POLICY ON E-INFRASTRUCTURE MULTI-USER PILOT JOBS

Document identifier	EGI-SPG-PilotJobs_V2
Document Link	https://documents.egi.eu/document/2933
Last Modified	11/10/2016
Version	2
Policy Group Acronym	SPG
Policy Group Name	Security policy group
Contact Person	David Kelsey, STFC
Document Type	Security Policy
Document Status	Ready for Approval
Approved by	EGI Foundation Executive Board
Approved Date	14/11/2016

TABLE OF CONTENTS

AUTHORS LIST

	Name	Partner/Activity/Organisation/Function	Date
From	David Kelsey on behalf of EGI SPG	STFC/SPG Chair	14/11/2016

DELIVERY SLIP

	Body	***Date***
Reviewed by:	EGI Foundation Executive Board	14/11/2016
Approved by:	EGI Foundation Executive Board	14/11/2016

DOCUMENT LOG

Issue	***Date***	***Comment***	***Author/Partner***
V1.3	23/10/2016	Full draft	Peter Solagna/EGI Foundation; Alessandro Paolini/EGI Foundation; David Kelsey/STFC
V2	14/11/2016	Review and approval by EGI Foundation Executive Board	

TERMINOLOGY

A complete project glossary is provided at the following page: https://wiki.egi.eu/wiki/Glossary_V3

APPLICATION AREA

This document is a formal EGI policy or procedure applicable to all participants and associate participants, beneficiaries and Joint Research Unit members, as well as its collaborating projects.

POLICY/PROCEDURE AMENDMENT PROCEDURE

Reviews and amendments should be done in accordance with the EGI "Policy Development Process" (https://documents.egi.eu/document/169).

1 POLICY ON MULTI-USER PILOT JOBS

This policy is effective from 14/11/2016 and replaces an earlier version of this document [R1]. This policy is one of a set of documents that together define the Security Policy [R2]. This individual document must be considered in conjunction with all the policy documents in the set.

Additional SPG terms are defined in the Glossary [R3].

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

- An e-Infrastructure 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 e-Infrastructure job begins to execute at a Resource Centre, 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 e-Infrastructure, 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 Resource Centre the VO must have approval from the e-Infrastructure and from that Resource Centre.*
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 e-Infrastructure and by the Resource Centre 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 e-Infrastructure 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 Resource Centre 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 e-Infrastructure and/or the Resource Centres 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 e-Infrastructure Security Traceability and Logging policy, and must assist e-Infrastructure 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 e-Infrastructure Security Operations and/or Resource Centres on request.*

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

2 REFERENCES

R 1	(Old version) Policy on Grid Multi-User Pilot Jobs. https://documents.egi.eu/document/84
R 2	Approved EGI Security Policies. https://wiki.egi.eu/wiki/SPG:Documents
R 3	SPG Security Policy Glossary of Terms. https://documents.egi.eu/document/71