EGEE and OSG: Common Security Policies?

OSG Consortium Meeting
Seattle, 21 Aug 2006

David Kelsey
CCLRC/RAL
d.p.kelsey@rl.ac.uk

Overview

- **Joint Security Policy Group**
  - Introduction and History
- **The Grid/VO/Site/User "model"**
- **Interoperable Policy and Procedures**
- **The set of Security Policy documents**
  - Recent & current work
- **EGEE and OSG commonalities and divergences**
- **N.b. not discussing security operations or vulnerability handling activities**

History

- **LCG Security Group was created in early 2003**
  - LHC Computing Grid (Particle Physics)

Mandate

- **To advise and make recommendations to the Grid Deployment Manager and LCG GDB on all matters related to Security**
  - *Policies are agreed and adopted by GDB for LCG*
- **To produce and maintain**
  - Policies and procedures on
    Registration, Authentication, Authorization and Security
- **Where necessary recommend the creation of focussed task-forces made-up of appropriate experts**
  - E.g. Task force on *LCG User Registration*

JSPG

- **Following first EGEE collaboration meeting (April 2004)**
  - Scope of group extended
  - To include a proposed EGEE SA1 Site Security Group
- **Joint Security Policy Group (JSPG)**
  - "Joint" initially means EGEE *and* LCG
  - Strong participation by USA Open Science Grid
  - Now "Joint" = EGEE/OSG/WLCG
- **An activity of EGEE SA1 (Deployment & Operations)**
  - Discusses all documents with ROC Managers
  - Participation of site managers/security officers
- **Strong links to EGEE Middleware Security Group**
- **New "task force" (added after 2nd EGEE meeting)**
  - SA1 Operational Security Coordination Team (OSCT)

JSPG membership

- **Application representatives/VO managers**
  - Discussions with VO managers as/when required
- **Site Security Officers**
  - Bob Cowles (SLAC), Denise Heagerty (CERN), & in the past - Dane Skow (FNAL)
- **Site/Resource Managers/Security Contacts**
  - Dave Kelsey (RAL) – Chair
  - Miguel Cardenas Montes (Spain)
- **Security middleware experts/developers**
  - Joni Hahkala (JRA3), David Groep (JRA3), Andrew McNab (GridPP), Yuri Demchenko (JRA3)
- **CERN Deployment team**
  - Maria Dimou, Ian Neilson (Security Officer)
- **Now expanding to include other EU Grid projects**
  - SEE-Grid, DEISA, Diligent
- **Other EU Infrastructure projects use our policies**
  - BalticGrid, EELA, EUMedGrid, EUChinaGrid

Grid/VO/Site/User Model

- **Users**
  - only need a single electronic identity
  - They register *once* per VO (and renew)
  - Can/do belong to *more than one* VO
  - do *not* register at sites or Grids
- **Virtual Organisations (VO)**
  - register with Grid (again once per Grid)
  - Aim for *single instance* of VO membership database
  - To be used across *multiple* Grids
- **Sites**
  - can/do provide resources to multiple Grids
  - register with Grid (once per Grid)
  - decide which VOs to support
    - Distributed Grid Operations facilitates this
      - *Deployment, configuration etc*

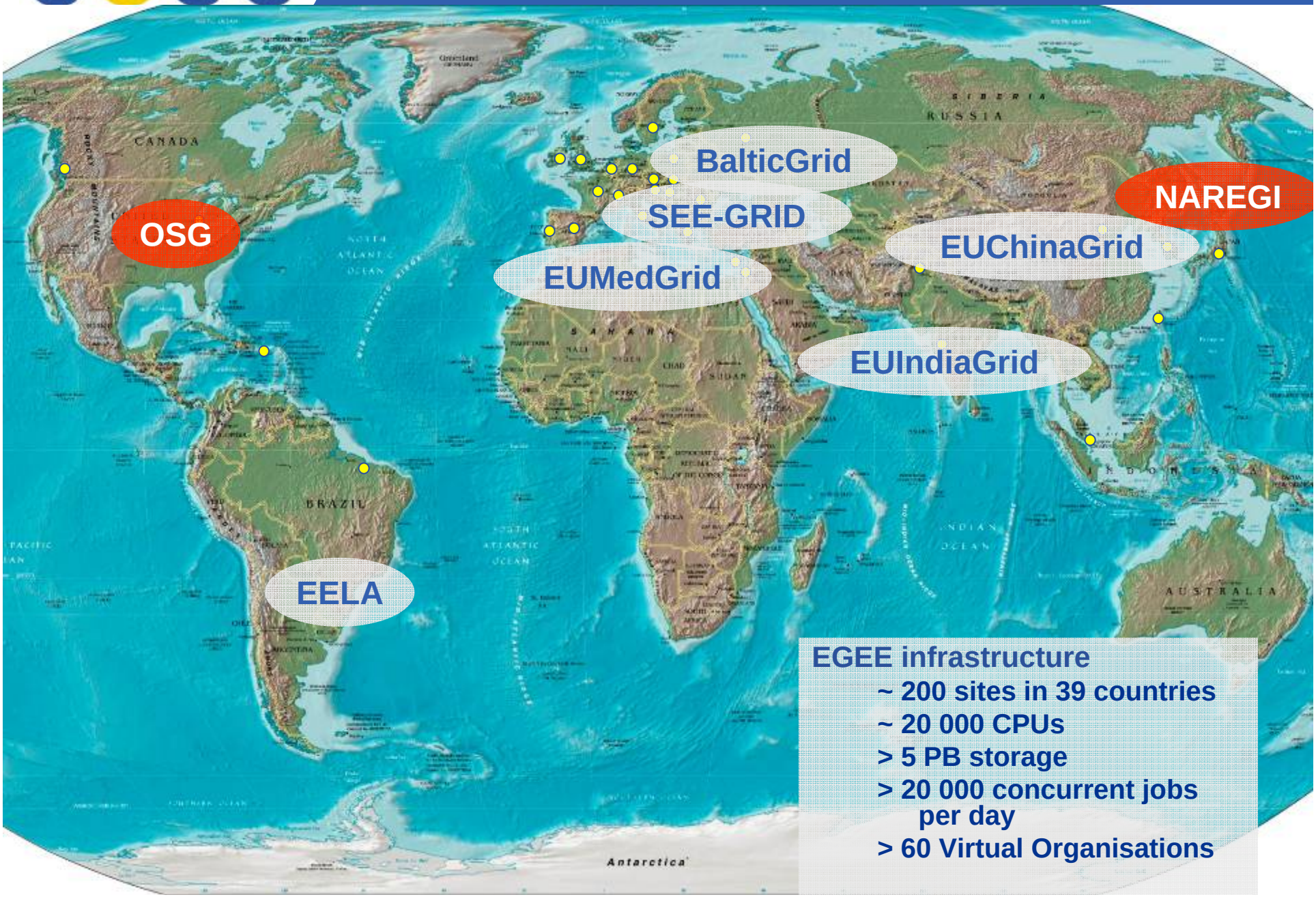
Grid Trust

- **Many components (in ascending scale of difficulty)**
  - Technical
    - Interoperable security, standards-based
  - Policy and Procedures
    - Ensure participants act in a predictable way
  - Legal
    - International aspects particularly hard
    - Data and personal privacy issues
  - Social
    - Have spent last 6 years building “trust” (IGTF)
    - Many face to face meetings
    - Last 2 years, working towards a federated approach
- **Sites need to trust VO’s (and vice versa)**
  - To take care of Users, Data, Operations, …

Interoperable Policies

- **Aim to allow applications (VO's) to easily use resources in multiple Grids**
- **The simplest approach**
  - Common Policies
    - User AUP
    - Site AUP
    - VO AUP
    - Operational procedures and other policies
- **If not common then at least not conflicting**
  - Does NOT override local site and network security policy
- **EGEE working with other EU Grid projects**
  - Common policies and procedures
- **EU eInfrastructure Reflection Group (eIRG)**
  - Common approach at highest level
    - EGEE inputs policy for consideration

A global, federated e-Infrastructure

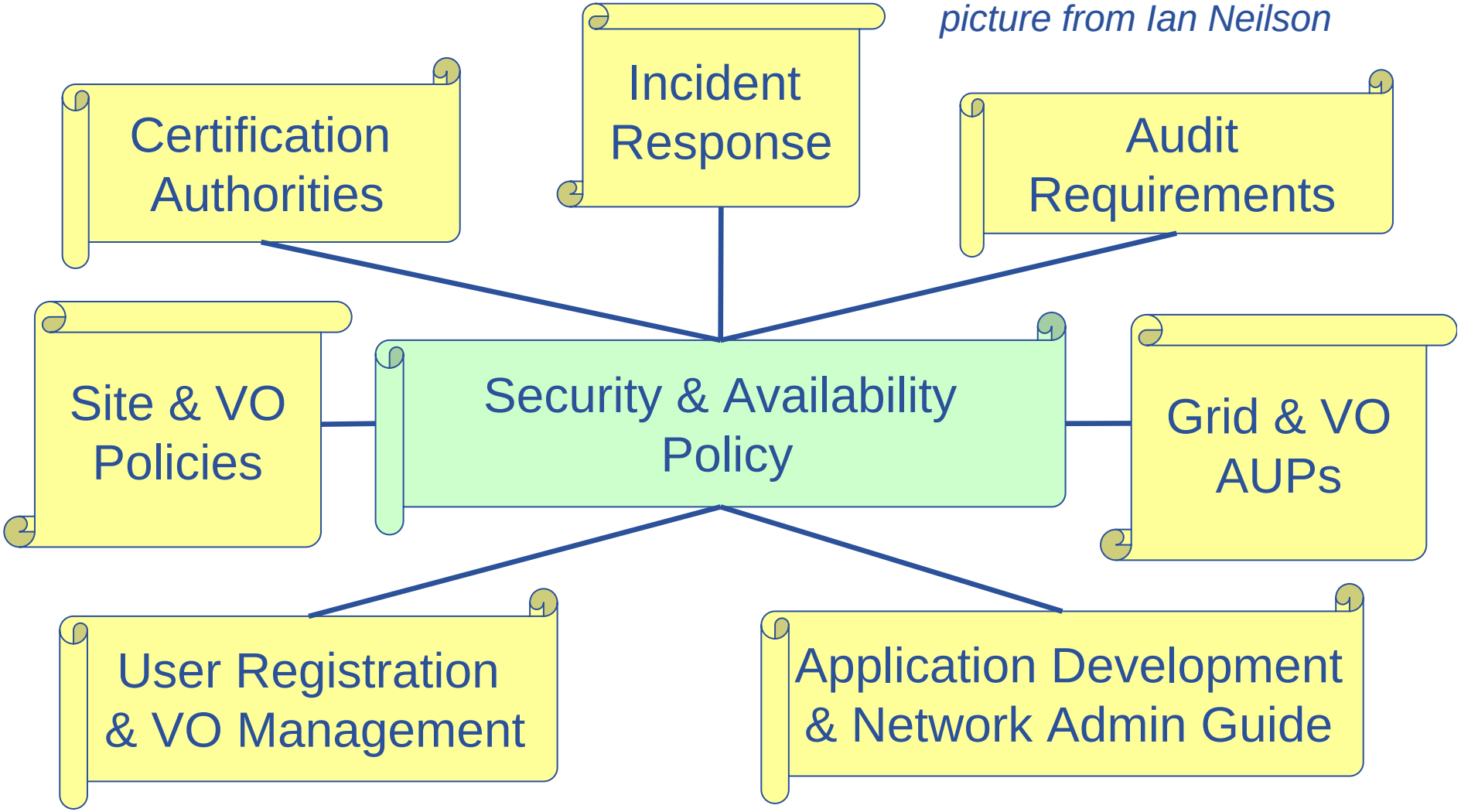


EGEE infrastructure

- ~ 200 sites in 39 countries
- ~ 20 000 CPUs
- > 5 PB storage
- > 20 000 concurrent jobs per day
- > 60 Virtual Organisations

EGEE/LCG Policy

picture from Ian Neilson



Recent/Current JSPG work

- **Recently approved**
  - Grid AUP
  - VO Security Policy (requires a VO AUP)
  - CA Approval (using IGTF accredited CA's)
- **All other documents need updating (this year)**
- **Current work**
  - Top-level Security Policy document
    - Defines roles and responsibilities, sanctions etc
  - Site Operational Procedures Policy
  - VO Naming (use DNS style)
  - User-level Accounting data policy (privacy issues)
- **All new documents are aimed to be simple and general, e.g. apply to "Grid" not "EGEE" (like the Grid AUP)**

EGEE/OSG Commonalities and Divergences?

- **Some initial thoughts**
  - Hopefully more will become clear during this meeting!
- **Common**
  - Grid AUP
  - Security Incident Response
  - CA Approval
- **Divergent**
  - EGEE assumes Sites already have appropriate policies
    - Just add the Grid specific extras
  - VO AUP?
    - Will VO's be willing to assume responsibility for users?
    - VO's are not legal entities
    - Are VO's capable of operations and risk analysis?
  - Data Privacy legal issues?
  - We do need to work jointly on these issues
- **JSPG working on new top-level policy document**
  - Can we agree a common version for use in OSG and EGEE?

Summary

- **To date, JSPG has successfully created some policies which are common between EGEE and OSG**
- **OSG Risk Analysis**
  - Very useful input to EGEE
- **Very desirable that we continue to aim for common policies**
  - To allow VO's to easily use multiple Grids
- **If this is not possible, then understand why not**
  - And fix it?
- **Where there are/need to be differences**
  - Keep these as separate components

JSPG Meetings, Web etc

- **Meetings - Agenda, presentations, minutes etc**

http://agenda.cern.ch/displayLevel.php?fid=68

- **JSPG Web site**

http://proj-lcg-security.web.cern.ch/

- **Membership of the JSPG mail list is closed, BUT**
  - Requests to join stating reasons to D Kelsey
  - Volunteers to work with us are always welcome!
- **Policy documents at**

http://cern.ch/proj-lcg-security/documents.html

Grid AUP (1)

By registering with the Virtual Organization (the "VO") as a GRID user you shall be deemed to accept these conditions of use:

1. ***You shall only use the GRID to perform work, or transmit or store data consistent with the stated goals and policies of the VO of which you are a member and in compliance with these conditions of use.***
2. ***You shall not use the GRID for any unlawful purpose and not (attempt to) breach or circumvent any GRID administrative or security controls. You shall respect copyright and confidentiality agreements and protect your GRID credentials (e.g. private keys, passwords), sensitive data and files.***
3. ***You shall immediately report any known or suspected security breach or misuse of the GRID or GRID credentials to the incident reporting locations specified by the VO and to the relevant credential issuing authorities.***

Grid AUP (2)

4. *Use of the GRID is at your own risk. There is no guarantee that the GRID will be available at any time or that it will suit any purpose.*
5. *Logged information, including information provided by you for registration purposes, shall be used for administrative, operational, accounting, monitoring and security purposes only. This information may be disclosed to other organizations anywhere in the world for these purposes. Although efforts are made to maintain confidentiality, no guarantees are given.*
6. *The Resource Providers, the VOs and the GRID operators are entitled to regulate and terminate access for administrative, operational and security purposes and you shall immediately comply with their instructions.*
7. *You are liable for the consequences of any violation by you of these conditions of use.*

Example VO AUP

This acceptable Use Policy applies to all members of <The VO> Virtual Organization, hereafter referred to as the VO, with reference to use of the LCG/EGEE Grid infrastructure, hereafter referred to as the Grid. The Geant4-Spokesman, <name> owns and gives authority to this policy. The goal of the VO is to validate the software they provide to their users (HEP experiments as ATLAS, CMS, LHCb, Babar, etc, Astrophysics applications, biomedical communities) twice per year within the Grid environment. This procedure should cover a wide range of parameters and physical models which are high CPU demanding. At the same time they are planning to use regularly the LCG/EGEE resources to make analysis and studies of their toolkit. Members and Managers of the VO agree to be bound by the Grid Acceptable Use Policy, VO Security Policy and other relevant Grid Policies, and to use the Grid only in the furtherance of the stated of the VO.

Site Operational Procedures Policy

- **DRAFT (under discussion)**

By registering with the Infrastructure as a Site, you and your organization will be deemed to have accepted these operational procedures and policies, complementary to any agreements that may be in place between the Site and any specific Virtual Organization (VO) or any specific Project, and subject to applicable legislation:

- 1. *You shall provide and maintain accurate contact information as specified in the Site Registration Policy, including but not limited to at least one Administrative Contact (Site Manager) and one Site Security Contact, in a central repository provided by the Project. Both shall respond to enquiries in a timely fashion, but at least within 3 business days;*
- *2. You shall read and abide by the security policies, as published by the Joint Security Policy Group (JSPG) and approved by the Project. You shall periodically self-assess your compliance with these policies, inform the Security Officer of violations encountered in the assessment, and correct such violations forthwith. The Security Officer shall apply appropriate restrictions to the circulation of disclosed information consistent with enforcement and improvement of operational and security policies and procedures.*
- 3. *Before publishing resource information in resource information systems designated by the Project, you shall ascertain that such resource information is valid and correct to the extent this can be realistically validated. You shall not intentionally publish resource information to resource information systems that is detrimental to the operation of the Infrastructure, or mislead users or their agents into submitting workload, data or information to your Site;*

Site Policy (2)

- *4. By accepting workload, data or information from a specific User or VO, you agree to comply with the User or VO requirements as expressed in their respective Acceptable Use Policies, including those relating to accounting and audit data;*
- 5. *You shall implement all relevant patches for security vulnerabilities and for flaws that may impair operation of the Infrastructure, for all pieces of software installed at your Site, and – to the extent possible – on other systems that affect the integrity of your Site;*
- 6. *Logged information, including information provided to you by Users or by the Project, shall be used for administrative, operational, accounting, monitoring and security purposes only. You should exert due diligence in maintaining the confidentiality of this information;*
- 7. *Provisioning of resources to the Infrastructure is at your own risk. Software is provided by the Project only as-is, and subject to its own license conditions, and there is no guarantee that any procedure used by the Project is either correct or sufficient for any particular purpose;*

Site Policy (3)

- *8. Your Site shall support at least one VO, designated by the Project, for the sole purpose of evaluating the availability of Grid Services at your Site, subject to the provisions made in Article 9. The Project provides to the Site the Acceptable Use Policy and the Security Plan of said VO;*
- *9. You have the right to regulate and terminate access to Users and VOs at any time for administrative, operational and security purposes. In the case of the Project VO described in Article 8 above, support for the VO must be restored as soon as reasonably possibly. You shall inform the affected Users or VO(s) and comply with the Grid Incident Handling policy regarding the notification of security incidents;*
- 10. *The Project, the Infrastructure management, and their delegates have the right to block your access to the Infrastructure, and to remove or block your resource information from resource information systems, in the case that you consistently fail to comply with this Policy or any of its subordinate Policies (managerial removal), and at any time in case of urgent operational reasons (operational removal). After managerial removal, the mention of your site in both resource information directories as well as in any other publications may be withdrawn. The Project reserves the right to announce, within the Project, any policy violations by your Site, if you fail to respond to and correct such violations in a timely fashion. The Project will facilitate communications between Sites, VOs, Software providers, and Users, in order to enable your Site's compliance with this Policy;*
- This policy shall be signed by an Authorized Signatory of your Organization.