EGI Foundation

Helpdesk service (xGUS) for EOSC

OPERATIONAL LEVEL AGREEMENT

Service Provider	EGI Foundation
Component Provider	**KIT**
Start Date	1st April 2021
End Date	30th September 2023
Status	Draft
Agreement Date	12th May 2021
OLA Link	https://documents.egi.eu/document/3756

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
0.1	27/04/2021	First draft	Alessandro Paolini, Matthew Viljoen
1.0	12/05/2021	version finalised	

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 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 **1st April 2021** to **30th September 2023**.

The Agreement was discussed and approved by EGI Foundation and the Component Provider 12th **May 2021.**

The Component Provider 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	xGUS is the helpdesk system for EOSC providing a single access point for both the backend EOSC-Core services and EOSC Exchange providers who wish to make use of a central EOSC helpdesk. It 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: ● 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. ● Engagement with the EOSC-Future project for the policy, operational and user requirements

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

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 ▪ 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 xGUS 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 EOSC Infrastructure or remote systems deployed by integrated and peer *infrastructures that interoperate with the central EOSC components of the system. ● requirements gathering. ● documentation.

[2] a specific AvCo plan will be created for the EOSC instance of the service

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 EOSC Helpdesk Service[3] Support Unit: to create a specific support unit different than EOSC-hub First Level Support

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 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.

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

[3] https://helpdesk.eosc-portal.eu/

- 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.

EGI Foundation contact	Matthew Viljoen operations@egi.eu
Component Provider contacts	Pavel Weber: pavel.weber@kit.edu Guenter Grein: guenter.grein@kit.edu Torsten Antoni: torsten.antoni@kit.edu
Service Support contact	See Section 3

6.2 Regular reporting

Reporting will be done according to the EOSC-Future project.

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 EOSC Helpdesk Service. 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 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 by the Component Provider:

- The Component Provider must make every effort to maximise security level of users' data and minimise possible harm in the event of an incident. Incidents must be immediately reported to the EGI CSIRT according to the SEC01 procedure[4].
- EGI Foundation holds the role of the Data Controller while the Component Provider holds the role of Data Processor. Data Processing Agreements[5] covering the provided services 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[6] and provide a Privacy Policy. This Privacy Policy must be prepared together with EGI Foundation and must be based on the Privacy Policy template provided by the AARC Policy Development Kit (PDK)[7].
- The Component Provider must enforce the EGI WISE Acceptable Usage Policy[8].
- The Component Provider shall comply with all principles set out by the GÉANT Data Protection Code of Conduct[9] version 1.0.

[4] https://wiki.egi.eu/wiki/SEC01
[5] https://documents.egi.eu/document/3755
[6] https://documents.egi.eu/public/ShowDocument?docid=2732
[7] https://aarc-project.eu/policies/policy-development-kit/
[8] https://documents.egi.eu/public/ShowDocument?docid=3600
[9] https://wiki.refeds.org/display/CODE/Code+of+Conduct+for+Service+Providers

- The Component Provider must meet all requirements of any relevant EGI policies or procedures[10] 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
    - SEC01: EGI CSIRT Security Incident Handling Procedure - EGIWiki

8 Responsibilities

8.1 Of the Component Provider

Additional responsibilities of the Component Provider are as follow:

- Adhering to all applicable operational and security policies and procedures[11] and to other policy documents referenced therein;
- Using communication channel defined in this Agreement;
- Attend relevant operations meeting when needed;
- Accepting EOSC monitoring services provided to measure fulfilment of agreed service level targets.
- The service with associated roles are registered in GOC DB[12] as site with the "EOSCCore" scope tag. .
- 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 (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[13].) All releases should be appropriately tagged.

[10] https://www.egi.eu/about/policy/policies_procedures.html

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

[12] https://gocdb.eosc-portal.eu/portal/

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

- 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 through 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.
- Component Providers should have clear interfaces with the EGI Service Management System processes and provide the required information.
- Component Providers should commit to the continuous improvement 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 a ISO 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 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 Component 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 Component 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.