AAF is enabled by NCRIS

[PDK06]

Community Membership Management Policy

Context
Clear and consistent Membership Management is a key function and benefit of a Collaboration. This policy establishes a baseline for the management of the User's membership lifecycle, and the expectations for Community Managers and their delegates.

In developing this policy, the Collaboration should also review the following technical considerations:

- How can the User experience best be streamlined if there are multiple Service Providers in the Collaboration? How often is a User required to acknowledge and Acceptable Use Policy? How many Acceptable Use Policies will be in effect for the Collaboration?
- What level of trust and identity assurance is required across the Collaboration? Will this inform how Users are organised?
- What is the minimum User information that needs to be collected to inform Community procedures, and how is this information (attributes) expressed?
- What attributes are required to facilitate membership and access to the Collaboration, what do they mean, and where is this expressed?
- How are the activities of Users and Collaboration Management (audit and traceability) managed on a technical level?
- What is the term of the membership lifecycle? How is User Registration Data verified?

*delete this box after completing the policy.

1 Introduction and Purpose

1.1 Objectives

This Policy is designed to establish trust in Collaboration that Community Membership (User) management and associated information management is implemented consistently and in compliance with the Scntfi framework.[1] It places requirements on the management of the membership lifecycle of Users, and further outlines the functions of the Community Manager.[2]

1.2 Scope

This Policy applies to the Community Manager and other relevant personnel that may be designated by the Collaboration, and Users as it pertains to their lifecycle as members of the Community and Collaboration.

In executing their responsibilities as outlined in this Policy, Community Managers will draw on Collaboration Policies, including the Privacy Policy, Policy on the Processing of Personal Information and the Acceptable Use Policy.

This Policy does not apply to the management of Communities or Users outside of the Collaboration.

[1] The *Scalable Negotiator for a Community Trust Framework in Federated Infrastructures*. Refer to www.igtf.net/snctfi/.
[2] Refer to [link to PDK01]

© Owned by the authors and made available under license: https://creativecommons.org/licenses/by-nc-sa/4.0/
Other Sources / Attribution / Acknowledgements: EGI Community Membership Management, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

This document is provided as guidance only. Each organisation or Collaboration must consider its own unique context, legislative obligations, and trust and identity requirements to complete and implement the Trust and Identity Policy Development Kit. AAF and other national research infrastructure members of the Policy Working Group, are not liable for any loss or damage, from any implementation or action taken to implement this Policy.

1.3 Definitions

Personal information: Information about an identified individual, or a reasonably identifiable individual.

Sponsor: A person who is a trusted agent (such a representative of an organisation or manager of a Service or Service Provider) that may be delegated specific Community Management responsibilities. A Sponsor is not considered Collaboration personnel or a part of Collaboration Management.

Additional terms are defined in the Top-Level Collaboration Policy.[2]

2 Membership Management

2.1 Aims and Purpose

For each Community, the Acceptable Use Policy must define the collective aims and purpose of the Community, such as its research and scholarship goals to facilitate decisions on resource allocation and the basis of User membership [RC6]. This definition must be shared with Collaboration Management who must also be promptly informed of any material changes to that definition.

2.2 Membership Lifecycle

The Community Manager is responsible for the Membership lifecycle process of their designated Community of Users. The Community Manager may delegate this responsibility to Collaboration personnel, Community personnel, or Sponsors.

Procedures implemented to manage membership in accordance with this policy must:

- unambiguously name the individuals who take responsibility for the validity of the Registration Data provided,
- ensure there is a way of contacting the User identified as responsible for an action while using Collaboration Services as a member of the Community, and
- identify those with the authority to exercise control over the rights of its members to use Services assigned to the Community.

Users must be aware that inappropriate actions by an individual member of the Community may adversely affect the ability of other members of the Community to use a Service.

All personal information, including Registration Data, must be stored and processed in accordance with the Policy on the Processing of Personal Information and applicable privacy legislation.

All procedures developed by the Community Manager as it pertains to membership management should be shared with Collaboration Management.

2.2.1 Registration

Membership Registration is the process by which an applicant joins a Community and becomes a User. The Community Manager must implement procedures that ensure the accuracy of Registration Data for all Users. Contact information for all Users must be verified at both initial collection (registration) and on an ongoing basis through periodic review, or at membership renewal.

Registration Data must be collected at the time of Registration, verified and stored in accordance with the Policy on the Processing of Personal Information. In order to be registered, the applicant must agree to abide by all relevant Acceptable Use Policies and agree to use Collaboration Services exclusively for the aims and

© Owned by the authors and made available under license: https://creativecommons.org/licenses/by-nc-sa/4.0/
Other Sources / Attribution / Acknowledgements: EGI Community Membership Management, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

This document is provided as guidance only. Each organisation or Collaboration must consider its own unique context, legislative obligations, and trust and identity requirements to complete and implement the Trust and Identity Policy Development Kit. AAF and other national research infrastructure members of the Policy Working Group, are not liable for any loss or damage, from any implementation or action taken to implement this Policy.

purposes listed in those Policies. This agreement must be logged in accordance with s3.2 of this Policy. All required Registration Data is listed in Schedule 1 of the Policy on the Processing of Personal Information.[3]

The Community Manager must operate, or have operated on the Community's behalf, a Registry that contains the Registration Data of the Community and is operated in compliance with the Sirtfi Framework[4].

2.2.2 Assignment of Attributes

Assignment of attributes (such as group membership, entitlements, or roles) shall be the responsibility of the Community Manager or of designated person(s) responsible for the management of such attributes. Attribute management may be subject to an assurance profile agreed upon between the Community and Service Providers. Attributes shall be assigned only for as long as they are applicable.

2.2.3 Renewal

Membership Renewal is the process by which a User remains a member eligible to use Collaboration Services assigned to the Community. Membership Renewal procedures must make a reasonable effort to

- ensure that accurate Registration Data is maintained for all eligible Users
- confirm continued eligibility of the User to use Collaboration Services assigned to the Community,
- confirm continued eligibility of the User to any attributes, and
- ensure the reaffirmation of acceptance of the AUP of the Community.

The maximum time span between Registration and Renewal, and between Renewals, for all Users shall be <INSERT RENEWAL TIMESPAN>. The User shall be able to correct and amend their Registration Data at any time as detailed in the Privacy Policy.[5]

2.2.4 Suspension

The Suspension of Community membership is the temporary revocation of full or partial rights and of any attributes. Suspension is enacted by or on behalf of the Community Manager.

A User should be suspended when the Community Manager is presented with reasonable evidence that the member's identity or credentials have been used, with or without the User's consent, in breach of relevant Policies.

Suspension can be requested by

- the Community Manager, the Sponsor of the User, those responsible for the assignment of attributes, or the User,
- Security Contact(s) or designated operational staff of the Collaboration, and
- Service Providers participating in the Collaboration.

The Community Manager must cooperate fully with the investigation and resolution of security incidents reported by the Security Contact(s) of any Service Provider, including acting on any requests for suspension without delay.

---

[3] [Link to PDK03
[4] The *Security Incident Response Trust Framework for Federated Identity* (v2.0). Refer to refeds.org/sirtfi. Entities must be compliant with Sirtfi Framework v1.0 for v2.0 compliance.
[5] [Link to PDK02]

© Owned by the authors and made available under license: https://creativecommons.org/licenses/by-nc-sa/4.0/
Other Sources / Attribution / Acknowledgements: EGI Community Membership Management, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

This document is provided as guidance only. Each organisation or Collaboration must consider its own unique context, legislative obligations, and trust and identity requirements to complete and implement the Trust and Identity Policy Development Kit. AAF and other national research infrastructure members of the Policy Working Group, are not liable for any loss or damage, from any implementation or action taken to implement this Policy.

Unless it is considered detrimental to the investigation and resolution of a security incident, the Community Manager should contact the User that was or is about to be suspended. The Community may define a dispute resolution process by which a User can challenge a Suspension.

User's rights shall not be reinstated unless the Community Manager has sent timely prior notification to all those who requested the Suspension.

2.2.5 Termination

The Termination of Community membership is the removal of a User from the Community. Following Termination, the former member is no longer eligible to use Collaboration Services, and the Community must no longer assert membership or attributes for the former member.

In the absence of overriding reasons, a request by the User for removal must be honoured.

The events that shall trigger re-evaluation of the User's membership of the Community include:

- request by the Sponsor,
- failure to complete a membership Renewal process within the specified time,
- end of association between the User and the Community,
- end of association between the User's Sponsor and the Community, if applicable,
- end of association between the User and his/her Sponsor, if applicable, and
- breach of Collaboration policies.

3 Information Management

3.1 Protection and Processing of Data

Communities must be managed in accordance with the Policy on the Processing of Personal Information and relevant legislation as it pertains to the personal information collected as a result of Users' membership to the Collaboration and its Communities. The Community Manager must ensure that, upon registration and through Acceptable Use Policies, Users explicitly acknowledge acceptance of relevant Collaboration Policies.

Any personal information stored by or on behalf of the Collaboration should be timestamped to assist in determining the appropriate retention and disposal period for that information in accordance with audit, traceability and legal requirements.

3.2 Audit and Traceability Requirements

The Community Manager must ensure that an audit log of all membership lifecycle transactions is recorded and maintained. The audit log must be kept for a minimum period consistent with the Traceability and Logging Policies of all Service Providers that that supply Services to the Community. Audit logs containing Registration Data must not be retained beyond the maximum period permitted by the Collaboration Policy on the Processing of Personal Information.

Events that must be logged include every request for:

- membership
- assignment or change to a member's attributes
- membership renewal
- membership suspension

© Owned by the authors and made available under license: https://creativecommons.org/licenses/by-nc-sa/4.0/
Other Sources / Attribution / Acknowledgements: EGI Community Membership Management, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

This document is provided as guidance only. Each organisation or Collaboration must consider its own unique context, legislative obligations, and trust and identity requirements to complete and implement the Trust and Identity Policy Development Kit. AAF and other national research infrastructure members of the Policy Working Group, are not liable for any loss or damage, from any implementation or action taken to implement this Policy.

- membership termination or re-evaluation
- acknowledgement of Acceptable Use Policies.

Each logged event should record:

- the date and time of the request
- the originator of the request
- details of the event
- whether or not the request was approved
- the identity of the person granting or refusing the request and any verification steps and people consulted in reaching that decision, including Sponsors.

4 Associated Documents

4.1 Collaboration Policies

- Top-Level Collaboration Policy [PDK01]
- Privacy Policy [PDK02]
- Policy on the Processing of Personal Information [PDK03]
- Acceptable Use Policy [PDK04]
- Acceptable Authentication Assurance Policy [PDK05]
- Service Operations Security Agreement [PDK07]
- Security Incident Response Procedure [PDK08]

Note
Any Collaboration-level procedures that are developed to manage Communities should be listed here. Collaboration Management should have any Community management-specific procedures on file.

*Delete this box after completing the policy.

4.2 Service Provider Audit and Traceability Policies

- [Insert policy and link]

4.3 Relevant Legislation, Standards & Frameworks

[Include all legislation, standards, and frameworks relevant to the Collaboration, highlighting their alignment with Australian laws as well as applicable international standards and regulations.]

- *Privacy Act (1988)* (Cth) (Australian Privacy Principles)
- *...*
- *Other relevant international standards and legislation (e.g. General Data Protection Regulation (GDPR), FAIR and CARE Principles)*

© Owned by the authors and made available under license: https://creativecommons.org/licenses/by-nc-sa/4.0/
Other Sources / Attribution / Acknowledgements: EGI Community Membership Management, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

This document is provided as guidance only. Each organisation or Collaboration must consider its own unique context, legislative obligations, and trust and identity requirements to complete and implement the Trust and Identity Policy Development Kit. AAF and other national research infrastructure members of the Policy Working Group, are not liable for any loss or damage, from any implementation or action taken to implement this Policy.

AAF is enabled by NCRIS

Version Control

Document Control			
Document Approved:		**Date Effective:**	
Last Review Date:		**Next Review Date:**	
Version Control			
Version	**Author**	**Summary of Changes**	**Date**
1.5	AAF	Update to reflect PWG recommendations, review and alignment of language, transposition of Community Membership Management governance to Top-Level Collaboration Policy, revision of title to 'Community Membership Management Policy' from 'Collaboration Membership Management Policy' to reflect user administration (cf management of the collaboration). Refinement of context statements. Corrected attributions. Updated disclaimer. Updated references to international legislations/frameworks (if relevant).	March 2026

AAF NRI Policy Development Kit – Community Membership Management Policy [PDK06]
© Owned by the authors and made available under license: https://creativecommons.org/licenses/by-nc-sa/4.0/
Other Sources / Attribution / Acknowledgements: EGI Community Membership Management, used under CC BY-NC-SA 4.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

This document is provided as guidance only. Each organisation or Collaboration must consider its own unique context, legislative obligations, and trust and identity requirements to complete and implement the Trust and Identity Policy Development Kit. AAF and other national research infrastructure members of the Policy Working Group, are not liable for any loss or damage, from any implementation or action taken to implement this Policy.