VO PORTAL POLICY

Document identifier	EGI-SPG-VOPortal-V2
Document Link	https://documents.egi.eu/document/2932
Last Modified	11/10/2016
Version	2
Policy Group Acronym	SPG
Policy Group Name	Security Policy Group
Contact Person	David Kelsey/STFC
Document Type	Security Policy
Document Status	Approved
Approved by	EGI Foundation Executive Board
Approved Date	16/11/2016

TABLE OF CONTENTS

COPYRIGHT NOTICE

AUTHORS LIST

	Name	Partner/Activity/Organisation/Function	Date
From	David Kelsey on behalf of EGI SPG	STFC/SPG Chair	14/11/2016

DELIVERY SLIP

	Body	***Date***
Reviewed by:	EGI Foundation Executive Board	14/11/2016
Approved by:	EGI Foundation Executive Board	16/11/2016

DOCUMENT LOG

Issue	***Date***	***Comment***	***Author/Partner***
V1	11/10/2016	Full draft	Alessandro Paolini / EGI Foundation; David Kelsey / STFC
V2	14/11/2016	Version for EGI Foundation Executive Board approval	

TERMINOLOGY

A complete project glossary is provided at the following page: https://wiki.egi.eu/wiki/Glossary_V3

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 VO PORTAL POLICY

1.1 Preamble

This policy is effective from 14/11/2016 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.

Addition SPG terms are defined in the Glossary [R3].

This Policy applies to all Portals operated by Virtual Organisations that participate in the e-Infrastructure.

1.2 Portal Classes

Portal Classes			
Portal Class	**Executable**	**Parameters**	**Input**
Simple one-click	provided by portal	provided by portal	provided by portal
Parameter	provided by portal	chosen from enumerable and limited set	chosen from repository vetted by the portal
Data processing	provided by portal	chosen from enumerable and limited set	provided by user
Job management	provided by user	provided by user	provided by user

This Policy applies to Portals that belong exclusively to one of the following classifications:

Simple one-click portals

The Web User invokes functionality on the Portal where jobs submitted to the e-Infrastructure use executable code that is provided by the Portal to the e-Infrastructure as part of the job submission process. All parameters and input data are defined exclusively by the Portal and cannot be influenced by the user.

Parameter portals

The Web User invokes functionality on the Portal where jobs submitted to the e-Infrastructure use executable code that is provided by the Portal to the e-Infrastructure as part of the job submission process. The Web User may only provide run-time parameter settings from an enumerable and limitative set, and may select data files from an enumerable repository of data files that are pre-vetted for use by the Portal.

Data processing portals

The Web User invokes functionality on the Portal where jobs submitted to the e-Infrastructure use executable code that is provided by the Portal to the e-Infrastructure as part of the job submission process. The Web User may provide run-time parameter settings from an enumerable and limitative set, and may provide non-validated input data to the executable code, but where the user cannot influence the instructions executed.

Job Management portals

The Web User invokes functionality on the Portal where jobs submitted to the e-Infrastructure use executable code that is provided by the Web User. Whether this code is passed through unmodified by the Portal and is submitted to the e-Infrastructure as-is, or whether this code is inspected and analysed on the Portal does not change the classification of this Portal.

Frameworks that submit jobs to the e-Infrastructure for multiple users based on a late-binding mechanism are subject to the 'security policy for operation of multi-user pilot jobs' and are not covered in this Policy.

Portals that cannot be classified within the framework laid down by this policy should be reviewed independently, in accordance with the spirit and intention of this Policy, after such an evaluation this policy should be amended with this portal class, or they should be classified as a Job Management portal.

Portals whose functionality fits multiple classes must ensure they comply with the conditions that are applicable to the currently selected functionality.

2 GENERAL CONDITIONS

All Portals, operated by or on behalf of a Virtual Organisation, must comply with the Virtual Organisation Operations Policy [R5].

In addition to all other Policies, the following conditions apply to all Portals:

- The Portal, the VO to which the Portal is associated, the Portal manager are all individually and collectively responsible and accountable for all interactions with the e-Infrastructure, unless a credential of a Strongly Identified Web User is used to interact with the e-Infrastructure.
- The Portal must be capable of limiting the job submission rate.
- The Portal must keep audit logs for all interactions with the e-Infrastructure as defined in the Traceability and Logging Policy [R5].
- The Portal manager and operators must assist in security incident investigations by the e-Infrastructure and by any Resource Provider who can justifiably claim to provide or to have provided resources to the Portal.
- Where relevant, private keys associated with (proxy) certificates must not be transferred across a network, not even in encrypted form. Other re-useable password or private key data should not be transferred across a network, but if transferred must be encrypted when sent across a network.

- The Portal must not persistently store passwords or private keys for its end-users that can be used to authenticate to the e-Infrastructure past 1 million seconds. This is aligned with the definition of "short-lived" authentication credentials used on the e-Infrastructure.
- When a Portal Credential is used to store data on the e-Infrastructure as a result of an action by a User, it may only be stored in locations that have been specifically agreed between the Portal and designated Resource Providers and only for as long as the User is associated with the portal. Transient data may be stored in designated scratch areas on the computational resources provided to the running jobs. When an e-Infrastructure User Credential is used, data may be stored in all the e-Infrastructure locations where the e-Infrastructure User has permission to store such data.

3 SPECIFIC CONDITIONS

Depending on the Portal class, the following conditions will specifically apply.

3.1 "Closed Self-Contained Simple One-Click" Portals

By registering a Closed self-contained simple one-click Portal in a Virtual Organisation, you agree to the conditions laid down in this section and documents references therein.

1. The Portal may offer services to all Web Users.
2. The Portal must use a Robot Certificate to interact with the e-Infrastructure.
3. Maximum submission rate must be specifically agreed between Portal and e-Infrastructure
4. The Portal must keep enough information to associate any interactions with the e-Infrastructure with a particular Internet address and (tcp) port used by the requester.

3.2 "Parameter" Portals

By registering a Parameter Portal in a Virtual Organisation, you agree to the conditions laid down in this section and documents references therein.

1. The Portal may offer services to Pseudonymous, Identified or Strongly Identified Web Users.
2. The Portal may either use a Robot Certificate, or use the e-Infrastructure credential for Strongly Identified Web Users.
3. The job submission rate may be limited differently for Pseudonymous, Identified and Strongly Identified Web Users, and the maximum submission rate by the Portal induced by Pseudonymous and Identified Web Users must be specifically agreed between you and the e-Infrastructure.
4. The Portal must keep enough information to associate any interactions with the e-Infrastructure with a particular user. If the user was Identified or Strongly Identified, relevant authentication information must be recorded and archived.

3.3 "Data Processing" Portals

By registering a Data Processing Portal in a Virtual Organisation, or by connecting a Data Processing Portal to the e-Infrastructure, you agree to the conditions laid down in this section and documents references therein.

1. The Portal may offer services to Identified or Strongly Identified Web Users.
2. The Portal may use a Robot Certificate, or use the e-Infrastructure credential for Strongly Identified Web Users.
3. The Portal must keep enough information to associate any interactions with the e-Infrastructure with a particular Web User. Relevant authentication information must be recorded and archived.
4. The system used to authenticate Identified Users must be adequately secured. In particular additional requirements apply:
    1. Web Users must be notified of all registrations, modifications and of removal of their data in the authentication database.
    2. The authentication database must contain enough information to contact the Web User for as long as the user is registered.
    3. Entering authenticating information in the database, including resets of such information, must be appropriately authenticated.

3.4 "Job Management" Portals

By connecting a Job Management Portal to the e-Infrastructure, you agree to the conditions laid down in this section and documents references therein.

1. The Portal may offer services only to Strongly Identified Web Users.
2. The Portal must use e-Infrastructure User credentials specific to the Web User and use these for all interactions with the e-Infrastructure.
3. The Portal operations must comply with the Service Operations Security Policy [R6].

4 REFERENCES

R 1	(Old version) VO Portal Policy. https://documents.egi.eu/document/80
R 2	Approved EGI Security Policies. https://wiki.egi.eu/wiki/SPG:Documents
R 3	SPG Security Policy Glossary of Terms. https://documents.egi.eu/document/71
R 4	VO Operations Policy. https://documents.egi.eu/document/77
R 5	Traceability and Logging Policy. https://documents.egi.eu/document/81
R 6	Service Operations Security Policy. https://documents.egi.eu/document/1475