



EGI Foundation

Workload Manager

OPERATIONAL LEVEL AGREEMENT

| | |
|-------------------------|---|
| Service Provider | EGI Foundation |
| Service Supplier | CNRS |
| Start Date | 1 st April 2021 |
| End Date | 30 th June 2023 |
| Status | FINAL |
| Agreement Date | 20 th April 2021 |
| OLA Link | https://documents.egi.eu/document/3672 |



This work by EGI Foundation is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

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 |
|--------------|-------------|---|---|
| | | | Giuseppe La Rocca Małgorzata Krakowian |
| 0.2 | 27/06/2017 | Draft under discussion | Alessandro Paolini |
| 1.0 | 09/11/2017 | Final version valid until 31/12/2017 | Alessandro Paolini |
| 2.0 | 30/05/2018 | New OLA covering 2018, 2019, 2020 | Alessandro Paolini |
| 2.1 | 20/08/2019 | yearly review; updated Violations, Escalation, and Complaints sections; added the distinction between Component Providers involvement | Alessandro Paolini |
| 2.2 | 13/11/2020 | Updated section 7 on security requirements; renamed EGI Corporate Level as EGI Default OLA; updated the GGUS SU name Name of the service updated Extension agreed for three months - until 31Mar 2021 | Alessandro Paolini Catalin Condurache |
| 3.0 | 20/04/2021 | Covering EGI ACE from Apr 2021 to June 2023; updated section 1; changed frequency of the reports; A/R targets are 99%; 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, Catalin Condurache, Ghita Rahal, Gino Marchetti |
| 3.1 | 07/06/2022 | Yearly review; introduced the term Service Supplier; updated section 7 and section 8; corrected some typos; | 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

| | | |
|-------|--|----|
| 1 | The Services | 4 |
| 2 | Service hours and exceptions | 5 |
| 3 | Support | 5 |
| 3.1 | Incident handling | 5 |
| 3.2 | Service requests | 5 |
| 4 | Service level targets | 6 |
| 5 | Limitations and constraints | 6 |
| 6 | Communication, reporting and escalation | 6 |
| 6.1 | General communication | 6 |
| 6.2 | Regular reporting | 6 |
| 6.3 | Violations | 7 |
| 6.4 | Escalation and complaints | 7 |
| 7 | Information security and data protection | 7 |
| 8 | Responsibilities | 8 |
| 8.1 | Of the Service Supplier | 8 |
| 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 Agreement (“the Agreement”) is made between **EGI Foundation (the Service Provider)** and **CNRS (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 April 2021** to **30th June 2023**.

The Agreement was discussed and approved by EGI Foundation and the Service Supplier **20th April 2021**.

The Service Supplier is bound by the terms and conditions of the EGI Default Operational Level Agreement¹ supplemented by the terms and conditions of this specific Agreement:

1 The Services

The Services are defined by the following properties:

| | |
|---------------------|---|
| Technical | <p>The EGI Workload Manager (DIRAC) service is a set of interfaces to allow users to submit computational tasks to the HTC and Cloud resources, monitor the status and retrieve the results. Users interact with DIRAC both using Web GUI and API.</p> <p>The components of the EGI Workload Manager service are:</p> <ul style="list-style-type: none"> ● DIRAC WMS server (multiple high performance machines) ● DIRAC DB (MySQL) server (high performance, large memory machine) ● DIRAC REST server (medium sized machine) ● DIRAC Web server (low CPU, high memory machine) ● DIRAC Configuration server (low CPU, high memory machine) ● DIRAC Data Management service (low CPU, high memory machine) |
| Coordination | <p>This activity is responsible for:</p> <ul style="list-style-type: none"> ● the coordination of the system operations and upgrade activities with those partners that are in charge of operating other systems that depend on it to ensure continuity of the service ● With the virtual organisations: to support the technical configuration and training ● With EGI user support team and Operations: to gather requirements and use cases |
| Operation | <ul style="list-style-type: none"> ● Daily running of the service instances ● Configure new VOs in the EGI Workload Manager service ● Handle security requests |

¹ <https://documents.egi.eu/document/2752>

| | |
|--------------------|--|
| | <ul style="list-style-type: none"> ● Provision usage statistics upon request ● Provisioning of a high availability configuration <ul style="list-style-type: none"> ○ Configuration Management recovery procedure ○ Database redundancy and daily backup <ul style="list-style-type: none"> ▪ daily backup retention period: 6 months ● Creating an Availability and Continuity Plan and implementing countermeasures to mitigate the risks defined in the related risk assessment² |
| Maintenance | <ul style="list-style-type: none"> ● Bug fixing, proactive maintenance, improvement of the system. ● Maintenance of probes to test the functionality of the service. ● Documentation. |

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 Desk³ Support Unit: Workload Manager (DIRAC).

Access requires a valid X.509 or the login via an EGI Check-in account⁴

Support is available between:

- Monday and Friday
- 9:00 and 17:00 CET/CEST time

This excludes public holidays at the same time in all organisations providing the service.

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.

² <https://confluence.egi.eu/x/zlf4AQ>

³ <http://helpdesk.egi.eu/>

⁴ <https://docs.egi.eu/providers/check-in/>

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 (Section 3)

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 Services in the scope of this Agreement.

| | |
|---------------------------------|---|
| Service Provider contact | Catalin Condurache operations@egi.eu EGI Foundation Operations officer |
| Service Supplier contact | Ghita Rahal ghita.rah@cc.in2p3.fr Gino Marchetti gino.marchetti@cc.in2p3.fr Andrei Tsaregorodtsev atsareg@in2p3.fr |
| Service Support contact | See Section 3 |

6.2 Regular reporting

As part of the fulfilment of this Agreement and provisioning of the Services, 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 the reference reporting period | 10 months (first report covering the period Jan – Oct 2021) | Service Supplier | Survey form prepared by EGI Foundation |
|----------------------------|---|---|------------------|--|

All reports shall follow predefined templates⁵.

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 Service Supplier 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 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 Service Supplier, EGI Foundation Director director@egi.eu should be informed.

7 Information security and data protection

As defined by the EGI Default Operational Level Agreement.

⁵ <https://documents.egi.eu/document/2748>

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 SEC01⁶ 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 Data⁷ 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)⁸.
- The Service Supplier must enforce the EGI WISE Acceptable Usage Policies⁹.
- The Service Supplier shall comply with all principles set out by the GÉANT Data Protection Code of Conduct¹⁰ in its most current version, which will be made available to the Service Supplier by EGI Foundation upon request.
- The Service Supplier must meet all requirements of any relevant EGI policies or procedures¹¹ 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 follows:

⁶ <https://go.egi.eu/sec01>

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/Data+Protection+Code+of+Conduct+Home>

¹¹ https://www.egi.eu/about/policy/policies_procedures.html

- Adhering to all applicable operational and security policies and procedures¹² and to other policy documents referenced therein.
- Using the communication channels defined in this Agreement.
- Attending OMB¹³ and other operations meeting when needed
- Accepting EGI monitoring services provided to measure fulfilment of agreed service level targets.
- The Service endpoints with associated roles is registered in GOC DB¹⁴ as site entity under the EGI.eu Operations Centre hosting EGI central operations tools¹⁵.
- Changes in the system must be rolled in production in a controlled way in order to avoid service disruption.
- Putting in place 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.
- 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 GitHub¹⁶.) All releases should be appropriately tagged.
- Adopt best practices:
 - Defining and enforcing code style guidelines.
 - Using Semantic Versioning.
 - Using a Configuration Management frameworks such as Ansible.
 - Taking security aspects into consideration at every point in time.
 - Having automated testing in place.
 - Using code reviewing.
 - Treating documentation as code.
 - Documentation should be available for Developers, administrators and end users.

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

¹³ <https://confluence.egi.eu/display/EGIBG/Operations+Management+Board>

¹⁴ <http://goc.egi.eu/>

¹⁵ https://goc.egi.eu/portal/index.php?Page_Type=NGI&id=4

¹⁶ <https://github.com/EGI-Federation>

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 standards and best practices such as FitSM, ITIL, ISO 20000 etc.
- Key staff and service owners should have advanced/professional training and certification covering the key processes for their services
- Providers should have clear interfaces with the EGI SMS processes and provide the required information.
- Service Suppliers should commit to improving their management system used to support the services they provide.

8.2 Of the Service Provider

The responsibilities of the Service Provider are:

- Delivering and planning the Services according to an ISO compliant manner.
- Raising any issues deemed necessary to the attention of the Service Supplier.
- Collecting requirements from the Resource infrastructure Providers.
- Supporting coordination and integration with other EGI services.
- Providing monitoring to measure fulfilment of agreed service level targets.
- Providing 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 this 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 at a reasonable frequency. These will aim to evaluate the effective provision of the agreed service or 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. EGI Foundation will announce audits at least one month in advance. The Service Supplier / 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 Service Supplier / federation member is obliged to provide the auditors, upon request, with the information and evidence necessary. Efforts connected to supporting these audits by the Service Supplier / federation member will not be reimbursed.