Virtual Organisation Membership Management Policy

This policy is effective from November 18th, 2020.

1 INTRODUCTION

This policy is designed to establish trust between a Virtual Organisation and other Virtual Organisations, Infrastructures, and the R&E federations. The behaviour of the Virtual Organisation and its Users must be appropriate and facilitate the Virtual Organisation's compliance with the requirements of *Snctfi* [1].

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

2 DEFINITIONS

Data supplied by the User is defined as follows.

User Data comprises verified information on at least:

- family name(s)
- given name(s)
- the employing organisation's name and address (this is required if the User's membership eligibility derives from his/her institutional affiliation)
- contact telephone number (this is optional, but the Virtual Organisation Management may need to contact the User promptly during investigation of security incidents)

Registration Data — authentication (AuthN) related information:

- *User Data*
- email address
- unique and non-reassigned identifier(s) of the User and the source of authority of each identifier
- registration timestamp

The principles of data protection should apply to any processing of personal data and information concerning an identified or identifiable User.

3 INDIVIDUAL USERS

The Virtual Organisation must define an Acceptable Use Policy (AUP). The AUP must be shown to all persons joining the Virtual Organisation. Acceptance of the AUP by Virtual Organisation 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 Virtual Organisation. Virtual Organisation 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, as soon as is feasible. The Virtual Organisation is recommended to ensure that their AUP comprises specific AUPs of the individual Services used by the Virtual Organisation. Experience shows that some Services require different AUPs.

Hosts, Services and/or Robots (automated processes acting on behalf of the Virtual Organisation or a User) may be registered as members of the Virtual Organisation. 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 Services that support the Virtual Organisation.

4 VIRTUAL ORGANISATION MANAGEMENT

The Virtual Organisation must define a Virtual Organisation Management role and assign this role to two or more individuals. The Virtual Organisation Management role can be performed only by individuals who can authenticate via an Identity Provider that is part of the Infrastructure. The Virtual Organisation Management 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.

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

The Virtual Organisation Management must implement procedures that ensure the accuracy of individual User *Registration Data* for all Virtual Organisation 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, please refer to the topic *Membership Life Cycle: Renewal*) and only stored and processed in compliance with applicable Data Protection legislation.

Other Virtual Organisation roles, such as additional management personnel and security contacts must be defined and assigned to individuals as required by the Infrastructure.

5 VIRTUAL ORGANISATION

5.1 Aims and Purposes

The Virtual Organisation must define, in its AUP, its collective aims and purposes, i.e., the research or scholarship goals of the Virtual Organisation. In order to allow Infrastructures to make decisions on resource allocation, the Virtual Organisation should make this definition available to them, and subsequently inform them of any material changes therein.

5.2 Membership

The Virtual Organisation Management is responsible for the Virtual Organisation Membership life cycle process of its Users. This responsibility may be devolved to designated personnel in the Virtual Organisation or in the Infrastructure, and their trusted agents (such as Institute Representatives or Service Managers), hereafter collectively called Sponsors.

The Virtual Organisation procedures 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 Infrastructure Services as a member of the Virtual Organisation, and
- identify those with the authority to exercise control over the rights of its members to use the Infrastructure Services that support the Virtual Organisation.

The Virtual Organisation must be aware that inappropriate actions by an individual member of the Virtual Organisation may adversely affect the ability of other members of the Virtual Organisation to use an Infrastructure.

5.3 Membership Life Cycle: Registration

Membership Registration is the process by which an applicant joins the Virtual Organisation 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. Reasonable efforts must be spent to validate the data.

The applicant must agree to abide by the AUP of the Virtual Organisation, and agree to use Services of the Infrastructures exclusively for the Aims and Purposes of the Virtual Organisation.

5.4 Membership Life Cycle: Assignment of Attributes

Assignment of attributes (such as group membership, entitlements, or roles) shall be the responsibility of the Virtual Organisation Management 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 Virtual Organisation and the Infrastructures. Attributes shall be assigned only for as long as they are applicable.

5.5 Membership Life Cycle: Changes of Assurance Level

In some cases, it may be necessary to increase the assurance of a User (for example, changing the identity assurance profile from low to medium). This shall be the responsibility of the Virtual Organisation Management and must be done in accordance to the assurance framework in which the statement was made.

5.6 Membership Life Cycle: Renewal

Membership Renewal is the process by which a User remains a member of the Virtual Organisation. 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 Infrastructure Services that support the Virtual Organisation
- confirm continued eligibility of the User to any attributes
- ensure the reaffirmation of acceptance of the AUP of the Virtual Organisation

The maximum time span between Registration and Renewal, and between Renewals, for all Virtual Organisation 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.

5.7 Membership Life Cycle: Suspension

The Suspension of Virtual Organisation membership is the temporary revocation of full or partial rights and of any attributes. Suspension is done by or on behalf of the Virtual Organisation Management.
A User should be suspended when the Virtual Organisation Management 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 Virtual Organisation Management, the Sponsor of the User, those responsible for the assignment of attributes, or the User;
- Officer(s) or operational staff of the Infrastructure designated by the Infrastructure Management;
- Service Providers participating in the Infrastructure.

The Virtual Organisation Management must cooperate fully with the investigation and resolution of security incidents reported by the Security Officer(s) of any Infrastructure, including acting on any requests for suspension without delay.

Unless it is considered detrimental to the investigation and resolution of a security incident, the Virtual Organisation Management should contact the User that was or is about to be suspended. The Virtual Organisation may define a dispute resolution process by which a User can challenge a Suspension.
User's rights shall not be reinstated unless the Virtual Organisation Management has sent timely prior notification to all those who requested Suspension.

5.8 Membership Life Cycle: Termination

The Termination of Virtual Organisation membership is the removal of a member from the Virtual Organisation. Following Termination, the former member is no longer eligible to use Infrastructure Services that support the Virtual Organisation and the Virtual Organisation 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 honored.
The events that shall trigger re-evaluation of the User's membership of the Virtual Organisation 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 Virtual Organisation,
- end of collaboration between the User's Sponsor and the Virtual Organisation, if applicable,
- end of collaboration between the User and his/her Sponsor, if applicable.

6 PROTECTION AND PROCESSING OF PERSONAL DATA

The Virtual Organisation 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 Virtual Organisation and of their access to Services 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 (through the AUP and registration process).

The Virtual Organisation must inform the User (through the AUP and registration process) of the policies on the processing of *Personal Data* of those Service Providers with which it has entered into agreements and that can access the User's *Personal Data*.

It is recommended that any *Personal Data* stored by the Virtual Organisation 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 Virtual Organisation 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 Services to the Virtual Organisation. 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 Virtual Organisation (e.g. for as long as a member is registered and entitled to use Services 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,
- assignment of or change to a member's assurance information,
- 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 Virtual Organisation must operate, or have operated on its behalf, a Registry that contains the membership data of the Virtual Organisation. This registry must be operated in a secure and trustworthy manner and in compliance with the security requirements of the Virtual Organisation and of the Infrastructures 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 Sirtfi [2].

The Registry must store at least:

- *Registration Data,* including *Personal Data* of the User
- attributes assigned to members

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

9 REFERENCES

[1] Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (Snctfi) - https://www.igtf.net/snctfi/
[2] Security Incident Response Trust Framework for Federated Identity (Sirtfi) - https://refeds.org/sirtfi