# EGI Foundation

# Accounting Repository and Portal

# OPERATIONAL LEVEL AGREEMENT

| | |
|---|---|
| **Customer** | EGI Foundation |
| **Provider** | **UKRI, CESGA** |
| **Start Date** | 1st January 2021 |
| **End Date** | 30th June 2023 |
| **Status** | FINAL |
| **Agreement Date** | 10th Dec 2020 |
| **Agreement Link** | https://documents.egi.eu/document/3672 |

## DOCUMENT LOG

| ***Issue*** | ***Date*** | ***Comment*** | ***Author*** |
|---|---|---|---|
| **0.1** | | | Małgorzata Krakowian |
| **0.2** | 31/03/2016 | Edits from Peter Solagna and Stuart Pullinger | Stuart Pullinger |
| **0.3** | 29/04/2016 | Final version from Peter Solagna | P.Solagna |
| **1.0** | 13/06/2017 | First review, added a reference to the availability and continuity plans | Alessandro Paolini |
| **2.0** | 17/11/2017,<br>02/08/2018 | New OLA covering 2018, 2019, 2020 years | Alessandro Paolini,<br>Adrian Coveney |
| **2.1** | 12/09/2019 | yearly review. STFC renamed in UKRI, introduced Service Provider and Component Provider roles, updated Violation, Escalation and Complaints sections; | Alessandro Paolini |
| **3.0** | 04/12/2020 | Covering EGI ACE from Jan 2021 to June 2023; renamed EGI Corporate Level as EGI Default OLA; 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,<br>Adrian Coveney, Carlos Fernandez |

## TERMINOLOGY

The EGI glossary of terms is available at: https://wiki.egi.eu/wiki/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

This Operational Level Agreement ("the Agreement') is made between the **EGI Foundation (the Service Provider),** and **UK Research and Innovation (UKRI) and Centro de Supercomputación de Galicia (CESGA) (the Component Providers)** 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 Component Providers on **10 December 2020.**

The Component Providers are 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** | The Accounting Repository stores compute (serial and parallel jobs), storage, and cloud resource accounting data collected from Resource Centres of the EGI Federation. Accounting information is gathered from a variety of distributed sensors, some of which are developed by the APEL team, into a central accounting repository where it is processed to generate summaries that are available through the EGI Accounting Portal. The Accounting Repository is based on the APEL software and provides interfaces for the exchange of accounting data in a standard format.<br>● This service component is operated by UKRI<br>The Accounting Portal receives the site, user, and VO level aggregated summaries generated by the Accounting Repository, and provides views via a web portal, for example, by grouping sites in a country on custom time intervals. The databases are organized into a CPU record database, a user record database, and a topology database.<br>● This service component is operated by CESGA |
| **IT Service Management** | ● All staff involved in the delivery of the service have achieved the Foundation level FitSM certification and the service owner for the service has achieved both of the Advanced level FitSM certifications. New team members will receive Foundation FitSM training as a minimum.<br>● The Service team interacts with EGI's Service Management System, providing the required information to the following processes: |

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

| | |
|---|---|
| | Service Portfolio Management, Service Level Management, Service Reporting Management, Service Availability and Continuity Management, Information Security Management, Change Management.<br>● The Service team will work with other service teams across the Scientific Computing Department to consolidate the service management system within UKRI.<br>● The Accounting Repository and Accounting Portal teams will work together to ensure their respective SMS processes don't conflict. |
| **Coordination** | This activity is responsible for:<br>● Coordination between the service partners, STFC and CESGA<br>● The coordination of the APEL database operations and upgrade activities with those partners that are in charge of operating systems that depend on the central APEL Accounting Repository and Portal, or on which the accounting infrastructure depends.<br>● The Coordination with the EGI Operations to support accounting clients' upgrade campaigns and other operational activities aiming at improving the accuracy and completeness of the accounting information gathered.<br>● Requirements gathering from service providers and end-users. |
| **Operation** | ● Daily running of the system including the repositories and the Portal for compute and storage accounting<br>● Provisioning of a high availability configuration:<br>○ The Accounting Portal service is available in a dedicated virtual machine running in the CESGA cloud framework based on OpenNebula software, which offers high availability thanks to its resources:<br>▪ A pool of physical servers where the virtual machine can run<br>▪ Storage is provided in a NetApp HA storage solution, providing redundant configuration for data movers (servers) and RAID protection for the disks; the backup of this storage is performed on a daily basis<br>○ The Accounting Repository runs on a dedicated physical machine running in the STFC RAL Data Centre. It is powered via a generator-backed UPS.<br>▪ The database and filesystem are backed up daily. |

| | |
|---|---|
| | ▪ Server hardware is covered by a 4-hour mission critical support contract that ensures that service can be restored in minimum time.<br>▪ In a disaster recovery situation, the latest database can be recovered from backup. Additionally, the accounting messages are cached in the messaging system, so in case of a disruption lasting more than one day, the data can be retrieved once service is restored.<br>● A testing infrastructure to verify interoperability and the impact of software upgrades on depending systems<br>● Maintaining an Availability and Continuity Plan[2] and implementing countermeasures to mitigate the risks defined in the related risk assessment<br>● A testing infrastructure to verify interoperability and the impact of software upgrades on depending systems<br>● Deployment of new releases in production |
| **Maintenance** | This activity includes:<br>● Bug fixing, proactive maintenance, and improvement of the system<br>● 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.<br>● Maintenance of probes to test the functionality of the service<br>● Gathering information on changing and developing requirements<br>● Documentation |

# 2 Service hours and exceptions

As defined in the EGI Default Operational Level Agreement.

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

# 3 Support

As defined in the EGI Default Operational Level Agreement.

Support is provided via the following EGI Service Desk[3] Support Units:

- Accounting Repository: *APEL client & Accounting Repository*
- Accounting Portal: *Accounting Portal*

Support is available between:

- Monday and Friday
- 9:00 and 17:00 GMT/BST
  - during the months between June and September, the Accounting Portal provides support from 8:00 to 15:00 CET

This excludes public holidays and site closures for the Component Providers. During holidays of supporting staff, support will be provided on a best-effort basis. For that period of time an AT RISK downtime should be declared in the Service Registry 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.
- Minimum (as a percentage per month): 99%

**Monthly Reliability**

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

**Quality of Support level**

- Medium (Section 3)

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

# 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** | Alessandro Paolini<br>operations@egi.eu |
| **Component Provider contact** | Adrian Coveney (APEL Team Leader)<br>apel-admins@stfc.ac.uk<br>Ian Collier<br>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 last 9 months | 10 months (first report covering the period Jan – Oct 2021) | Component Provider | Survey form prepared by EGI Foundation |

## 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 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 violation 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 Component Provider, the EGI Foundation 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 Component Provider agrees to make every effort to maximise security level of users' data and minimise possible harm in the event of an incident.
- EGI Foundation holds the role of the Data Controller while the Component Provider holds the role of Data Processor. Data Processing Agreements 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[4] 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)[5].
- The Component Provider must enforce the EGI WISE Acceptable Usage Policies[6].

[4] https://documents.egi.eu/public/ShowDocument?docid=2732

[5] https://aarc-project.eu/policies/policy-development-kit/

[6] https://documents.egi.eu/public/ShowDocument?docid=3600

- The Component Provider shall comply with all principles set out by the GÉANT Data Protection Code of Conduct[7] in its most current version, which will be made available to the Component Provider by EGI Foundation upon request.
- The Component Provider must meet all requirements of any relevant EGI policies or procedures[8] 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 Component Provider

Additional responsibilities of the Component Provider are as follows:

- Adhere to all applicable operational and security policies and procedures and to other policy documents referenced therein.
- Use communication channels defined in the agreement.
- Attend the OMB[9] and other operations meeting when needed.
- Accept EGI monitoring services provided to measure fulfilment of agreed service level targets.
- Services with associated roles are registered in GOCDB[10] as site entities under EGI.eu Operations Centre hosting EGI central operations tools[11].
- Any loss of accounting data stored in the APEL repositories should be recovered 100%.
- The Provider shall support EGI Operations and the resource centres to recover any loss of accounting data not directly imputable to the APEL service.
- Changes in the system must be rolled out to production in a controlled way in order to avoid service disruption.

[7] https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home

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

[9] https://wiki.egi.eu/wiki/OMB

[10] http://goc.egi.eu/

[11] https://goc.egi.eu/portal/index.php?Page_Type=NGI&id=4

### 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[12].) All releases should be appropriately tagged.
- Adopt best practices:
    - Defining and enforcing code style guidelines.
    - Using Semantic Versioning.
    - Using a Configuration Management framework such as Ansible.
    - Taking security aspects into consideration through at every point in time.
    - Having automated testing in place.
    - Using code reviews.
    - Treating documentation as code.
    - Documentation should be available for developers, administrators, and end users.

### 8.1.2 IT Service Management compliance

- Key staff who deliver services should have foundation or basic level ITSM training and certification.
    - ITSM training and certification could include FitSM, ITIL, ISO 20000 etc.
- Key staff and service owners should have advanced/professional training and certification covering the key processes for their services.
- Component Providers should have clear interfaces with the EGI SMS processes and provide the required information.
- Component Providers should commit to the continuous 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 EGI services.

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

- Provide monitoring to measure fulfilment of agreed service level targets.
- Provide clear interfaces to the EGI 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 Service Provider according to the following rules:

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