EGI Foundation

Data Transfer

Operational level Agreement

Service Provider	EGI Foundation
Component Provider	**CERN, UKRI**
First day of service delivery	1st January 2021
Last day of service delivery	30th June 2023
Status	FINAL
Agreement finalization date	26th May 2021
Agreement Link	https://documents.egi.eu/document/3672

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
0.1	2018/07/03	First version	Baptiste Grenier
0.2	2018/07/03	Review	Alessandro Paolini
0.3	2018/08/17	Address comments	Baptiste Grenier
0.4	2018/09/18	Update according to CERN's feedback	Baptiste Grenier
0.5	2018/09/26	Update according to CERN's feedback	Baptiste Grenier
0.8	2018/12/05	Update according to UKRI(STFC)'s feedback; new template.	Alessandro Paolini
1.0	2019/02/18	Document finalised	
1.1	2020/01/30	yearly review; OLA extension until Dec 2020, updated Component Provider contacts, updated Violations, Escalations and Complaints sections.	Alessandro Paolini
2.0	2020/12/10, 2021/05/26	Covering EGI ACE from Jan 2021 to June 2023; updated section 7 on security requirements; changed frequency of the reports; 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, Luca Mascetti

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 **CERN, 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 **1st January 2021** to **30th June 2023**.

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

The Component Providers 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 services are made available to users for managing their data transfers: ● FTS3 is a low-level data management service, responsible for scheduling reliable bulk transfer of files from one site to another while allowing participating sites to control the network resources usage. FTS3 can be accessed through CLI or REST API. (CERN, UKRI). ● WebFTS is a web-based file transfer and management solution which allows users to invoke reliable, managed data transfers on distributed infrastructures. WebFTS uses an FTS3 endpoint as a transfer engine. (CERN)
Coordination	● This activity is responsible for the system operation and upgrade activities of the aforementioned services.
Operation	● Daily running and maintenance of the system, including managing updates and support. ● Support for new VOs must be explicitly requested as they need to be configured in WebFTS and on the FTS cluster nodes (vomses files). ● CERN ○ FTS3 is deployed as a load-balanced alias across a number of machines (4 at time of writing). ○ WebFTS is a single instance. ● UKRI ○ FTS3 service is provided as a HA Proxy load-balanced alias across a pool of servers

[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.

2 Service hours and exceptions

As defined in the EGI Default Operational level Agreement.

3 Support

As defined in the EGI Default Operational Level Agreement.

Support is provided via the following EGI Service Desk[3] Support Unit: Data Transfer.

Access requires a valid X.509 or the login via an EGI CheckIn account[4].

The service support is available between:

- Monday and Friday
- 09:00 and 17:00 CET/CEST time for CERN
- 09:00 and 17:00 GMT/BST time for UKRI

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 the EGI Default Operational Level Agreement.

3.2 Service requests

As defined in the EGI Default Operational Level Agreement.

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

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

[4] https://docs.egi.eu/providers/check-in/

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% (CERN), 95% (UKRI)

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% (CERN), 97% (UKRI)

Quality of Support level

- Medium (Section 3)

5 Limitations and constraints

As defined in 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	Baptiste Grenier operations@egi.eu Senior Operations Officer
Component Provider contact	● CERN ○ Edward Karavakis Edward.Karavakis@cern.ch FTS project leader ○ Oliver Keeble Oliver.Keeble@cern.ch ○ Luca Mascetti luca.mascetti@cern.ch ● UKRI ○ Alastair Dewhurst alastair.dewhurst@stfc.ac.uk

	○ Ian Colllier ian.collier@stfc.ac.uk FTS Service Managers
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)	Component Provider	Survey form prepared by EGI Foundation

All reports shall follow predefined templates[5].

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 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 EGI Foundation

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

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[6].
- EGI Foundation holds the role of the Data Controller while the Component Provider holds the role of Data Processor. Data Processing Agreements[7] 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[8] 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)[9].
- The Component Provider must enforce the EGI WISE Acceptable Usage Policy[10].
- The Component Provider shall comply with all principles set out by the GÉANT Data Protection Code of Conduct[11] version 1.0.
- The Component Provider must meet all requirements of any relevant EGI policies or procedures[12] 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

[6] https://wiki.egi.eu/wiki/SEC01

[7] https://documents.egi.eu/document/3755

[8] https://documents.egi.eu/public/ShowDocument?docid=2732

[9] https://aarc-project.eu/policies/policy-development-kit/

[10] https://documents.egi.eu/public/ShowDocument?docid=3600

[11] https://wiki.refeds.org/display/CODE/Code+of+Conduct+for+Service+Providers

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

    - 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[13] and to other policy documents referenced therein.
- Using the communication channels defined in this Agreement.
- Attending OMB[14] 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[15] as site entity under the EGI.eu Operations Centre hosting EGI central operations tools[16].
- 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[17].) 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 or Puppet, ...
    - Taking security aspects into consideration through at every point in time.
    - Having automated testing in place.
    - Using code reviewing.
    - Treating documentation as code.

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

[14] https://wiki.egi.eu/wiki/OMB

[15] http://goc.egi.eu/

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

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

    - Documentation should be available for Developers, administrators and end users.

8.1.2 IT Service Management compliance

With regards to the production service delivered by UKRI:

- 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 the customer 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 the agreement and targets will be reviewed on a yearly basis.

- With regards to the production service delivered by UKRI, 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.