EGI-InSPIRE

GRID SECURITY POLICY

Document identifier	EGI-SPG-SecurityPolicy-V1_0
Document Link	https://documents.egi.eu/document/86
Last Modified	**14/07/2010**
Version	**1.0**
Policy Group Acronym	**SPG**
Policy Group Name	**Security Policy Group**
Contact Person	**David Kelsey/STFC, UK**
Document Status	**Submitted**
Approved by	**Body who approved the doc**
Approved Date	**DD/MM/YYYY**

Policy Statement

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

I. COPYRIGHT NOTICE

II. DELIVERY SLIP

	Body	Date
Approved by	EGI.eu Executive Board	DD/MM/YYYY

III. DOCUMENT LOG

Issue	Date	Comment	Author/Organization
1.0	14/07/2010	Imported from JSPG policy document with the same title. The only changes to wording made relate to updating titles of and links to other security policy documents. Also changed references to JSPG to SPG and updated Appendix 1 to contain the full list of documents. See https://edms.cern.ch/document/428008 (V5.7a, dated 10 Oct 2007) for the old JSPG document.	David Kelsey/STFC
2.0			
3.0			
4.0			

IV. 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 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, information about or controls *resources*.
- A *resource* is the *equipment* and *software* required to run a *service* on the *Grid*, 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 *Virtual Organisations* 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 Security Policy Group, approved by *management* and thereby endorsed and adopted by the *Grid* as a whole.

This *policy* will be revised by the 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://documents.egi.eu/document/86

2 ROLES AND RESPONSIBILITIES

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

2.1 Grid Management

The *management* provides, through the adoption of this *policy* and through its 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

The *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 Security Incident Response Policy [6].
- Handling requests for exceptions 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 Policies

VOs are required to abide by the Virtual Organisation Operations Policy [9] and the Virtual Organisation Registration 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 and VO Membership Service

The *user* registration procedure of the *VO* is required to be consistent with the Virtual Organisation Membership Management Policy [8]. Approval to join the *VO* must be restricted to individuals who are recognised as having legitimate rights to membership and who agree to be bound by the AUPs. A VO membership service must be provided with appropriate interfaces to generate authentication, authorization and other identity mapping data for the services running on the *sites*. *VO*s are required to maintain the accuracy of the information held and published about their members, and to promptly remove individuals who lose their right to such membership.

2.3.3 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*.

2.3.4 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 Security Policy [7] and the Grid Security Traceability and Logging 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 *resources* during an incident in accordance with the 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 *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* and *VOs*. If this is not possible, for example due to legal or contractual obligations, exceptions may be made. Such exceptions must be justified in a document submitted to the Grid Security Officer for authorisation and, if required, approval at the appropriate level of management.

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 of the *management* 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 *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 versions may always be found in the EGI document database at
EGI Document Database

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://documents.egi.eu/document/74

[2] Virtual Organisation Registration Security Policy, https://documents.egi.eu/document/78

[3] Grid Site Operations Policy, https://documents.egi.eu/document/75

[4] Approval of Certification Authorities, https://documents.egi.eu/document/83

[5] Grid Security Traceability and Logging Policy, https://documents.egi.eu/document/81

[6] Security Incident Response Policy, https://documents.egi.eu/document/82

[7] Site Registration Security Policy, https://documents.egi.eu/document/76

[8] Virtual Organisation Membership Management Policy,
https://documents.egi.eu/document/79

[9] Virtual Organisation Operations Policy, https://documents.egi.eu/document/77

[10] VO Portal Policy, https://documents.egi.eu/document/80

[11] Policy on Grid Multi User Pilot Jobs, https://documents.egi.eu/document/84

[12] Grid Policy on the Handling of User-Level Job Accounting Data,
https://documents.egi.eu/document/85

[13] Security Policy Glossary of Terms, https://documents.egi.eu/document/71