Joint Security Policy Group

Grid Security Policy

Date:	**11 December 2006**
Version:	**5.4**
Identifier:	**https://edms.cern.ch/document/428008/4**
Status:	**Draft**
Author:	**David Kelsey**

Document Log

Issue	Date	Author	Comment
1.0	19 Aug 2003	Trevor Daniels	Draft for meeting of LCG Security Group on 28 Aug 2003
2.0	1 Sep 2003	Trevor Daniels	Incorporates comments from meeting above; targeted for the GDB on 8 Sep 2003
3.0	3 Sep 2003	Trevor Daniels	Incorporates more comments from LCG Security Group mailing list. Sent to the GDB for Sept meeting.
4.0	30 Sep 2003	Trevor Daniels	Incorporates comments from the GDB, and from further consideration by the LCG Security Group. Sent to the GDB for Oct meeting.
4.0c	17 Oct 2003	David Kelsey	Minor changes following discussion at Oct GDB meeting. Approved by GDB. **Production version from this date on**.
5.0	6 March 2006	David Kelsey	New version. Simpler and more general. Draft for discussion at March 2006 JSPG meeting.
5.1	20 June 2006	David Kelsey	Updated after March 2006 JSPG meeting. For discussion at June 2006 JSPG meeting
5.2	25 Sep 2006	David Kelsey	Updated following discussions at the June JSPG meeting and other input
5.3	14 Nov 2006	David Kelsey	For discussion at November 2006 JSPG meeting. Many changes.
5.4	11 Dec 2006	David Kelsey	Include changes agreed in Nov 2006 JSPG meeting.

1 Introduction and Definitions

This document presents the ***Policy*** regulating those activities of Grid participants related to the security of Grid services and resources.

1.1 Definitions

The term ***Grid*** in this document is taken to apply to any project or operational infrastructure which decides to adopt this ***Policy***.

To fulfil its mission, it is necessary for the Grid to protect its ***Resources***. The Grid ***Resources*** are defined as the ***Equipment*** and ***Software*** required to run ***Services*** connected to the Grid, and the ***Data*** held on those services. Included in the definition of ***Equipment*** are processors and associated disks, tapes and other peripherals, storage systems and storage media, networking components and interconnecting media. ***Software*** includes, but is not restricted to, operating systems, supporting utilities, compilers and other general purpose applications, any software required to operate any equipment defined as a Grid Resource, software and middleware released and/or distributed by the Grid and any further software required to support any scientific application associated with the application communities. Included in the definition of ***Data*** are data required to operate any equipment defined as a Grid Resource, data required to operate any Grid Service, data intended to be processed or produced by any software defined as a Grid Resource, and any application data.

The various boards, committees, groups and individuals mandated to oversee and control the Grid are collectively defined to be the ***Grid Management***.

A ***Virtual Organisation (or VO)*** is a grouping of individuals, often not bound to a single institution, who, by reason of their common membership and in sharing a common goal, are granted rights to use a set of Resources on the Grid. The various individuals and groups mandated to oversee and control the VO are collectively defined to be the ***VO Management***. Included in the definition of a VO are cases where Grid Resources are offered to individual Users who are not members of a formal VO. These Users are, however, usually associated with an ***Application Community***, and these communities are treated in this document as though they are a VO.

A ***Site*** is an entity having administrative control of Resources provided to the Grid. This may be at one physical location or spread across multiple physical locations. The various individuals and groups mandated to oversee and control the Grid Site are collectively defined to be the ***Site Management***.

1.2 Objectives

This ***Policy*** gives authority for actions which may be carried out by certain individuals and bodies and places responsibilities on all Grid participants.

1.3 Scope

This ***Policy*** applies to all Grid participants.

Every Site participating in the Grid autonomously owns and follows their own local security policies with respect to the system administration and networking of all the resources they own, including resources which are part of the Grid. This ***Policy*** augments local policies by setting out additional Grid-specific requirements.

The ***Policy*** requires Procedures, Rules, Guides and other detailed technical requirements to exist to ensure the ***Policy*** is properly implemented and followed. These documents are referenced in Appendix

1 and carry the same force as if they were part of this ***Policy***. In this document, the word ***Policy*** should always be interpreted as including these additional documents.

1.4 Ownership and Maintenance

This ***Policy*** is prepared and maintained by the Joint Security Policy Group, approved by Grid Management and thereby endorsed by the Grid as a whole.

This ***Policy*** will be revised as required by the Joint Security Policy Group and/or Grid Management and resubmitted for formal approval and adoption whenever significant changes are needed.

The most recently approved version is available at https://edms.cern.ch/document/428008

2 Roles and Responsibilities

This section defines roles and responsibilities.

2.1 Grid Management

The Grid Management provide, through the adoption of this ***Policy*** and through their representations on the various approving bodies of the Grid, the overall authority for the decisions and actions resulting from this ***Policy***.

2.2 Virtual Organisation Management

The responsibilities of the VO Management include:

2.2.1 VO Security Policy

VOs are required to abide by the VO Security Policy (https://edms.cern.ch/document/573348). They must have a VO Acceptable Use Policy and ensure that only individuals who have agreed to abide by the VO AUP are registered as members of the VO.

2.2.2 User Registration

VOs are required to set up and operate a registration procedure consistent with the User Registration Policy (https://edms.cern.ch/document/428034) for approving requests for joining the VO. Approval must be restricted to individuals who are recognised as having legitimate rights to membership and agree to be bound by AUPs. VOs are subsequently required to maintain the accuracy of the information held and published about their members, and to promptly remove membership from individuals who lose their right to membership.

2.2.3 Controlling Access to Resources

Some Grid resources will be restricted to all members of certain VOs or to certain individuals within VOs. VOs will provide access to information as necessary to enable such controls to be implemented and maintained accurately.

2.2.4 Applying Sanctions to Users

VOs are responsible for promptly investigating reports of users failing to comply with the provisions of this ***Policy*** and for taking appropriate action to ensure compliance in the future, as defined in Section 6.

2.3 Site Management

The responsibilities of the Site Management include:

2.3.1 Quality of Services

Sites hosting Grid Resources are required to provide reliable and well managed services and abide by the Site Registration Policy (https://edms.cern.ch/document/503198) and the Site Operational Procedures Policy (https://edms.cern.ch/document/726129). Sites must abide by the Audit Requirements Policy (https://edms.cern.ch/document/428037).

2.3.2 Mitigating Risks

Sites acknowledge that participating in the Grid increases the risk from security incidents, to both Grid and non-Grid hosts on each site. Sites are responsible for mitigating this risk.

2.3.3 Incident Response

Sites accept the duty to cooperate with Grid Security Operations and others in investigating and resolving security incidents, and to take responsible action as necessary to safeguard Grid resources during an incident in accordance with the Incident Response policy (https://edms.cern.ch/document/428035).

2.3.4 Access Control

Access to all Grid resources is controlled by a common grid security infrastructure which includes both authentication and authorization components. The global components of this infrastructure must be deployed by all Grid sites and resources. The deployment of additional local security measures is permitted should the local security policies of the site or resource administration require this.

2.3.5 Notification of Legal Compliance Issues

If exceptions or extensions to this ***Policy*** are required because of local legislation, the Site must inform the Grid Security Officer (see section 5).

2.4 Resource Administrators

In addition to their local site policy Resource Administrators must ensure their implementations of Grid services comply with this ***Policy***.

The responsibilities of Resource Administrators include:

2.4.1 Notifying Site Personnel

Resource Administrators are responsible for ensuring that their Site is registered with the Grid and that all appropriate personnel concerned with security or system management at their Site are notified of and accept the requirements of this ***Policy*** before implementing any Grid services.

2.4.2 Resource Administration

The Resource Administrators are responsible for the installation and maintenance of Resources assigned to them, including ongoing security, and subsequently for the quality of the operational service provided by those Resources.

2.5 Users

All Grid Users must be members of one of the registered VOs or Application Communities.

The responsibilities of Users include the following:

2.5.1 Acceptable Use

Users must accept and agree to abide by the VO and Grid Acceptable Use Policies (https://edms.cern.ch/document/428036) when they register or renew their registration with a VO.

Users must be aware that their work may utilise shared resources and may therefore seriously affect the work of others. They must show responsibility, consideration and respect towards other users in the demands they place on the Grid.

Users must have a suitable authentication credential issued by one of the approved Certification Authorities (https://edms.cern.ch/document/428038). They must ensure that others cannot use their credentials to masquerade as them or usurp their access rights. Users may be held responsible for ***all*** actions using their credentials, whether carried out personally or not. No intentional sharing of credentials for Grid purposes is permitted.

Users must be aware that their jobs will often be running on equipment and using resources owned by others. They must observe any restrictions on access to resources that they encounter and must not attempt to circumvent such restrictions.

Application software written or selected by Users for execution using Grid Resources must be directed exclusively to the legitimate purposes of their VO. Such software must respect the autonomy and privacy of the host sites on whose Resources it may run.

2.6 Grid Security Officer and Grid Security Operations

Grid Management must appoint a Grid Security Officer who leads and/or coordinates the team providing the operational security capability, known as Grid Security Operations.

The Grid Security Officer may, in consultation with Grid Security Operations, Grid Management and other appropriate persons, require actions by Grid participants as are deemed necessary to protect the Grid infrastructure from or contain the spread of Grid security incidents.

The responsibilities of Grid Security Operations include:

- The maintenance of contact details of security personnel at each participating Site and the facilitation of Grid-related communications between them.

- Ensuring that security operational problems are tackled and resolved.

- Providing incident response teams who will act according to the agreed policies and procedures (https://edms.cern.ch/document/428035).

3 Physical Security

All the requirements for the physical security of Grid Resources are expected to be adequately covered by each site's local security policies and practices. These should, as a minimum, reduce the risks from intruders, fire, flood, power failure, equipment failure and environmental hazards.

Stronger physical security may be required for equipment used to provide certain critical Grid services such as VO membership services or credential repositories. The technical details of such additional requirements are contained in the Procedures for operating and approving such services.

4 Network Security

All the requirements for the networking security of Grid Resources are expected to be adequately covered by each site's local security policies and practices. These should, as a minimum, reduce the risks from intruders and failures of hardware or software by implementing appropriate firewall protection, by the timely application of all critical security-related software patches and updates, and by maintaining and observing clearly defined incident response procedures.

It is Grid policy to minimise the security risk exposed by applications which need to communicate across the Internet; even so, the peripheral firewall on every participating site will be required to permit the transit of inbound and outbound packets to/from certain port numbers between a number of external and internal hosts in order to run or reach Grid services. These are defined in the Grid Guide for Network Administrators (https://edms.cern.ch/document/452128).

5 Limits to Compliance

Exceptions to compliance with this ***Policy*** include but are not limited to the following:

Wherever possible, Grid policies and procedures will be designed so that they may be applied uniformly across all sites without violating the legislation in force in any participating country. If this is not possible, country-specific exceptions or extensions will be made. Such exceptions or extensions will be described explicitly in a separate document with the reasons for the exception or extension clearly stated.

In exceptional circumstances it may be necessary for Grid participants to take emergency action in response to some unforeseen situation which may violate some aspect of this ***Policy*** for the greater good of pursuing or preserving legitimate Grid objectives. If such a ***Policy*** violation is necessary, the exception should be minimised, documented, time-limited and authorised at the highest level commensurate with taking the emergency action promptly, and the details notified to the Grid Security Officer at the earliest opportunity.

6 Sanctions

Sites or Resource Administrators who fail to comply with this ***Policy*** in respect of a Service they are operating may lose the right to have that service instance recognised by the Grid until compliance has been satisfactorily demonstrated again.

Users who fail to comply with this ***Policy*** may lose their right of access to and/or collaboration with the Grid, and may have their activities reported to their home institute or, if those activities are thought to be illegal, to appropriate law enforcement agencies.

VOs which fail to comply with this ***Policy,*** together with all the Users whose rights with respect to the Grid derives from that VO, may lose their right of access to and/or collaboration with the Grid.

7 Appendix 1

The current list of referenced documents describing Procedures, Rules, Guides and other more detailed documents which are required to implement this ***Policy*** are presented here. These explicitly referenced documents have the same force as the ***Policy*** itself.

Up to date versions may always be found on the JSPG web site at
http://proj-lcg-security.web.cern.ch/proj-lcg-security/documents.html

The documents with their web links are as follows:

Grid Acceptable Use Policy, https://edms.cern.ch/document/428036
LCG/EGEE Virtual Organisation Security Policy, https://edms.cern.ch/document/573348
Site Operational Procedures Policy, https://edms.cern.ch/document/726129
Approval of Certification Authorities, https://edms.cern.ch/document/428038
Audit Requirements for LCG, https://edms.cern.ch/document/428037
LCG/EGEE Incident Handling and Response Guide, https://edms.cern.ch/document/428035
Site Registration Policy and Procedure, https://edms.cern.ch/document/503198
Requirements for LCG User Registration and VO Membership Management,
https://edms.cern.ch/document/428034
Guide to LCG Application, Middleware and Network Security,
https://edms.cern.ch/document/452128