Marketplace Services for EOSC

Operational level Agreement

Service Provider	EGI Foundation
Component Provider	CYFRONET
First day of service delivery	1st April 2021
Last day of service delivery	30th September 2023
Status	Draft
Agreement finalization date	27th May 2021
Agreement Link	https://documents.egi.eu/document/3756

DOCUMENT LOG

Issue	***Date***	***Comment***	***Author***
v0.1	27/04/2021	First draft	Alessandro Paolini, Matthew Viljoen
v1.0	27/05/2021	Final version	Alessandro Paolini, Matthew Viljoen, Bartosz Wilk

TERMINOLOGY

The EGI glossary of terms is available at: https://ims.egi.eu/display/EGIG/EGI+Glossary+Home

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 Agreement ("the Agreement') is made between **EGI Foundation (the Service Provider)** and **CYFRONET (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 the **1st April 2021** to **30th September 2023**.

The Agreement was discussed and approved by EGI Foundation and the Provider on **27th May 2021**.

The providers are bound by the terms and conditions of the EGI Default Operational Level Agreement[1], which supplements the terms and conditions of this specific Agreement.

1 The Services

The Services are defined by the following properties:

Marketplace Provisioning	The Marketplace provides functionality necessary for bringing together offering and demand for making research. These functions include basic services for registering business entities, publishing and retrieving offerings and demands, the searching and discovery of offerings according to specific research communities requirements, submitting and managing service orders as well as lateral functions like review, rating and recommendation. The service provide access and ordering capabilities for the following scopes: - Services of the EOSC-portal Exchange service catalogue (EOSC Portal Marketplace). The definition of the services in scope is defined by the EOSC-Future project service portfolio management process. These services are publicized and offered through the EOSC Portal. - The EOSC Portal Marketplace is complemented by the EOSC Portal website, which provides information content about the EOSC initiative.
Support	This activity is about running the business processes needed by the functionality of the Marketplace, this includes the workflow from service discovery to access: ● Gathering and maintenance of an up to date information for the services in the scope of the Marketplace, including services of the EGI external service catalogue and other services from service providers willing to participate to the EOSC enlisted through the

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

	EOSC Portal, and services from the EOSC-portal consortium and collaborations. ● Handling of support to service providers and users, including the handling of service quote requests, and the support to providers that require the enlisting of their services (service definition, service validation, service registration). ● Accountability of CYFRONET is limited to: ▪ Delivering technical services within the agreed service level targets; ▪ Operations activity related strictly to technical services. ▪ Software maintenance. ▪ Support related to technical services issues and services requests.
Coordination	The activity will coordinate with: ● In the EOSC Portal context: the operators of other components of the EOSC Portal, e.g. partners of the e-InfraCentral project and follow-on projects, for coordinated joint support to users and service providers. ● In the EGI context: the managers of relevant EGI Service Management System Processes like Service Portfolio Management, SLA Management, Service Report Management, Customer Relationship Management, and Supplier, Federation Member Relationship Management. ● Service providers and technology providers for the integration of services into the Marketplace. ● The EOSC-Future project for the policy, operational and user requirements
Operations	The activity will take care of the daily running and maintenance of the Marketplace. These services may require sub-components: e.g. authentication modules, database back-end, therefore services require multiple hosts (a good approximation is 2 for each service). The operational requirements include for the Marketplace and the EOSC Portal Website ● The provisioning of a high availability configuration for all the service configuration items: there are three VMs served in the data centre zone dedicated for production services, spread on

	more than one physical nodes. The physical nodes are connected with two separate network links to two different switches. ● Storage is provided from datacentre HSM solutions: this supports failover on various levels. A standard daily backup policy is applied and includes all relevant data. ● Installation (both hardware and software services) is under monitoring including performance and capacity monitoring. In case of growing usage upgrade of capacity and/or new instances under load balancer can be provided. ● Implementation of all the measures for mitigating the risks listed in the Availability and Continuity Plan for the Marketplace[2]
Software Maintenance	● Requirements gathering ● Documentation ● Bug fixing, proactive maintenance, and deployment of software updates

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 Units:

- EOSC Portal (Content Component)
- EOSC Portal (Provider Component)
- EOSC Portal (Technical Support)
- EOSC Portal (User Component - Marketplace)

Support is available between:

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

This excludes common public holidays of all organizations involved in the provisioning of the services.

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

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

3.1 Incident handling

The response to incidents will be handled according to the following response times:

Incident Priority	Response Time
Less urgent	5 working days
Urgent	1 working day
Very urgent and Top Priority	4 hours

3.2 Service requests

The response to service requests will be handled according to the following response times:

Service request Priority	Response Time
Less urgent	5 working days
Urgent	1 working day
Very urgent and Top Priority	4 hours

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): 90%

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

- See Section 3

5 Limitations and constraints

As defined by 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.

EGI Foundation contact	Matthew Viljoen operations@egi.eu
Component Providers contact	CYFRONET: Bartosz Wilk b.wilk@cyfronet.pl Roksana Wilk r.wilk@cyfronet.pl Wojciech Ziajka w.ziajka@cyfronet.pl
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.
- 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

[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

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

    - 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:

- Adhere to all applicable operational and security policies and procedures[11] and to other policy documents referenced therein;
- Use communication channel defined in the agreement;
- Attend relevant operations meeting when needed;
- Accept EOSC monitoring services provided to measure fulfilment of agreed service level targets.
- Service endpoints with associated roles are registered in GOCDB[12] as a site entity 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.
- 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.

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

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

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

    - 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.
- Component Providers should have clear interfaces with the EGI Service Management System processes and provide the required information.
- Component Providers should commit to improving their management system used to support the services they provide.

8.2 Of EGI Foundation

The responsibilities of EGI Foundation are:

- Delivering and planning the Services according to a Service Management System meeting the requirements of FitSM[14].
- Raise any issues deemed necessary to the attention of the Component Provider;
- 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 this Agreement and targets will be reviewed on a yearly basis

[14] https://www.fitsm.eu/

- 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.