EGI Foundation

Configuration Database (GOCDB)

OPERATIONAL LEVEL AGREEMENT

Service Provider	EGI Foundation
Component Provider	**UKRI**
Start Date	1st April 2021
End Date	30th September 2023
Status	Draft
Agreement Date	19th May 2021
Agreement Link	https://documents.egi.eu/document/3756

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
0.1		First draft	Alessandro Paolini, Matthew Viljoen
1.0		final version	Alessandro Paolini, Matthew Viljoen, Greg Corbett

TERMINOLOGY

The EGI glossary of terms is available at: http://go.egi.eu/glossary

For the purpose of this Agreement, the following terms and definitions apply. 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.

Contents

1 The Services 4

2 Service hours and exceptions 5

3 Support 5

3.1 Incident handling 6

3.2 Service requests 6

4 Service level targets 6

5 Limitations and constraints 6

6 Communication, reporting and escalation 7

6.1 General communication 7

6.2 Regular reporting 7

6.3 Violations 7

6.4 Escalation and complaints 7

7 Information security and data protection 8

8 Responsibilities 9

8.1 Of the Component Provider 9

8.1.1 Software compliance 9

8.1.2 IT Service Management compliance 10

8.2 Of the Service Provider 10

9 Review, extensions and termination 10

The present Operational Level Agreement ("the Agreement') is made between EGI Foundation **(the Service Provider)** and UKRI **(the Component Provider)** to define the provision and support of the provided services as described hereafter. Representatives and contact information are defined in Section 6.

This Agreement is valid from **1st April 2021** to **30th September 2023**.

The Agreement was discussed and approved by the Service Provider and the Component Provider **19th May 2021.**

The Component Provider is bound by the terms and conditions of the EGI Default Operational Level Agreement[1] supplemented by the terms and conditions of this specific agreement:

1 The Services

The Services are defined by the following properties:

Technical	• GOCDB is a central service registry and topology database to record information about an e-Infrastructure. This includes entities such as Operations Centres, Resource Centres, service endpoints and their downtimes, contact information and roles of users responsible for operations at different levels. The service enforces a number of business rules and defines different grouping mechanisms and object-tagging for the purposes of fine-grained resource filtering.[2]
IT Service Management	• All staff involved in the delivery of the service will have achieved (or be seeking to achieve) the Foundation level FitSM certification (or equivalent). The service owner will have achieved (or be seeking to achieve) both the Advanced level FitSM certifications (or equivalent). • The Service team interacts with EOSC's Service Management System, providing the required information to the following processes: Service Portfolio Management, Service Level Management, Service Reporting Management, Service Availability and Continuity Management, Information Security Management, Change Management. • The Service team will work with other service teams across the Scientific Computing Department to consolidate the service management system within UKRI.
Coordination	• Over the course of EOSC-Future, the service will integrate the web portal and API with the EOSC AAI service for authentication.

[1] https://documents.egi.eu/document/2752

[2] The technology behind the services may change if new technical requirements emerge.

	• The coordination of the system operation and upgrade activities with those partners that are in charge of operating other systems that depend on it. • This activity will coordinate with the EOSC-Future project for the policy, operational and user requirements
Operation	• Daily running of the system and user support (See Section 3.). • The current equipment costs includes a virtual machine (VM) hosted in the STFC Cloud with production monitoring, power and basic systems administration. The GOCDB databases are hosted by the STFC DB-Services group on production infrastructure. This includes nightly DB back-ups to the STFC tape storage facility and UPS support. • Over the course of EOSC-Future, the system will be reconfigured into a high availability configuration. • Over the course of EOSC-Future, a test infrastructure will be set upto verify interoperability and the impact of software upgrades on depending systems • Implementing all the measures for mitigating the risks listed in the Availability and Continuity Plan for GOCDB[3]
Maintenance	• Bug fixing, proactive maintenance, improvement of the system and its documentation. • Coordination of software maintenance activities with other technology providers that provide software for the EOSC Infrastructure or remote systems deployed by integrated and peer infrastructures that interoperate with the central EOSC components of the system.

2 Service hours and exceptions

As defined in the EGI Default Operational Level Agreement.

3 Support

As defined in the EGI Default Operational Level Agreement.

Support is provided via EOSC Helpdesk Service[4] Support Unit: EOSC CMDB(GOCDB) (to be created)

[3] a specific AvCo plan will be created for the EOSC instance of the service

[4] https://helpdesk.eosc-portal.eu/

Support is available between:

- Monday and Friday
- 9:00 and 17:00 GMT/BST time

This excludes public holidays and other days when the host organisation(s) providing the service are closed. During these times, support will be provided on a Best effort basis. For that period of time AT RISK downtime will be declared in the Configuration database GOCDB.

3.1 Incident handling

As defined in the EGI Default Operational Level Agreement.

3.2 Service requests

As defined in the EGI Default Operational Level Agreement.

4 Service level targets

Monthly Availability

- Defined as the ability of a service or service component to fulfil its intended function at a specific time or over a calendar month.
- Minimum (as a percentage per month): 99%

Monthly Reliability

- Defined as the ability of a service or service component to fulfil its intended function at a specific time or over a calendar month, excluding scheduled maintenance periods.
- Minimum (as a percentage per month): 99%

Quality of Support level

- Medium (As defined in Corporate-level EGI Operational Level Agreement, chapter 2.1)

5 Limitations and constraints

As defined in the EGI Default Operational Level Agreement.

6 Communication, reporting and escalation

6.1 General communication

The following contacts will be generally used for communications related to the service in the scope of this Agreement.

Service Provider contact	Matthew Viljoen operations@egi.eu
Component Provider contact	Generic: gocdb-admins@mailman.egi.eu - Greg Corbett, GOCDB Team lead and Service Owner: greg.corbett@stfc.ac.uk Ian Collier: ian.collier@stfc.ac.uk
Service Support contact	See Section 3

6.2 Regular reporting

Reporting will be done according to the EOSC-Future project.

6.3 Violations

The Component Provider commits to inform the Service Provider, if this Agreement is violated or violation is anticipated. The following rules are agreed for communication in the event of violation:

- In case of any violations of the Services targets, the Component Provider will provide justifications and a plan for Services enhancement to the Service Provider. The Component Provider will produce a status report and a Service enhancement plan for the improvement of the Services within one month from the date of the first notification.
- The Service Provider will notify the supporting Resource Centres in case of suspected violation via the EOSC Helpdesk Service. The case will be analysed to identify the cause and verify the violation.

6.4 Escalation and complaints

For escalation and complaints, the component Provider contact point shall be used, and the following rules apply.

- In case of repeated violations of the Services targets for two consecutive months or four months over a period of 12 months, a review of the Agreement and of the Services enhancement plan will take place involving the parties of the Agreement.
- Complaints or concerns about the Services provided should be directed to the Component Provider contact who will promptly address these concerns. Should the Service Provider still feel dissatisfied, about either the result of the response or the behaviour of the Provider, EGI.eu Director director@egi.eu should be informed.

7 Information security and data protection

As defined in the EGI Default Operational Level Agreement.

The following rules for Information Security and data protection should be enforced by the Component Provider:

- The Component Provider must make every effort to maximise security level of users' data and minimise possible harm in the event of an incident. Incidents must be immediately reported to the EGI CSIRT according to the SEC01 procedure[5].
- EGI Foundation holds the role of the Data Controller while the Component Provider holds the role of Data Processor. Data Processing Agreements[6] covering the provided services must be signed between EGI Foundation (the Data Controller) and Component Provider (the Data Processor).
- The Component Provider must comply with the EGI Policy on the Processing of Personal Data[7] and provide a Privacy Policy. This Privacy Policy must be prepared together with EGI Foundation and must be based on the Privacy Policy template provided by the AARC Policy Development Kit (PDK)[8].
- The Component Provider must enforce the EGI WISE Acceptable Usage Policy[9].
- The Component Provider shall comply with all principles set out by the GÉANT Data Protection Code of Conduct[10] version 1.0.
- The Component Provider must meet all requirements of any relevant EGI policies or procedures[11] and also must be compliant with the relevant national legislation. Regarding EGI requirements, please refer to the following reference documentation:
    - EGI-doc-3015: e-Infrastructure Security Policy

[5] https://wiki.egi.eu/wiki/SEC01
[6] https://documents.egi.eu/document/3755
[7] https://documents.egi.eu/public/ShowDocument?docid=2732
[8] https://aarc-project.eu/policies/policy-development-kit/
[9] https://documents.egi.eu/public/ShowDocument?docid=3600
[10] https://wiki.refeds.org/display/CODE/Code+of+Conduct+for+Service+Providers
[11] https://www.egi.eu/about/policy/policies_procedures.html

- EGI-doc-3601: Service Operations Security Policy
- EGI-doc-2732: Policy on the Processing of Personal Data
- EGI-doc-3600: Acceptable Use Policy and Conditions of Use
- EGI-doc-2934: Security Traceability and Logging Policy
- EGI-doc-2935: Security Incident Response Policy
- SEC01: EGI CSIRT Security Incident Handling Procedure - EGIWiki

8 Responsibilities

8.1 Of the Component Provider

Additional responsibilities of the Component Provider are as follow:

- Adhere to all applicable operational and security policies and procedures[12] and to other policy documents referenced therein;
- Use communication channel defined in the agreement;
- Attend relevant operations meeting when needed;
- Accept EOSC monitoring services provided to measure fulfilment of agreed service level targets.
- Service with associated roles are registered in GOC DB[13] as site entity with the "EOSCCore" scope tag.
- Changes in the system must be rolled into production in a controlled way in order to avoid service disruption.

8.1.1 Software compliance

Unless explicitly agreed, software being used and developed to provide the service should:

- Be licensed under an open source and permissive license (like MIT, BSD, Apache 2.0,...).
- The license should provide unlimited access rights to the EGI community.
- Have source code publicly available via a public source code repository (if needed a mirror can be put in place under the EGI organisation in GitHub[14].) All releases should be appropriately tagged.
- Adopt best practices:
  - Defining and enforcing code style guidelines.
  - Using Semantic Versioning.
  - Taking security aspects into consideration through at every point in time.
  - Having automated testing in place.

[12] https://www.egi.eu/about/policy/policies_procedures.html

[13] https://gocdb.eosc-portal.eu/

[14] https://github.com/EGI-Federation

- Using code review.
- Treating documentation as code.
- Documentation should be available for Developers, administrators and end users.

8.1.2 IT Service Management compliance

- Services should make use of Configuration Management frameworks such as Ansible
- All staff involved in service delivery will have (or be seeking to achieve) foundation or basic level ITSM training and certification
  - ITSM training and certification could include FitSM, ITIL, ISO 20000 etc.
- Service owners will have (or be seeking to achieve) advanced/professional training and certification covering the key processes for their services
- Component Providers should have clear interfaces with the EOSC SMS processes and provide the required information
- Component Providers should commit to the continuing improvement of their management system used to support the services they provide

8.2 Of the Service Provider

The responsibilities of the Service Provider are:

- Raise any issues deemed necessary to the attention of the Component Provider;
- Collect requirements from the Resource infrastructure Providers;
- Support coordination with other EOSC services
- Provide monitoring to measure fulfilment of agreed service level targets.
- Provide clear interfaces to the EOSC SMS processes.

9 Review, extensions and termination

There will be reviews of the service performance against service level targets and of this Agreement at planned intervals with the Customer according to the following rules:

- Technical content of the agreement and targets will be reviewed on a yearly basis.
- EGI Foundation shall be entitled to conduct audits or mandate external auditors to conduct audits of suppliers and federation members. These will aim at evaluating the effective provision of the agreed service or service component and execution of activities related to providing and managing the service prior to the commencement of this agreement and then on a regular basis. EGI Foundation will announce audits at least one month in advance. The provider / federation member shall support EGI Foundation and all auditors acting on behalf of EGI Foundation to the best of their ability in carrying out the audits. The provider / federation member is obliged to provide the auditors, upon request, with the information and evidence necessary. Efforts connected to supporting these audits by the provider / federation member will not be reimbursed.