



## EGI DEFAULT OPERATIONAL LEVEL AGREEMENT

---

<b>Service Provider</b>	EGI Foundation
<b>Service Supplier</b>	EGI Federation member
<b>Status</b>	FINAL
<b>Start Date</b>	1/03/2016
<b>Document Link</b>	<a href="https://documents.egi.eu/document/2752">https://documents.egi.eu/document/2752</a>

---



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](http://www.fitsm.eu).

## DOCUMENT LOG

<b>Issue</b>	<b>Date</b>	<b>Comment</b>	<b>Author</b>
<b>FINAL</b>	17/02/2016	Final version	Małgorzata Krakowian
<b>v. 1.1</b>	16/03/2017	Yearly review	Alessandro Paolini
	30/04/2018	Yearly review, mentioned EGI ChekIn as login option to the EGI Helpdesk system	Alessandro Paolini
<b>v. 1.2</b>	26/11/2018	Change roles naming: Customer -> Service Provider Provider -> Component Provider	Małgorzata Krakowian
<b>v. 1.2.1</b>	15/01/2019	Some minor corrections	Alessandro Paolini
<b>v. 1.3</b>	29/11/2019	Document renamed "EGI Default OLA", updated the violations section	Małgorzata Krakowian, Alessandro Paolini
<b>v. 1.4</b>	14/02/2020	added in section 6 a rule about Data Controller and Data Processor roles, and the need to sign Data Processing Agreements; added requirement on CoCo compliance	Alessandro Paolini
<b>v 1.5</b>	11/06/2021 , 03/09/2021	updated some old links; updated section 6	
<b>v 1.6</b>	17/10/2022	The EGI Federation Member role is Service Supplier; updated some links; updated section 6	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	Service hours and exceptions.....	4
2	Support .....	4
2.1	Incident handling .....	4
2.2	Service requests .....	5
3	Service level targets .....	5
4	Limitations and constraints.....	6
5	Violations .....	6
6	Information security and data protection.....	6

This Default Level operational level agreement (OLA), the Agreement, is valid for all services provided to support business processes according to the current valid service catalogue, if no other agreements are in place. The Agreement may be extended or replaced by specific OLAs.

## 1 Service hours and exceptions

IT services according to the service catalogue are in general delivered during 24 hours per day, 7 days per week (i.e. 365 days or 8,760 hours), to seamlessly support business operations. Planned and announced interruptions may reduce the effective operating time of a service.

The following exceptions apply:

- Planned maintenance windows or service interruptions (“scheduled downtimes”<sup>1</sup>) will be notified via email in a timely manner i.e. 24 hours before the start of the outage<sup>2</sup>, to the Customer through the Broadcast Tool<sup>3</sup>.
- Downtime periods exceeding 24 hours need justification.
- Human services are provided during support hours.

## 2 Support

The services covered by the scope of this Agreement are provided with the following level of support.

Support is provided via EGI Helpdesk<sup>4</sup>. Access requires a valid X.509 or the login via an EGI Check-in account<sup>5</sup>.

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 organisations providing the service.

### 2.1 Incident handling

Incidents will be handled according to the Quality of Support level that is estimated according to the impact of the outage or service quality degradation.

---

<sup>1</sup> <https://docs.egi.eu/internal/configuration-database/downtimes/>

<sup>2</sup> <http://goc.egi.eu/>

<sup>3</sup> <https://operations-portal.egi.eu/broadcast>

<sup>4</sup> <http://helpdesk.egi.eu/>

<sup>5</sup> <https://docs.egi.eu/providers/check-in/>

The Quality of Support levels are defined as follows:

**Base level** defines a response time of 5 working days regardless of the GGUS ticket priority.

**Medium level:**

Incident priority <sup>6</sup>	Response time
Less urgent	5 working days
Urgent	5 working days
Very Urgent,	1 working day
Top Priority	1 working day

**Advanced level:**

Incident priority	Response time
Less urgent	5 working days
Urgent	1 working days
Very Urgent,	1 working day
Top Priority	4 working hours

Response time is provided as a service level target.

## 2.2 Service requests

In addition to resolving incidents, standard service requests (e.g. change requests, information requests, documentation) will be fulfilled through the defined support channels in the same way as incidents. Service requests are classified as “Less urgent”.

## 3 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): 80%

### Monthly Reliability

---

<sup>6</sup> <https://docs.egi.eu/internal/helpdesk/features/ticket-priority/>

- 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): 85%

#### Quality of Support level

- Medium

## 4 Limitations and constraints

The provisioning of the service under the agreed service level targets is subject to the following limitations and constraints:

- Support is provided in the following language: English
- Downtimes caused due to upgrades for fixing critical security issues are not considered Agreement violations.
- Force Majeure. A party shall not be liable for any failure or delay in the performance of this Agreement for the period that such failure or delay is due to causes beyond its reasonable control. Means any
  - fire, flood, earthquake or natural phenomena,
  - war, embargo, riot, civil disorder, rebellion, revolution
 which is beyond the Component Provider's control, or any other causes beyond the

Component Provider's control.

## 5 Violations

The Service Supplier 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 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.
- The Service Provider will notify the supporting Resource Centres in case of suspected violation via the EGI Helpdesk. The case will be analysed to identify the cause and verify the violation.

## 6 Information security and data protection

The following rules for Information Security and data protection must be enforced by the Service Supplier:

- The Service Supplier must make every effort to maximise the 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](mailto:ism@mailman.egi.eu) and will have to be reported to EGI CSIRT using [abuse@egi.eu](mailto:abuse@egi.eu) within 4 hours after their discovery and handled according to the SEC01 procedure<sup>7</sup>.
- EGI Foundation holds the role of the Data Controller while the Service Supplier holds the role of Data Processor. Data Processing Agreements<sup>8</sup> covering the provided services must be signed between EGI Foundation (the Data Controller) and the Service Supplier (the Data Processor).
- The Service Supplier must comply with the EGI Policy on the Processing of Personal Data<sup>9</sup> 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)<sup>10</sup>.
- The Service Supplier must enforce the EGI WISE Acceptable Usage Policy<sup>11</sup>.
- The Service Supplier must comply with all principles set out by the GÉANT Data Protection Code of Conduct<sup>12</sup> version 1.0.
- Security incidents affecting the services must be reported to [abuse@egi.eu](mailto:abuse@egi.eu) within 4 hours after their discovery and handled according to [SEC01: EGI CSIRT Security Incident Handling Procedure - EGIWiki](#)
- The Service Supplier must meet all requirements of any relevant EGI policies or procedures<sup>13</sup> 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](#)

---

<sup>7</sup> <https://go.egi.eu/sec01>

<sup>8</sup> <https://documents.egi.eu/document/3755>

<sup>9</sup> <https://documents.egi.eu/public/ShowDocument?docid=2732>

<sup>10</sup> <https://aarc-project.eu/policies/policy-development-kit/>

<sup>11</sup> <https://documents.egi.eu/public/ShowDocument?docid=3600>

<sup>12</sup> <https://wiki.refeds.org/display/CODE/Code+of+Conduct+for+Service+Providers>

<sup>13</sup> <https://confluence.egi.eu/x/iYZQC>