Community Membership Management Policy

Document identifier	EGI-SPG-Community-Member-Manage-V1
Document Link	https://documents.egi.eu/document/3234
Last Modified	03/11/2017
Version	1
Policy Group Acronym	SPG
Policy Group Name	Security Policy Group
Contact Person	David Kelsey/STFC
Document Type	Policy
Document Status	Final Draft – awaiting approval
Approved by	EGI Foundation Executive Board
Approved Date	dd/mm/yyyy

TABLE OF CONTENTS

COPYRIGHT NOTICE

AUTHORS LIST

	Name	Partner/Activity/ Organisation/Function	Date
From	David Kelsey	STFC/SPG	3/11/2017

DELIVERY SLIP

	Body	*Date*
Reviewed by:	Presented to EGI OMB in July 2017 and November 2017 and approved by EGI OMB (by email) in Nov 2017	27/07/2017 & 2/11/2017
Reviewed by:	EGI UCB and approved in Nov 2017	dd/mm/yyyy
Reviewed by:	EGI Foundation Executive Board	dd/mm/yyyy
Approved by:	EGI Foundation Executive Board	dd/mm/yyyy

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author/Partner*
V0.1	9/06/2017	New security policy replacing old policy "VO Membership Management Policy". Worked on during joint EGI SPG/AARC2 NA3 "Community Engagement" meeting in Karlsruhe 8-9 June 2017	David Kelsey /STFC
V0.2	7/07/2017	Updated version coming out of joint EGI SPG/AARC2 NA3 meeting in Amsterdam 5-7 July 2017	David Kelsey /STFC
V0.3	26/07/2017	Online and email edits. Version presented to EGI OMB and widely distributed for comment during Aug and Sep.	David Kelsey /STFC
V0.4	10/10/2017	Agreed at Vidyo Conference of joint EGI SPG/AARC2 NA3. Addresses all feedback received.	David Kelsey /STFC
V0.5	1/11/2017	A few final tweaks before EGI OMB.	David Kelsey /STFC
V1	dd/mm/yyyy	Approved and adopted version	David Kelsey/STFC

TERMINOLOGY

A complete project glossary is provided at the following page: http://www.egi.eu/about/glossary/

APPLICATION AREA

This document is a formal EGI.eu policy or procedure applicable to all participants and associate participants, beneficiaries and Joint Research Unit members, as well as its collaborating projects.

POLICY/PROCEDURE AMENDMENT PROCEDURE

Reviews and amendments should be done in accordance with the EGI.eu "Policy Development Process" (https://documents.egi.eu/document/169).

This policy is effective from 01/12/2017 and replaces an earlier security policy document [R1]. This policy is one of a set of documents that together define the Security Policy [R2] and must be considered in conjunction with all the policy documents in the set.

1 INTRODUCTION

This policy is designed to establish trust between a Community[1] and other Communities, Infrastructures, and the R&E federations. The behaviour of the Community and its users must be appropriate and facilitate the Community's compliance with the requirements of the *Snctfi* document [R3]. The identifiers of requirements from the *Snctfi* document are provided here in this document for ease of reference.

This Policy applies to the Community Manager and other designated Community management personnel. It places requirements on Communities regarding eligibility, obligations and rights of their Users, and it governs their relationships with all Infrastructures with which they have a usage agreement. The Community management personnel must ensure awareness and acceptance, by the Community and its Users, of the responsibilities documented in this Policy.

2 DEFINITIONS

A Community is a set of one or more groups of persons (Users), organised with a common purpose, with a Community Management willing to take responsibility for all sub-groups, jointly granted access to one or more Infrastructures. It may serve as an entity which acts as the interface between the individual Users and an Infrastructure. In general, the members of the Community will not need to separately negotiate access with Service Providers or Infrastructures (hereafter jointly called Infrastructures).

Examples of Communities include, but are not limited to: User groups, Virtual Organisations, Research Communities, Research Infrastructures, Virtual Research Communities, Projects, and Communities authorised to use particular portals or gateways, and geographically organised communities.

Other terms are defined in the Glossary [R4].

[1] See later for the definition of "Community". Other terms are defined in the Glossary [R4]

3 INDIVIDUAL USERS

The Community must define an Acceptable Use Policy (AUP) [RU1][2]. The AUP must be shown to all persons joining the Community. Acceptance of the AUP by Community members who act as responsible persons towards the Infrastructure must be an explicit action, must be recorded, and must be a prerequisite for registration in the Community [RU2]. The AUP must address at least the following areas:

- The aims and purposes, and the basis of membership of the Community
- Acceptable use
- Non-acceptable use
- Maintenance of user registration data
- Protection and use of credentials
- Data protection and privacy

The Community may rely on an Infrastructure AUP to address one or more of these requirements, provided that acceptance of such an Infrastructure AUP, in addition to the Community AUP, by the User is a prerequisite for registration. The Community AUP must not be in conflict with the referenced Infrastructure AUPs.

The data protection and privacy section of the AUP must address the relationship with the Infrastructure policies on the Processing of Personal Data, Security Traceability and Logging, and Service Operations Security.

Community procedures must ensure that the User is informed of and explicitly consents to material changes to the AUP, including those that arise out of new collaborative partnerships [RU3], as soon as is feasible.

Hosts, Services and/or Robots (automated processes acting on behalf of the Community or a User) may be registered as members of the Community. In the case of such registrations, the Registration Data must include the personal details of the individual requesting registration who must assume, as a User, ongoing responsibility for the registered entity, and may be subject to additional policy requirements of the Infrastructure.

All Users are deemed to be acting in a professional capacity when interacting with or using Infrastructure Resources assigned to the Community.

[2] This identifier is identical to that used in the *Snctfi* document.

4 COMMUNITY MANAGER AND OTHER ROLES

The Community must define a Community Manager role and assign this role to two or more individuals. The Community Manager is responsible for meeting the requirements of this Policy and those of the applicable Policies of the Infrastructures, and for implementing the necessary procedures and operational requirements [RC2].

The Community Manager does not necessarily have to be a member of the Community. The role may be performed by any individual so designated by the Community, including Infrastructure personnel.

The Community Manager must implement procedures that ensure the accuracy of individual user registration data for all Community members who act as responsible persons towards the Infrastructure. The contact information must be verified both at initial collection (registration) and on an ongoing basis (through periodic renewal or review) [RC1] and only stored and processed in compliance with applicable Data Protection legislation.

Other Community roles, such as additional management personnel and security contacts must be defined and assigned to individuals as specified in the Community Operations Security Policy [R5] or as required by the Infrastructure.

5 COMMUNITY

5.1 Aims and Purposes

As described above, the Community must define, in its AUP, its collective aims and purposes, i.e., the research or scholarship goals of the Community. In order to allow Infrastructures to make decisions on resource allocation [RC6], the Community should make this definition available to them, and subsequently inform them of any material changes therein [RC7].

5.2 Membership

The Community Manager is responsible for the Community Membership life cycle process of its Users [RC5]. This responsibility may be devolved to designated personnel in the Community or in the Infrastructure, and their trusted agents (such as Institute Representatives or Resource Centre Managers), hereafter collectively called Sponsors.

The Community procedures must

- unambiguously name the individuals who take responsibility for the validity of the Registration Data provided [RC1],
- ensure there is a way of contacting the User identified as responsible for an action while using Infrastructure services as a member of the Community [RC4], and

- identify those with the authority to exercise control over the rights of its members to use the Infrastructure Resources assigned to the Community.

The Community 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 an Infrastructure [RC3].

5.3 Membership life cycle: Registration

Membership Registration is the process by which an applicant joins the Community and becomes a Member. Registration Data must be collected at the time of Registration, verified and stored in compliance with the Data Protection and Privacy Policy [OS3]. Reasonable efforts must be spent to validate the data.

The applicant must agree to abide by the AUP of the Community, and agree to use Resources of the Infrastructures exclusively for the Aims and Purposes of the Community.

5.4 Membership life cycle: 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 the Infrastructures. Attributes shall be assigned only for as long as they are applicable.

5.5 Membership life cycle: Renewal

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

- ensure that accurate Registration Data is maintained [RC4,RC5] for all eligible Users
- confirm continued eligibility of the User to use Infrastructure Resources assigned to the Community
- confirm continued eligibility of the User to any attributes
- ensure the reaffirmation of acceptance of the AUP of the Community

The maximum time span between Registration and Renewal, and between Renewals, for all Community members who act as responsible persons towards the Infrastructure, shall be one year.
The User shall be able to correct and amend their Registration Data at any time.

5.6 Membership life cycle: Suspension

The Suspension of Community membership is the temporary revocation of full or partial rights and of any attributes. Suspension is done 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 Officer(s) or designated operational staff of the Infrastructure
- Resource Centres participating in the Infrastructure

The Community Manager must cooperate fully with the investigation and resolution of security incidents reported by the Security Officer(s) of any Infrastructure [OS2], including acting on any requests for suspension without delay.

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 Suspension.

5.7 Membership life cycle: Termination

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

In 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:

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

6 PROTECTION AND PROCESSING OF PERSONAL DATA

The Community must have policies and procedures addressing the protection of the privacy of individual Users with regard to the processing of their personal data collected as a result of their membership in the Community and of their access to resources provided by any Infrastructure. These policies must be made available in a visible and easily accessible way and Users must explicitly acknowledge acceptance of these policies [DP2] (through the AUP and registration process).

The Community must inform the User (through the AUP and registration process) of the policies on the processing of Personal Data of those providers with which it has entered into agreements and that can access the User's Personal Data [DP1].

The Policy on the processing of Personal Data of the Community [DP1] shall address at least the items in A.5 section 7 of the *Template Policy on the Processing of Personal Data* of the AARC *Recommendations and template policies for the processing of personal data* [R6], as amended from time to time.

It is recommended that any personal data stored by the Community is time-stamped in order to determine when it is appropriate to remove data that is no longer necessary for audit, traceability or any legal requirements.

7 AUDIT AND TRACEABILITY REQUIREMENTS

The Community must record and maintain an audit log of all membership lifecycle transactions. This audit log must be kept for a minimum period consistent with the Traceability and Logging Policies of all Infrastructures that provide resources to the Community. Audit logs containing personal registration data must not be retained beyond the maximum period allowed by the Policy on the processing of Personal Data of the Community (e.g. for as long as a member is registered and entitled to use resources and one year after this data is no longer associated with such an active membership or attribute assignment).

Events that must be logged include every request for:

- membership,
- assignment of or change to a member's attributes,
- membership renewal,
- membership suspension,
- membership termination or re-evaluation.

Each logged event should record the date and time, the originator, the details of the event, and whether or not it was approved. The identity of the person granting or refusing the request should be recorded, including any verification steps involved and other people consulted, such as Sponsors.

8 REGISTRY AND REGISTRATION DATA

The Community must operate, or have operated on its behalf, a Registry that contains the membership data of the Community. This registry must be operated in a secure and trustworthy manner and in compliance with the security requirements of the Community and of the Infrastructures [OS1] in terms of authentication, authorisation, access control, physical and network

security, security vulnerability handling and security incident handling. The Registry must also be operated in a manner compliant with REFEDS Sirtfi version 1 [R7] [OS3].

The Registry must store at least:

- Registration data, including personal data of the User
- attributes assigned to members

The Registration data for a User comprises verified information on at least:

- family name(s)
- given name(s)
- the employing organisation name and address
- any applicable Sponsor identity
- a professional email address
- unique and non-reassigned identifier(s) of the User and the source of authority of each identifier

and is recommended to contain:

- professional contact telephone number so as to inform the User promptly during the investigation of security incidents and of lifecycle events
- other contact information, as voluntarily provided and maintained by the User.

The types of information recorded must be listed in the Policy on the processing of Personal Data of the Community.

9 REFERENCES

R 1	Virtual Organisation Membership Management Policy. https://documents.egi.eu/document/79
R 2	Approved EGI Security Policies. https://wiki.egi.eu/wiki/Policies_and_Procedures
R 3	Snctfi. https://www.igtf.net/snctfi/
R 4	EGI Glossary. https://wiki.egi.eu/wiki/Glossary SPG Security Policy Glossary of Terms. https://documents.egi.eu/document/71
R 5	Community Operations Security Policy. https://documents.egi.eu/document/3233
R 6	AARC Template Policy for the Processing of Personal Data. Deliverable DNA3.5. https://aarc-project.eu/wp-content/uploads/2016/12/AARC-DNA3.5_Recommendations-for-Processing-Personal-Data_2016_11_07_v4_DG.pdf
R 7	Sirtfi. https://refeds.org/sirtfi