Information Sharing Policy

Version 3.1 (April 2023)

Contents

Change Log

Publication Date	Document Version	Notes
2023-Apr-07	3.1	• Adoption of TLP 2.0 • Clarifies definition of “members of their own organization” as used with TLP:AMBER and TLP:AMBER+STRICT • Examples added to clarify TLP usage

1.0 Background

1.1 The REN-ISAC is a private community for sharing sensitive information regarding cyber security protection and response. Information shared within the REN-ISAC community relates to IT security measures and is privileged and confidential.

1.2 An institution or organization is the REN-ISAC "member" and is represented in information sharing by "member representatives". Information is shared to the member representative, not to the institution. Certain classifications of information cannot be further disseminated by the member representative. The member representative uses the shared information to formulate protection and response actions for the institution.

1.3 To maintain active status, all member representatives must agree to this policy.

2.0 Disclaimer

2.1 Information is shared by or within REN-ISAC for the objective of cyber security protection and response. Information is shared in good faith and there are no explicit or implied guarantees or warranties to the veracity or applicability of the information shared within REN-ISAC, and Members agree that such information is provided “as is”.

2.2 Information received from any REN-ISAC service, product, or member must be analyzed fully by representatives of the receiving institution, and inherent risks determined and understood. Any local action taken must be informed by local technical expertise and applied as appropriate to the local technical, functional, and cultural environments. Each Member is solely responsible for its own actions and determinations.

2.3 The REN-ISAC, its sponsoring organizations, and members accept no responsibility for negative impacts of any sort that result from local actions taken on information distributed within or by REN-ISAC publicly, to the membership generally, or to specific institutions.

3.0 Traffic Light Protocol

REN-ISAC utilizes a Traffic Light Protocol to classify and govern information sharing, as defined by the Cybersecurity Infrastructure Security Agency of the U.S. Federal Government [1]. The Traffic Light Protocol (TLP) was created to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s).

3.0.1 Sources are at liberty to specify additional intended limits of the sharing such as the Chatham House Rule (see Appendix I for definition): these must be explicitly stated and adhered to.

3.0.2 REN-ISAC requires the removal of REN-ISAC attribution unless otherwise indicated. This includes mailing list and member names. Therefore, emails from REN-ISAC lists should not be forwarded due to header contents potentially leaking those details. Rather, content should be paraphrased and redistributed.

3.1 TLP:CLEAR (Disclosure is not limited)

3.1.1 WHEN TO USE: Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

3.1.2 HOW TO USE: Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For examples, see Appendix II.

3.2 TLP:GREEN (Limited disclosure, restricted to the community)

3.2.1 WHEN TO USE: Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.

3.2.2 HOW TO USE: Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

3.3 TLP:AMBER (Limited disclosure, restricted to participants' organizations and their clients and customers on a need to know basis)

Note: The default scope for TLP:AMBER is all of REN-ISAC and any member organizations' clients and customers who need to know for operational protection. TLP:AMBER+STRICT restricts sharing to the REN-ISAC member organization only, the definition for which changes with the addition of the +STRICT scope (see Appendix I for definitions).

3.3.1 WHEN TO USE: Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

3.3.2 HOW TO USE: Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers (see Appendix I for definitions) who need to know the information to protect themselves or prevent further harm. Information marked TLP:AMBER+STRICT cannot be shared outside the organization, such as with outsourced non-member service providers or members of an education network.

3.3.3 Consider the following before sharing information marked TLP:AMBER:

1. Can be shared only for the purpose of a specific operational protection or response action - cannot be shared for general purpose situational awareness or enrichment.

2. Can be shared only with members of one's own organization, or its clients or customers (see Appendix I) who have need-to-know for operational defense, threat mitigation, or response.
3. Sharing must be guided by the principle of least privilege: i.e., to protect data, sources, methods, and relationships, only the minimum information necessary for local assessment and action should be shared.
4. The member who shares must have a reasonable expectation of trust in the recipient and must communicate that expectation to the recipient.
5. Must not contain identification of institutions, organizations, or individuals who have not authorized the release, unless the information is otherwise publicly available, or if the information is directly applicable to a warranted protection or response action.
6. If appropriate, may mention REN-ISAC, but must be scrubbed of the identification of REN-ISAC channel names (e.g., mailing list names, etc.), and the names of REN-ISAC information sources.

3.3.4 REN-ISAC member representatives are responsible and accountable for the disposition of TLP:AMBER and TLP:AMBER+STRICT information that they share within their organization, according to the terms described in section 7.0, Breach, and in the REN-ISAC Disclaimer.

3.4 TLP:RED (Not for disclosure, restricted to participants only)

3.4.1 WHEN TO USE: Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Therefore, TLP:RED should primarily be used for context and not for marking threat intelligence.

3.4.2 HOW TO USE: Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

3.5 Default Classification

3.5.1 All information shared within REN-ISAC is considered TLP:AMBER unless otherwise explicitly stated. As such, the default classification of TLP:AMBER applies to information shared in any manner, including, but not limited to, web pages, live chat, meetings, webinars, and other communications. The exceptions to this rule are noted below.

3.5.1.1 The XSec mailing list defaults to TLP:RED (see Appendix II for specific examples).

4.0 TLP and Automated Threat Intelligence (ATI)

4.1 The default classification of all data contributed to automated threat intelligence (ATI) is TLP:AMBER. However, each contributing member may change the default classification of the original data they contribute.

4.2 ATI data marked TLP:GREEN may be reshared with trusted third parties and other organizations that fit the TLP:GREEN redistribution audience.

4.3 REN-ISAC central adheres to all TLP markings. However, certain SES clients may allow a contributor to add modifications to TLP and therefore change the way submitted data may be shared by REN-ISAC. e.g., ATI data marked as TLP:AMBER will NOT be shared outside its TLP definition unless the contributor also clicks the "Submit anonymously to trusted partners" option in some of the ATI clients. The same would be true for TLP:AMBER+STRICT. The TLP marking is to be kept intact on the reshared indicator(s).

4.4 REN-ISAC members may share ATI data marked as TLP:GREEN or TLP:AMBER with their members, in the cases of SOCs and RENs; and with employees at their institutions who have a need to know. For example, a block list gleaned from SES can be shared with firewall administrators at the institution or members of a SOC or REN. Care must be taken to remove attribution and source information.

4.5 REN-ISAC members who do not wish to have their ATI contributions assigned attribution at all may contact soc@ren-isac.net to arrange for an anonymous partner ID for their indicators.

5.0 Non-Attribution

5.1 Under certain circumstances, a member or other information sharing partner may possess useful information, but not wish to be attributed when sharing the information. In that case, the member or partner can pass the information directly to the REN-ISAC security operation center (soc@ren-isac.net), and/or staff, and request non-attribution, also known as the Chatham House Rule. If the information is appropriate for the membership, REN-ISAC staff will forward, without attribution.

6.0 Disclosure

6.1 In the event that a member is required, by open records, freedom of information, subpoena, or any other law or regulation, to disclose information pertaining to the non-public activities of REN-ISAC, or non-public use information that was shared within REN-ISAC, the member shall promptly notify the REN-ISAC Executive and/or Technical Directors before responding to the request, consult regarding whether there are legitimate grounds to narrow or contest disclosure, and disclose only information that the member determines in their sole discretion is legally obligated to disclose.

7.0 Breach

7.1 Inappropriate disclosure of information shared within the REN-ISAC private trust community would expose methods of protection and response to our adversaries, and could expose institutions to unwanted scrutiny, publicity, and damage to reputation. Additionally, inappropriate disclosure would damage the vital trust relationships that sustain the flow of information within and to our community.

7.2 It is imperative that information shared within the REN-ISAC community be handled in accordance with policy. Failure to adhere to the Information Sharing Policy will result in membership review and consequences proportionate to the breach of trust. Consequences may include, but not be limited to: reaffirmation of the information sharing policies, counseling, reprimand, or loss of membership.

7.3 Actual or suspected breaches of the Information Sharing Policy, whether intentional or accidental, must be immediately reported to the Membership Committee via email at MEMBERSHIP@REN-ISAC.NET. Anonymity of third-party reporters will be honored.

8.0 Copyright

8.1 The copyright of a work product submitted by a member is retained by the member.

8.2 The copyright holder may further publish a work outside REN-ISAC provided the work does not contain, in whole or part, non-public information derived from REN-ISAC sources for which the author does not hold copyright or have permission of the copyright holder.

8.3 A member may use their copyright of a work to distribute the work freely within their institution beyond the restrictions of the TLP, even though another member receiving the information through REN-ISAC may not enjoy the same right.

Appendix I – Definitions

Chatham House Rule: When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

Broader community: In the context of TLP:GREEN, REN-ISAC defines the use of the words "broader community" and "community" to mean REN-ISAC members and trusted partners such as CERTS, law enforcement, SLTT agencies, private trust communities, and other ISACs.

Sector: In the context of TLP:GREEN, REN-ISAC defines the use of the word "sector" to mean higher education institutions, research institutions, and other REN-ISAC eligible institutions, regardless of membership in REN-ISAC. However, it should be noted that the EDUCAUSE Security List cannot be used for sharing TLP:GREEN information, as that list is publicly accessible.

Members of their own organization: In the context of TLP:AMBER, REN-ISAC defines the use of the phrase "members of their own organization" to mean employees of the same legal entity, such as full-time IT or student worker staff in a department who have a need to know; and non-member service providers who are contractually obligated to the institution to preserve confidentiality. In the narrowed scope of +STRICT, it becomes *prohibited* to share with non-member service providers such as third-party Incident Response providers and Managed Security Service Providers; and it becomes *prohibited* to share with clients or customers such as constituents of a REN.

Clients or customers: In the context of TLP:AMBER, REN-ISAC defines the use of the phrase "clients or customers" to mean the constituents of a REN-ISAC member organization that may have their own members such as the customers a SOC is contracted to serve, or the members of a regional or statewide research network.

Non-member service providers: Contractors, consultants, or others who provide operational security services to the institution who have not gone through nomination and vetting as full REN-ISAC member representatives. Examples may include third-party Incident Response teams, Managed Security Service Providers, and outsourced Security Operations Centers.

Trusted Third Party: Organizations with which REN-ISAC has a data sharing agreement.

Appendix II - TLP Examples

TLP:CLEAR: Information marked TLP:CLEAR can be shared with anyone via any communications channel you choose. TLP:CLEAR can even be shared publicly. However, before redistributing, you must remove sensitive details like email headers, member names, and email list names. You may give attribution to REN-ISAC if that is the source.

> **EXAMPLE:** *REN-ISAC shares a position paper on the RI-DISCUSS list marked TLP:CLEAR. You may forward that document to anyone you wish but be sure not to forward the full email itself (to prevent leaking info from email headers) and scrub any other sensitive data such as the full address of the REN-ISAC email list before sending it.*

TLP:GREEN: Information marked as TLP:GREEN may be shared with anyone at your institution and with peers in the broader community. For example, if you are a REN or SOC, you may share TLP:GREEN privately with peers or partner organizations in other industries. You may **not** share publicly (i.e., Twitter, public web page). As above, you must remove the name of email lists used to distribute the information. You may give attribution to REN-ISAC if that is the source.

> **EXAMPLE:** *REN-ISAC forwards a document from the FBI marked TLP:GREEN. You may share the document widely at your institution, but not publicly. Always use the original TLP classification and remove the full address of any REN-ISAC email lists.*

> **EXAMPLE:** *A REN-ISAC member representative shares a document marked TLP:GREEN. You may share within your organization, and even the higher education community. However, sharing with the EDUCAUSE Security List would **not** be allowed, since the archive is publicly accessible.*

TLP:AMBER: Anything marked as TLP:AMBER should be shared cautiously, deliberately, **never** publicly, and only with those who need to know who fit the AMBER definition above of "client or customer." Special attention always needs to be paid to any additional restriction that may accompany information, such as the Chatham House Rule (attribution removal). The source of the information can ask for tighter restrictions than those listed above.

> **EXAMPLE:** *Via the RI-OPS email list Cara Nguyen at State College shares indicators of compromise they learned while investigating an attack. Cara marks the information TLP:AMBER, with no further restrictions. You may share that information with those at your institution, and with your members in the case of a REN or SOC, who need to know and who can act to protect your institution and themselves from that threat.*

> **EXAMPLE:** *Via the RI-OPS email list Chris Smith at State University shares indicators of compromise they learned while investigating an attack. Chris marks the information TLP:AMBER, with a disclaimer that the information cannot be shared with non-REN-ISAC member institutions. You may share that information with those at your institution who need to know and who can act to protect your institution and themselves from that threat. A REN or SOC member could protect their own systems but would not be able to share with their own members who are not in the REN-ISAC. As always, non-attribution can be requested (see section 5.0).*

EXAMPLE: *Alex Garcia in central Information Security at State University uses their REN-ISAC API key to routinely download a list of high-confidence malicious domains shared among the community as part of ATI Data. All the indicators are marked TLP:AMBER or less restrictive. Alex passes along that list of indicators to the DNS admin in State University's College of Veterinary Medicine to load into that college's RPZ for operational protection. Since the DNS admin is a member of Alex's organization, this abides by the TLP designations.*

EXAMPLE: *State College contracts with ACME Security, a managed security service provider, to augment their organizational security personnel. Since ACME has access to State College's IPS ruleset that is derived from ATI Data received from REN-ISAC, ACME indirectly has access to this ATI Data. Sharing ATI Data with MSSPs may be allowed by REN-ISAC's definition of "members of their own organization" (see Definitions) provided the indicators are marked TLP:AMBER or less restrictive. Any TLP:AMBER+STRICT scoped data can no longer be shared with "non-member service providers" (see Definitions). To share at that restriction, the appropriate staff at ACME Security would need to be vetted into the REN-ISAC OPS community by the member institution.*

EXAMPLE: *State University is a customer of a security vendor that uses a management app in the cloud to configure threat protection which is then downloaded to protection devices. Each employee at State University who needs access has their own individual account to login to the cloud configuration app. Once logged in, they can use their unique REN-ISAC API KEY to configure loading protection data from REN-ISAC community ATI. Since the ATI data is isolated within a member institution's account, this is fine; if the vendor had no customer separation or made ingested data available to all customers on the platform, then this would be a sharing violation.*

EXAMPLE: *Shannon Elway notices an interesting thread on the RI-OPS email list and wishes to include REN-ISAC members that are not in the OPS community. Before Shannon cross-posts to the RI-DISCUSS list, they must first obtain permission from those who contributed to the thread on the RI-OPS list. Additionally, it would be good form to let the OPS community know the thread is being moved or duplicated on the RI-DISCUSS list.*

TLP:AMBER+STRICT: Anything marked as TLP:AMBER+STRICT should be shared cautiously, deliberately, **never** publicly, and only with those within one's own organization with a need to know; it cannot be shared with clients or customers.

EXAMPLE: *Javier sends a set of indicators to the RI-OPS list marked TLP:AMBER+STRICT. Tonya, a REN-ISAC member representative who uses an outsourced Managed Security Services Provider, recognizes she cannot redistribute the information from Javier to the outsourced SOC due to the +STRICT marking. She'd have to request special permission from Javier asking to redistribute to her contracted provider.*

EXAMPLE: *Melissa shares a threat briefing to the RI-DISCUSS list that contains details of an unpatched zero-day vulnerability. Due to the contents, she marks it TLP:AMBER+STRICT to ensure there is not wide distribution about an unpatched vulnerability. A member rep from ACME-REN, a regional education network (REN) with membership in REN-ISAC, recognizes they cannot redistribute the information from Melissa to their constituents due to the +STRICT marking. They'd have to request special permission from Melissa asking to redistribute to their constituency.*

EXAMPLE: *State University contracts with ACME Security, a managed security service provider, to augment their organizational security personnel. ACME Security has allocated specific individuals to State University who underwent nomination and vetting as REN-ISAC OPS member representatives according to the Membership Guide. As full REN-ISAC member reps, these ACME Security staff are bound by the REN-ISAC Information Sharing Policy and are therefore eligible recipients of TLP:AMBER+STRICT. They are no longer considered* ***non-member*** *service providers (see Definitions).*

TLP:RED is so restrictive that information shared by or within REN-ISAC will rarely have this designation. In such an event, information marked TLP:RED cannot be further shared or distributed in any manner without explicit consent from the author.

EXAMPLE: *In a conference call with REN-ISAC and the FBI, an FBI agent informs you that your institution is being targeted by a state actor. They provide you with more details of their investigation and declare that the meeting is considered TLP:RED. You cannot discuss anything about this meeting with anyone who was not in attendance on the conference call. However, you could, as part of your investigation, request host logs from a system administrator without disclosing why you need it.*

EXAMPLE: *An XSec representative shares a list of threat indicators and other sensitive information with the XSec community. Other XSec representatives ask the author whether they can share those threat indicators with their teams. The author agrees that parts of the message can be further shared and resends the message with appropriate markings. In this example, the part of the message with threat indicators could be marked TLP:AMBER, while the "other sensitive information" could be marked as TLP:RED. The part marked as TLP:RED could not be further shared in any manner.*