Joint Security Policy Group

Policy on Grid Multi-User Pilot Jobs

Date:	**1 October 2007**
EDMS Reference:	https://edms.cern.ch/document/855383
Internal Version:	**V0.3**
Status:	**Draft**
Author:	**Joint Security Policy Group**

Document Log			
Issue	**Date**	**Author**	**Comment**
0.1	3 July 2007	FNAL, JSPG, David Kelsey.	First draft produced during JSPG meeting of 26/27 June 2007. Heavily based on similar policy document from FNAL (with many thanks to them)
0.2	2 August 2007	David Kelsey, JSPG	Changes agreed during today's JSPG meeting.
0.3	1 Oct 2007	David Kelsey, JSPG	Include suggestions received during and after the LCG GDB meeting on 31 August.

1 Policy on Multi-User Pilot Jobs

A multi-user pilot job, hereafter referred to simply as a pilot job, is a Grid job owned and submitted by one member of a Virtual Organisation (VO) which during execution at a Site 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.

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. *Pilot jobs are only acceptable from VOs whose trust relationships with the Grid and/or Site include authorisation to use them.*

2. *Pilot jobs must be owned and submitted by one of a limited number of authorised and registered members of the VO. The VO is responsible for implementing a process for authorising pilot jobs owners and ensuring that they accept the conditions laid down here. The pilot job owners are held personally 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. *If a Site allows the switching of user identity within the pilot job to that of the owner of the user job, the pilot job must use the system utility provided by the Grid to map the application and data files to the actual owner of the workload. When user identity is switched, the owner of the user job is liable for all actions of that user job.*

5. *If a Site does not allow switching of the user identity within the pilot job the pilot job must still use the system utility provided by the Grid to allow proper callout to local Site authorization, audit and accounting services. When user identity is not switched, the pilot job owner is liable for all actions of the pilot job and its associated user jobs.*

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.*

8. *If a pilot job executes multiple user jobs, these must be executed serially and not in parallel.*

9. *A pilot job must delete all local data files created during the execution of one user job before the next user job starts.*

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

11. *The Grid reserves the right to terminate any pilot 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.*

12. *The VO and/or pilot job owner must produce and keep audit logs and must assist Grid Security Operations in security incident response.*

13. *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 Jobs owners..