



# EGi Foundation

## UMD and CMD quality assurance

### OPERATIONAL LEVEL AGREEMENT

---

<b>Service Provider</b>	EGi Foundation
<b>Component Provider</b>	IBERGRID (CSIC, LIP)
<b>Start Date</b>	1 <sup>st</sup> January 2021
<b>End Date</b>	30 <sup>th</sup> June 2023
<b>Status</b>	FINAL
<b>Agreement date</b>	21 <sup>st</sup> January 2021
<b>OLA Link</b>	<a href="https://documents.egi.eu/document/3672">https://documents.egi.eu/document/3672</a>

---



This work by EGI Foundation is licensed under a

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 .

## DOCUMENT LOG

<b>Issue</b>	<b>Date</b>	<b>Comment</b>	<b>Author</b>
			Małgorzata Krakowian
	14/09/2016	Added LIP, IFCA and CESGA as providers. Updated GGUS SU and contact information.	Peter Solagna
<b>2.0</b>	29/01/2018, 02/10/2018	New OLA covering 2018, 2019, 2020. Added more hardware details about the infrastructure. Added links to Stage Rollout and Software Provisioning processes.	Alessandro Paolini, Joao Pina
<b>2.1</b>	21/10/2019	Yearly review; introduced the roles Service Provider and Component Provider; updated contacts; updated sections on Violations, Escalations, and Complaints	Alessandro Paolini
<b>3.0</b>	07/01/2021, 23/02/2021	Covering EGI ACE from Jan 2021 to June 2023; renamed EGI Corporate Level as EGI Default OLA; updated section 1; updated GGUS SU in section 3; 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, Vincenzo Spinoso, Isabel Campos

## 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

1	The Services	4
2	Service hours and exceptions	6
3	Support	6
3.1	Incident handling	6
3.2	Service requests	6
4	Service level targets	6
5	Limitations and constraints	7
6	Communication, reporting and escalation	7
6.1	General communication	7
6.2	Regular reporting	7
6.3	Violations	8
6.4	Escalation and complaints	8
7	Information security and data protection	8
8	Responsibilities	9
8.1	Of the Component Provider	9
8.1.1	Software compliance	10
8.1.2	IT Service Management compliance	10
8.2	Of the Service Provider	10
9	Review, extensions and termination	11

The present Operational Level Agreement (“the Agreement”) is made between **EGI Foundation (the Service Provider)** and **IBERGRID (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 **1<sup>st</sup> January 2021** to **30<sup>th</sup> June 2023**.

The Agreement was discussed and approved by the Customer and the Provider **21<sup>st</sup> January 2021**.

The providers are bound by the terms and conditions of the EGI Default Operational Level Agreement<sup>1</sup> supplemented by the terms and conditions of this specific Agreement:

## 1 The Services

The Services are defined by the following properties:

<b>Technical</b>	<p>All the products released in UMD and CMD must be verified against the relevant acceptance criteria. Products must be deployed in a controlled environment. Every product in every distribution must have a verification report associated with the results of the verification process. Verifiers must be familiar with the core products used in EGI, the most common site configurations and third party components such as DBMS and LRMS. The software to be verified involves user facing services, HTC services, storage services, cloud services, and all the products that are critical for EGI communities and are part of the supported distribution.</p> <p>This task will also test the release candidates to check the dependencies and installability of the packages before the official release.</p> <p>The distributions maintained per year are expected to be about 4-5. The software releases per distribution are expected to be 6-10 minor releases per year, and supporting 3-4 operating system platforms.</p> <p>Staged Rollout is performed by Early Adopter (EA)<sup>2</sup> sites who volunteer to deploy products fulfilling the acceptance criteria in the production infrastructure, exposing them to real users and real use cases.</p>
<b>Coordination</b>	<p>The task must coordinate the verifications when the process is outsourced to developers or user communities, this means: overview to advancements in the process and collect the reports produced during verification, making</p>

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

<sup>2</sup> [https://wiki.egi.eu/wiki/Staged\\_Rollout](https://wiki.egi.eu/wiki/Staged_Rollout)

	<p>sure that the relevant information (GGUS tickets opened, known issues) are properly propagated to the software releases.</p> <p>During staged rollout this task is responsible for the coordination of the Early Adopters activity, namely assign and monitor the progress of each individual product and corresponding EA teams, collect and analyse the reports provided by the EA team and in case of issues found make sure that relevant information is properly handled.</p>
<b>Operation</b>	<p>This task will operate two cloud infrastructures based on OpenNebula and OpenStack to be used as a testbed for the verification of the software products. The size of the infrastructure, each VM with a maximum of 12 VCPU40 GB memory and 400 GB disk, should allow the deployment of several VM / Containers in parallel to test also for service interoperability. Verification of products should be outsourced only when the effort required would be too high (for example for lack of expertise), or for technical limitations that prevent to deploy the service in the testbed.</p> <p>Release candidates must be tested for the installation of all the components, new and already available in the repositories. The test, possibly automated, must be able to generate a report in few hours (less than one working day, possibly 2-4 hours).</p> <p>This task is also responsible for producing and maintaining the UMD release notes and known issues wiki pages. The task leader must participate to the periodic EGI Operations meetings and report about the status of the UMD and CMD releases. Together with those activities it also includes:</p> <ul style="list-style-type: none"> <li>● maintenance of the EA tables</li> <li>● create the corresponding xml file for each Product per Platform and Architecture (PPA)</li> <li>● monitor and handle the software provisioning process<sup>3</sup></li> </ul>
<b>Maintenance</b>	<ul style="list-style-type: none"> <li>● Enhance the definition of the EGI Quality Criteria</li> <li>● Adapt existing Ansible roles (and Puppet modules) to the new versions of UMD and CMD software &amp; maintenance/new features of umd-verification source code</li> <li>● Publish quick start guidelines for deploying UMD and CMD products<sup>13</sup></li> <li>● Jenkins CI system operation: new job definitions &amp; resource provisioning mechanisms --e.g. container orchestration--, software &amp; security updates</li> </ul>

<sup>3</sup> [https://wiki.egi.eu/wiki/Software\\_Provisioning\\_Process](https://wiki.egi.eu/wiki/Software_Provisioning_Process)

- Review the early adopter process

## 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 EGI Service Desk<sup>4</sup> Support Units: UMD/CMD Quality Assurance, UMD Product Submission, Software Provisioning.

Support is available between:

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

This excludes public holidays and site closures for the Component Providers.

### 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

Estimated number of products to verify in one year is 200 PPA.

Each PPA should be verified within 1 month from the submission of the PPA by the developers.

### Quality of Support level

- Medium (Section 3)

---

<sup>4</sup> <http://helpdesk.egi.eu/>

## 5 Limitations and constraints

As defined in the EGI Default Operational Level Agreement.

The provisioning of the service under the agreed service level targets is subject to the following limitations and constraints:

- Support is provided in the following language: English
- Downtimes caused due to upgrades for fixing critical security issues are not considered Agreement violations.
- Force Majeure. A party shall not be liable for any failure or delay in the performance of this Agreement for the period that such failure or delay is due to causes beyond its reasonable control. Means any
  - fire, flood, earthquake, or natural phenomena,
  - war, embargo, riot, civil disorder, rebellion, revolutionwhich is beyond the Provider's control, or any other causes beyond the Provider's control

## 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.

<b>Service Provider contact</b>	Alessandro Paolini: <a href="mailto:operations@egi.eu">operations@egi.eu</a>
<b>Component Provider contacts</b>	Jorge Gomes: <a href="mailto:jorge@lip.pt">jorge@lip.pt</a> Mário David: <a href="mailto:david@lip.pt">david@lip.pt</a> Joao Pina: <a href="mailto:jpina@lip.pt">jpina@lip.pt</a> Isabel Campos: <a href="mailto:isabel@campos-it.es">isabel@campos-it.es</a> Pablo Orviz: <a href="mailto:orviz@cern.ch">orviz@cern.ch</a>
<b>Service Support contact</b>	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	10 months (first report covering the	Component Provider	Survey form prepared by EGI Foundation

	assessment of service performance (per month) and OLA target performance achieved during reporting period	period Jan – Oct 2021)		
--	---	------------------------	--	--

### 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 EGI Foundation still feel dissatisfied, about either the result of the response or the behaviour of the Component Provider, EGI Foundation Director 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<sup>5</sup> 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)<sup>6</sup>.
- The Component Provider must enforce the EGI WISE Acceptable Usage Policies<sup>7</sup>.
- The Component Provider shall comply with all principles set out by the GÉANT Data Protection Code of Conduct<sup>8</sup> 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<sup>9</sup> 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 follow:

- Adhere to all applicable operational and security policies and procedures<sup>10</sup> and to other policy documents referenced therein.
- Use communication channels defined in the agreement.
- Attend OMB<sup>11</sup> and other operations meetings when needed.

---

<sup>5</sup> <https://documents.egi.eu/public/ShowDocument?docid=2732>

<sup>6</sup> <https://aarc-project.eu/policies/policy-development-kit/>

<sup>7</sup> <https://documents.egi.eu/public/ShowDocument?docid=3600>

<sup>8</sup> <https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home>

<sup>9</sup> [https://www.egi.eu/about/policy/policies\\_procedures.html](https://www.egi.eu/about/policy/policies_procedures.html)

<sup>10</sup> [https://www.egi.eu/about/policy/policies\\_procedures.html](https://www.egi.eu/about/policy/policies_procedures.html)

<sup>11</sup> <https://wiki.egi.eu/wiki/OMB>

- Accept EGI monitoring services provided to measure fulfilment of agreed service level targets.
- Changes in the system must be rolled in 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<sup>12</sup>.) 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.

---

<sup>12</sup> <https://github.com/EGI-Foundation>

- Collect requirements from the Resource infrastructure Providers.
- Support coordination with other EGI services.
- Provide monitoring to measure fulfilment of agreed service level targets.

## 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
- 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 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.