EGI Foundation

DataHub

OPERATIONAL LEVEL AGREEMENT

Customer	EGI Foundation
Provider	**CYFRONET**
Start Date	1st April 2021
End Date	30th June 2023
Status	Final
Agreement Date	26th May 2021
OLA Link	https://documents.egi.eu/document/3672

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
v0.1	2018/07/05	First version	Baptiste Grenier
v0.2	2018/11/21	Some corrections	Alessandro Paolini
v0.3	2019/05/22	Update service description	Baptiste Grenier
v1.0	2019/08/14	Updated terminology about roles, addressed Yannick's comments, updated Violations, Escalations, and Complaints sections, extended duration until Dec 2020.	Alessandro Paolini
v1.1	2020/09/28	updated EGI and Cyfronet contacts, extended OLA last day of delivery. Updated Support unit name	Andrea Manzi
v2.0	2021/03/16, 2021/05/26	Covering EGI ACE from Apr 2021 to June 2023; updated section 1; renamed EGI Corporate Level as EGI Default OLA; updated section 7 on security requirements; changed frequency of the reports; A/R targets are 99%; 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, Andrea Manzi

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

The Agreement was discussed and approved by EGI Foundation and the Component Provider **26th May 2021**.

The Component Provider(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 following service components are made available: ● EGI DataHub Onezone instance: https://datahub.egi.eu ● EGI DataHub "default/central" Oneprovider instance: https://plg-cyfronet-01.datahub.egi.eu/ The Onezone instance is able to federate providers deployed by other EGI participants. It provides the main interface allowing users to manage their accounts and to discover spaces and providers. The Oneprovider instance is used to provide storage to some spaces depending on agreements between the provider, the consumers and EGI Foundation.
Coordination	This activity is responsible for the coordination of the service maintenance activities with the EGI operations team and other relevant technology providers.
Operation	Daily running of the system, including: ● supporting Oneproviders operators to connect to the EGI DataHub Onezone, ● enabling access for new VO/user groups having an agreement for accessing the service, ● Providing storage space on the "default/central" provider to users according to future agreements between the provider, the consumers and EGI Foundation,

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

	• maintaining integration with the EGI Check-in to satisfy AAI requirements, • putting in place announcements related to the services' operations (update, downtime…) on the Onezone page. • Provisioning of a high availability configuration ○ Onezone is operated by 4 VMs, two for database redundancy, two for service redundancy • Creating an Availability and Continuity Plan and implementing countermeasures to mitigate the risks defined in the related risk assessment[2]
Maintenance	• Maintenance, bug fixing, implementation of required and agreed Onedata features. • Proactive maintenance of the services being operated, following EGI policies and procedures. • 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

As defined by the EGI Default Operational Level Agreement.

Support is provided via EGI Service Desk[3] Support Unit: DataHub.

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.

[2] https://wiki.egi.eu/wiki/Services_Availability_Continuity_Plans

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

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 Services in the scope of this Agreement.

Service Provider contact	Andrea Manzi techsolutions@egi.eu Data Solutions Manager
Component Provider contact	Lucasz Dutka lukasz.dutka@cyfronet.pl
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)	Provider	Survey form prepared by EGI Foundation

All reports shall follow predefined templates[4].

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 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 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 the Service Provider 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.

[4] https://documents.egi.eu/document/2881

The following rules for Information Security and data protection should be enforced when they are applicable:

- The Component Provider agrees to make every effort to maximise security level of users' data and minimise possible harm in the event of an incident.
- EGI Foundation holds the role of the Data Controller while the Component Provider holds the role of Data Processor. Data Processing Agreements 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[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 Component Provider must enforce the EGI WISE Acceptable Usage Policies[7].
- The Component Provider 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 Component Provider 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 Component Provider

Additional responsibilities of the Component Provider are as follows:

- Adhering to all applicable operational and security policies and procedures[10] and to other policy documents referenced therein.

[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

- Using the communication channels defined in this Agreement.
- Attending OMB[11] and other operations meeting when needed
- Accepting EGI monitoring services provided to measure fulfilment of agreed service level targets.
- The Service endpoints 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.

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[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 through 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.

[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

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

- 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 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 the Service Provider 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.