EGI Long Tail of Science Scoped Service Security Policy

Version 03 – Draft –

Scope

The EGI Long-Tail-of-Science (LToS) Scoped Service Security Policy is applicable to all Participants involved in the EGI LToS Service.

Vocabulary

This Policy and the associated Implementation Guidelines use the controlled vocabulary of the EGI Glossary[1], the Security Policy Glossary of Terms[2], and Glossary of the Security for Collaborating Infrastructures (SCI) document[3]. 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 human individual that seeks to gain access to the Service by providing information to the Registry
Registry	The Service that hold information about the 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[4]
LToS	Long Tail of Science as meant in the context of the EGI Long Tail of Science Service[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.

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 LToS Services, 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 LToS Service 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

[1] https://wiki.egi.eu/wiki/Glossary
[2] https://documents.egi.eu/document/71
[3] http://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf
[4] See http://www.edugain.org/
[5] https://wiki.egi.eu/wiki/Long-tail_of_science_pilot

Centres and Science Gateways. The Guidelines contain normative information on how to implement the Policy.

LToS Security Policy (Scoped)

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 a reviewed 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 communication method. That 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 LToS Service for the User.
5. The Registry shall have a Data Protected and Privacy Policy and practice statement, and must implement appropriate technical and organisational measures to protect the data contained in the Registry. In addition to information sharing permitted by the Security Policy, information in the Registry may also be shared with any Resource Centre and Science Gateway participating in the LToS Service.
6. The Resource Provider shall configure the Services such that capabilities are limited to those necessary to execute permitted Workflows.
7. The Resource Provider shall apply any controls necessary to ensure that the risk posed to other Resource Providers and to the e-Infrastructure Participants does not change in a significant way as a result of its participation in the LToS Service.
8. The Management of the Resource Centre and of the Resource Infrastructure Provider shall accept the risk involved with participation in the LToS Service, and shall have the capability to absorb the consequences of any residual risk with respect to the other Participants.
9. Users shall comply with the Acceptable Use Policy, and shall respect any further restrictions placed on permissible use by Resource Centres and Science Gateways.

By adopting this policy, the LToS Service shall qualify as having security controls sufficient for the operation of Job Management Portals as meant in the VO Portal Policy[7] for qualified LToS Users, when used within the ensemble of Service Providers participating in the LToS Service.

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

LToS Security Implementation Guidelines

The Implementation Guidelines are intended to give additional substance to the policy, and provide specific hints 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 LToS service.

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 by sharing information about suspect activity, and should provide qualified personnel to joint teams that deal with incidents related to the LToS Service.

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 accept '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 as well as to the Registry administrators and the administrators of known Science Gateways. 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.

iv. The EGI CSIRT centrally maintains a list of entities for which access it to be suspend because of an emergency situation. Changes to this list are rare events, and it is recommended that Resource Centres, Science Gateways, and the Registry materially implement controls that reflect the central emergency suspension list, possibly in a manual way, and that the Registry and Registrars prevent registration of suspended people from becoming LToS Users whilst the emergency suspension lasts.

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

Requests and allocation

vi. For applicant Users 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 an verified institutional email address, supported by mention of the applicant on an institutional web page (e.g. in a published organisational chart).

vii. Any application shall include the quantity and type of resources requested.

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 LToS Service 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.

Identification and registration

x. An Applicant of the LToS Service should be identified via authentication through eduGAIN, and may be identified by other 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. Mere ability to authenticate with eduGAIN should not be construed as to imply that the User or Applicant is European. 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 LToS Service).

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 LToS Services (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 LToS Service.

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 LToS 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 identifier to each User, which may be shared with 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 LToS Service. The Science Gateways may treat positive assertions by the Registry as sufficient proof of compliance and offer the LToS Service to an authenticated User, provided the User is not explicitly suspended.

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 LToS Service, and are therefore made explicit here

xxii. Systems providing the Service shall offer no more (but also no less) capabilities than only those needed to execute the intended Workflows.

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

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

xxv. The LToS Service 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 LToS Services must be traceable to specific Users. To this end, User Workflows must be isolated from each other and from any Workflows executed by non-LToS 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.

User awareness and permissible use

xxviii. Any Applicant must be made aware of the Acceptable Use Policy, 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 LToS 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.

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 an 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 LToS Service, 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 LToS Service.