EGI Foundation

Infrastructure Manager

Operational level Agreement

Service Provider	EGI Foundation
Service Supplier	**UPV-GRyCAP**
First day of service delivery	1st January 2021
Last day of service delivery	30th June 2023
Status	Final
Agreement finalisation date	18th 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*
1.0	17/12/2020, 22/02/2021	First version of the OLA, covering EGI ACE from Jan 2021 to June 2023	Enol Fernandez, Alessandro Paolini
1.1	13/01/2022	yearly review; replaced the word “Component Provider” with “Service Supplier”; updated sections 7 and 8.	Alessandro Paolini
1.2	24/01/2023	yearly review; minor corrections; replaced some old links	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 Agreement ("the Agreement') is made between **EGI Foundation (the Service Provider)** and **UPV-GRyCAP (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 EGI Foundation and the Service Supplier on 18th December 2020.

The Service Supplier(s) is (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	Infrastructure Manager (IM) is an open-source service that deploys complex and customised virtualized infrastructures on multiple back-ends. The IM automates the deployment, configuration, software installation, monitoring and update of virtual infrastructures. It supports a wide range of public and on-premises Cloud back-ends, thus making user applications Cloud agnostic. In addition, it features DevOps capabilities, based on Ansible to enable the installation and configuration of all the user required applications providing the user with a fully functional virtualized infrastructure. The service should be offered as a centrally managed instance that will be run by the project and will provide access to both generic and thematic users. Additionally, the provider should be capable of setting up dedicated instances to specific communities as needed upon request. IM instance for EGI should : ● integrate with EGI Check-in for authentication and authorisation of users ● support the main IaaS APIs available in EGI Cloud (OpenStack, OpenNebula) and optionally support other IaaS APIs of commercial cloud providers (AWS, GCP, Azure) ● integrate with EGI information discovery to facilitate the use of resources
Coordination	This activity is responsible for the coordination of the service maintenance activities with the EGI operations team and other technology providers for the EGI Core Infrastructure.
Operation	● Daily running of the service. ● Provisioning of a high availability configuration:

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

	○ All the components of the service (IM service, IM Web and IM Dashboard) are deployed on top of a Kubernetes cluster. In particular the IM service is served behind an HAproxy used as a load balancer using at least four IM server instances spread in at least two different working nodes, for increased redundancy. ● Creating an Availability and Continuity Plan and implementing countermeasures to mitigate the risks defined in the related risk assessment.
Maintenance	This activity includes: ● Requirements gathering ● 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

Support is provided via EGI Service Desk[2] Support Unit: Infrastructure Manager.

Access requires a valid X.509 or the login via an EGI Check-in account[3].

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.

[2] http://helpdesk.egi.eu/
[3] https://docs.egi.eu/providers/check-in/

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): 95%

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): 95%

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 service in the scope of this Agreement.

Service Provider contact	Alessandro Paolini operations@egi.eu EGI Foundation Operations officer
Service Supplier contact	Miguel Caballer micafer1@upv.es
Service Support contact	See Section 3

6.2 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.

6.3 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 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).

[4] https://go.egi.eu/sec01

- 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.
- 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 theService Supplier are as follows:

- Adhering to all applicable operational and security policies and procedures[10] and to other policy documents referenced therein.
- Using communication channel defined in the agreement.
- Attending OMB[11] and other operations meeting when needed.
- Accepting EGI monitoring services provided to measure fulfilment of agreed service level targets.
- The Services with associated roles is registered in GOC DB[12] as site entity under EGI.eu Operations Centre hosting EGI central operations tools[13].

[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/Code+of+Conduct+for+Service+Providers
[9] https://confluence.egi.eu/display/EGIPP/EGI+Policies+and+Procedures+Home
[10] https://confluence.egi.eu/display/EGIPP/EGI+Policies+and+Procedures+Home
[11] https://confluence.egi.eu/display/EGIBG/Operations+Management+Board
[12] http://goc.egi.eu/
[13] https://goc.egi.eu/portal/index.php?Page_Type=NGI&id=4

- 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 GitHub[14].) 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.

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 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 improving their management system used to support the services they provide.

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

8.2 Of the Service Provider

The responsibilities of the Service Provider are:

- Delivering and planning the Services component according to an ISO 20000 compliant manner.
- Raising any issues deemed necessary to the attention of the Component Provider.
- 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 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.