Service Operations Security Policy

Document identifier	EGI-SPG-ServiceOperations-V3.9
Document Link	https://documents.egi.eu/document/3601
Last Modified	05/05/2020
Version	3.9 (Draft of V4)
Policy Group Acronym	SPG
Policy Group Name	Security Policy Group
Contact Person	David Kelsey / STFC
Document Type	Security Policy
Document Status	Draft
Approved by	EGI Foundation Executive Board
Approved Date	dd/mm/yyyy

TABLE OF CONTENTS

COPYRIGHT NOTICE

AUTHORS LIST

	Name	Partner/Activity/Organisation/Function	Date
From	David Kelsey on behalf of EGI SPG	STFC/SPG Chair	05/05/2020

DELIVERY SLIP

	Body	*Date*
Reviewed by:	EGI OMB	May 2019
Reviewed by:	EGI UCB	Aug/Sep 2019
Approved by:	EGI Foundation Executive Board	

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author/Partner*
V1.0	15/11/2012	New version to replace document #669. Document number is #1475.	David Kelsey/STFC
V2.0	12.4.2013	Changes for central emergency user suspension	David Kelsey/STFC
V3.0	24/5/2013	Released version. Document #1475	David Kelsey/STFC
V3.9 (draft V4.0)	April 2019 last modified on 5/5/2020	New version based on AARC2 Policy Development Kit and as developed for EOSC-hub (1st March 2019). New document #3601	David Kelsey/STFC

TERMINOLOGY

A complete project glossary is provided at the following page: https://wiki.egi.eu/wiki/Glossary_V2

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 SERVICE OPERATIONS SECURITY POLICY

This policy is effective from dd/mm/yyyy 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 EGI (the "Infrastructure"), by providing a Service that is part of the Infrastructure, or retaining state that is related to the Infrastructure, you agree to the conditions below.

1. You shall comply with all pertinent Information Security Management (ISM) policies [R2] as approved by the Infrastructure Management.
2. You shall provide and maintain accurate contact information, including at least one Security Contact who shall support Sirtfi [R3] on behalf of the service.
3. You are held responsible for the safe and secure operation of the Service. Any information you provide regarding the suitability and properties of the Service should be accurate and maintained. The Service shall not be detrimental to the Infrastructure nor to any of its Participants.
4. You should follow IT security best practices including pro-actively applying updates or configuration changes related to security. You shall respond appropriately, and within the specified time period, on receipt of security notices from the Infrastructure or any of its participants.
5. You shall document your processing of personal data in a Privacy Notice that is displayed to the User and made available to the Infrastructure.
    a. You shall apply due diligence in maintaining the confidentiality of user credentials and of any data you hold where there is a reasonable expectation of privacy.
    b. You shall collect and retain sufficient auditing information to be able to assist the Infrastructure in security incident response.
    c. You shall use logged information, including personal data, only for administrative, operational, accounting, monitoring and security purposes. You shall apply due diligence in maintaining the confidentiality of logged information.
6. Provisioning of Services is at your own risk. Any software provided by the Infrastructure 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 is correct or sufficient for any particular purpose. The Infrastructure and any other participants acting as service hosting providers are not liable for any loss or damage in connection with your participation in the Infrastructure.
7. You may control access to your Service for administrative, operational and security purposes and shall inform the affected users where appropriate.
8. Your Service's connection to the Infrastructure may be controlled for administrative, operational and security purposes if you fail to comply with these conditions.

Upon retirement of your Service, the obligations specified in clauses 1, 2 and 5 shall not lapse for the retention period agreed with the Infrastructure.

2 REFERENCES

R 1	(Old version) Service Operations Security Policy: https://documents.egi.eu/document/1475
R 2	Approved EGI Security Policies: https://wiki.egi.eu/wiki/SPG:Documents
R 3	The Security Incident Response Trust Framework for Federated Identity (Sirtfi) v1.0: https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf