EGI Foundation

Helpdesk service (GGUS)

OPERATIONAL LEVEL AGREEMENT

Service Provider	EGI Foundation
Service Supplier	**KIT**
Start Date	1st January 2021
End Date	30th June 2023
Status	FINAL
Agreement Date	4th March 2021
OLA Link	https://documents.egi.eu/document/3672

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
FINAL	21/03/2016	Final version	Małgorzata Krakowian
1.1	18/05/2017	Yearly review, no changes	Alessandro Paolini
2.0	12/12/2017	New OLA covering 2018, 2019, 2020	Alessandro Paolini, Helmut Dres, Guenter Grein
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	16/12/2019	yearly review; introduced the Service Provider and the Component Provider roles; updated Violations, Escalation, and Complaints sections; Corporate-level EGI OLA renamed to EGI Default OLA; helpdesk support unit has been renamed	Alessandro Paolini
3.0	11/12/2020, 05/03/2021	Covering EGI ACE from Jan 2021 to June 2023; 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, Guenter Grein
3.1	09/03/2022	yearly review; introduced the term Service Supplier; updated section 7 and section 8; corrected some typos; updated the contacts section;	Alessandro Paolini, Guenter Grein
3.2	28/03/2023	yearly review; updated some 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

The present Operational Level Agreement ("the Agreement') is made between **EGI Foundation (the Service Provider)** and **KIT (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 **4th March 2021.**

The Service Supplier is 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 GGUS system is divided into three environments: development, test and production environment. Every environment includes three layers: ● Presentation - web frontend to provide the entry point for the graphical user interface; ● Logic - AR Server which executes the workflow rules and performs the main tasks. AR Server is providing the communication interface between external systems and is accompanied by the email-engine to provide the additional mail-based interface into the helpdesk system; ● Backend - Oracle DBMS
Coordination	This activity is responsible for the coordination of the system operation and upgrade activities with those partners that are in charge of operating other systems that depend on it. Coordination with user communities, technology providers and operators is provided by dedicated Advisory Board meetings.
Operation	● Service operations ○ Daily running of the system ○ Support Unit maintenance ○ Provisioning of a high availability configuration ▪ Two identical stacks at two locations ▪ F5 load balancer that distributes network or application traffic across the two stacks ▪ Presentation and Logic on virtual machines

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

	▪ Backend (Oracle Database Appliance, a physical system consisting of 2 real servers and a disk system on which 2 virtual servers built a RAC) ▪ Tape backup (IBM Tivoli Storage Manager) ▪ Stacks being monitored by ICINGA and integrated into a 24/7 on-call duty service. ○ A test infrastructure to verify interoperability and the impact of software upgrades on depending systems ● Ticket oversight ○ This activity includes the administrative and reporting functions of the helpdesk infrastructure, e.g. collecting ticket statistics, and internal and external reporting of statistics for SLAs monitoring and other reporting duties. Ticket follow-up includes notifying supporters when the reaction to high-priority tickets is not fast enough, requesting information from ticket submitters when they do not react, and ensuring assigners/resolvers will react sufficiently fast when the submitter provides additional information. ● Implementing all the measures for mitigating the risks listed in the Availability and Continuity Plan for the GGUS helpdesk system[2]
Maintenance	This activity includes: ● bug fixing, proactive maintenance, improvement of the system. ● 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. ● requirements gathering. ● documentation.

2 Service hours and exceptions

As defined by the EGI Default Operational Level Agreement.

[2] https://confluence.egi.eu/x/5oOoBw

3 Support

As defined by the EGI Default Operational Level Agreement.

Support is provided via EGI Service Desk[3] Support Unit: Helpdesk (GGUS)

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.

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)

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

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.

EGI Foundation contact	Alessandro Paolini operations@egi.eu
Service Supplier contacts	Guenter Grein: guenter.grein@kit.edu Torsten Antoni: torsten.antoni@kit.edu
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

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 violations 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 EGI Foundation 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).
- 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].

[4] https://go.egi.eu/sec01
[5] https://documents.egi.eu/public/ShowDocument?docid=2732
[6] https://aarc-project.eu/policies/policy-development-kit/

- 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
    - EGI-doc-710: Security Incident Handling Procedure

8 Responsibilities

8.1 Of the Service Supplier

Additional responsibilities of the Service Supplier are as follow:

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

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

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

[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/x/vwXpB

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

[13] 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 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.
    - Making the documentation to 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 Suppliers should have clear interfaces with the EGI Service Management System processes and provide the required information.
- Service Suppliers 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:

- Delivering and planning the Services according to an ISO 20000 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.

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

- 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 EGI Foundation 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 provider / federation member will not be reimbursed.