Community Operations Security Policy

Document identifier	EGI-SPG-Community-Opsec-V1
Document Link	https://documents.egi.eu/document/3233
Last Modified	03/11/2017
Version	1
Policy Group Acronym	SPG
Policy Group Name	Security Policy Group
Contact Person	David Kelsey/STFC
Document Type	Policy
Document Status	Final Draft – awaiting approval
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	STFC/SPG	3/11/2017

DELIVERY SLIP

	Body	*Date*
Reviewed by:	Presented to EGI OMB in July 2017 and November 2017 and approved by EGI OMB (by email) in Nov 2017	27/07/2017 & 2/11/2017
Reviewed by:	EGI UCB and approved in Nov 2017	dd/mm/yyyy
Reviewed by:	EGI Foundation Executive Board	dd/mm/yyyy
Approved by:	EGI Foundation Executive Board	dd/mm/yyyy

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author/Partner*
V0.1	9/06/2017	New security policy replacing old policies "VO Registration Security Policy" and "VO Operations Policy". Worked on during joint EGI SPG/AARC2 NA3 "Community Engagement" meeting in Karlsruhe 8-9 June 2017	David Kelsey /STFC
V0.2	7/07/2017	Updated version coming out of joint EGI SPG/AARC2 NA3 meeting in Amsterdam 5-7 July 2017	David Kelsey /STFC
V0.3	26/07/2017	Online and email edits. Version presented to EGI OMB and widely distributed for comment during Aug and Sep.	David Kelsey /STFC
V0.4	10/10/2017	Agreed at Vidyo Conference of joint EGI SPG/AARC2 NA3. Addresses all feedback received.	David Kelsey /STFC
V0.5	1/11/2017	A few final tweaks before EGI OMB.	David Kelsey /STFC
V1	dd/mm/yyyy	Approved and adopted version	David Kelsey/STFC

TERMINOLOGY

A complete project glossary is provided at the following page: http://www.egi.eu/about/glossary/

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.

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).

This policy is effective from 01/12/2017 and replaces two earlier security policy documents [R1]. This policy is one of a set of documents that together define the Security Policy [R2] and must be considered in conjunction with all the policy documents in the set.

1 INTRODUCTION

The purpose of this policy is to ensure that the Community's use of the Infrastructure is appropriate, and that the Infrastructure and Communities will respond together to accidental or malicious use that is excessive, harmful to others, or not for appropriate purposes.

This policy applies to the Community Manager and other designated Community management personnel. It places requirements on Communities and it governs their relationships with all Infrastructures with which they have a usage agreement. The Community management personnel must ensure awareness and acceptance, by the Community and its Users, of the responsibilities documented in this Policy.

2 DEFINITIONS

A Community is a set of one or more groups of persons (Users), organised with a common purpose, with a Community Management willing to take responsibility for all sub-groups, jointly granted access to one or more Infrastructures. It may serve as an entity which acts as the interface between the individual Users and an Infrastructure. In general, the members of the Community will not need to separately negotiate access with Service Providers or Infrastructures (hereafter jointly called Infrastructures).

Examples of Communities include, but are not limited to: User groups, Virtual Organisations, Research Communities, Research Infrastructures, Virtual Research Communities, Projects, and Communities authorised to use particular portals or gateways, and geographically organised communities.

Other terms are defined in the Glossary [R3].

3 COMMUNITY OPERATIONS SECURITY POLICY

By participating in the Infrastructure, a Community Manager agrees to the conditions laid down in this document and other referenced documents which may be revised from time to time.

1. *The Community must choose a globally unique name that identifies the Community in the Infrastructure. This name shall be based on a URN prefix that is persistently assigned to the Community or a fully-qualified domain name from the global domain name system assigned to the Community, by the relevant naming authority.*
2. *The Community shall provide and maintain, in a repository designated by the Infrastructure, accurate contact information as specified by the Infrastructure. These contacts must include at least two people in a Community management role, and one or more in a security contact role.*
3. *The Community contacts shall be authoritative for management decisions, security actions and operational issues relating to the Community's use of the Infrastructure, and any services operated by or on behalf of the Community that interact with the Infrastructure. They shall respond to enquiries in a timely fashion as defined in the Infrastructure operational procedures, giving priority to security actions.*
4. *The Community must define, and provide to the Infrastructure, a Community Acceptable Use Policy (AUP) as described in the Community Membership Management Policy [R4], and ensure that its Users are aware of and agree to abide by this AUP.*
5. *The Community shall comply with the Infrastructure Security Policy [R2]. The Community shall assess its compliance with this Policy at least once per year, and inform the Infrastructure Security Officer of any violations encountered in the assessment, and correct such violations in a timely manner.*
6. *The Community shall comply with the Infrastructure security incident response policies [R2] and procedures and respond promptly to requests from Infrastructure Security Operations.*
7. *The Community shall ensure that a Community membership Registry is provided in compliance with the Community Membership Management Policy [R4]. It shall release relevant attributes and assertions to the Infrastructure sufficient to make access control decisions. The real name of the member should be released whenever possible.*
8. *The Community shall ensure that any services operated by or on behalf of the Community that interact with the Infrastructure are operated in compliance with the Service Operations Security Policy [R2].*
9. *The Community shall ensure that information provided by the Infrastructure is only used for administrative, operational, accounting, monitoring and security purposes. The Community shall ensure that due diligence is applied in maintaining the confidentiality of such information.*
10. *The Infrastructure and the Resource Centres may control access to their resources for administrative, operational and security purposes.*
11. *The Community shall apply all reasonable diligence to ensure that its use of any software at a Resource Centre complies with applicable license conditions and the Community shall hold the Resource Centre free and harmless from any liability with respect thereto.*

12. *Any software provided by the Infrastructure is provided on an as-is basis only, and may be subject to its own license conditions. Without prejudice to provisions set forth in more specific agreements, there is no guarantee that any service operated by the Infrastructure is suitable for any particular purpose. In particular, they are not to be used for any purpose which creates the possibility of personal injury, material loss, or the design of safety-critical products and clinical decision support, if they fail or malfunction. The Infrastructure, the Resource Centres and other Communities are not liable for any loss or damage in connection with participation of the Community in the Infrastructure.*

4 REFERENCES

R 1	Virtual Organisation Registration Security Policy. https://documents.egi.eu/document/78 Virtual Organisation Operations Policy. https://documents.egi.eu/document/77
R 2	Approved EGI Security Policies. https://wiki.egi.eu/wiki/Policies_and_Procedures
R 3	EGI Glossary. https://wiki.egi.eu/wiki/Glossary SPG Security Policy Glossary of Terms. https://documents.egi.eu/document/71
R 4	Community Membership Management Policy. https://documents.egi.eu/document/3234