Information Sharing Policy

Version 2.2 (May 2018)

Contents

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.

The following principles apply.

2.0 Disclaimer

2.1 Information is shared 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.

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.

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

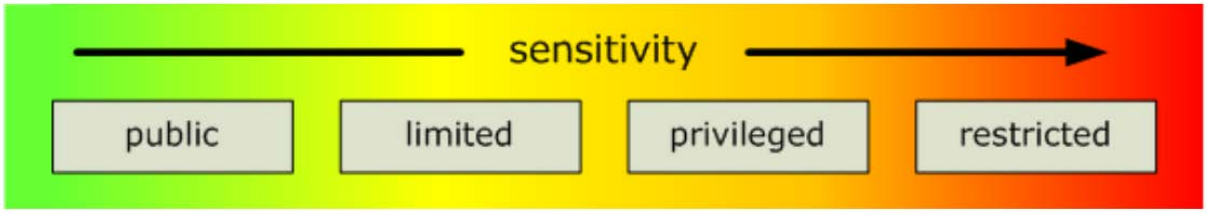
3.0 Information Sharing Categorizations

3.1 Information shared within REN-ISAC must be categorized according to Sensitivity, and optionally according to Criticality, Confidence, and Target Audience.

Category	**Requirement**	**Purpose**
Sensitivity	Mandatory	Defines the limits of distribution
Criticality	Optional	Advises regarding urgency of response
Confidence	Optional	Helps determine response and timing
Target Audience	Optional	Routes information to the appropriate audience

4.0 Sensitivity Classification

Four classifications of Sensitivity are defined. In order of increasing sensitivity they are: Public Use, Limited Use, Privileged Use, and Restricted Use.



4.1 Default classification

4.1.1 All information shared within REN-ISAC is considered Privileged Use unless otherwise explicitly stated, or if the information is shared in a channel that has a specific sensitivity classification, e.g. the XSec-only Restricted Use mailing list. The default classification applies to

information shared in any manner, including, but not limited to, mailing lists, web pages, Internet Relay Chat, meetings, etc.

4.2 Public Use Information

4.2.1 The Public Use classification is self-descriptive. In general, REN-ISAC is not a channel for sharing public use information. Such information should be shared in forums where the widest possible audience may benefit.

4.3 Limited Use Information

4.3.1 Limited Use information is often derived from open sources, however, value has been added through consolidation or analysis, such that the information may prove useful for persons intending to commit malicious acts.

4.3.2 Limited Use information can be redistributed outside the REN-ISAC membership when meeting the following criteria:

1. Can be shared only to trusted persons within your organization who are involved in security protection or response, for example, to a trusted private mailing list that supports the security needs of IT support providers in schools and departments at your institution.
2. Must not be redistributed in any manner in which the information will become publicly accessible. Members should be cautious of private mailing lists that have public archives.
3. 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.
4. 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.
5. The following Information Sharing Restriction and Disclaimer must be placed at the head of the redistribution:

Information Sharing Restrictions and Disclaimer: *The following information must not be publicly released. It can be shared ONLY to trusted persons within your organization who are involved in security protection or response. There are no guarantees for accuracy of the information, or to its impact when applied in protection or response measures. Each recipient must evaluate the information and assume all risks of use. The text of this restriction and disclaimer must accompany all redistribution. No other dissemination is permitted.*

4.4 Privileged Use Information

4.4.1 Privileged Use information can be shared among REN-ISAC Member Representatives, and may be further shared within a member's organization, only when meeting the following criteria:

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 to persons within the member's organization, 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.
7. The following Information Sharing Restriction must be placed at the head of the share:

Information Sharing Restrictions and Disclaimer: *The following information must not be publicly released. It can be shared ONLY for the purpose of a carrying out a specific operational protection or response action, only to trusted persons within your own organization who have need-to-know, and only the minimum information necessary for local assessment and action should be shared. An expectation of trust must be communicated to the recipient. There are no guarantees for accuracy of the information, or to its impact when applied in protection or response measures. Each recipient must evaluate the information and assume all risks of use. The text of this restriction and disclaimer must accompany all redistribution. No other dissemination is permitted.*

4.4.2 REN-ISAC member representatives are responsible and accountable for the disposition of Privileged Use information that they share within their organization, according to the terms described in section 11.0, Breach, and in the REN-ISAC Disclaimer.

4.5 Restricted Use Information

4.5.1 Restricted Use information cannot be redistributed or further shared in any manner. The member representative who receives Restricted Use information should assimilate the information and formulate corresponding protection and response actions for the institution.

4.5.2 Whenever sharing Restricted Use information in a REN-ISAC channel that defaults to a lower sensitivity classification, the following should be placed at the head of the information:

Information Sharing Restrictions: *The following information is classified as Restricted Use in accordance with the REN-ISAC Information Sharing Policy. The information must not be redistributed or further shared in any manner.*

4.5.3 For well-defined and limited purposes, operational data that is classified as Restricted Use may be shared with General, Officer, or Security Operations (Ops) Member Representatives who can act on the data.

5.0 Criticality

5.1 The optional Criticality indicates the potential impact of the information and the need for timely action based on the information. The levels are:

Criticality	Expected action
Routine	Routine interest, does not require immediate action, general advice regarding normally-experienced malicious activity.
Important	Requires action in response to specific threat activity, or for protection due to an increase in attacks, or vulnerability.
Urgent	Requires immediate and decisive action. Reflects a potentially catastrophic issue.

6.0 Confidence

6.1 The optional Confidence designation provides rough guidance for decisions on received information. It can also facilitate the timely sharing of information, with caveat, prior to complete analysis. The Confidence designation should not substitute for providing additional narrative assessment of the reliability of the source and/or data. Confidence designations are:

Confidence
High
Medium
Low

7.0 Target Audience

7.1 The optional Target Audience designation can be used to provide focus for action or consideration. The designations are:

Target Audience
Operations/administration
Management/decision
Executive

8.0 Non-Attribution

8.1 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. If the information is appropriate for the membership, REN-ISAC staff will forward, without attribution.

9.0 Information Sharing Procedures

9.1 Information is shared within the REN-ISAC community by means of various channels, including but not limited to: mailing lists, IRC, webcasts, conference calls, in-person meetings, wiki, data feeds, and person-to-person.

9.2 In all cases other than person-to-person, the channel will have an explicitly defined Sensitivity Classification. In general, channels that support information sharing among all member representatives are marked Privileged Use. Channels that support XSec-only communications are Restricted Use. In the absence of an explicit marking for the channel, or on information shared in the channel, the default classification is Privileged. Information classified to a lower sensitivity can be shared on the channels, but should be explicitly marked as carrying the lower classification.

9.3 In the case of person-to-person communications, without a priori agreement, it may be unclear whether the communication is personal, or under REN-ISAC auspices. The parties should agree at the outset to parameters guiding the communication.

9.4 Members can share information directly to the REN-ISAC community, or indirectly, and if desired, without attribution, via REN-ISAC handlers. Refer to section 8.0 Non-Attribution.

9.5 Regardless of the method of communication and attribution chosen, the member should first decide on sensitivity and share and/or mark appropriately. Optionally, the information may be marked for criticality, confidence, and target audience (sections 5.0, 6.0, and 7.0).

9.6 Considerations for classifying sensitivity as Privileged or Restricted Use include:

1. The degree of recipient vetting required for comfortable and safe sharing.
2. The extent to which the information can be shared to non-members within a recipient member's organization.
3. The organizational capability of the recipients to act on the information.

9.7 A member may, at its discretion, expand the distribution of information that it was the sole source of, by reclassifying to a lower sensitivity.

9.8 If a Member Representative (in any community) possesses information that requires Restricted Use sharing, the member is encouraged to send that information to a REN-ISAC handler for redistribution.

10.0 Disclosure

10.1 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.

11.0 Breach

11.1 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.

11.2 It is imperative that information shared within the REN-ISAC community be handled in accordance with policy. Failure to adhere to 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.

11.3 Actual or suspected breaches of the Information Sharing Policy, whether intentional or accidental, must be immediately reported to the Membership Committee. Anonymity of third-party reporters will be honored.

12.0 Copyright

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

12.2 By submitting a work to REN-ISAC, the member agrees to use of the work in accordance with marked Sensitivity Classification (section 4.0), Information Sharing Procedures (section 9.0), and the REN-ISAC Disclaimer.

12.3 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.

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