EGI Foundation

Helpdesk human support

OPERATIONAL LEVEL AGREEMENT

Service Provider	EGI Foundation
Component Provider	**CESNET**
Start Date	1st January 2021
End Date	30th June 2023
Status	FINAL
Agreement Date	24th February 2021
OLA Link	https://documents.egi.eu/document/3672

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
			Małgorzata Krakowian
1.1	18/05/2017	Yearly review, added the provider contacts	Alessandro Paolini
2.0	11/12/2017	New OLA covering 2018, 2019, 2020 years	Alessandro Paolini
2.1	27/06/2018	Changed the reporting period to 9 months	Alessandro Paolini
2.2	16/12/2019	yearly review; introduced the Service Provider and the Component Provider roles; updated Violations, Escalation, and Complaints sections; Corporate-level EGI OLA renamed to EGI Default OLA	Alessandro Paolini
3.0	11/12/2020, 24/02/2021	Covering EGI ACE from Jan 2021 to June 2023; updated section 1; updated section 7 on security requirements; changed frequency of the reports; added in section 9 the requirement about periodic supplier process audits conducted by EGI Foundation	Alessandro Paolini, Baptiste Grenier, Zdenek Sustr

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 Operational Level Agreement ("the Agreement') is made between **EGI Foundation (the Service Provider)** and **CESNET (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 Component Provider **24th February 2021.**

The 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	First level support is responsible for ticket triage and assignment. Ticket triage must be regularly and continuously provided during business days. The first-level assigner is responsible for initial analysis of the incoming ticket, requesting additional information from the submitter, and assigning the ticket to 2nd level experts to resolve, to NGIs or specific service managers in case of operational incidents, to VO managers in case of VO membership issues, etc. Tickets should be reassigned mostly when there is a clear action for a specific support unit, when the analysis of the issue identified a software bug, or when after the initial support to the user no solution can be found. If reassigned, the helpdesk support must ensure that the issue is clear and that the user provided all the information needed. The support should be provided for the user facing services, such as HTC services, cloud, storage and authentication issues. Second level support is provided through the DMSU support unit for software services comprising the EGI Core, Cloud and Community platforms. Second level support deals with configuration and deployment issues or suspected software defects. In case a software defect is indeed confirmed, the ticket is reassigned to the appropriate 3rd level support unit to fix. Otherwise, the issue is resolved at 2nd level.
IT Service	● The component provider is certified for ISO27000 and ISMS

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

Management	● Key personnel is trained in ITIL (in the 1 St level support team) and FitSM (in the 2 nd level support team). ● Additional team members may receive FitSM training as required.
Coordination	● This activity is also responsible for liaison with support teams in charge of 2nd level and 3rd level support aiming at timely and effective incident resolution. ● 1st level support will be provided by dedicated CESNET HelpDesk, and overseen by responsible personnel, who will also maintain 1st level support processes and knowledge base. ○ The HelpDesk (ServiceDesk) at CESNET operates non-stop to attend to requests by the NREN users, and performs 1st -level processing of incoming EGI-related issues. Service availability during business hours is thus assured, and 1 st level support outside business hours is also possible on a best effort basis. ● 2nd level support will be performed by CESNET's experts with long-term experience in service development, operation and support. ○ The core team providing 2nd level support during the current period will remain involved. ○ Responsible personnel at CESNET will provide adequate support and also liaise with product teams and external projects or organizations (such as EGCF, INDIGO, NorduGrid or UNICORE) in case support is required for their products.
Operation	1st level support: ● incoming support tickets will be checked for formal accuracy, and forwarded to the responsible 2nd level Support Unit. 2nd level support: ● members of the support team will monitor issues incoming into the 2nd level issue tracker (currently DMSU queue in GGUS), pick those for which they possess expertise, and initiate solution or involve other experts. ● Tickets unassigned in this way will be processed, at the very latest, during the nearest twice-weekly checkup pass. Experts in the 2nd level support team will also cooperate with EGI Operations to maintain the recently started Known Errors DataBase (KEDB)
Maintenance	n.a.

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 EGI Service Desk[2] Support Unit:

- For 1st level of support: TPM
- For 2nd level of support: DMSU

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 in the EGI Default Operational Level Agreement.

3.2 Service requests

As defined in the EGI Default Operational Level Agreement.

4 Service level targets

Quality of Support level for the TPM SU

- Maximum time to assign a ticket to a support unit within support hours: 1h
- Maximum response time to tickets that are internally handled by 1st level support: 1 h

Quality of Support level for the DMSU SU

- Medium

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

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 service in the scope of this Agreement.

Service Provider contact	Alessandro Paolini operations@egi.eu
Component Provider contacts	DMSU: Zdeněk Šustr sustr4@cesnet.cz TPM: Petr Hanousek petr.hanousek@cesnet.cz
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	10 months (first report covering the period Jan – Oct 2021)	Component Provider	Survey form prepared by EGI Foundation

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 Component Provider 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 by the same support unit 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 the 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).
- The Component Provider must comply with the EGI Policy on the Processing of Personal Data[3] 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)[4].
- The Component Provider must enforce the EGI WISE Acceptable Usage Policies[5].

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

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

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

- The Component Provider shall comply with all principles set out by the GÉANT Data Protection Code of Conduct[6] 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[7] 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[8] and to other policy documents referenced therein.
- Use communication channels defined in the agreement.
- Attend OMB[9] and other operations meetings when needed.
- Accept EGI monitoring services provided to measure fulfilment of agreed service level targets.

8.2 Of the Service Provider

The responsibilities of 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.

[6] https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home

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

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

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

- Provide 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. 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.