Membership Guide

Version 3.0 (May 2018)

Contents

1.0 Overview of Membership Structure

1.1 REN-ISAC is a private community composed of trusted representatives of member institutions. The fundamental underpinning of REN-ISAC is shared trust among its members. Trust is critical to the activities conducted within the organization.

1.2 An institution or organization is the REN-ISAC "member", and is represented by people occupying various roles. Those roles are:

> **Management Representative:** the key point of contact for membership; someone with responsibility for information security at the institution; this role is required for membership
>
> **Member Representative:** security practitioners, analysts, and engineers who will participate in the information sharing communities; this role is required for membership
>
> **Affiliate:** close, trusted associates of a member institution who have a special interest in cyber security; this role is not required for membership
>
> **[EDITOR'S NOTE]:** The Affiliate role/community is not currently supported but is planned for Q4, 2018.

A second Management Representative can be added, provided the occupant qualifies as a member of the Officer, General, or Security Operations (Ops) core communities (see sections 1.3 and 7.0 below). There is no limit to the number of Member Representatives or Affiliates, provided the occupants qualify (see sections 1.3 and 7.0 below).

The individual Management and Member Representative(s) must belong to one or more of the core communities described in section 1.3 below.

1.3 REN-ISAC membership is divided into four core communities: General, Security Operations (Ops), Officer, and Affiliate. The communities differ in the criteria for membership, the degree of trust assurance, and in the types of information and services that are shared within the tier. In addition to the four core communities, there exists the XSec community (described in sections 7.2 and 7.6), which requires the highest degree of trust assurance and is only available to members of the Ops core community.

1.3.1 Core Community definitions

> **General:** Practitioners whose operational security responsibilities are associated with specific systems or services such as enterprise applications, networks, DNS; or, whose responsibilities aren't strictly "security operational", such as risk, compliance, training, and identity and access management (IAM); or, those with key security responsibilities that are not necessarily institution-wide.
>
> **Security Operations (Ops):** Security analysts and engineers who have or share principal responsibility for security protection and response for the entire institution; members of the

Ops community typically take action in response to an incident or threat intelligence, manage firewalls, intrusion detection/prevention systems, vulnerability scanners, and other defensive systems

Officer: Executive level decision makers with a stake in information security at their institution; members of the Officer community may hold titles such as CIO, CTO, CISO, Associate Vice President for IT, or Director of Risk and Compliance; this list is not exhaustive

Affiliate: Close, trusted associates of an institution whose expertise can provide insights or value to a REN-ISAC special interest group; examples include cyber-security researchers, communications experts, disaster recovery experts, or administrators of a particular software product

[EDITOR'S NOTE]: The Affiliate role/community is not currently supported but is planned for Q4, 2018.

1.3.2 Roles, Functions, and Community Eligibility

Role	Function	Who is Eligible	Core Community	Eligible Communities	Full Definition
Management Rep	Institutional contact; nominates Members and Affiliates	CIO, VP, AVP, Chancellor, CISO, or delegate	Officer	General, Ops	Sections 6.2, 6.3
Member Rep	Participate in information sharing communities	Security practitioners, analysts, and engineers	General or Ops	Officer	Sections 6.4, 6.5
Affiliate	Participate in special interest groups (SIGs)	Faculty, researchers, experts in an InfoSec subject	Affiliate		Section 6.7

[EDITOR'S NOTE]: The Affiliate role/community is not currently supported but is planned for Q4, 2018.

1.4 The Management Representative nominates individuals to become Member Representatives or Affiliates, and is responsible for timely maintenance of the institution's membership roster.

1.5 All active role occupants may participate in sensitive information sharing. The Information Sharing Policy document describes what, how, and to whom, a Member Representative may redistribute information that was shared in REN-ISAC. ***Certain sensitive information cannot be redistributed under any circumstance.*** It is imperative that the recipient of sensitive information analyzes the information and formulates protection, response, and/or communication measures accordingly.

1.6 The Management Representative, Member Representatives, and affiliates must familiarize themselves with the following documents:

1. This Membership document
2. REN-ISAC Information Sharing Policy

3. REN-ISAC Membership Terms and Conditions
4. REN-ISAC Charter
5. REN-ISAC Disclaimer

1.7 When an institution joins REN-ISAC, the Management Representative must explicitly agree to the Membership Terms and Conditions, and the Information Sharing Policy.

1.8 When a prospective Member Representative or Affiliate joins REN-ISAC, he or she must explicitly agree to the Information Sharing Policy.

1.9 The identities of member institutions can be publicly disclosed. Name and contact information of individual Member Representatives and Affiliates are shared within the membership, but are not to be publicly disclosed, either by the REN-ISAC organization or by members, except by self-identification. Names and institutional associations of advisory group and analysis team members, and members of certain project teams can be publicly disclosed.

2.0 The requirement for trust among members

2.1 REN-ISAC is a private trust community for sharing sensitive information regarding cybersecurity threat, incidents, response, and protection.

2.2 The private and trusted character of the community permits members to safely share information about such things as incident experiences, methods, sources, and infected systems -- without concern that the information will draw unwanted attention to the institution or abet our adversaries.

2.3 Strong trust among members is required for a community in which members and external partners are willing to share sensitive security threat and experience information.

2.4 Individuals participating in the REN-ISAC community are required to accurately represent themselves, reliably act in the interests of their organizations and community, and earnestly abide the REN-ISAC Information Sharing Policy and Membership Terms and Conditions.

3.0 Compartmentalized community membership

3.1 Short of conducting costly background checks, trust can be established through personal knowledge. Scaling strong trust to a large community requires trust in a process rather than complete n-way personal relationships. Communities often rely on trusted member vouches for prospective members.

3.2 The two objectives, reach of service to the entire higher education and research community, and maintenance of a strong trust community, are difficult bedfellows. Scaling strong trust to a community of thousands of members encounters difficulties of process, organization, and cost. The process of vouching is ineffective for reaching institutions at which prospective members are not well known in the community.

3.3 In order to achieve the two objectives of reach and strong trust, REN-ISAC employs a compartmentalized community membership model. Four member core communities – the participatory Affiliate community, the basic trust General and Officer Communities, and the advanced trust Ops Community – differ in both criteria for membership and in the types of information sharing and services available for member participation. The strong trust required for the XSec community offers further distinction in terms of membership criteria and the type of information shared.

4.0 Benefit and trust matrix for the Core Communities and XSec

	Membership Communities				
Benefit / Trust	**Affiliate**	**Officer**	**General**	**Ops**	**Xsec**
Membership Trust					
Nomination vetted by community	No	Yes*	Yes	Yes	Yes
Considered a Member Representative	No	Yes	Yes	Yes	Yes
Default information classification	Limited	Limited	Limited	Privileged	Restricted
Use of Mailing Lists					
Affiliate group lists (as assigned)	Yes	Eligible	Eligible	Eligible	Eligible
Discuss List	No	Eligible	By default	By default	By default
Ops List	No	No	No	By default	By default
XSec List	No	No	No	No	By default
Information Products & Other Resources					
Daily Watch Report	No	Eligible	By default	By default	By default
TechBurst Webinars	*By invitation*	Eligible	By default	By default	By default
Affinity Group-specific products	Yes	Eligible	Eligible	Eligible	Eligible
Member wiki	No	By default	By default	By default	By default
Governance Eligibility					
Board Membership	*Depends*	Yes	Yes	Yes	Yes
Membership Committee	*No*	No	No	No	Yes
Technical Advisory Group	*No*	No	No	No	Yes
Ad hoc analysis teams	*By invitation*	*By invitation*	*By invitation*	Yes	Yes
Ad hoc advisory groups	*By invitation*	*By invitation*	*By invitation*	Yes	Yes
Ad hoc Special Interest Groups	*By invitation*	Yes	Yes	Yes	Yes
Attend Membership Meeting	*No*	Yes	Yes	Yes	Yes
Voting Privileges					
Board Elections	*No*	Yes	Yes	Yes	Yes
General Vote	*No*	Yes	Yes	Yes	Yes

** when an institution first joins REN-ISAC, the initial Officer Member Representative is accepted for membership after review by the REN-ISAC Membership Services team to allow the join process to complete*

5.0 Is an institution or an individual the "member"?

5.1 The institution is the member, and is eligible, through a Management Representative, to nominate one or more Member Representatives and Affiliates. Nominees must meet membership criteria, pass vetting requirements, and abide policies and trust requirements.

5.2 Information, of various sensitivity classifications, is shared with each of the core communities. The members of those communities participate in the information sharing – the institution does not. It is imperative that the recipient of sensitive information analyzes the information and formulates protection, response, and/or communication measures accordingly. This important distinction places limits on the dissemination of information within and outside the institution. Refer to Information Sharing Policy for details.

6.0 How is an institution represented in REN-ISAC?

6.1 An institution must have a Management Representative and one or more Member Representatives. Both Management Representatives and Member Representatives must belong to one or more of the following core communities: General, Officer, or Ops. Those holding the Affiliate role may only belong to the Affiliate core community. It is possible to belong to more than one core community. For example, a Management Representative can belong to the Officer and Ops communities, provided they qualify for each. The communities for which an individual Member Representative is eligible is determined according to the job functions, capabilities, needs, and choice of the institution and individual, and by vouched trust in the case of XSec (see section 8 below).

6.1.1 Eligible Core Communities, by Role

Role	Eligible Core Communities	Default
Affiliate	Affiliate	Affiliate
Member Rep	General, Officer, Ops	General
Management Rep	General, Officer, Ops	Officer

[EDITOR'S NOTE]: The Affiliate role/community is not currently supported but is planned for Q4, 2018.

6.2 Management Representative:

6.2.1 As the steward of membership for their institution, the Management Representative is responsible for nominating Member Representatives and Affiliates (section 14), for the timely maintenance of membership changes, withdrawals, and terminations (section 9), and for all other administrative actions.

6.2.2 The Management Representative must be: (A) a CIO, vice president, associate VP, or chancellor, who has been verified by the Membership Committee; (B) a similarly verified CISO who reports directly to A; or (C) a Membership Committee-accepted delegate of A. The delegate

must be a manager, with the security function in the subordinate reporting chain. Delegates are identified when A performs institutional registration.

6.2.3 By default, the Management Representative is automatically nominated as a Member Representative in the Officer core community. The Management Representative can also be, but is not expected to be, a Member Representative in either the General or Ops core community (in addition to the Officer community). A Management Representative may self-nominate for any core community for which they are eligible.

6.2.4 The Management Representative receives quarterly reports on REN-ISAC activities, has access to a Management Representative mailing list, and is eligible to participate in management advisory groups and committees.

6.3 Member Representative - Officer:

6.3.1 Referred to as "Officer Member Rep", these individuals represent their institutions in the information sharing and services community at a security classification of Limited Use. The Officer community provides a level of participation in the community for those individuals whose information security-related job functions do not meet the requirements of Security Operations.

6.4 Member Representative - General:

6.4.1 Referred to as "General Member Rep", these individuals represent their institutions in the information sharing and services community at a security classification of Limited Use. The General community provides a level of participation in the community for those individuals whose information security-related job functions do not meet the requirements of Security Operations.

6.5 Member Representative - Operations:

6.5.1 Referred to as “Ops Member Rep", these individuals represent their institutions in the information sharing and services community at a security classification of Privileged Use. The Security Operations community provides a level of participation in the community for those individuals whose job function doesn't require access to the additional XSec resources, or who don't meet XSec criteria.

6.6 Member Representative - XSec:

6.6.1 Within the REN-ISAC membership framework, XSec is a special community (not a *core* community) that first requires a person to be in good standing in the Security Operations (Ops) core community before being eligible for XSec. Referred to as "XSec member", these individuals represent their institutions in the information sharing and services community at a security classification of Restricted Use (highest level). XSec membership provides access to additional sensitive data and information sources, and levels of participation in the community.

6.7 Affiliate:

6.7 This community is meant for close associates of an institution whose expertise can provide insights or value to REN-ISAC, typically through participation in a special interest group (SIG). Participants in the SIG may consist of Affiliates and Member Representatives, and the group decides the mission and desired outcomes of their collaboration. The group may disband once their goals are reached, while other SIGs may last in perpetuity.

Persons in the Affiliate community differ from other core community members in one key way -- they are not considered Member Representatives. Their role is focused on a particular subject, and in some cases, their membership is short-lived.

[EDITOR'S NOTE]: The Affiliate role/community is not currently supported but is planned for Q4, 2018.

7.0 Membership criteria:

7.1 General and Officer Core Communities

7.1.1 The institution must be a college or university, teaching hospital, research and education network provider, government-funded research organization, or as otherwise defined in the REN-ISAC Bylaws.

7.1.2 The individual must be full-time permanent staff and have, share, or oversee significant information security or information risk assurance responsibilities at the institution, with the following exceptions:

7.1.2.1 The individual may be a consultant or other outsourced employee hired by the member institution, provided all of the following are true:

a. The individual is a full-time, permanent employee of the consulting company hired by the member institution
b. The individual is substantially dedicated to the operational security of the member institution; where this condition is in question the Membership Committee will review on a case-by-case basis
c. A copy of the Information Sharing Policy Addendum for Contractors is signed by a representative with signatory power for the consulting company
d. The individual meets all other criteria for membership defined in the Membership Guide

7.1.2.2 The consultant must have an email address associated with the member institution or consortium in order to associate the consultant with the institution for which they are providing services, unless:

a. Policy at the member institution prohibits provision of such an email address, in which case the Membership Committee will review on a case-by-case basis

7.1.3 The individual must agree to abide the REN-ISAC Information Sharing Policy.

7.1.4 The individual's participation must conform to the frameworks established by the Charter, the Membership Terms and Conditions, and the Information Sharing Policy.

7.2 Security Operations (Ops) Core Community and XSec:

7.2.1 The institution must be a college or university, teaching hospital, research and education network provider, government-funded research organization, or as otherwise defined in the REN-ISAC Bylaws.

7.2.2 The individual must be full-time permanent staff and have or share principal responsibility for security protection and response at the institution, with the following exceptions:

7.2.2.1 The individual may be a consultant or other outsourced employee hired by the member institution, provided all of the following are true:

a. The individual is a full-time, permanent employee of the consulting company hired by the member institution
b. The individual is substantially dedicated to the operational security of the member institution; where this condition is in question the Membership Committee will review on a case-by-case basis
c. A copy of the Information Sharing Policy Addendum for Contractors is signed by a representative with signatory power for the consulting company
d. The individual meets all other criteria for membership defined in the Membership Guide

7.2.2.2 The consultant must have an email address associated with the member institution or consortium in order to associate the consultant with the institution for which they are providing services, unless:

a. Policy at the member institution prohibits provision of such an email address, in which case the Membership Committee will review on a case-by-case basis

7.2.3 The individual must have institution or organization-wide responsibility, that is, the individual must represent security for the institution. Responsibility for a single campus of a multi-campus system is okay. Individuals with responsibility within a division, such as a department or school, don't qualify for membership unless by exception (section 7.8).

7.2.4 The individual must agree to abide the REN-ISAC Information Sharing Policy.

7.2.5 The individual's participation must conform to the frameworks established by the Charter, the Membership Terms and Conditions, and the Information Sharing Policy.

7.3 Acceptance in General Core Community:

7.3.1 Prospective General Member Representatives must be accepted for membership by existing Member Representatives of the REN-ISAC trust community. Existing Member Representatives are not required to positively vouch, but are given the opportunity to express concern regarding the fitness or trustworthiness of the prospect. See Vouching, Dissent, and Reproach (section 8.0) and Membership Application and Processing (section 14).

7.4 Acceptance in Officer Core Community:

7.4.1 Prospective Officer Member Representatives must be accepted for membership by existing Member Representatives of the REN-ISAC trust community. Existing Member Representatives are not required to positively vouch, but are given the opportunity to express concern regarding the fitness or trustworthiness of the prospect. See Vouching, Dissent, and Reproach (section 8) and Membership Application and Processing (section 14).

7.4.2 The provisions of section 7.4.1 are not in effect when an institution first joins REN-ISAC. In such a case the initial Officer Member Representative is accepted for membership after review by the REN-ISAC Membership Services team to allow the join process to complete. The provisions set forth in section 7.4.1 are then followed.

7.5 Acceptance in Security Operations Core Community:

7.5.1 Prospective Ops Member Representatives must be accepted for membership by existing Member Representatives of the REN-ISAC trust community. Existing Member Representatives are not required to positively vouch, but are given the opportunity to express concern regarding the fitness or trustworthiness of the prospect. See Vouching, Dissent, and Reproach (section 8) and Membership Application and Processing (section 14).

7.6 Acceptance in XSec:

7.6.1 The prospective XSec Member Representative must be an Ops Member Representative in good standing, for a minimum of six weeks.

7.6.2 The prospective XSec Member Representative must receive two vouches from active XSec Member Representatives. One vouch must come from an external institution. A vouch must affirm that the prospect meets membership criteria, and importantly, must explicitly express personal trust in the individual. Guidance for proper vouching is provided in Vouching, Dissent, and Reproach (section 8).

7.6.3 The prospective XSec Member Representative must have responsibilities dedicated to operational security protection and response, or to a combination of networking and security with security responsibilities at minimum 50% assignment.

7.6.4 The prospective XSec Member Representative must have organizational responsibility to assess threat and incident, and to develop plans of action that have impact to the organization. The prospective XSec Member Representative must have the authority to independently carry out these responsibilities with nominal management oversight.

7.6.5 The institution must have the capability to actively defend against known threats, identify and remediate compromised machines, and must respond to compromised machines in a timely manner.

7.7 Acceptance in Affiliate Core Community:

7.7.1 Prospective Affiliate members are accepted for membership by the REN-ISAC Membership Services team. The membership community is informed of accepted Affiliates via regular announcements to the private email lists.

[EDITOR'S NOTE]: The Affiliate role/community is not currently supported but is planned for Q4, 2018.

7.8 Exceptions:

7.8.1 Requests for membership in which the institution, organization, or individual doesn't meet membership criteria are reviewed by the Membership Committee and REN-ISAC directors. For example, if an institution has no central IT security function, consideration for departmental memberships might be made on a case-by-case basis.

7.8.2 Ex officio memberships may be granted at the discretion of REN-ISAC directors for persons in relationship to the community, such as members of advisory groups or analysis teams, directors of sponsoring organizations, etc.

8.0 Vouching, Dissent, and Reproach

8.1 Vouching

8.1.1 Vouches must be sent to the mailing list on which the vouch request originated. Vouches sent privately to the Membership Committee or REN-ISAC staff are not accepted.

8.1.2 The reliability of a member's vouch for a prospective member is crucial to the trustworthiness of the REN-ISAC community. To vouch is not a trivial undertaking - it is an exercise of foundational principle for the community, and highlights how security comes down to individual decisions and actions.

8.1.3 There are two parts to a proper vouch: (1) an assertion that the individual meets the membership criteria, and (2) an expression of your personal trust in the individual.

8.1.4 Vouches must be independent sources of information, based on your own first-hand knowledge and personal experience with a candidate. Don't vouch for a candidate because someone you trust has recommended the individual to you.

8.1.5 When vouching, include as much relevant information as you can. A simple "vouch!" is insufficient. Include, at minimum, the following:

1. How long you've known the person

2. How you know the person, specifically concerning work relationships (e.g. worked incidents together, work in other trusted communities), and how you've communicated (in-person, phone, e-mail)
3. Confirmation of the applicant's position and responsibilities, if known
4. An explicit statement of trustworthiness - your personal trust in the individual

8.1.6 Members are encouraged to ask questions about a candidate. Questions can be communicated to the mailing list, or privately to the Membership Committee.

8.2 Dissent

8.2.1 Members are encouraged to express concern or dissent regarding the fitness or trustworthiness of a candidate. Although concern and dissent can be expressed on the mailing list, we encourage dissent to be expressed in confidence directly to the Membership Committee at MEMBERSHIP@REN-ISAC.NET. The Committee will investigate all cases of dissent, and make a recommendation regarding disposition.

8.3 Reproach

8.3.1 In order to maintain a sound and trusted community, the membership must police itself. At any time, one member may call to question the fitness of another member, based on consideration of the membership criteria or trustworthiness. Challenges are encouraged by REN-ISAC management, and should be communicated in private to the Membership Committee.

9.0 Change, withdrawal, and termination

9.1 An individual's participation in REN-ISAC is directly linked to representation of the institutional membership, role at the institution, and trust of the community.

9.2 The Management Representative and individual member are responsible for timely communication to the Membership Committee regarding changes of employment or other changes in an individual's status that relate to membership eligibility.

9.3 Two or more member institutions may, through organizational change or other circumstances, require consolidation into a single membership. For example, a university system may consolidate all campuses under a single CIO/CISO, allowing a single membership in accordance with section 3.2 of the REN-ISAC Terms & Conditions. In such a case:

a. REN-ISAC will work with each of the Management Representatives to identify the new member institution name (if applicable) and the Management Representative of the new, consolidated entity
b. REN-ISAC will work with each of the Management Representatives to verify that each of the existing Member Representatives still qualify according to section 7 of the REN-ISAC Membership Guide; Member Representatives who no longer qualify will be removed
c. When the institutions consolidate under a single REN-ISAC membership, a qualified Member Representative or XSec member in good standing need ***not*** be re-vetted if:

i. The Management Representatives at the original institutions agree the Member Representative or XSec member is in good standing; and

ii. There is no lapse in employment (and therefore REN-ISAC membership) of more than 6 weeks

iii. If either of the above criteria are not met, a nomination is required per the normal processes in section 7.3.1, 7.4.1, or 7.5.1 of the REN-ISAC Membership Guide, or section 7.6 for those in XSec

d. The Membership Committee will be consulted before any decisions are made final

e. An announcement will be made to the membership welcoming the new member institution and naming the Management Representative and Member Representatives

9.4 A member institution may, through organizational change or other circumstances, require more than one membership. For example, a university's medical center may split off organizationally, requiring a separate membership in accordance with section 3.2 of the REN-ISAC Terms & Conditions. In such a case:

a. The separating institution may apply for membership once the organization changes are complete (or nearly so)

b. The Membership Committee may review the application, at their discretion

c. Once accepted, the new member institution may begin making nominations for Member Representatives

d. Should any of the nominees be Member Representatives or XSec members in good standing at the original member institution, vetting requirements described in section 7.3, 7.4, 7.5, or 7.6 (as the case may be) of the REN-ISAC Membership Guide do not apply if:

i. The Management Representative at the original institution agrees the Member Representative or XSec member is in good standing; and

ii. There is no lapse in employment (and therefore REN-ISAC membership) of more than 6 weeks

iii. If either of the above criteria are not met, the nomination will go through the normal processes required in section 7.3.1, 7.4.1, or 7.5.1 of the REN-ISAC Membership Guide, or section 7.6 for those in XSec.

e. An announcement will be made to the membership welcoming the new member institution and naming the new Management Representative and Member Representatives

9.5 In the event of institutional disciplinary suspension or termination, or other cause for doubt regarding an individual's trustworthiness, it's important -and required- for the Management Representative to immediately notify the REN-ISAC Membership Committee. If the Management Representative is unable to immediately notify, a peer Member Representative from the same institution should communicate to the Committee.

9.6 Emergency notification of member status change should be made by phoning the 24x7 REN-ISAC Watch Desk at +1 (317) 274-7228. Normal priority changes can be made by contacting the Membership Committee via email at MEMBERSHIP@REN-ISAC.NET.

9.7 REN-ISAC reserves the right to unilaterally terminate the membership of an individual or institution without notice.

9.8 Actions of the Membership Committee will be reported to the member and Management Representative, and new status information will be reported to the membership.

9.9 The requirements for controlling the dissemination of received information, described in this document, survive the expiration or termination of membership.

10.0 Maintenance of the member roster

10.1 The status of Management and Member Representatives will be confirmed on a periodic basis by the Membership Committee. Members are required to promptly respond to status inquiries.

10.2 REN-ISAC may at its discretion reissue vouch requests, either privately or to the membership mailing list, to confirm a member's standing.

11.0 Referred Trusts

[EDITORIAL NOTE: This role is currently required for technical reasons. Once the technical reasons are resolved, the Membership Guide will be updated to remove this section]

11.1 General description

11.1.1 At times, it may be necessary for REN-ISAC to establish formal association with certain individuals at member institutions who are not eligible for REN-ISAC membership. Depending on the purpose of the association, it may be of a specific duration or standing. For example, a short-term association could be established with mail system administrators during the development phase of a project aimed at spam-fighting. A standing association might be established with DNS administrators who can sinkhole bad actor domain names. The participating individuals are called associates. Associates are organized under a structure called a Referred Trust. A unique Referred Trust is established for each uniquely-scoped purpose.

11.2 General Policies

11.2.1 A set of general policies guide all Referred Trusts, and each Trust will have additional unique policies that further describe behaviors and participation for that Trust.

11.2.2 Referred Trusts are defined and established by the REN-ISAC Technical Director. Associate participation is under the purview of the Membership Committee.

11.2.3 Referred-Trust Associates are not full REN-ISAC members, but have relationship to REN-ISAC exclusively for the purpose of the Referred-Trust. Associates do not have any other privileges or benefits of REN-ISAC membership.

11.2.4 The prospective associate must be a trusted individual who meets role-based, appointment, and other requirements noted in the particular Referred Trust definition. Appointments are subject to Membership Committee review.

11.2.5 At a change in tenure of the appointing individual, past appointments made by that individual must be confirmed by someone at the institution who meets the appointer criteria of the specific Referred Trust. A grace period of three weeks permits the appointments to continue unimpeded.

11.2.6 Appointments must be reconfirmed on a periodic basis, determined by REN-ISAC Technical Director.

11.2.7 In the event of any conflict between the Referred Trust General Policies, and the more specific policies unique to a particular Referred Trust, the latter is the policy in force.

11.3 Data Feed Referred-Trust

11.3.1 The Data Feed Referred Trust is a standing Referred Trust, with the purpose to provide data access to individuals at a member institution, who have specific role-based responsibilities, when those individuals would not normally be eligible to be a REN-ISAC membership representative.

11.3.2 REN-ISAC provides data feeds regarding active sources of threat. Member institutions can use the feeds to identify local compromised machines, and to block known threats. Access to, and use of the data is controlled by the Information Sharing Policy. At some organizations, the REN-ISAC Member Representative may not be in a position to apply the data, and the person(s) with that access may not be eligible for REN-ISAC membership. Or, use of the data by a REN-ISAC Member Representative might expose the data on machines that REN-ISAC-ineligible individuals have access to.

11.3.3 When it's not possible for an organization to address the underlying access issues, a Management Representative, can sponsor trusted persons to become Data Feed Referred-Trust Associates - permitting access to the data. In order to protect sensitive data, the number of persons designated should be kept to the minimum necessary to achieve operational protection.

11.3.4 In order to qualify for a Data Feed Referred Trust appointment, there must be a clearly defined operational protection and response requirement for the data, the use must involve protection for the entire institution or organization, and existing operational structures must dictate the data access by someone other than a REN-ISAC Member Representative.

11.3.5 The Data Feed Referred-Trust Associate:

1. Must be nominated by a Management Representative at the involved institution
2. Must be a full-time, permanent staff member

3. Must have institution or organization-wide operational responsibilities. Responsibility for a single campus of a multi-campus system is okay. Individuals with responsibility within a division, such as a department or school, don't qualify
4. Must agree to abide the REN-ISAC Information Sharing Policy
5. Must conform to the frameworks established by the Charter, Membership Terms and Conditions, and the Information Sharing Policy
6. Must be accepted by existing REN-ISAC Member Representatives and the Membership Committee. Member Representatives are not required to vouch for the prospective Associate, but are given opportunity to express concern regarding the fitness or trustworthiness of the prospect. See Vouching, Dissent, and Reproach (section 8). The Membership Committee holds final decision making authority

12.0 Member information

12.1 The identities of member institutions can be publicly represented in REN-ISAC communications, such as papers, presentations, and marketing materials. Representation other than the fact of membership, such as endorsement or work within REN-ISAC, cannot be made without written permission from the Management Representative of that institution, except as noted in section 12.4

12.2 Contact and registration information for all institutions, member and Management Representatives, and referred-trust associates is made available to member and Management Representatives.

12.3 Contact and registration information, including the fact of membership, may not be disclosed outside the membership, either by REN-ISAC employees or its members, other than with the exclusive and case-by-case permission of the member, except as noted in section 12.4.

12.4 Name and institution of Advisory Group, Analysis Team, Membership Committee, and certain project team members may be publicly represented on REN-ISAC web pages and communicated in papers, publications, or marketing materials.

13.0 Membership Committee

13.1 A standing Membership Committee conducts all membership business. Details, and how to contact the Committee are on the Membership Committee web page.

14.0 Membership application and processing

14.1 Management Representatives and prospective Member Representatives and Affiliates must familiarize themselves with:

1. This Membership document
2. REN-ISAC Information Sharing Policy
3. REN-ISAC Membership Terms and Conditions
4. REN-ISAC Charter
5. REN-ISAC Disclaimer

Questions can be directed to the Membership Committee at MEMBERSHIP@REN-ISAC.NET.

14.2 Institutional first-time registrations, and all Member Representative and Affiliate nominations, are made by the Management Representative. See section 14.8 for information on institutional applications. Member Representatives and Affiliates are nominated by the Management Representative via authenticated access to REN-ISAC's Registry (from https://ren-isac.net click the "Login" link in the upper right corner). For help logging into the Registry, feel free to contact SOC@REN-ISAC.NET.

14.3 After six weeks in good standing as an Ops Member Representative, if appropriate, and as needed, a member may request XSec privileges, by e-mailing the Membership Committee at MEMBERSHIP@REN-ISAC.NET.

14.4 Ops and General Member Representative nominations are vetted by the full REN-ISAC membership, and the Membership Committee. The vetting period is a minimum of six business days, during which Member Representatives may express dissent or request additional information regarding the nominee (section 8 Vouching, Dissent, and Reproach).

14.5 XSec requests are vetted by the current XSec Member Representatives and Membership Committee. The vetting period is a minimum of six business days, during which XSec Member Representatives may vouch, express dissent, or request additional information regarding the applicant (see section 8 Vouching, Dissent, and Reproach). The Membership Committee holds final decision making authority.

14.6 Ops Member Representatives who leave REN-ISAC and reenter when transitioning employment may carry forward time accrued toward XSec eligibility, as long as (1) prior employment was terminated in good standing, and (2) time away from REN-ISAC did not exceed six calendar weeks.

14.7 Suggestions on how to develop the individual and the institution, in order to qualify for XSec status, are provided in Appendix B.

14.8 Membership Application

New member ***institutions*** should follow the above link to begin the member application process. Please note that the person submitting the institutional application must be the CIO, CISO, or CTO (or equivalent), and hold information security responsibility for the entire institution. This person should also be able to obtain, or provide, fiscal approval to pay the annual membership fee (see our Fee Structure).

For Member Representatives nominations, see section 14.2 above.

15.0 Technical Liaison

15.1 Purpose

15.1.1 The Technical Liaison (TL) class provides for REN-ISAC participation of trusted persons who do not meet membership eligibility criteria but whose participation would bring substantial and continuing value to the broad REN-ISAC community. The TL class is not a path for member institutions to gain participation of general staff who don't meet membership eligibility criteria. Persons at member institutions are not excluded, however all TL candidates must meet the requirement to have specific expertise or capacities that widely benefit the REN-ISAC community.

15.2 Eligibility

1. The candidate may represent a private, commercial, or governmental organization or interest, from nations considered eligible for REN-ISAC membership.
2. The candidate must have specific expertise or capacities that widely benefit the REN-ISAC community.
3. There must not be a conflict of interest, as determined by the Membership Committee, concerning a candidate's occupation or avocation and the needs of a trusted information sharing community; for example, someone whose occupation is to publicly report incidents would likely not be eligible.
4. The candidate must pass admittance requirements as stated below.

15.3 Admittance

15.3.1 A Technical Liaison must be nominated and sponsored by an XSec member in good standing. Nominations are submitted to the Membership Committee, via email to MEMBERSHIP@REN-ISAC.NET, which deliberates along with the REN-ISAC Executive and Technical Directors.

15.3.2 The Committee may also consult with the Technical Advisory Group or Board at its choosing. A decision on the nomination is made by the Membership Committee, Executive Director, and Technical Director. A two-thirds majority vote is required to pursue, with each Committee member and Director holding a single vote. Active nominations are then submitted to the membership for trust vouching according to the standards required for General membership.

15.3.3 In submitting a nomination the XSec member must provide: a short description of the person's background and current roles, a description of value the community will derive from the Liaison, and a statement of personal trust in the person. Nominations may be made privately to the Membership Committee or openly (including the membership). If a nomination is made privately and is voted down notification of the results will be private. Private nominations that are voted up will be openly disclosed to the membership including identification of who made the nomination.

15.4 Maintenance of Status

15.4.1 The Technical Liaison must always have an XSec member sponsor. Obligations of the Sponsor are identified below. In the event of an unforeseen lapse in sponsorship the Membership Committee will temporarily serve.

15.4.2 The Membership Committee can, at any time without explanation, revoke a Technical Liaison. Members may request for the Membership Committee to review the status of a Technical Liaison or petition for revocation.

15.4.3 Technical Liaisons are reviewed by the Membership Committee at least annually and are subject to renewal or cancellation at each review. The review process looks for ongoing and consistent value in the relationship, changes in the status or position of the person, and feedback from the membership.

15.5 Obligations of the Technical Liaison

15.5.1 Technical Liaisons are expected to actively contribute to REN-ISAC.

15.5.2 Technical Liaisons must diligently abide the Information Sharing Policy and, unless modified by this document, the policies and guidelines for membership outlined in the Membership Guide and Terms and Conditions.

15.5.3 If the circumstances under which the Technical Liaison was admitted into REN-ISAC, such as title, job responsibilities, or events which may affect trust considerations change, the Technical Liaison is obligated to notify the Membership Committee. The Membership Committee will then re-evaluate eligibility.

15.5.4 Membership fees are waived for Technical Liaisons in view of the substantial and exceptional value brought to membership.

15.6 Rights and Limitations of the Technical Liaison

15.6.1 Technical Liaisons will have the full rights as REN-ISAC General Members, except for the following limitations:

1. No access to bulk threat indicator data in SES (does have singleton query access, pending a SES role-based feature request)
2. Eligibility to apply for XSec membership is determined by the Membership Committee
3. May serve and participate only on technical committees, mailing lists, and other technical forums serving the membership
4. No voting rights and not eligible to hold voting seats

15.7 Obligations of the Sponsor

1. Nominate and vouch for the Technical Liaison; advocate for the nomination (see Admittance)
2. Advocate for the annual renewal of the Technical Liaison; assist the Membership Committee as-required for renewal evaluation
3. Identify a replacement sponsor as-needed

16.0 Appendix A - Membership Eligibility Examples

16.1 Brian is nominated for Ops Member Representative. He is the lead systems administrator for institutional servers supporting the primary financial and student systems of the university. He is specifically tasked with security for the systems. Although he has explicit security responsibilities in his job description, he doesn't meet the requirement 7.2.3 to "represent security for the institution." Brian is not eligible for membership in the Operations (Ops) community, but he is eligible for the General community.

16.2 Melody is nominated for Ops Member Representative. She is an IT support provider in the College of Arts and Sciences at the University, concentrating on security matters for the College. The University has a central IT organization including a central security team. Melody is not eligible for membership in the (Ops) community because she doesn't meet the requirement 7.2.3 of having security duties of "institution or organization-wide responsibility". However, she is eligible for membership in the General community.

16.3 Kyle is nominated for General Member Representative. He is part of a three-person team handling security incidents for the University. The team is composed of students who rotate duty according to their class schedules. Kyle is not eligible for membership because he doesn't meet the requirement 7.1.2 for full-time permanent staff.

16.4 John is nominated for Ops Member Representative. He is a network engineer in the central networking group. He's responsible for wired and wireless campus infrastructure, DHCP, DNS, he provides assistance to the security team for network taps, NetFlow data, and he maintains the campus firewall. John and the member institution would benefit from John having access to feed data as well as critical news about vulnerabilities in core services like recent DNS bugs. John actively participates in technical discussions about security but ultimately works at the direction of the security team to disable access to compromised systems, alter the firewall policy, or establish new sensor taps.

John is not eligible for membership in the Ops community, because he doesn't meet the requirement 7.2.2 to have a principal responsibility in security protection and response. Rather, he conducts tasks at the direction of the security team. However, the institution would benefit by nominating John as a General Member Representative and requesting data feed access. That will allow him to employ specific REN-ISAC data feeds, in conjunction with NetFlow and DNS, to block active threats and identify infected systems. Additionally, the security team would be able to share DNS-related vulnerability information with John, as long as the information is classified privileged-use or below, and the sharing meets guidelines (see Information Sharing Policy, Sensitivity Classification).

16.5 Meryl is nominated as an Ops Member Representative. She is a senior network engineer in the NOC. Meryl spends 50% of her time working on security matters. Although the University has a separate IT Security Office, formal responsibility for security is split between the security and network offices. Meryl is tasked to work independently and in conjunction with the Security Office for network security matters. Meryl is eligible for membership because she shares principal responsibility for security protection and response.

16.6 MrX is nominated for Ops Member Representative. He is the sole security engineer for a university. MrX meets all the role-based criteria for membership. MrX has been known to disclose confidences given him regarding incident experiences at other institutions. MrX should not be granted membership because he has demonstrated untrustworthiness.

16.7 Professor Williams and her graduate student Thomas are conducting cyber-security research on log data analytics and wish to interact with security practitioners and other researchers. The Management Representative at their institution nominates Professor Williams and Thomas as Affiliates and then requests a special interest group called "Log Analytics Project". Since both are trusted members of the institution whose expertise can add value to the REN-ISAC membership, their nominations as affiliates are accepted.

16.8 Diego is nominated for Ops Member Representative. He is the manager of the Identity and Access Management team within the IT Security Office at his university. He reports to the CISO. As vital as Diego's team is to the overall information security posture of the university, he is not eligible for the Ops core community, as 7.2.2 requires protection and response responsibilities. However, Diego is certainly a great candidate for the General community.

17.0 Appendix B - On Becoming XSec

17.1 In order for an individual to gain XSec status, the individual must receive two vouches of personal trust from existing XSec Member Representatives - at least one from outside the member's own institution. Garnering the vouches is often difficult for persons who don't have strong peer relationships outside their institution. Personal networking and community engagement are key to developing the necessary relationships. Fertile areas for developing those relationships include:

- As an active REN-ISAC General member, communicating on the mailing list and IRC, participating in project groups, etc.
- Inter-organizational incident handling
- At EDUCAUSE conferences, and security working groups
- At Internet2 conferences, and security working groups
- At state and regional security conferences and working groups
- At InfraGard meetings

The relationship experience required for an XSec member to give a vouch of personal trust can't come from just a few hallway conversations at a conference. Persistent engagement in the community will develop the needed relationships.