EGI.eu

SERVICE OPERATIONS SECURITY POLICY

Document identifier	EGI-SPG-ServiceOperations-1475-V3
Document Link	https://documents.egi.eu/document/1475
Last Modified	24/05/2013
Version	3
Policy Group Acronym	SPG
Policy Group Name	Security Policy Group
Contact Person	David Kelsey/STFC
Document Type	Policy
Document Status	APPROVED
Approved by	EGI.eu Executive Board
Approved Date	31/05/2013

Policy Statement

This security policy presents the conditions that apply to anyone running a Service on the Infrastructure, or to anyone providing a Service that is part of the Infrastructure. This policy is effective from 1st June 2013 and replaces an earlier version of this document [R1].



I. AUTHORS LIST

	Name	Partner/Activity/ Organisation/Function	Date
From	David Kelsey	STFC	24/05/2013

II. DELIVERY SLIP

	Body	Date
Reviewed by	OMB	12/04/2013
Reviewed by	UCB	06/05/2013
Approved by	EGI.eu Director	23/05/2013
Approved by	EGI.eu Executive Board	30/05/2013

III. DOCUMENT LOG

Version	Date	Comment	Author/Organization
1.0	15/11/2012	New version of this policy to replace document #669. This addresses end of security support for a software component, removes the IPR statement, adds a new requirement to implement a central banning service and addresses the retirement of a service. The new document number is #1475.	David Kelsey/STFC
2.0	12/04/2013	New wording for central emergency user suspension (rather than "banning"). This version was approved by EGI OMB and UCB.	David Kelsey/STFC

3.0	24/05/2013	Minor mods to set start date to 1st June 2013 and various formatting changes. No change to wording of the policy.	David Kelsey/STFC

IV. APPLICATION AREA

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

V. POLICY/PROCEDURE AMENDMENT PROCEDURE

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

VI. ORGANISATION SUMMARY

To support science and innovation, a lasting operational model for e-Infrastructure is needed – both for coordinating the infrastructure and for delivering integrated services that cross national borders. The objective of EGI.eu (a foundation established under Dutch law) is to create and maintain a pan-European Grid Infrastructure in collaboration with National Grid Initiatives (NGIs) in order to guarantee the long-term availability of a generic e-infrastructure for all European research communities and their international collaborators.

In its role of coordinating grid activities between European NGIs, EGI.eu will:

- Operate a secure integrated production grid infrastructure that seamlessly federates resources from providers around Europe
- Coordinate the support of the research communities using the European infrastructure coordinated by EGI.eu
- Work with software providers within Europe and worldwide to provide high-quality innovative software solutions that deliver the capability required by our user communities
- Ensure the development of EGI.eu through the coordination and participation in collaborative research projects that bring innovation to European Distributed Computing Infrastructures (DCIs)

The EGI.eu is supporting 'grids' of high-performance computing (HPC) and high-throughput computing (HTC) resources. EGI.eu 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 will collect user requirements and provide support for the current and emerging user communities. 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 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, 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 Service Operations Security Policy 6
2 References 8

1 SERVICE OPERATIONS SECURITY POLICY

This policy is effective from 1st June 2013 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.

By running a Service on the IT Infrastructure, by providing a Service that is part of the IT Infrastructure, or retaining state that is related to the IT Infrastructure, either provided as an independent Service or hosted in a Resource Centre, you agree to the conditions laid down in this document and other referenced documents, which may be revised from time to time.

1. *You shall provide and maintain accurate contact information to the Infrastructure Organisation and any Resource Centres involved, including but not limited to at least one Security Contact who shall respond to enquiries in a timely fashion.*
2. *You shall comply with all security policies [R2] and procedures [R3] of the Infrastructure Organisation and of any Resource Centres involved in operating your Service.*
3. *You are held responsible by the Infrastructure Organisation and by any Resource Centres involved for the safe and secure operation of the Service. You shall not mislead Users regarding the suitability of a Service for their needs, nor mislead the IT Infrastructure, Infrastructure Organisation, or any Resource Centres involved about your Service. The Service shall not be detrimental to the IT Infrastructure and any Resource Centres involved.*
4. *You should follow IT security best practices that include pro-actively applying software patches, updates or configuration changes related to security. When notified by the Infrastructure Organisation or any Resource Centres involved of software patches, updates or configuration changes required for security or end of security support, you shall respond appropriately within the specified time period.*
5. *You shall collect and retain sufficient auditing information as defined in the Traceability and Logging Policy [R4] and procedures, and must assist the Infrastructure Organisation and any Resource Centres involved in security incident response.*
6. *You shall use logged information, including information provided to you by Users, other Resource Centres, Service operations or by the Infrastructure Organisation, only for administrative, operational, accounting, monitoring and security purposes. You shall apply due diligence in maintaining the confidentiality of logged information.*
7. *Provisioning of Services is at your own risk. Any software provided by the Infrastructure Organisation is provided on an as-is basis only, and subject to its own license conditions. There is no guarantee that any procedure applied by the Infrastructure Organisation is correct or sufficient for any particular purpose. The Infrastructure Organisation and other Resource Centres acting as service hosting providers are not liable for any loss or damage in connection with your participation in the IT Infrastructure.*
8. *You may control access to your Service for administrative, operational and security purposes and shall inform the affected users if you limit or suspend their access. You shall comply with all relevant incident response procedures regarding the notification of security incidents.*
9. *You must implement automated procedures to download the security emergency suspension lists defined centrally by Security Operations and should take appropriate actions based on these lists, to be effective within the specified time period.*
10. *The Infrastructure Organisation and any Resource Centres involved may control your access to the IT Infrastructure or Resource Centres for administrative, operational and security purposes if you fail to comply with these conditions*

.

All terms are defined in the Glossary [R5]. Upon retirement of a service, the obligations specified in clauses 1, 2, 5 and 6 shall not lapse for the retention period specified in the Traceability and Logging Policy [R4].

2 REFERENCES

R 1	(Old version) Service Operations Security Policy. https://documents.egi.eu/document/669
R 2	Approved EGI Security Policies. https://wiki.egi.eu/wiki/SPG:Documents
R 3	EGI Security Procedures. https://wiki.egi.eu/wiki/Operational_Procedures#Security
R 4	Grid Security Traceability and Logging Policy. https://documents.egi.eu/document/81
R 5	EGI Glossary. https://wiki.egi.eu/wiki/Glossary_V1 SPG Security Policy Glossary of Terms. https://documents.egi.eu/document/71