

**Technology Provider**

**Underpinning Agreement**

|  |  |
| --- | --- |
| **Service Provider** | EGI Foundation |
| **Technology Provider** | [please provide] |
| **Technology** | Support of [please provide] |
| **First day of service delivery** | [please provide] |
| **Last day of service delivery** | [please provide] |
| **Status** | [please provide] |
| **Agreement Link:** | [please provide] |

**DOCUMENT LOG**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Issue*** | ***Date*** | ***Comment*** | ***Author*** |
|  |  |  |  |

**TERMINOLOGY**

For the purpose of this document, 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. For a complete list of term definitions see the EGI Glossary (<http://go.egi.eu/glossary> ).

**Contents**

[1 Introduction 4](#_30j0zll)

[2 Scope of the services 4](#_1fob9te)

[3 Support 4](#_3znysh7)

[4 Service level targets 5](#_1t3h5sf)

[4.1 Targets for handling of security vulnerability 5](#_4d34og8)

[5 Limitations & constraints 5](#_2s8eyo1)

[6 Communication, reporting & escalation 6](#_17dp8vu)

[6.1 General communication 6](#_3rdcrjn)

[6.2 Agreement violations 6](#_26in1rg)

[6.3 Escalation & complaints 6](#_lnxbz9)

[7 Information security & data protection 7](#_35nkun2)

[8 Additional responsibilities of the Technology Provider 7](#_1ksv4uv)

[9 EGI Foundation responsibilities 7](#_44sinio)

[10 Review 8](#_2jxsxqh)

# Introduction

This agreement is made between [please provide] (the Technology Provider) and the EGI Foundation to cover the provision and support of the service as described hereafter. The relevant contacts and representatives may be found in section 6.1.

This agreement is valid from [please provide] to [please provide].

The Technology Provider retains the right to terminate the Agreement at any time. If parties agree to end the Agreement, then the Provider is no longer part of UMD or CMD Release Team.

The agreement is a document discussed and approved between the EGI Foundation, and the Technology Provider.

Amendments, comments and suggestions must be addressed tothe EGI Foundation contact given to the Technology Provider (see section 6.1).

# Scope of the services

This agreement applies to provision of support for following software:

* [please provide]
* [please provide]

# Support

Support is provided via the GGUS portal which is the single point of contact for infrastructure users to access the EGI Service Desk. The EGI Service Desk within GGUS is organized in Support Units (SU). Every SU is responsible for one or more services. The number and definition of the EGI SUs in GGUS is not regulated by this agreement and can change at any time to fulfil the EGI Incident and Problem Management requirements.

The SU name related to services is documented at Technology Provider wiki page[[1]](#footnote-1),[[2]](#footnote-2).

Service communication support is available:

• between Monday and Friday

• during the regular working hours of supporting organization

This excludes public holidays of the supporting organization.

Request for technical support for the Software in scope for this agreement will be handled according to an appropriate Quality of Support level based on priority of the incident[[3]](#footnote-3). In this context, the following guidelines apply:

* Three GGUS Quality of Support (QoS) levels have been defined, in terms of response time limits: base, medium and advanced[[4]](#footnote-4)
* The QoS levels apply to the service documented at Technology Provider wiki page.

# Service level targets

The following are the agreed service level targets for the service:

* QoS level (see section 3)

## Targets for handling of security vulnerability

Security vulnerabilities affecting UMD or CMD software are assessed by the EGI Security Vulnerability Group. Requests for fixing security vulnerabilities affecting the software provided by the Technology Provider will be handled accordingly to the Vulnerability Issue Handling Procedure[[5]](#footnote-5).

The software free from the vulnerability should be made available for releasing in UMD or CMD within a deadline determined by the risk category:

* Critical: timeline agreed ad hoc between EGI SVG and the Provider
* High: 6 weeks
* Moderate: 4 months
* Low: 1 year

# Limitations & constraints

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

* Support is provided in following language: English
* Failures in the normal operation of the service caused by failures in Federated Operations service components (i.e. GGUS) are not considered UA violations.
* Force Majeure. A party shall not be liable for any failure of 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 Provider's control, or any other causes beyond the Provider's control

# Communication, reporting & escalation

## General communication

The following contacts will be generally used for communications related to the service in the scope of this agreement.

|  |  |
| --- | --- |
| **EGI Foundation contact** | Matthew Viljoen  [operations@egi.eu](mailto:Operations@egi.eu)  EGI Foundation Service Delivery and Information Security Lead[[6]](#footnote-6) |
| **Technology Provider contact** | Documented at Technology Provider wiki page. |
| **Contact for service users** | According to defined support channels |

## Agreement violations

The Technology Provider commits to inform the EGI Foundation contact, if this agreement is violated or violation is anticipated. The following rules are agreed for communication in the event of agreement violation:

In case of violating the service targets specified in this document for three consecutive months it is requested to provide justifications and a plan for service enhancement. The violating party must provide to the EGI Foundation contact(see section 6.1) a status report and a plan for the improvement of the service within one month from the date of notification. The EGI Foundation will be notified of this situation.

## Escalation & complaints

For escalation and complaints, the defined EGI Foundation contact (see section 6.1) point shall be used, and the following rules apply:

* In case of violating the service targets for four consecutive months, review of the Agreement will be taken by EGI Foundation contact(see section 6.1) and reported to parties of the Agreement.
* Complaints should be directed to the EGI Foundation contact(see section 6.1).
* The EGI Foundation contact(see section 6.1) will be contacted in case of received complaints.

# Information security & data protection

A series of guidelines[[7]](#footnote-7) for software development should be considered when developing a product for the EGI Federation. In particular, for what concerns the security aspects:

* Security best practices must be taken into account.
* Security-related aspects must be considered from the beginning.
* Security issues must be addressed with priority and following the EGI SVG recommendations and must take into account the points mentioned in the SVG Secure Coding[[8]](#footnote-8) and Software Security Checklist[[9]](#footnote-9).
* The Open Web Application Security Project (OWASP) provides extensive documentation, standards (such as ASVS) and tools to ensure that your software has capabilities to defend its usage against common attacks.

The following rules for information security and data protection apply:

* The software must allow data protection policies to be adhered to and in particular support configurable log retention periods, possibly with anonymization of long-lived records.

# Additional responsibilities of the Technology Provider

Additional responsibilities of the Technology Provider are as follow:

* Adhere to all applicable operational and security policies and procedures and to other policy documents referenced therein.
* Use communication channel defined in the agreement (see section 6.1).
* Accept EGI monitoring services provided to measure fulfilment of agreed service level targets.
* Handle security issues in timely manner.
* Deliver service components according to EGI Software Component Delivery procedure[[10]](#footnote-10).

# EGI Foundation responsibilities

The responsibilities of the EGI Foundation are:

* Raise any issues deemed necessary to the attention of the Technology Provider;
* Provide monitoring to measure fulfilment of agreed service level targets.
* Provide the EGI Service Desk, through the GGUS portal
* Provide the Unified Middleware Distribution (UMD) or Cloud Middleware Distribution (CMD), that integrates Provider services, after successfully passed through the UMD or CMD Software Provisioning Process[[11]](#footnote-11) and is deployed on the EGI’s production e-infrastructure
* Provide the UMD or CMD software provisioning infrastructure composed of:
  + UMD or CMD repositories, supporting multiple operating systems
  + Community repositories - through EGI Artefact Registry Service[[12]](#footnote-12) Provider has access to a repository-as-a-service platform to upload their software release
  + Web front-end – containing information about UMD or CMD releases (release notes, list of components, configuration configuration)
* Communicate collected and prioritized requirements and use cases from the EGI community.
* Define generic and specific acceptance criteria related to all software components contributed to EGI.
* Involve the Technology Provider in the triaging of the issues mentioned above through the appointed EGI second level support team.
* Provide access to boards, process and knowledge of EGI’s Software Vulnerability Group[[13]](#footnote-13) to the Technology Provider in order to develop and contribute corrections necessary to the maintained software components.

# Review

There will be reviews of the service performance against service level targets and of this SLA at planned intervals with the EGI Foundation according to the following rules:

* Content of the agreement and targets will be reviewed on a yearly basis.

1. <https://confluence.egi.eu/x/eIILCQ> [↑](#footnote-ref-1)
2. <https://confluence.egi.eu/x/foILCQ> [↑](#footnote-ref-2)
3. <https://docs.egi.eu/internal/helpdesk/features/ticket-priority/> [↑](#footnote-ref-3)
4. <https://docs.egi.eu/internal/helpdesk/features/quality-of-support-levels/> [↑](#footnote-ref-4)
5. <https://documents.egi.eu/document/2538> [↑](#footnote-ref-5)
6. <https://goc.egi.eu/portal/index.php?Page_Type=NGI&id=4> [↑](#footnote-ref-6)
7. A list of suggested material and references: <https://docs.egi.eu/internal/guidelines-software-development/> [↑](#footnote-ref-7)
8. <https://confluence.egi.eu/display/EGIBG/Secure+Coding> [↑](#footnote-ref-8)
9. <https://confluence.egi.eu/display/EGIBG/Software+Security+Checklist> [↑](#footnote-ref-9)
10. <https://confluence.egi.eu/display/EGIBG/Instructions+for+Technology+Providers> [↑](#footnote-ref-10)
11. <https://confluence.egi.eu/x/aYILCQ> [↑](#footnote-ref-11)
12. <https://registry.egi.eu/> [↑](#footnote-ref-12)
13. SVG: <https://confluence.egi.eu/x/zAXpB> [↑](#footnote-ref-13)