EGI Access Platform - Security Policy

Document identifier	EGI-SPG-AccessPlatform-Security-Policy-v5
Document Link	https://documents.egi.eu/document/2734
Last Modified	21/10/2016
Version	v5
Policy Group Acronym	SPG
Policy Group Name	Security Policy Group
Contact Person	David Kelsey / STFC
Document Type	Security Policy
Approved by	EGI Foundation Executive Board
Approved Date	10/10/2016

TABLE OF CONTENTS

COPYRIGHT NOTICE

AUTHORS LIST

	Name	Partner	Date
From	David Groep	Nikhef	11/01/2016

DELIVERY SLIP

	Body	***Date***
Reviewed by:	EGI Operations Management Board (OMB)	31/03/2016
Approved by:	EGI Foundation Executive Board	10/10/2016

DOCUMENT LOG

Issue	***Date***	***Comment***	***Author/Partner***
V1-3	2015	Internal versions	David Groep/Nikhef
v4	11/01/2016	Version from SPG as discussed and modified during 2015	David Groep/Nikhef
	10/10/2016	Review and approval by EGI Foundation Executive Board	
v5	21/10/2016	Updated terminology (Access Platform instead of LToS), fixed metadata	Gergely Sipos/EGI.eu

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 INTRODUCTION

1.1 Scope

This document is applicable to all and only the Participants involved in the provisioning of the 'EGI Access platform', hereafter referred to as the Platform. This policy is one of a set of documents that together define the Security Policy[1].

The goal of the Platform is to offer user-friendly access to e-infrastructure services for members of the long tail of science, i.e. for individual researchers and small research teams who do not belong to any of the established EGI Virtual Organisation communities.

1.2 Vocabulary

This Policy and the associated Implementation Guidelines use the controlled vocabulary of the EGI Glossary[2], the Security Policy Glossary of Terms[3], and Glossary of the Security for Collaborating Infrastructures (SCI) document[4]. The following terms are specific to this Policy and implementation guidelines:

Application	The information provided by an Applicant and recorded by a Registry that describes the personal information, contact details, and research use case, and on which basis a resource allocation is made
Applicant	A natural person that seeks to gain access to the Platform by providing information to the Registry
Registry	The Service that holds information about the Platform Users and/or Applicants (also known as the User Management Portal (UMP) and any supporting systems that hold data about Users or Applicants)
Management	Those individuals or organisational bodies that have control over Resource Centres, Resource Infrastructures, and any associated personnel, and who are capable and authorized to assume risks.
eduGAIN	The service interconnecting Research and/or Education identity federations around the world[5]

The key words "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC 2119.

[1] Approved EGI Security Policies: https://wiki.egi.eu/wiki/SPG:Documents
[2] https://wiki.egi.eu/wiki/Glossary
[3] https://documents.egi.eu/document/71
[4] http://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf
[5] See http://www.edugain.org/

1.3 Aims

This Policy and the Implementation Guidelines aim to enable a low-barrier Service to be offered to a wide range of research users in Europe and their collaborators world-wide, by any Resource Centre organisation that elects to do so. In offering such Platform, the Resource Centre shall not negatively affect the security or change the security risk of any other Resource Centre or any other part of the e-Infrastructure. In particular, security incidents originating in the Platform should not impact the IT Infrastructure in ways that are incompatible with the operational model of other, more tightly controlled, parts of the infrastructure. This document also provides guidelines on the implementation of security procedures and controls to facilitate offering of the Service by Resource Centres and Science Gateways. The Guidelines contain normative information on how to implement the Policy.

2 SECURITY POLICY

Within the scope of this Policy:

1. Any Participant, including the Registry, shall be subject to the Grid Security Policy and any subordinate Policies, insofar as they are not superseded explicitly by this specific Policy.
2. Access granted to Users under this policy shall be limited in time and shall be subject to an approved resource allocation that is not yet exhausted. All access shall be exclusively through Science Gateways based on User information contained in the Registry. The Registry and Science Gateways should implement the material implications of the EGI CSIRT Central Emergency Suspension mechanism[6]
3. The Registry shall determine the origin of all Applicants and Users in a way sufficient to identify their organisational affiliation, and shall record at least one method of communication with the Applicant or User. This contact information shall include an electronic mail address identifiably linked by name to the organisational affiliation. The contact information for Users shall be verified at least every 13 months.
4. Information about Users shall be kept in the Registry for at least 13 months and no more than 18 months after terminating access to the Platform for the User.
5. The Registry shall have a Data Protection and Privacy Policy and practice statement, and must implement appropriate technical and organisational measures to protect the data contained in the Registry.
6. In addition to information sharing permitted by the Security Policy, all information in the Registry may also be made available to the body or bodies reviewing Applications, and pertinent information in the Registry to any Resource Centre and Science Gateway participating in the Platform.
7. The Resource Provider shall configure the Services such that capabilities are limited to those necessary to execute permitted workflows.
8. The Resource Provider shall apply any controls necessary to ensure that the risk posed to other Resource Providers and to the Infrastructure Participants does not change in a significant way as a result of its participation in the Platform.
9. The Management of the Resource Centre and of the Resource Infrastructure Provider shall accept the risk involved with participation in the Platform, and shall have the capability to absorb the consequences of any residual risk with respect to the other Participants.
10. Users shall comply with the Acceptable Use Policy[7], and shall respect any further restrictions placed on permissible use by Resource Centres and Science Gateways.

By adopting this policy, the Platfpr, shall qualify as having security controls sufficient for the operation of Job Management Portals as meant in the VO Portal Policy[8] for members of the long tail of science, when used within the ensemble of Service Providers participating in the Platform.

[6] https://wiki.egi.eu/wiki/EGI_CSIRT:Central_emergency_suspension_project
[7] https://documents.egi.eu/document/2635
[8] https://documents.egi.eu/document/80

3 SECURITY IMPLEMENTATION GUIDELINES

The Implementation Guidelines are intended to give additional substance to the policy, and provide specific recommendations as to how the above policy can be implemented in a practical way. In particular, it emphasises ways to address the mitigation of residual risk, how to register users in a reasonable way, and what capabilities are expected from those participating in the Platform.

3.1 Operational Security Capability

i. The Service Provider shall have demonstrable capability to identify, contain, analyse, and remedy Security Incidents. The Service Provider shall proactively work with the EGI CSIRT[9] by sharing information about suspect activity, and should provide qualified personnel to joint teams that deal with incidents related to the Platform.

ii. The Service Providers, including Science Gateways operators, Resource Centres, and those operating coordinating Services like the User management portal, the VO membership registry, and the AAI components, shall participate in 'security service challenges' to evaluate the readiness of their computer security incident response team (CSIRT) capability.

iii. All suspect activity detected at a Service must be reported immediately to both the EGI CSIRT (abuse@egi.eu) as well as to the Registry administrators and the administrators of known Science Gateways (accessible through long-tail-providers@mailman.egi.eu). The Registry and Science Gateway administrators shall react by suspending access to any Users identified in the suspect activity, and then promptly follow any instruction from the EGI CSIRT. The Service Provider shall also follow all applicable local incident response processes.

iv. The EGI CSIRT centrally maintains a list of entities for which access is to be suspended because of an emergency situation[10]. It is recommended that Resource Centres, Science Gateways, and the Registry materially implement controls that reflect the central emergency suspension list, even if in a manual way and where possible assisted by the EGI-CSIRT, and that the Registry and Registrars prevent registration of suspended people from becoming Platform Users whilst the emergency suspension lasts.

v. Participating Resource Centres, the Registry, and administrators of Science Gateways should be willing and capable to accept the increased incident response load that may result from participating in a low-barrier or open Service offering.

3.2 Application and allocation

vi. For Applicants outside the European EGI scope, additional information about the applicant must be collected before access is granted. Such additional information shall include verified institutional affiliation, out-of-band communication information (such as a telephone number), and the name and contact details of a sponsor (collaborating researchers) within the European EGI scope. The verification of institutional affiliation may be based on the possession of a verified institutional email address, supported by mention of the applicant on an institutional web page (e.g. in a published organisational chart).

[9] https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting

[10] Changes to this list are rare events.

vii. Any application shall include an estimate of the quantity and type of resources needed.

viii. The research use case – elaborated in the Application – shall be reviewed by a designated Registrar. These may be NGI International Liaisons, the EGI.eu User Support team and their designates, people so designated by an EGI.eu Council member, or any Registrar so appointed by relevant Management. The results of such a review, specifically the identity of the Registrar, the time of review, and the outcome, shall be recorded for audit purposes.

ix. The Management of the Platform may specify a quantitative threshold below which applications are only reviewed for correctness of contact details (and European sponsor information where relevant) and the mere reasonable presence of a research use case description.

3.3 Identification and registration

x. An Applicant of the Platform should be identified via authentication through eduGAIN, and may be identified by other appropriate means when such an authentication is not possible.

xi. eduGAIN is a mechanism to provide authentication services for entities in some way affiliated with research, education, scholarship, and educational use in its widest sense across the world. It is based on federating national Research and Education federations, which of which may have different policies and practices related to eligibility, registration, authentication, and attribute release.

xii. Ability to authenticate with eduGAIN should not be taken to mean that the User or Applicant is within the European EGI scope. Through eduGAIN, it will be possible to identify the affiliation of the IdP and (possibly indirectly) the originating national federation.

xiii. When attributes are released by an IdP ("Identity Provider" as conventionally used in a federation context) or federation through eduGAIN, it is reasonable to assume that those attributes are linked to the authenticating entity at time of issuance.

xiv. Any entity inside eduGAIN could of course be compromised at any point in time. Implementers should not expect that the ability to authenticate to eduGAIN is suspended during account compromise, and they should not expect to be informed of compromised identities.

xv. eduGAIN may release only a limited set of attributes for a user. It may be only an identifier that is specific to the combination of user-IdP-SP – where the SP ("Service Provider" in conventional federation context) is the specific Service that receives assertions from the IdP (e.g. the Registry or a 'SP Proxy' operated for the Platform).

xvi. The registry may need to augment eduGAIN provided attributes with Applicant-provided contact information. In such cases, the Applicant-provided contact information shall be reviewed by a Registrar.

xvii. There may be one or more 'catch-all' self-service IdPs that permit authenticating to the Registry and and other services of the Platform (including the Science Gateways). Any contact and affiliation information provided by the User or Applicant shall be verified by a Registrar before access is granted to the Platform.

xviii. User contact information contained in the Registry shall be verified at least once every 13 months, e.g. by sending an electronic email challenge to the User.

xix. It should not be possible for a User to register multiple times with the Registry, and it must not be possible for the same User to re-register with a different identifier within a 1 month period.

xx. The Registry should assign a persistent, unique, and non-transferrable identifier to each User, which may be disclosed to any Participant.

xxi. The Registry or Services co-located with the Registry (such as an 'SP Proxy') may act as a trusted source of User data and attributed for any Science Gateway participating in the Platform. The Science Gateways may treat positive assertions by the Registry as sufficient proof of compliance and offer the Platform to an authenticated User, provided the User is not explicitly suspended.

3.4 Compensatory Controls

To mitigate the risks emanating from the lower effective assurance level and controls on Users, the Service shall implement controls. Although such controls are equally relevant to the other Platforms offered in the Infrastructure, they become more important as containment mechanisms for incidents originating in the Platform, and are therefore made explicit here

xxii. Systems providing the Service shall offer no more capabilities than only those needed to execute the intended workflows.

xxiii. The use of capabilities necessary for executing intended workflows shall be monitored, and such monitoring should include automated alerting in case anomalies are detected.

xxiv. It is recommended that the Platform be provided on resources that are identifiable and logically distinguished from other Service offerings. Specifically, offering the Platform service based on virtualised services and using designated (virtual) local area networks. Alternative compensatory controls include the use of dedicated clusters.

xxv. The Platform may be connected to the Internet with specifically designated IP address space to mitigate the risk of being subject to black holing of network blocks used for other Services.

xxvi. The systems running User-provided workflows shall have no inbound IP network connectivity from outside the network perimeter of the Resource Centre in which they are located; only in case the Service provides for the capability to selectively permit specific protocols (and for the tcp and udp protocol specific port numbers) to pass, in which case those specific inbound protocols (and for tcp and udp specific ports) necessary to perform the workflow may be permitted.

Outbound network access shall be restricted to only necessary ports. In particular, it must not be possible to send unauthenticated email ('smtp'), or use the system as an endpoint for tunnelled traffic (e.g. VPN gateway, TOR exit node). It should not be possible to become a source of untended large traffic streams (e.g. participate in a DoS attack).

xxvii. Any use of the Platform must be traceable to specific Users. To this end, User Workflows must be isolated from each other and from any Workflows executed by non-Platform users. This may be accomplished by different means, including the provision of virtual machines, through 'container' technology, or by Unix account switching at either the ingress point(s) to the Service or on the system(s) executing the Workflow.

3.5 User awareness and permissible use

xxviii. Any Applicant must be made aware of the Acceptable Use Policy[11], and must be required to explicitly accept it before becoming an accepted User.

xxix. The User must be made aware that any information provided to the Registry, the Science Gateways, and the Resource Centres on which the Workflow will be executed, may process any information provided by the User.

xxx. The User must be made aware of the Grid Policy on the Handling of User-Level Job Accounting Data or its successor.

xxxi. Additional restrictions on permissible use may be set by Resource Centres or specific Science Gateways. For example, access may be permitted only for public, non-competitive, or pre-competitive work, or certain work may only be permitted in the context of a specific contract.

Any such restrictions must be made known to the user explicitly, e.g. by publicising such conditions when filing an Application with the Platform, or by explicitly consent when submitting a workflow to a Science Gateway.

xxxii. A Science Gateway shall not knowingly send a Workflow to a Resource Centre where executing the workflow would constitute a violation of permissible use. This clause notwithstanding, both the Science Gateway and the Resource Centre jointly accept responsibility for executing any workflow that may violate the additional terms and conditions of either the Resource Centre or Science Gateway that are above and beyond the standard terms and acceptable use of the Platform.

[11] https://documents.egi.eu/document/2635