EGI Foundation

Service Monitoring

OPERATIONAL LEVEL AGREEMENT

Customer	EGI Foundation
Argo Service Providers	**GRNET, SRCE, CNRS**
Start Date	1 January 2021
End Date	30 June 2023
Status	FINAL
Agreement Date	16th September 2021
OLA Link	https://documents.egi.eu/document/3672

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
			Małgorzata Krakowian
			Peter Solagna
1.1	13/06/2017	First review, added a reference to the availability and continuity plans	Alessandro Paolini
2.0	17/11/2017, 27/06/2018	New OLA covering 2018-2020 Period	Alessandro Paolini, Kostas Koumantaros
2.1	07/10/2019	yearly review: introduced the roles Service Provider and Component Provider, updated sections on Violations, Escalations, and Complaints	Alessandro Paolini
3.0	11/12/2020, 16/09/2021	Covering EGI ACE from Jan 2021 to June 2023; renamed EGI Corporate Level as EGI Default OLA; 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; changed the roles name: “Customer” for EGI Foundation, “Argo Service Providers” for the federation members.	Alessandro Paolini, Kostas Koumantaros
3.1	01/11/2022	Yearly review; updated some links; updated section 7	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

The present Operational Level Agreement ("the Agreement') is made between **EGI Foundation (the Customer)** and **GRNET, SRCE, CNRS (the Argo Service Providers),** who jointly operate the ARGO Service, 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 2020** to **30th June 2023**.

The Agreement was discussed and approved by the Customer and the **the Argo Service Providers 16th September 2021**

The **Argo Service 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	ARGO Monitoring is a distributed system supporting EGI/NGI operations. It provides remote monitoring of services, visualisation of the service status, Operations portal interfacing and generation of availability and reliability reports. The central monitoring services are needed to ensure the aggregation of all EGI metric results and the access to the data at an EGI-wide scope through the central ARGO user interface. These results are exposed through the central ARGO web service and its programmatic interface (JSON supported). On top of that, the ARGO Reporting System generates monthly availability reports about sites and operational tools for use by the service owners. In addition to the central services described above, the activity provides also: ● Monitoring of EGI.eu technical services: a centralised installation in high availability is currently running in production to monitor the performance of EGI.eu operations tools and user community support tools. ● Maintenance and Deployment of probes as required to support operations activities as requested by EGI Operations coordination: ○ Maintenance of existing operations probes ○ Requirements gathering ● A notification service to inform Service Providers for possible errors/problems.
Coordination	The activity will have to coordinate with:

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

	• EGI Operations for the support of the operational activities with monitoring data, and for the planning of new releases and updates of the monitoring system • With the service developers to support them in the development of probes for their services • With the other operational tools where interaction is necessary (for example messaging network, GOCDB)

Operation	• Daily running of the system
	  ○ Monitor Services (Site, NGIs, Service_Groups)
	  ○ Availability/Reliability computation engine
	  ○ User interface to browse the data
	• Provisioning of a high availability configuration
	  ○ Min. two ARGO Monitoring boxes for the monitoring of the services. The ARGO Monitoring boxes are deployed all in two different sites.
	• Implementing all the measures to mitigate the risks listed in the Availability and Continuity Plan for the Service Monitoring document[2]
	• The monitoring infrastructure must allow to test new probes without affecting the production monitoring
	• Deployment in production of the releases of the monitoring system (ARGO). At least 2 per year, given that there are new versions of ARGO released.

Maintenance	This activity includes: • bug fixing • maintenance of probes to test the functionality of the service • integration (configuration and packaging) of new probes into ARGO • coordination of software maintenance activities with other technology providers of the Operational tools part of the EGI Core Infrastructure or remote systems deployed by integrated and peer infrastructures that interoperate with the central EGI components of the system (on a best effort basis for the peer infrastructures providers interoperability). • Producing the monthly reports on the performances of the resource centres, NGI central services and EGI central tools requirements gathering • documentation

[2] https://confluence.egi.eu/x/MYSoBw

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: Monitoring (ARGO)

Support is available between:

- Monday and Friday
- 9:00 and 17:00 EET/EEST time

This excludes public holidays at the same time in all organisations providing the service.

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) for the ARGO Monitoring Engine: 99%
- Minimum (as a percentage per month) for the ARGO User Interface: 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) for the ARGO Monitoring Engine: 99%
- Minimum (as a percentage per month) for the ARGO User Interface: 95%

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

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.

Customer contact	Alessandro Paolini operations@egi.eu
Argo Service Providers contact	Kostas Koumantaros: kkoum@grnet.gr Themis Zamani: themis@grnet.gr Emir Imamagic: eimamagi@srce.hr Cyril L'Orphelin: cyril.lorphelin@cc.in2p3.fr
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)	ARGO Service Providers	Survey form prepared by EGI Foundation

6.3 Violations

The **Argo Service Providers** commit to inform the Customer 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 Argo Service Providers will provide justifications and a plan for Services enhancement to the Customer. The Argo Service Providers 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 Customer 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 Argo Service Providers 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 Argo Service Providers 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 Argo Service Providers, 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 Argo Service Providers:

- The Argo Service Providers must 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 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 SEC01[4] procedure.
- EGI Foundation holds the role of the Data Controller while the Argo Service Providers holds the role of Data Processor. Data Processing Agreements[5] covering the provided services must be signed between EGI Foundation (the Data Controller) and Argo Service Providers (the Data Processors).

[4] https://go.egi.eu/sec01

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

- The Argo Service Providers 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 Argo Service Providers must enforce the EGI WISE Acceptable Usage Policy[8].
- The Argo Service Providers shall comply with all principles set out by the GÉANT Data Protection Code of Conduct[9] version 1.0.
- The Argo Service Providers 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
    - EGI-doc-2934: Security Traceability and Logging Policy
    - EGI-doc-2935: Security Incident Response Policy
    - SEC01: EGI CSIRT Security Incident Handling Procedure

8 Responsibilities

8.1 Of the Argo Service Providers

Additional responsibilities of the Argo Service Providers are as follow:

- Adhering to all applicable operational and security policies and procedures[11] and to other policy documents referenced therein.
- Using the communication channels defined in this Agreement.
- Attending OMB[12] and other operations meeting when needed
- Accepting EGI monitoring services provided to measure fulfilment of agreed service level targets.

[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://confluence.egi.eu/display/EGIPP/EGI+Policies+and+Procedures+Home
[11] https://confluence.egi.eu/display/EGIPP/EGI+Policies+and+Procedures+Home
[12] https://confluence.egi.eu/display/EGIBG/Operations+Management+Board

- The Service endpoints with associated roles is registered in GOC DB[13] as site entity under the EGI.eu Operations Centre hosting EGI central operations tools[14].
- 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 licence (e.g. MIT, BSD, Apache 2.0,...).
- Allow to grant unlimited access and exploitation rights upon request.
- 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[15].) 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 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.
- Argo Service Providers should have clear interfaces with the EGI Service Management System processes and provide the required information.
- Argo Service Providers should commit to improving their management system used to support the services they provide.

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

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

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

8.2 Of the Customer

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 Argo Service Providers.
- 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. 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.