EGI Foundation

Configuration Database (GOCDB)

OPERATIONAL LEVEL AGREEMENT

Service Provider	EGI Foundation
Service Supplier	**UKRI**
Start Date	1st January 2021
End Date	30th June 2023
Status	FINAL
Agreement Date	11th December 2020
Agreement Link	https://documents.egi.eu/document/3672

This work by EGI Foundation is licensed under a
Creative Commons Attribution 4.0 International License

This template is based on work, which was released under a Creative Commons 4.0 Attribution License (CC BY 4.0). It is part of the FitSM Standard family for lightweight IT service management, freely available at www.fitsm.eu.

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
FINAL	23/03/2016	Final version	Małgorzata Krakowian
2.0	17/11/2017, 04/07/2018	New OLA covering the 2018, 2019, 2020 years	Alessandro Paolini
2.1	11/10/2019	yearly review; introduced the Service Provider and the Component Provider roles; updated Contacts and Violations, Escalation, and Complaints sections; STFC is now UKRI.	Alessandro Paolini
3.0	04/12/2020, 11/12/2020	Covering EGI ACE from Jan 2021 to June 2023; renamed EGI Corporate Level as EGI Default OLA; updated the support unit name;updated section 1; updated section 7 on security requirements; changed frequency of the reports; added Software and ITSM compliance in section 8; added in section 9 the requirement about periodic supplier process audits conducted by EGI Foundation	Alessandro Paolini, Greg Corbett
3.1	08/03/2022	yearly review; introduced the term Service Supplier; updated section 7 and section 8;	Alessandro Paolini

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

Contents

The present Operational Level Agreement ("the Agreement') is made between EGI Foundation **(the Service Provider)** and UKRI **(the Service Supplier)** 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 January 2021** to **30th June 2023**.

The Agreement was discussed and approved by the Service Provider and the Service Supplier **11th December 2020**

The Service Supplier 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.
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 EGI'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	• The service must integrate with EGI Check-in service for authentication. Over the course of EGI-ACE, the existing integration will be extended to include access to the API.

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

	• The coordination of the system operation and upgrade activities with those partners that are in charge of operating other systems that depend on it. • Gathering information on changing and developing requirements.
Operation	• Daily running of the system and user support (See Section 3.). • Provisioning of a high availability configuration: the equipment costs include a number of virtual machines (VMs) in a highly available setup and hosted in the STFC's production VM infrastructures, a failover VM at Daresbury Labs, power and basic systems administration. Each server requires production monitoring. 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. • A test infrastructure (gocdb-preprod.egi.eu) to 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[2]
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 EGI Core Infrastructure or remote systems deployed by integrated and peer infrastructures that interoperate with the central EGI components of the system.

2 Service hours and exceptions

As defined by the EGI Default Operational Level Agreement.

3 Support

As defined by the EGI Default Operational Level Agreement.

Support is provided via EGI Service Desk[3] Support Unit: Configuration and Topology Database (GOCDB)

Support is available between:

[2] https://wiki.egi.eu/wiki/Services_Availability_Continuity_Plans

[3] http://helpdesk.egi.eu/

- 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 by the EGI Default Operational Level Agreement.

3.2 Service requests

As defined by 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 by 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	Alessandro Paolini operations@egi.eu
Service Supplier contact	General: 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

As part of the fulfilment of this Agreement and provisioning of the service, the following reports will be provided:

Report title	Contents	Frequency	Produced by	Delivery
Service Performance Report	The document provides the overall assessment of service performance (per month) and OLA target performance achieved during reporting period	10 months (first report covering the period Jan – Oct 2021)	Service Supplier	Survey form prepared by EGI Foundation

6.3 Violations

The Service Supplier 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 Service Supplier will provide justifications and a plan for Services enhancement to the Service Provider. The Service Supplier 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 EGI Service Desk. 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 Service Supplier 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 when they are applicable:

- The Service Supplier agrees to make every effort to maximise security level of users' data and minimise possible harm in the event of an incident. Security Incidents affecting the services described in Section 1 must be immediately reported to the EGI Foundation using ism@mailman.egi.eu and will have to be reported to EGI CSIRT using abuse@egi.eu within 4 hours after their discovery and handled according to the SEC01[4] procedure
- EGI Foundation holds the role of the Data Controller while the Service Supplier holds the role of Data Processor. Data Processing Agreements must be signed between EGI Foundation (the Data Controller) and Service Supplier (the Data Processor).
- The Service Supplier must comply with the EGI Policy on the Processing of Personal Data[5] and provide a Privacy Notice. This privacy Notice must be agreed with EGI Foundation and must be based on the Privacy Policy template provided by the AARC Policy Development Kit (PDK)[6].
- The Service Supplier must enforce the EGI WISE Acceptable Usage Policies[7].
- The Service Supplier shall comply with all principles set out by the GÉANT Data Protection Code of Conduct[8] in its most current version, which will be made available to the Component Provider by EGI Foundation upon request.

[4] https://go.egi.eu/sec01
[5] https://documents.egi.eu/public/ShowDocument?docid=2732
[6] https://aarc-project.eu/policies/policy-development-kit/
[7] https://documents.egi.eu/public/ShowDocument?docid=3600
[8] https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home

- The Service Supplier must meet all requirements of any relevant EGI policies or procedures[9] 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
    - 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
    - EGI-doc-710: Security Incident Handling Procedure

8 Responsibilities

8.1 Of the Service Supplier

Additional responsibilities of the Service Supplier are as follow:

- Using communication channel defined in the agreement.
- Attending OMB[10] and other operations meeting when needed.
- Accepting EGI monitoring services provided to measure fulfilment of agreed service level targets.
- The Services with associated roles are registered in GOC DB[11] as site entity under EGI.eu Operations Centre hosting EGI central operations tools[12]
- Changes in the system must be rolled into production in a controlled way in order to avoid service disruption.
- An effective way to manage and control configuration items and changes such that they can meet the CHM requirements coming from EGI as a customer including making risk assessments and considering high risk changes.

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 licence (e.g., MIT, BSD, Apache 2.0, ...).
- Unless otherwise agreed, be licensed to provide unlimited access and exploitation rights to the EGI Federation.

[9] https://www.egi.eu/about/policy/policies_procedures.html
[10] https://wiki.egi.eu/wiki/OMB
[11] http://goc.egi.eu/
[12] https://goc.egi.eu/portal/index.php?Page_Type=NGI&id=4

- 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[13].) All releases should be appropriately tagged.
- Adopt best practices:
    - Defining and enforcing code style guidelines.
    - Using Semantic Versioning.
    - Taking security aspects into consideration at every point in time.
    - Having automated testing in place.
    - 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 standards and best practices such as FitSM, ITIL, ISO 20000 etc.
- Service owners will have (or be seeking to achieve) advanced/professional training and certification covering the key service management processes for their services.
- Service Supplier should have clear interfaces with the EGI SMS processes and provide the required information.
- Service Supplier 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:

- Support the ITSM of the Service via procedures and policies of an ISO 20000 compliant Service Management System.
- Raising any issues deemed necessary to the attention of the Component Provider.
- Collecting requirements from the Resource infrastructure Providers.
- Supporting coordination with other EGI services.
- Providing monitoring to measure fulfilment of agreed service level targets.
- Providing clear interfaces to the EGI SMS processes.

[13] https://github.com/EGI-Foundation

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.