# EGI Foundation

# Virtual appliances and software database (AppDB)

# OPERATIONAL LEVEL AGREEMENT

| | |
|---|---|
| **Service Provider** | EGI Foundation |
| **Service Supplier** | IASA |
| **Start Date** | 1st January 2021 |
| **End Date** | 30th June 2023 |
| **Status** | FINAL |
| **Agreement Date** | 11th February 2021 |
| **OLA Link** | https://documents.egi.eu/document/3672 |

## DOCUMENT LOG

| *Issue* | *Date* | *Comment* | *Author* |
|---|---|---|---|
| **FINAL** | 18/04/2016 | Final version | Małgorzata Krakowian |
| **1.1** | 18/05/2017 | Yearly review, no changes | Alessandro Paolini |
| **2.0** | 05/01/2017 | New OLA covering 2018, 2019, 2020 years | Alessandro Paolini, Marios Chatziangelou |
| **2.1** | 27/06/2018 | Changed the reporting period to 9 months; added the requirement for the availability and continuity plan. | Alessandro Paolini |
| **2.2** | 16/09/2019 | Introduced the roles Service Provider and Component Provider; updated contacts; updated sections on Violations, Escalations, and Complaints | Alessandro Paolini |
| **3.0** | 16/12/2020, 11/02/2021 | Covering EGI ACE from Jan 2021 to June 2023; renamed EGI Corporate Level as EGI Default OLA; updated section 1; updated section 7 on security requirements; added Software and ITSM compliance in section 8; added in section 9 the requirement about periodic supplier process audits conducted by EGI Foundation; removed the section about the performance reports since now the service is fully funded by the project and it is not necessary delivering a report to the EGI EB. | Alessandro Paolini, William Karageorgos |
| **3.1** | 14/02/2022 | 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 Agreement ("the Agreement') is made between **EGI Foundation (the Service Provider)** and **IASA (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 **11th February 2021**.

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** | The service is composed by the following components:<br>● Software marketplace: a registry to manage software items as applications, tools, utilities, etc. The software marketplace supports the following categories: Application, Tool, Science gateway, Workflow, Middleware product.<br>● Cloud marketplace: bundles a set of features that are part of the EGI Collaboration platform as:<br>○ Virtual and software appliances catalogue: open library of virtual appliances (bundle of one or more VM images) for use on a cloud or for personal download, supporting VM image management operations like: registration of new instances, reuse of existing ones and contextualization.<br>○ VO-wide image list management: a mechanism that allows to link a list of virtual and software appliances to a VO, which can be automatically and securely distributed to any resource provider supporting the VO.<br>○ Sites / Resources providers view: list of cloud RPs with information on endpoints, supported VOs, available VM images, flavours and etc.<br>○ Integration with the EGI Information System: information retrieved by the IS are used to enrich VA, SA and RP views with information useful to interact with the infrastructures.<br>● People registry: list of people involved in EGI with links to items registered on the AppDB.<br>● Database of VMI queried by the vmcatcher/cloudkeeper clients at site level, used to store the information about the VMI endorsed by the Federated cloud communities. |

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

| | |
|---|---|
| | • Community repository: generating and maintaining associative binary repositories for items of the Software marketplace<br>• VM Operations Dashboard, a GUI for the Federated cloud users to create and operate virtual machines in fedcloud sites, VM based on VMI stored in AppDB.<br>• Endorsements Dashboard, a GUI for the Federated cloud users to endorse VM images.<br>• Security Dashboard, a GUI for the Federated cloud security officers to tag VM images about potential security issues<br>• Information System: a service to correlate, process, and provide information collected by various other services, with respect to the EGI infrastructure.<br>• Continuous Delivery, a service that allows VM owners to integrate their VM building process with the AppDB virtual appliance management system in an automated fashion. |
| **Coordination** | The service providers must coordinate with the EGI Federated cloud working group, the EGI security for the requirements on VM endorsement and the VO Managers to support the distribution of VMIs through AppDB. |
| **Operation** | The activity includes the daily operations of the following user facing services:<br>• AppDB Portal<br>  ○ Rest API<br>  ○ VMCaster<br>  ○ Community Repository<br>  ○ Gadgets<br>  ○ Dashboards (VMOps, Endorsements, Security)<br>• Deployment in production of new developments<br>• Maintenance of the services<br>• Infrastructure Setup incl. HA and Backup:<br>At the moment (as it keeps evolving), the AppDB consists of 6 Virtual Machines and 7 physical servers.<br>Virtual Machines:<br>• vm1:appdb-main & vmcaster,<br>• vm2:dashboards<br>• vm3: dashboards backend,<br>• vm4:appdb-infosys frontend,<br>• vm5:appdb-infosys backend (collector)<br>• vm6:appdb-wiki, OAI-PHM harvesting, and Continuous Delivery<br>Physical servers: 4 servers for VM hosting, 2 db servers, 1 Infrastructure manager server (offering 10 IM docker instances). Everything on RAID 1. Backup: VMs weekly, data daily. |

| | |
|---|---|
| | • Creating an Availability and Continuity Plan for the Application Database[2] and implementing countermeasures to mitigate the risks defined in the related risk assessment |
| **Maintenance** | • Requirements gathering<br>• Documentation<br>• Maintenance of probes to test the functionality of the service<br>• Filesystem checks and disk usage scans<br>• Database management (auditing, updating, performance tuning, backup etc.).<br>• Operating system upgrades, updates, and patches<br>• Security management and log auditing<br>• Hardware inspection related tasks |

# 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: Virtual Appliance Catalogue (AppDB)

Support is available between:

- Monday and Friday
- 9:00 and 17:00 EET/EEST time

This excludes public holidays at the same time in all organizations 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/display/SUPAPPDB/AppDB+Availability+and+Continuity+plan
[3] http://helpdesk.egi.eu/

# 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<br>operations@egi.eu<br>EGI Foundation Operations officer |
| **Service Supplier contact** | William Karageorgos : wvkarageorgos@iasa.gr<br>Alexandros Nakos: nakos.al@iasa.gr<br>Contact email: appdb-support@iasa.gr |
| **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 by 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/sec01https://wiki.egi.eu/wiki/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 Service Supplier 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

# 8 Responsibilities

## 8.1 Of the Service Supplier

Additional responsibilities of the Service 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.
- Service 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/Data+Protection+Code+of+Conduct+Home
[9] https://www.egi.eu/about/policy/policies_procedures.html
[10] https://www.egi.eu/about/policy/policies_procedures.html
[11] https://wiki.egi.eu/wiki/OMB
[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 (like MIT, BSD, Apache 2.0,...).
- The licence 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[14].) All releases should be appropriately tagged.
- Adopt best practises:
    - 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 practises 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.
- 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.

## 8.2 Of the Service Provider

The responsibilities of the Service Provider are:

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

- Delivering and planning the Services component according to an ISO 20000 compliant manner.
- Raise any issues deemed necessary to the attention of the Service Supplier.
- Collecting requirements from the Resource infrastructure Providers.
- Supporting coordination with other EGI services.
- Providing 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. 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 supplier 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 supplier is obliged to provide the auditors, upon request, with the information and evidence necessary. Efforts connected to supporting these audits by the supplier will not be reimbursed.