EGI-InSPIRE

VIRTUAL ORGANISATION MEMBERSHIP MANAGEMENT POLICY

Document Identifier:	EGI-P.79-SPG-VOManagement
Document Link:	https://documents.egi.eu/document/79
Date:	**13/07/2010**
Version	**1.0**
Policy Group Acronym	**SPG**
Policy Group Name	**Security Policy Group**
Document Status:	**Submitted**
Contact Person	**David Kelsey/STFC, UK**
Approved By	**Body who approved the doc**
Approved Date	**13/07/2010**

Policy Statement

This policy defines the minimum requirements on Virtual Organisation (VO) Managers for managing the members of their VOs.

Document Log

Issue	Date	Comment	Author
1.0	13/07/2010	Imported from JSPG policy document with the same title. The only change to wording made was to update a link (URL). See https://edms.cern.ch/document/428034 (V3.7a, dated 15 July 2009) for the old JSPG document.	David Kelsey/STFC
2.0			
3.0			
4.0			

PROJECT SUMMARY

To support science and innovation, a lasting operational model for e-Science is needed − both for coordinating the infrastructure and for delivering integrated services that cross national borders.

The EGI-InSPIRE project will support the transition from a project-based system to a sustainable pan-European e-Infrastructure, by supporting 'grids' of high-performance computing (HPC) and high-throughput computing (HTC) resources. EGI-InSPIRE will also be ideally placed to integrate new Distributed Computing Infrastructures (DCIs) such as clouds, supercomputing networks and desktop grids, to benefit the user communities within the European Research Area.

EGI-InSPIRE will collect user requirements and provide support for the current and potential new user communities, for example the ESFRI projects. Support will also be given to the current heavy users of the infrastructure, such as high energy physics, computational chemistry and life sciences, as they move their critical services and tools from a centralised support model to one driven by their own individual communities.

The objectives of the project are:

1. The continued operation and expansion of today's production infrastructure by transitioning to a governance model and operational infrastructure that can be increasingly sustained outside of specific project funding.
2. The continued support of researchers within Europe and their international collaborators that are using the current production infrastructure.
3. The support for current heavy users of the infrastructure in earth science, astronomy and astrophysics, fusion, computational chemistry and materials science technology, life sciences and high energy physics as they move to sustainable support models for their own communities.
4. Interfaces that expand access to new user communities including new potential heavy users of the infrastructure from the ESFRI projects.
5. Mechanisms to integrate existing infrastructure providers in Europe and around the world into the production infrastructure, so as to provide transparent access to all authorised users.
6. Establish processes and procedures to allow the integration of new DCI technologies (e.g. clouds, volunteer desktop grids) and heterogeneous resources (e.g. HTC and HPC) into a seamless production infrastructure as they mature and demonstrate value to the EGI community.

The EGI community is a federation of independent national and community resource providers, whose resources support specific research communities and international collaborators both within Europe and worldwide. EGI.eu, coordinator of EGI-InSPIRE, brings together partner institutions established within the community to provide a set of essential human and technical services that enable secure integrated access to distributed resources on behalf of the community.

The production infrastructure supports Virtual Research Communities − structured international user communities − that are grouped into specific research domains. VRCs are formally represented within EGI at both a technical and strategic level.

TABLE OF CONTENTS

1 Virtual Organisation Membership Management Policy: Introduction

This policy defines the minimum requirements on Virtual Organisation (VO) Managers for managing the members of their VOs.

2 Scope and Audience

This document is aimed primarily at VO Managers. It defines the checks VO Managers must make to verify the eligibility of their members to join and to remain in the VO. These are independent of the implementation of the underlying technology. It does not address the security requirements for running the actual VO Membership service.

The VO Manager does not necessarily have to be a member of the VO or to have signed and agreed to the VO AUP. This function may be performed by a member of a Grid or Site operations team as a service for the VO.

3 Definitions

Data supplied by the user:

- **Personal user data:**
  - Family Name,
  - Given Name,
  - Institute name, i.e. the user's employing institute (this is required if the user's membership eligibility derives from his/her institutional affiliation)
  - Contact Phone number (this is optional, but the VO Manager may need to contact the user promptly during investigation of security incidents)
- **Registration Data:** Authentication (AuthN) related information:
  - Personal user data,
  - Email address,
  - DistinguishedName (DN) extracted from a valid personal digital certificate issued by his/her Certification Authority (CA).

Other relevant terms:

- **VO Database:** Authorisation (AuthZ) related information, i.e. the user's role(s) in the VO, is stored in this database. His/her access rights to a resource and on data stored at it will depend on this information.
- **VO Manager:** The responsible person recording in the VO Database, after appropriate checks, the status of a member of the VO, i.e. performing user entries, assignment of roles, information updates and user removals. The VO management function can be performed by a group of persons delegated by the VO Manager. The VO Manager does not necessarily have to be a member of the VO or to have signed and agreed to the VO AUP. This function may be performed by a member of a Grid or Site operations team as a service for the VO. All VO Managers must comply with the requirements of this policy.

- **Institute Representative (IR):** If appointed, this person at the user's employing institute is able to check the validity of his/her data and confirm the identity of the user and his/her right to become or remain a member of a VO.
- **VO Registration Information:** Data stored by the Grid describing information about the VO.

4 Membership Management Requirements

The VO must appoint a VO manager and at least one deputy who are responsible for implementing procedures meeting the requirements of this policy. These are important roles which carry operational responsibilities; non-responsiveness of the VO manager or deputies may lead to the suspension of the VO from the Grid.

The VO membership management procedures must ensure that:

- only individuals who have agreed to abide by the VO AUP are registered as members of the VO,
- accurate Registration Data is maintained for all VO members.

Membership of a VO is not necessarily restricted to real persons. Hosts, Services and/or Robots (unattended automated processes acting on behalf of the VO) may also be registered in the VO. In the case of these non-personal registrations, the Registration Data must include the personal details of the real person requesting registration and assuming ongoing responsibility for the entity.

The VO Manager must publish a description of the methods used to verify user data at registration time and periodically review users' affiliation with the VO according to the requirements in the following sub-sections.

4.1 Appointment of the VO manager

The VO should determine how it appoints and replaces its VO manager and deputies.

4.2 Membership Registration

Membership Registration is the process by which people first join the VO. An important objective of this process is to collect the user's Registration Data. Accurate Registration Data must be maintained for all VO members.

VO Managers must check the validity of the user Registration Data and check the user's eligibility for special authorisation (Groups/Roles).

Replication of Personal user data and multiple validation and authentication should be avoided so that Grid users register only once with each VO and their Registration Data are checked only in a single place.

The procedures must unambiguously assign the individuals who take responsibility for the validity of the Registration Data provided, and those with the authority to exercise control over the rights of the user to use Grid resources. This may include an Institute Representative, as defined above, and/or Site Managers.

4.3 Acceptable Use Policy

An important purpose of the registration process is to record the explicit acceptance by the user of the Grid AUP and the VO AUP as well as the acceptance, by the user, that part of his/her information including Personal user data may be made available to the Sites and Grid Operations.

4.4 Membership Renewal

The membership renewal process must include:

- Confirmation, by the VO Manager, that continued membership of VO is still allowed,
- Confirmation or update of all data provided during registration and all special authorisations,
- Reaffirmed acceptance by the user of the Grid AUP and the VO AUP.

Membership of the VO must be renewed at least every 12 months. Additionally all members of the VO should renew following a major change to the Grid Acceptable Use Policy.

4.5 Membership Removal

The following conditions should trigger a timely re-evaluation of the user's right to remain a member of a given VO:

- User or IR request. Ideally, the user should be able to remove themselves from the VO without involvement of the VO Manager,
- Renewal failed to complete in allotted time,
- End of collaboration between the user's institute and the VO, if applicable,
- End of collaboration between the user and the VO,
- End of collaboration between the user and his/her institute, if applicable.

Note that some VOs may not maintain relationships with institutes. The fact that the VO does not maintain relationships with institutes should be recorded on the VO Registration Information.

4.6 Membership Suspension

The suspension of VO membership is the temporary removal of the user from the VO.

The VO Manager must cooperate fully with Grid Security Operations in the investigation of Grid security incidents. A member should be suspended when the VO Manager is presented with reasonable evidence that the member's grid identity has been used, with or without the user's consent, in breach of relevant Grid and/or VO policies (security or otherwise).

The request for suspension may be made by the Grid Security Officer and/or by Grid Operations. Requests from Sites should be routed through and confirmed by the Grid Security Officer and/or Grid Operations. In emergency situations this confirmation may be provided after the actual suspension if the VO Manager decides this is appropriate.

All reasonable efforts must be made by the VO Manager to contact the member when he/she is suspended.

Prior to reinstating a suspended user the VO Manager must notify those who requested suspension.

There should be an agreed dispute resolution procedures which the VO and/or Grid can follow if the user wishes to challenge his/her suspension.

4.7 Audit requirements

The VO Membership Management system(s) must record and maintain an audit log of all VO membership transactions.

This audit log must be kept for a minimum period consistent with the Traceability and Logging Policy (https://documents.egi.eu/document/81). Audit logs containing personal registration data must not be retained for longer than one year.

The audit logs must include:

- every request for membership,
- every request for assignment of or change to VO authorisation attributes (groups, roles etc.),
- every membership renewal request,
- every membership suspension request,
- every membership removal.

Each of these requests should record the date and time of the request, the originator of the request, the details of the request and whether or not it was approved or successful. The identity of the person granting or refusing the request should be recorded including any verification steps involved and other people consulted, e.g. IR.

4.8 Data privacy

It is recommended that the VO should document its VO Membership data privacy policy. This should include statements on:

- which data, if any, is collected from a VO member in addition to the Registration Data and explain why this data is required,
- how and where the data is stored,
- for how long the data is kept and how expired data is deleted,
- explain who within the VO has access to the data and why,
- how the user can view their own data and request corrections,
- what happens to the VO membership data when the VO ceases to exist,
- describe any third parties to whom VO membership data is disclosed and why. The VO may decide, for example, to grant read access to the data by Grid and Security Operations.

