Group: The CERT-SOC telco network Working Group;

Working Group Activities: All activities organized either by the Working Group or by one or more of its Members acting in this capacity and related to such activities. They include, but are not limited to: projects, discussions, events, phone calls, meetings, videoconferences, e-mails exchanges, seminars, webinars, online calls, online community, annual community gathering, workshops, Tebit benchmark…, whether these activities take place in person or virtually.

2. Working Group CERT-SOC Guidelines

In accordance with article 13 of the Regulations, the Central Office establishes the Guidelines, which are then approved by the Management Board.

The present Guidelines were discussed among the Members then confirmed by the Central Office by a decision and approved by the management board by a Resolution.

The Central Office may, at any time, amend, update, delete or supplement all or part of the provisions of the Guidelines or their appendixes. Such amendments shall be notified by e-mail to the Members, who have one (1) month from the date of sending of this e-mail to express their suggestions, sent to the Central Office by e-mail. Any change must be approved according to article 13 of the Regulations.

3. Scope

The present Guidelines govern the functioning of the Working Group as well as the rights and obligations of Attendees in participating in Working Group Activities. According to article 13 of the Regulations, the Working Group, that is to say the Working Group Members, must follow the Guidelines. In the framework of the Working Group Activities, Members act on behalf of the Partner of which they come from.

Working Group Activities are a 'safe space', where topics can be discussed in a non-discriminatory and non-political way, without worry or fear that the information could be leaked to Third Parties. Working professionally and securely with sensitive Information is of the utmost importance for the Working Group. The leaking of sensitive Information can directly or indirectly harm the image and reputation of the Members and/or any other parties involved. Additionally, the mishandling of sensitive Information may impact the future willingness of Members to share Information.

Therefore, the Working Group has a strict set of rules on Information sharing to establish and maintain trust. The Guidelines govern the exchange of Information among the Attendees within the framework of the Working Group Activities.

4. Members, Guests and attendance

4.1 Membership

The following rules apply to Memberships:

- All candidates must be individuals coming from Partners that hold a position relevant to the subject matter of the Working Group;
- All candidates must have read and understood the Guidelines and declare that they have done so ;
- The application must indicate the candidate's position in the Partner, and his/her department and hierarchical level;
- In accordance with article 13 of the Regulations, the application is only valid as long as the Partner from which the candidate comes agrees and respects the Guidelines of that Working Group. It means that the Partner must have read, understood and agreed to respect the Guidelines.

Any individual who meets the above requirements may apply for membership in the Working Group. All applications must be sent to the Central Office. The Central Office may forward the

application to the Working Group core team, which may provide comments. Within one month of receiving an application, the Central Office will decide on it at its sole discretion. If the application is accepted, the Central Office notifies the candidate, who then immediately becomes a Member. If the application is rejected, the candidate may submit a new application within two months of the rejection.

4.2 The core team

The chairman(chairwoman) and three vice-chairmen are Members who form the "core team" that handles the day-to-day activities of the Working Group. They create long-term strategies and plans for the group, and moderate physical meetings.

The Special Conditions as defined in the Regulations apply to decisions taken by the core team.

The missions, rights and obligations of the core team Members are defined by the Central Office, which informs them of the content of these missions and of any possible modification. Such information is also transmitted to all Members.

Elections for the positions of the core team Members are held at least every two years within the Working Group. Specific elections, targeting one or more of the core team positions may be held at any time:

- Whenever at least two thirds of the Members request it;
- As soon as one of the core team Members leaves her/his position for any reason.

All elections are announced three (3) weeks before the election day through an e-mail sent by the chairman(chairwoman) to all Members. The e-mail mentions which position(s) is(are) open, the date of the next physical meeting when the vote will take place (or if the vote takes place via email), and the last day candidacies can be sent by Members to the chairman(chairwoman). To be valid, a candidacy must mention which position(s) it applies to and respect the deadline.

Members may run for the chairman(chairwoman) position, one vice-chairman(chairwoman) position, or both.

If the chairman(chairwoman) position was open, the vote for this position always takes place first. The candidate for that position with the most votes becomes the new chairman(chairwoman). She/he is no longer a candidate for the other position(s).

After the potential chairman(chairwoman) position has been filled:

> If one of the vice-chairmen positions was open, the vote for this position takes place among the remaining candidates. The candidate with the most votes becomes a vice-chairman(chairwoman).
>
> If several of the vice-chairmen positions were open, the votes take place in a successive way:
>
> > Firstly, the vote for the first open vice-chairman(chairwoman) position takes place among the remaining candidates. The candidate with the most votes becomes a vice-chairman(chairwoman). She/he is no longer a candidate for the other position(s).
> >
> > Secondly, the vote for the second open vice-chairman(chairwoman) position takes place among the remaining candidates. The candidate with the most votes

becomes a vice-chairman(chairwoman). She/he is no longer a candidate for the other position(s).

Thirdly, if there were three vice-chairmen positions to fill, the vote for the third open vice-chairman(chairwoman) position takes place among the remaining candidates. The candidate with the most votes becomes a vice-chairman(chairwoman).

If any difficulty arises which makes it difficult to appoint or elect any of the core team Members, the Management Board or the Council may nominate any of the core team Members.

4.3 Attendance

Only Central Office Representatives and Members may be Attendees, no Members substitutes are allowed. Any Attendee who notices that an unauthorized person is participating in a Working Group Activity must immediately notify the chairman(chairwoman).

However, by exception, the Central Office can authorize a Member substitution for a set period of time, if asked in advance, at least one day before a physical meeting, or at least two hours before a call/webinar.

If the Central Office takes such a decision, it informs the Members. The substitute Member must meet the requirements applicable for any Member.

4.4 Participating Guests

By exception to articles 4.1 to 4.3 and explicit written and prior permission only, given at their sole discretion by the Central Office, all the Core Members and Central Office Representatives participating to a particular Working Group Activity, specifically invited Participating Guests may be allowed to participate in an individual Working Group Activity. The Participating Guests are not considered as Members as defined in the Guidelines.

Participating Guests must meet the following requirements: before they are invited to a Working Group Activity, Participating Guests must read and understand the Guidelines:

- All Participating Guests must be individuals, and specify the capacity in which they attend: either acting on their own behalf or on behalf of an organization (*e.g.* employees, managers…);
- All Participating Guests must have read and understood the Guidelines and declare that they have done so;
- The Participating Guests must indicate their position in their organization, and his/her department and hierarchical level (if the Participating Guests act on their own behalf: their activity);
- The organization from which the Participating Guests come must have read, understood and agreed to respect the Guidelines (if the Participating Guests act on their own behalf: the Participating Guests themselves must have read, understood and agreed to respect the Guidelines).

4.5 Visiting Guests

When the Participating Guest's acceptance process would make it too difficult to invite certain people whose input to certain Working Group Activities is deemed valuable, they can be invited as Visiting Guests. The Visiting Guests are not subject to the Guidelines and are not Attendees as defined in the Guidelines.

By exception to articles 4.1 to 4.3 and explicit written and prior permission only, given at their sole discretion by the Central Office, all the Core Members and Central Office Representatives participating to a particular Working Group Activity, specifically invited Visiting Guests may be allowed to participate in part or whole of an individual Working Group Activity.

Visiting Guests must meet the following requirements:

- All Visiting Guests must be individuals, and specify the capacity in which they attend: either acting on their own behalf or on behalf of an organization (*e.g.* employees, managers…);
- The Visiting Guests must indicate their position in their organization, and his/her department and hierarchical level (if the Guests act on their own behalf: their activity);

5. The Traffic Light Protocol

5.1 Principles

The Traffic Light Protocol (TLP) v. 2.0, as defined by the FIRST (Forum of Incident Response and Security Teams) Traffic Light Protocol Special Interest Group and as available on https://www.first.org/tlp, is considered to be part of the Guidelines.

5.2 General information

The TLP is applied to Attendees, subject to the following clarifications:

- In conjunction with the TLP, The Chatham House Rule always applies to Information exchanged among Attendees within the framework of the Working Group Activities, unless otherwise specified;
- Whenever the TLP mentions "recipients", the relevant rule applies to Recipients;
- Whenever the TLP mentions "sources", the relevant rule applies to Sources;
- Whenever the TLP mentions "participants", the relevant rule applies to Attendees;
- Whenever the TLP mentions "organizations", the relevant rule applies to Partners (or organizations in the case of Participating Guests);
- Each Member having declared that they have read and understood the Guidelines, the above-mentioned obligation of the Sources to ensure that Recipients of TLP information understand and can follow TLP sharing guidance is considered to be properly performed.
- TLP:RED implies that a Member may not share Information within the Partner she/he comes from, either with her/his superiors or her/his hierarchical inferiors. This means that the Partners know that they cannot request any information on this subject from the Members, whether or not they are employed by them.

5.3 Details about the Information

Whenever Information is shared within the framework of the Working Group Activities, the Source will disclose the following details about the Information:

- A description of the Information, as detailed as possible;

- The origin of the Information (unless it comes from an anonymous source, *e.g.*, through a whistleblower, or the Source desires to keep this origin confidential for other reasons. In these cases, the reason the origin is not mentioned is indicated);

- If the Information has already been verified or not;

Sources shall endeavor to ensure that any Information shared during Working Group Activities is accurate. However, should it not be the case, all Attendees understand and accept that the Information is provided during Working Group Activities in good faith. Sources shall only share Information they consider useful. Sources will ensure that, as much as possible, the information shared is anonymous.

With the exception of written notes, Members will not record any Information without the Source and other present Attendee's explicit prior and written permission. This rule applies regardless of the type of Information recorded (including but not limited to audio, video, image, document) and regardless of the manner in which the Information is recorded (including but not limited to: microphone, camera, video camera, screenshot capture, video acquisition). Information shared in the context of the Working Group Activities must be handled objectively, for security purposes, and may not be used for gaining competitive, political or other advantages.

5.4 Rule by default

Any Information for which the applicability of the TLP and/or TLP classification and/or CHR is unknown or uncertain shall automatically fall under TLP: AMBER + CHR.

5.5 Contact with Third Parties

Attendees will not engage or talk to Third Parties about Information, unless the Guidelines specifically authorize it. Regarding Information of which the TLP classification authorizes sharing with Third Parties, all references to the Source that shared the Information must be removed. If a Recipient needs to share the Information more widely than indicated by the original TLP designation, he or she must obtain explicit permission from the Source. When in doubt, the Attendees are aware that even confirming or denying the authenticity or content of Information from Working Groups Activities may already constitute a potential breach of the Guidelines.

In their contacts with Third Parties, Members may, with the core team's written permission, limited to a particular event, indicate they are Members of the Working Group.

5.6 Inapplicability of the TLP/CHR

A Recipient shall not be required to treat Information pursuant to the TLP/CHR if and to the extent that this Recipient can show that the Information is:

- In the public domain otherwise than in breach of the Guidelines;
- Information which the Recipient can show to have been already in its possession without any obligation of confidentiality and prior to the confidential disclosure pursuant to the Guidelines;
- Information which the Recipient can show that he or she developed independently of the Source;
- Information obtained without obligation of confidentiality from a Third Party who is free to divulge it without obligation of confidentiality.

In this scenario, the Recipient immediately informs the Source before further sharing. If required, the Recipient will bear the burden of proof for the inapplicability of the TLP/CHR.

6. Members' responsibilities

Members must respect the Guidelines. Failure to comply with the Guidelines will engage the liability of the Partner they come from. In the event of a breach of the Guidelines, without

prejudice to the right of ETIS to demand compensation of damages caused, ETIS has the right to immediately, without period of notice and without cost to ETIS, terminate or suspend the membership(s) to the Working Group CERT-SOC of one, several or all the Member(s) coming from this Partner;

In the event of repeated or severe breach(es) of these Guidelines, without prejudice to the right of ETIS to demand compensation of damages caused, ETIS has the right to:

- immediately, without period of notice and without cost to ETIS, terminate or suspend the membership(s) to the Working Group CERT-SOC of one, several or all the Member(s) coming from this Partner;
- immediately, without period of notice and without cost to ETIS, terminate or suspend the membership(s) to any other Working Groups of one, several or all the member(s) coming from this Partner;
- terminate or suspend the collaboration with the Partner

In such an event, any and all Partner subscription fees shall not be reimbursed.

Information that is relevant to one Member may not be relevant to another. If ETIS withholds certain information, it could prevent some potentially interested Members from accessing it. To avoid such a situation, ETIS will inform the chairman(chairwoman) of all Information related to security incidents and threats that is brought to its attention, irrespective of the Information origin. The chairman(chairwoman) will then decide on the relevance of sharing this information with the Members. Each Member is then individually responsible for determining the reliability, relevance and potential impact of the Information, as well as the actions that should be taken. Members shall make their own judgement as regards the use of any shared Information. ETIS solely acts as a facilitator and platform for the Working Group Activities. ETIS does not act as an intermediary, e.g., by withholding Information. ETIS will not store, filter, process or act upon the data and will not be responsible regarding the accuracy or relevance of Information shared with Members.

7. Participating Guests' responsibilities

Participating Guests must respect the Guidelines. They must respect the rules and responsibilities to which Members are subject but without having their rights (especially: decision or election process, Mattermost and MISP uses). Failure to comply with the Guidelines will engage the liability of the organization they come from (if the Participating Guests act on their own behalf, failure to comply with the Guidelines will engage their own liability). In the event of breach of these Guidelines, ETIS has the right to immediately, without period of notice and without cost to ETIS, terminate or suspend the collaboration with said organization (said Participating Guest), without prejudice to the right of ETIS to demand compensation of damages caused. In this event, authorization(s) to attend any Working Group Activities of all Participating Guests coming from organizations (all Participating Guests) involved is(are) terminated/suspended as well, and any fees paid by organizations (Participating Guests) involved will not be reimbursed.

8. Mattermost

A Mattermost chat platform ('Mattermost') is available to the Members.

To use Mattermost, a Member must request access from the Central Office. The Central Office will decide on the request within two weeks at its sole discretion. If the request is granted, the Central Office notifies the Member and with the collaboration of the Mattermost maintainer, an access is granted. If the request is denied, the Member may submit a new application within two months of the denial.

For the use of Mattermost, the following additional rules apply.

Note: the rules and restrictions in this article only apply to a Member from the Moment they request access to Mattermost. They then apply for the entire duration of a Member's access, and will continue to apply to any Information contained in or obtained through Mattermost, even if a Member no longer has access to Mattermost".

For the use of Mattermost, the following additional rules apply.

1. There shall be 1 (one) central Mattermost instance.
2. Mattermost shall be provided and maintained by ETIS or 1 (one) Member ('the maintainer'), which is chosen through popular vote of the Working Group.
3. The maintainer is responsible for the safety and security of Mattermost.
4. Members shall be aware that Mattermost keeps a record of messages. This message history is visible to Members that have access to a channel. It is the channel Members' sole responsibility to exercise due diligence and care in disseminating Information in public or private channels, and to take appropriate actions to respect the Guidelines.
5. Members will only access Mattermost using the Mattermost web environment, desktop client or mobile application. Other forms of access (e.g. 'bots' or API-access) are not allowed without *explicit prior permission* by the maintainer.
6. Members shall not create a record or document of any Information on Mattermost without the explicit prior permission of the owners of that Information.
7. It is the responsibility of Members to observe the Guidelines when using the Mattermost environment. Therefore, prospective or new Members are encouraged to study Mattermost's features and controls to act in accordance with the Guidelines.

9. MISP Guidelines

A MISP Threat Intel ('TI') exchange platform ('the Platform') is available to the Members.

To use the Platform, a Member must request access from the Central Office. The Central Office will decide on the request within two weeks at its sole discretion. If the request is granted, the Central Office notifies the Member and with the collaboration of the Platform maintainer, an access is granted. If the request is denied, the Member may submit a new application within two months of the denial.

For the use of the Platform, the following additional rules apply.

Note: the rules and restrictions in this article only apply to a Member from the Moment they request access to the Platform. They then apply for the entire duration of a Member's access, and will continue to apply to any Information contained in or obtained through the Platform, even if a Member no longer has access to the Platform.

1. There shall be one (1) central MISP instance, functioning as the hub in a 'hub-spoke' model
2. The Platform shall be provided and maintained by ETIS or one (1) Member ('the maintainer'), which is chosen through popular vote of the Working Group.
3. The Platform is not world-reachable. Each Member is required to provide the maintainer with the IPs or IP-ranges that they will use to connect to the Platform. It is the Member's responsibility to inform the maintainer if this Information changes.
4. Members shall only submit Threat Intelligence ('TI') to the platform that is actionable in nature and that they have validated for authenticity and relevance to the community ('curated data'). Supplying automatically generated and unverified indicators, such as originating from sandboxes or 'bulk TI feeds' is undesirable, and may lead to a temporary or permanent removal of access rights. In layman's terms: the MISP platform is solely intended to share largely unique and relevant TI within the community, and this should be TI that is not otherwise available through existing TI feeds, organizations, etc.
5. Partners shall only submit TI to the platform that follows the best practices for MISP (these may change over time). This includes, but is not limited to, grouping large amounts of IoCs such as URLs/IPs/domains/etc. into single objects (not individual sub-objects) to prevent context, graph and parsing complexities.
6. The modification of existing events from other parties, e.g. in case of additions, removal or enrichment of Information, shall happen using the MISP proposal system.
7. The default TLP classification for any TI shared within the community will be TLP:AMBER + CHR.
8. TI cleared for propagation beyond the community will be explicitly earmarked as "shareable" (e.g.: TLP:GREEN or TLP:WHITE) by the Member supplying it.
9. When TI is shared with Third Parties, all references to the Source that shared the Information must be removed.
10. If sharing is done through MISP, the Source Member shall be overwritten with the name of the Member that forwards the intelligence.
11. Admission of new Members to the platform requires membership verification and approval of the community or the maintainer.

10. Personal data protection

All personal data processed within the context of the Working Group Activities is processed according to the ETIS privacy policy, available on https://www.etis.org/page/privacy_policy.