Joint Security Policy Group

Grid Security Policy

Date:	**24 April 2007**
Version:	**5.6**
Identifier:	**https://edms.cern.ch/document/428008/4**
Status:	**Draft**
Author:	**JSPG**

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.
5.5	12 Apr 2007	David Kelsey	Include changes agreed in Mar 2007 JSPG meeting and subsequent discussions
5.6	24 Apr 2007	JSPG	Include suggestions from Ian Neilson and changes agreed at JSPG meeting of 17 April

1 Introduction and Definitions

To fulfil its mission, it is necessary for the *Grid* to protect its *resources*. This document presents the policy regulating those activities of *Grid participants* related to the security of *Grid services* and *Grid resources*.

1.1 Definitions

The word *Grid*, when italicised in this document, means any project or operational infrastructure which uses grid technologies and decides to adopt this policy.

The other italicised words used in this document are defined as follows:

- *Policy* is interpreted to include rules, responsibilities and procedures specified in this document together with all those in other documents which are required to exist by stipulations in this document.

- A *participant* is any entity providing, using, managing, operating, supporting or coordinating one or more *Grid service(s).*

- A *service* is any computing or software system, based on grid technologies, which provides access to or information about or controls *Grid resources*.

- A *resource is* the *equipment* and *software* required to run a *Grid service*, and any *data* held on the *service*.

    - 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.

    - Included in the definition of *software* are operating systems, utilities, compilers and other general purpose applications, any software required to operate any *equipment*, software and middleware released and/or distributed by the *Grid* and any software required to support any application associated with *VOs* or other authorized *users*.

    - Included in the definition of *data* are data required to operate any equipment defined as a *resource*, data required to operate any *service*, data intended to be processed or produced by any software defined as a *resource*, and any application data.

- *Management* is the collection of the various boards, committees, groups and individuals mandated to oversee and control the *Grid*.

- A *user* is an individual who has been given authority to access and use *Grid resources*.

- A *Virtual Organisation (or VO)* is a grouping of *users* and optionally *resources*, often not bound to a single institution, who, by reason of their common membership and in sharing a common goal, are given authority to use a set of *resources*.

    - 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, often associated with an application community, and these communities, or even a single *user*, are treated in this document as though they are a *VO*.

- *VO management* is the collection of various individuals and groups mandated to oversee and control 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.

- *Site management* is the collection of various individuals and groups mandated to oversee and control a *site*.

- A *resource administrator* is the person responsible for installing, operating, maintaining and supporting one or more *resource(s)* at a *site*.

1.2 Objectives

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

1.3 Scope

This *policy* applies to all *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.

1.4 Additional policy documents

Appendix 1 defines additional policy documents which must exist for a proper implementation of this *policy*. These documents are referred to in section 2.

An accompanying document for each *Grid* adopting this *policy* must define the *Grid*-specific locations and version numbers of their approved and adopted additional policy documents.

1.5 Ownership and Maintenance

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

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

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

2 Roles and Responsibilities

This section defines the roles and responsibilities of *participants*.

2.1 Grid Management

The *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* including procedures for the resolution of disputes.

2.2 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, *management* and other appropriate persons, require actions by *participants* as are deemed necessary to protect *resources* 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.
- Handling of operational security problems as they arise.
- Providing incident response teams who will act according to the Grid Security Incident Response Policy [6].
- The maintenance of a list of the *sites* which are currently operating with exceptions or extensions to this *policy* as described in section 5.

2.3 Virtual Organisation Management

The responsibilities of the *VO management* include:

2.3.1 VO Security Policy

VOs are required to abide by the Virtual Organisation Security Policy [2]. They must have a VO Acceptable Use Policy (AUP) and ensure that only individuals who have agreed to abide by the Grid AUP [1] and the *VO* AUP are registered as members of the *VO*.

2.3.2 User Registration

The *user* registration procedure of the *VO* is required to be consistent with the User Registration and VO Membership Management Policy [8] 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 the 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 such membership.

2.3.3 Controlling Access to Resources

Some *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.

2.3.4 VO-specific resources

*VO*s are responsible for ensuring that their *software* does not pose security threats, that access to their databases is secure and is sufficiently monitored, that their stored *data* are compliant with legal requirements, and that VO-specific *services* are properly monitored and do not compromise *sites* or *resources*.

2.3.5 Applying Sanctions to Users

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

2.4 Users

All *users* must be members of one of the registered *VOs* or application communities.

The responsibilities of *users* include:

2.4.1 Acceptable Use

Users must accept and agree to abide by the Grid Acceptable Use Policy [1] and the *VO* AUP when they register or renew their registration with a *VO*.

Users must be aware that their work may utilise shared resources and may therefore 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 as approved by the *Grid*. 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 taken 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 use *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 on *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.

2.5 Site Management

The responsibilities of the *Site management* include:

2.5.1 Site Operations Policy

Sites hosting *resources* are required to provide reliable and well managed *services* and abide by the Grid Site Operations Policy [3]. *Sites* must abide by the Site Registration Policy [7] and the Audit Requirements Policy [5].

2.5.2 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.

2.5.3 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 Grid Security Incident Response Policy [6].

2.5.4 Access Control

Access to all *resources* is controlled by a common grid security infrastructure which includes both authentication and authorization components. The global components of this infrastructure, e.g. as specified in the Approval of Certification Authorities [4], must be deployed by all *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.

2.5.5 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).

2.6 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:

2.6.1 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 offering any *services*.

2.6.2 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*.

3 Physical Security

All the requirements for the physical security of *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 *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 *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* may 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 *services*.

5 Limits to Compliance

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

Wherever possible, *Grid* policies and procedures are designed so that they may be applied uniformly across all *sites* without violating the legal or contractual obligations in force at any participating *site*. If this is not possible, *site*-specific exceptions or extensions may be made. Such exceptions or extensions shall be described explicitly in a separate document submitted to the Grid Security Officer, with the reasons for the exception or extension clearly stated.

In exceptional circumstances it may be necessary for *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, Liability, Disputes and Intellectual Property Rights

Sites or *resource administrators* who fail to comply with this *policy* in respect of a *Grid 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*.

The issues of liability, dispute resolution and intellectual property rights, all of which may be *Grid*-specific, should be addressed in the additional policy documents.

7 Appendix 1: Additional policy documents

The current list of additional policy documents describing procedures, rules and other technical details required to implement this *policy* are presented here.

The current general versions may always be found on the JSPG web site at http://proj-lcg-security.web.cern.ch/proj-lcg-security/documents.html

An accompanying document for each *Grid* adopting this *policy* must define the *Grid*-specific locations and version numbers of their approved and adopted additional policy documents

The additional policy documents with their web links are as follows:

[1] Grid Acceptable Use Policy, https://edms.cern.ch/document/428036

[2] Virtual Organisation Security Policy, https://edms.cern.ch/document/573348

[3] Grid Site Operations Policy, https://edms.cern.ch/document/726129

[4] Approval of Certification Authorities, https://edms.cern.ch/document/428038

[5] Audit Requirements Policy, https://edms.cern.ch/document/428037

[6] Grid Security Incident Response Policy, https://edms.cern.ch/document/428035

[7] Site Registration Policy, https://edms.cern.ch/document/503198

[8] User Registration and VO Membership Management Policy, https://edms.cern.ch/document/428034