EGI Foundation

CVMFS Stratum-0

Operational level Agreement

Service Provider	EGI Foundation
Component Provider	UKRI
First day of service delivery	1/01/2021
Last day of service delivery	30/06/2023
Status	FINAL
Agreement finalization date	24/02/2021
Agreement Link	https://documents.egi.eu/document/3672

Issue	Date	Comment	Author
FINAL	1.09.2016	Final version	Giuseppe La Rocca Małgorzata Krakowian
	06/12/2017	Discussing one year extension, until Dec 2018	Alessandro Paolini
v1.1	22/01/2018	OLA extended until Dec 2018, added some information about HA configuration	Alessandro Paolini, Catalin Condurache
v1.2	30/01/2019	Yearly review, 1 year extension until Dec 2019	Alessandro Paolini, Catalin Condurache
v1.3	03/12/2019	yearly review, 1 year extension until Dec 2020, updated Component Provider contact, updated Violations, Escalations and Complaints sections.	Alessandro Paolini
v2.0	04/12/2020, 25/02/2021	Covering EGI ACE from Jan 2021 to June 2023; updated section 7 on security requirements; added the reporting section; changed frequency of the reports; added Software and ITSM compliance in section 8; added requirement in section 8 about controlled changes to the service; in section 9 the requirement about periodic supplier process audits conducted by EGI Foundation; mentioned in section 1 the need of AvCo plan	Alessandro Paolini, Catalin Condurache, Ian Collier

TERMINOLOGY

The EGI glossary of terms is available at: https://wiki.egi.eu/wiki/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 **UKRI (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 **1/01/2021** to **30/06/2023**.

The Agreement was discussed and approved by EGI Foundation and the Component Provider **24/02/2021.**

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	The CernVM File System (CernVM-FS or CVMFS) is a read-only file system designed to deliver scientific software onto virtual machines and physical worker nodes in a fast, scalable, and reliable way.
	CernVM-FS is a file system with a single source of data. This single source, the repository Stratum-0, is maintained on a dedicated release manager machine or CVMFS Uploader.
	The CVMFS Uploader is hosted by a server that offers read-write access to the repository maintainers via a GSI interface.
	The Stratum-0 server is publishing the current state of the repository from the release manager machine and is hosted by a node providing Scientific Linux OS, AUFS-enabled kernel (maintained by CERN developers), Apache HTTP server and specific CernVM-FS packages (maintained and distributed by CERN).
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.
Operation	- Daily running of the system. - Automated back-up process for each CVMFS repository on Uploader server - Critical parts of the service are part of the 365/24/7 RAL Tier-1 monitoring (host status, httpd status)

---

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

	● Creating an Availability and Continuity Plan[2] and implementing countermeasures to mitigate the risks defined in the related risk assessment
Maintenance	• Bug fixing, proactive maintenance, improvement of the system. • Maintenance of probes to test the functionality of the service. • Requirements gathering and development based on such

2 Service hours and exceptions

As defined in EGI Default Operational Level Agreement.

3 Support

Support is provided via EGI Service Desk[3] Support Unit: Software and Data Distribution (CVMFS)

Support is available between:

- Monday and Friday
- 09:00 and 17:00 GMT/BST

This excludes public holidays at the same time in all organizations providing the service. During holidays of supporting staff, support will be provided on a best effort basis.

3.1 Incident handling

As defined in EGI Default Operational Level Agreement.

3.2 Service requests

As defined in 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.

---

[2] https://wiki.egi.eu/wiki/Services_Availability_Continuity_Plans
[3] http://helpdesk.egi.eu/

- 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): 97%

Quality of Support level

- Medium (Section 3)

5 Limitations and constraints

As defined in 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	Alessandro Paolini: operations@egi.eu
Component Provider contact	Ian Collier: ian.collier@stfc.ac.uk Alastair Dewhurst: alastair.dewhurst@stfc.ac.uk
Service Support contact	See Section 3

6.2 Regular reporting

As part of the fulfilment of this Agreement and provisioning of the service, 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 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 EGI Foundation 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 violation 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.
- EGI Foundation 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 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 in EGI Default Operational Level Agreement.

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).

---

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

- 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 follow:

- Adhere to all applicable operational and security policies and procedures[10] and to other policy documents referenced therein.
- Use communication channels defined in the agreement.
- Attend OMB[11] and other operations meetings when needed.
- Accept EGI monitoring services provided to measure fulfilment of agreed service level targets.

---

[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

- Service with associated roles are registered in GOC DB[12] as site entity under EGI.eu Operations Centre hosting EGI central operations tools[13]
- Whilst the responsibility to maintain a master copy of the repository relies with the repository maintainers, the Component Provider should have in place a backup mechanism of the repository, so it could, at maintainers' request, provide a copy no older than 14 days of the repository.
- Shall ensure protection against data corruption at CVMFS Uploader and Stratum-0 server level.
- Due to the specifics of the CernVM File System, there is no read protection of the data as the repository has to be configured world-readable.
- 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 (like MIT, BSD, Apache 2.0,...).
- The license 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 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 FitSM, ITIL, ISO 20000 etc.
- Key staff and service owners should have advanced/professional training and certification covering the key processes for their services.

---

[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 SMS 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 the EGI Foundation are:

- 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 EGI Foundation 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 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 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.