EGI-InSPIRE

POLICY ON GRID MULTI-USER PILOT JOBS

Document Identifier:	EGI-P.84-SPG-PilotJobs
Document Link:	https://documents.egi.eu/document/84
Date:	**14/07/2010**
Version	**1.0**
Policy Group Acronym	**SPG**
Policy Group Name	**Security Policy Group**
Document Status:	**Submitted**
Contact Person	**David Kelsey/STFC, UK**
Approved By	**Body who approved the doc**
Approved Date	**14/07/2010**

Policy Statement

Security policy for operation of multi-user pilot jobs.

Document Log

Issue	Date	Comment	Author
1.0	14/07/2010	Imported from JSPG policy document with the same title. No changes to wording were made. See https://edms.cern.ch/document/855383 (V1.0, dated 18 Sep 2008) for the old JSPG document.	David Kelsey/STFC
2.0			
3.0			
4.0			

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   Policy on Multi-User Pilot Jobs

A multi-user pilot job, hereafter referred to simply as a pilot job, is a Grid job for which the following holds:

- a Grid job is submitted with a set of credentials belonging to either a member of the VO or to a service owned and operated by the VO

- when this Grid job begins to execute at a Site, it pulls down and executes workload, hereafter called a user job, owned and submitted by a different member of the VO or multiple user jobs owned and submitted by multiple different members of the VO.

The owner of the pilot job is the person submitting the job. In the case where pilot jobs are submitted by a service then the VO must name a person who takes responsibility for that service.

By submitting such a pilot job to the Grid, the VO and the owner of the pilot job agree to the conditions laid down in this document and other referenced documents, which may be revised from time to time.

1. *Before submitting pilot jobs to a Site the VO must have approval from the Grid and from that Site.*

2. *Each pilot job must be the responsibility of one of a limited number of authorised and registered members of the VO. The VO is responsible for implementing a process for authorising pilot job owners and ensuring that they accept the conditions laid down here. The pilot job owner and the VO on behalf of whom the job is submitted are held responsible by the Grid and by the Site for the safe and secure operation of the pilot job and its associated user job(s).*

3. *The pilot job must only execute user jobs belonging to registered and authorised members of the VO.*

4. *The pilot job framework must meet the fine-grained monitoring and control requirements defined in the Grid Security Traceability and Logging policy. The use of gLexec in identity switching-mode is one solution that meets these needs.*

5. *The pilot job must use the approved system utility to map the application and data files to the actual owner of the workload and interface to local Site authorization, audit and accounting services. The owner of the user job is liable for all actions of that user job.*

6. *The pilot job must respect the result of any local authorisation and/or policy decisions, e.g. blocking the running of the user job.*

7. *The pilot job must not attempt to circumvent job accounting or limits placed on system resources by the batch system, for example the execution of more parallel jobs than allowed.*

8. *The pilot job framework must isolate user jobs from one another, including any local data files created during execution and any inter-process communication.*

9. *When fetching a user job and credentials into the worker node, the pilot job must use means at least as secure as the original pilot job submission process.*

10. *The Grid and/or the Sites reserve the right to terminate any pilot jobs and associated user jobs that appear to be operating beyond their authorisation and/or are not in compliance with this policy. Other possible consequences include blacklisting of users or the VO as a whole.*

11. *The VO and/or pilot job owner must produce and keep audit logs, as defined in the Grid Security Traceability and Logging policy, and must assist Grid Security Operations in security incident response.*

12. *The VO must make a description of the architecture, the security model and the source code of their pilot job system available to Grid Security Operations and/or Sites on request.*

This policy shall be signed for agreement by each of the authorised Pilot Job owners, before pilot jobs are submitted.