



EGi Foundation

CVMFS Stratum-0

Operational level Agreement

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



This work by EGI Foundation is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

This template is based on work, which was released under a Creative Commons 4.0 Attribution License (CC BY 4.0). It is part of the FitSM Standard family for lightweight IT service management, freely available at www.fitsm.eu.

DOCUMENT LOG

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
v2.1	28/02/2022	yearly review; introduced the term Service Supplier; updated section 7 and section 8; corrected some typos; updated the contacts section;	Jose Caballero, 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

Contents

1	The Services	4
2	Service hours and exceptions	5
3	Support.....	5
3.1	Incident handling	5
3.2	Service requests.....	5
4	Service level targets	5
5	Limitations and constraints.....	6
6	Communication, reporting and escalation	6
6.1	General communication	6
6.2	Regular reporting	6
6.3	Violations	7
6.4	Escalation and complaints	7
7	Information security and data protection	7
8	Responsibilities	8
8.1	Of the Service Supplier.....	8
8.1.1	Software compliance	9
8.1.2	IT Service Management compliance.....	10
8.2	Of EGI Foundation.....	10
9	Review, extensions, and termination	10

The present Agreement (“the Agreement”) is made between **EGI Foundation (the Service Provider)** and **UKRI (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 **1/01/2021** to **30/06/2023**.

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

The Service Supplier is bound by the terms and conditions of the EGI Default Operational Level Agreement¹ supplemented by the terms and conditions of this Agreement:

1 The Services

The Services are defined by the following properties:

Technical	<p>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.</p> <p>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.</p> <p>The CVMFS Uploader is hosted by a server that offers read-write access to the repository maintainers. While authentication and authorisation is currently granted via a GSI interface, the service will be integrated with EGI Check-in and other federated, token-based, Identity Manager services.</p> <p>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, Apache HTTP server and specific CernVM-FS packages (maintained and distributed by CERN).</p>
Coordination	<p>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.</p>
Operation	<ul style="list-style-type: none"> ● Daily running of the system. ● Automated back-up process for each CVMFS repository on Uploader server ● Critical parts of the Services are part of the 365/24/7 RAL Tier-1 monitoring (host status, httpd status)

¹ <https://documents.egi.eu/document/2752>

	<ul style="list-style-type: none"> • Creating an Availability and Continuity Plan² and implementing countermeasures to mitigate the risks defined in the related risk assessment
Maintenance	<ul style="list-style-type: none"> • Bug fixing, proactive maintenance, improvement of the system. • Maintenance of probes to test the functionality of the service. • Requirements gathering

2 Service hours and exceptions

As defined by the EGI Default Operational Level Agreement.

3 Support

Support is provided via EGI Service Desk³ 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 organisations providing the service. During holidays of supporting staff, support will be provided on a best effort basis.

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): 95%

² <https://confluence.egi.eu/x/3YOoBw>

³ <http://helpdesk.egi.eu/>

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 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 contact	Ian Collier: ian.collier@stfc.ac.uk Alastair Dewhurst: alastair.dewhurst@stfc.ac.uk Jose Caballero: jose.caballero@stfc.ac.uk cvmfs-support@gridpp.rl.ac.uk
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	10 months (first report covering the period Jan – Oct 2021))	Service Supplier	Survey form prepared by EGI Foundation

	achieved during the reference reporting period			
--	--	--	--	--

All reports shall follow predefined templates⁴.

6.3 Violations

The Service Supplier 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 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.
- 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 Service Supplier 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 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

⁴ <https://documents.egi.eu/document/2881>

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 SEC01⁵ 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 Data⁶ 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)⁷.
- The Service Supplier must enforce the EGI WISE Acceptable Usage Policies⁸.
- The Service Supplier shall comply with all principles set out by the GÉANT Data Protection Code of Conduct⁹ in its most current version, which will be made available to the Component Provider by EGI Foundation upon request.
- The Service Supplier must meet all requirements of any relevant EGI policies or procedures¹⁰ 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 procedures¹¹ and to other policy documents referenced therein.
- Using the communication channels defined in this Agreement.

⁵ <https://go.egi.eu/sec01https://wiki.egi.eu/wiki/SEC01>

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/Data+Protection+Code+of+Conduct+Home>

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

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

- Attending OMB¹² 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 DB¹³ as site entity under the EGI.eu Operations Centre hosting EGI central operations tools¹⁴.
- Whilst the responsibility to maintain a master copy of the repository relies with the repository maintainers, the Service Supplier 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.
- The Service Supplier 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.
- 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

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 GitHub¹⁵.) All releases should be appropriately tagged.
- Adopt best practises:
 - 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.

¹² <https://confluence.egi.eu/display/EGIBG/Operations+Management+Board>

¹³ <http://goc.egi.eu/>

¹⁴ https://goc.egi.eu/portal/index.php?Page_Type=NGI&id=4

¹⁵ <https://github.com/EGI-Foundation>

- 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 practises 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 improving their management system used to support the services they provide.

8.2 Of EGI Foundation

The responsibilities of the EGI Foundation 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.
- 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 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 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 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 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 supplier / federation member will not be reimbursed.