



- Deleted: 6
- Deleted: 3
- Deleted: 28/10/05
- Deleted: 07/04/05



Joint Security Policy Group

LCG/EGEE Virtual Organisation Security Policy



<i>Date:</i>	28 October 2005
<i>EDMS Reference:</i>	https://edms.cern.ch/document/573348
<i>Internal Version:</i>	1.7
<i>Status:</i>	Draft
<i>Author:</i>	Ian Neilson & JSPG

- Deleted: 6
- Deleted: 3
- Deleted: 28/10/05
- Deleted: 07/04/05
- Deleted: 14 June 2005
- Deleted: <https://edms.cern.ch/document/573348>
- Formatted: Default Paragraph Font
- Deleted: 6
- Deleted: 3



Deleted: 6
Deleted: 3
Deleted: 28/10/05
Deleted: 07/04/05

Document Log			
Issue	Date	Author	Comment
1.0	15 March 2005	Ian Neilson	Initial version including comments from Maria Dimou
1.1	7 April 2005	Ian Neilson	Merge input from Dave Kelsey and JSPG meeting 6 April 2005
1.2	13 May 2005	Ian Neilson	Add suggestions from Dave Kelsey +? re: incident reporting point
1.3	14 June 2005	Ian Neilson	Incorporate comment from Pal Anderssen for single security contact point.
1.4	27 October 2005	Ian Neilson	Add changes following JSPG meeting at EGEE-4 conference
1.5	28 October 2005	Ian Neilson	Added reference to Approval of CA policy suggested by C. Kanellopoulos
1.6	28 October 2005	Ian Neilson	Integrated comments on EGEE-4 discussion by Dave Kelsey
1.7	31 October 2005	Ian Neilson	Comments from Ake Sandgren

Deleted: 6

Deleted: 3

Deleted: 28/10/05

Deleted: 07/04/05

1 Introduction

This policy defines a set of responsibilities placed on the members of the VO and the VO as a whole through its managers. It aims to ensure that all Grid participants have sufficient information to properly fulfil their roles with respect to interactions with a Virtual Organisation (VO).

1.1 Exclusions

This policy does not address the process by which disputes between Grid participants are resolved. It is expected that VO and Grid management bodies will agree appropriate mechanisms through which such disputes can be resolved.

2 Definitions

This document makes use of terms defined in the [LCG/EGEE Security Policy Glossary of Terms](#)¹

3 VO Registration Requirements

To satisfy Grid security requirements a VO enrolment process MUST capture and maintain at least the following information:

1. VO Name
2. VO Acceptable Use Policy
3. Contact details and certificates for the VO Manager and at least one Alternate:
 - a. Name
 - b. Employing Institute
 - c. VO Role (Manager or Alternate)
 - d. Email address
 - e. Telephone number
 - f. X.509 certificate from an [approved](#) Certification Authority²
4. Email address of a generic VO contact point for the VO managers
5. A single email address of the security contact point to be used for accepting reports of suspected identity compromises, misuse of resources or other security events related to the VO.
6. URL of one or more VO Membership Servers

Deleted: accepted

4 VO Acceptable Use Policy

The VO Acceptable Use Policy (AUP) is a statement which, by clearly describing the goals of the VO, defines the expected and acceptable usage of the Grid by the members of the VO. By requiring that all members of the VO who participate in the Grid agree to act within the constraints of the VO AUP the VO Manager defines a community of responsible users with a common goal. This definition enables Site Managers to decide whether to allow VO members to use their resources.

The VO AUP MUST:

1. bind VO members to abide by the Grid Acceptable Use Policy³.
2. state which VO management body gives authority to the Policy.

- Deleted: 6
- Deleted: 3
- Deleted: 28/10/05
- Deleted: 07/04/05

5 VO Community Responsibilities

The VO community comprises both ordinary VO members and VO management. The VO Manager may delegate authority to Alternate VO Managers who can act on their behalf.

5.1 VO Manager and Alternates

Whilst the operation and maintenance of the VO services may be delegated to an operations infrastructure, the VO Manager accepts overall responsibility for the content of the VO Membership Servers. In particular he or she MUST ensure that:

1. the VO member registration process and membership servers are managed in accordance with the LCG/EGEE User Registration Requirements⁴. This includes, but is not limited to, ensuring that:
 - a. only individuals who have agreed to abide by the VO AUP are registered as members of the VO.
 - b. accurate contact and identity information is maintained for all VO members.
 - c. privacy policy related to users' personal registration information is maintained.
2. mechanisms of removal or suspension of a member are understood and can be exercised if required.
3. the security contact point (see section 3 above) is published in an appropriate and widely accessible location.
4. a member is suspended when 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 security policies.
5. all reasonable efforts are made to contact a member when the member is suspended.
6. prior to reinstating a suspended user, notify those who requested suspension.
7. full cooperation is given in the investigation of Grid security incidents⁵.

- Deleted: The VO Manager MUST:¶
- Deleted: ensure that
- Formatted: Bullets and Numbering
- Formatted: Font: (Default) Times New Roman, 12 pt
- Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.29" + Tab after: 0.54" + Indent at: 0.54"
- Deleted: suspend a member
- Deleted: if requested to do so by a registered site security contact, GOC or ROC responsible. In case of doubt, the VO Manager should suspend the member as a precautionary measure prior to further investigation of the request.
- Deleted:
- Deleted: make
- Formatted: Bullets and Numbering
- Deleted: cooperate fully
- Deleted: ⁵
- Deleted: ⁴
- Comment [11]: Note here that the User Registration Requirements only seem to bind the user to accept the LCG Usage Rules
- Deleted: Grid
- Deleted: ²
- Formatted: Bullets and Numbering
- Formatted: Superscript
- Deleted: , resource administrator or site security contact.
- Deleted:

5.2 VO Members

Members of a VO MUST agree to:

1. abide by the VO Acceptable Use Policy,
2. abide by the Grid Acceptable Use Policy³.
3. immediately cease any actions when requested to do so by a VO Manager or Alternate,
4. cooperate fully in the investigation of Grid security incidents⁵.

6 Sample VO Acceptable Use Policy

The following text is presented as an example of a minimal VO Acceptable Use Policy.

"This Acceptable Use Policy applies to all members of [VO Name] Virtual Organisation, hereafter referred to as the VO, with reference to use of the LCG/EGEE Grid infrastructure, hereafter referred to as the Grid. The [owner body] owns and gives authority to this policy. The goal of the VO is to [describe here the objectives of the VO]. Members and Managers of the VO agree to be bound by the Grid Acceptable Usage Rules, VO Security Policy and other relevant Grid Policies, and to use the Grid only in the furtherance of the stated goal of the VO."



Deleted: 6
Deleted: 3
Deleted: 28/10/05
Deleted: 07/04/05

¹ LCG/EGEE Security Policy Documents' Glossary of Terms - <https://edms.cern.ch/document/573613>

² [LCG/EGEE Approval of Certification Authorities - https://edms.cern.ch/document/428038](https://edms.cern.ch/document/428038)

³ LCG/EGEE Acceptable Use Policy - <https://edms.cern.ch/document/428036> (to be updated)

⁴ LCG/EGEE User Registration and VO Management - <https://edms.cern.ch/document/428034>

⁵ LCG/EGEE Agreement on Incident Response - <https://edms.cern.ch/document/428035>