CORPORATE-LEVEL TECHNOLOGY PROVIDER UNDERPINNING AGREEMENT

Customer	EGI Foundation
Provider	Technology Provider
Service	Support
Status	Final
Document Link:	https://documents.egi.eu/document/2589

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
v. 1	11/09/2015	Initial version	Małgorzata Krakowian
v. 1.1	01/07/2016	Minor updates in formatting and corrected links	Małgorzata Krakowian Matthew Viljoen
v. 1.2	18/07/2016	Now more appropriate for Technology Providers – removed text in Section 6 relating to Service Providers. Now refers to CMD and UMD	Matthew Viljoen, Peter Solagna
v. 1.3	29/07/2016	In Section 4, removed the stipulation that support communication should be '8 hours a day' as the working day is not 8 hours in all countries	Matthew Viljoen
v. 1.4	11/08/2016	Miscellaneous corrections. Changed 'Customer' to 'EGI Foundation'	Peter Solagna
v. 2.0	10/08/2017	Yearly review, document reorganized and minor corrections	Alessandro Paolini
v. 2.1	28/09/2018	Yearly review, updated the EGI Foundation contact	Alessandro Paolini
v. 2.2	18/11/2020	yearly review, updated some links and section 7 (security)	Alessandro Paolini
v 2.3	11/07/2023	yearly review, minor corrections, updated section 7	Alessandro Paolini, Maarten Litmaath, Baptiste Grenier

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

This agreement is made between the Technology Provider (the 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.

Once approved, this Agreement is valid for as long as the Technology Provider is part of the UMD or CMD Release Team[1], i.e. while the Provider is registered in the Technology Provider catalogue (whose historical wiki[2,3] pages are to be replaced with a different technology themselves).

The 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 partner or consortium of partners (the Provider) selected for delivery of the service.

The agreement is a document discussed and approved by the EGI Operations Management Board (OMB). Amendments, comments and suggestions must be addressed by the EGI Foundation to the OMB by opening a GGUS[4] ticket to the Operations support unit. The EGI Foundation will promptly inform the Provider about changes introduced to the requirements, service levels and targets defined in this document, and will ensure that the impact of the changes is understood.

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

2 Scope of the services

This agreement applies to provision of support for software produced by the Provider.

3 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 on the Technology Provider catalogue pages.

Service communication support is available:

[1] https://ims.egi.eu/display/EGIBG/URT

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

[3] https://confluence.egi.eu/x/foILCQ

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

- Monday through Friday
- during the regular working hours of supporting organisation

This excludes public holidays of the supporting organisation.

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[5]. 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[6]
- The QoS levels apply to the service documented on the Technology Provider catalogue pages.

4 Service level targets

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

- QoS level (see section 3).

4.1 Targets for handling of security vulnerability

Security vulnerabilities affecting UMD or CMD software are assessed by the EGI Software Vulnerability Group[7]. Requests for fixing security vulnerabilities affecting the software provided by the Provider will be handled accordingly to the Vulnerability Issue Handling Procedure[8].

Updated versions of affected software that are free from the vulnerabilities under consideration 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

5 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 the following language: English

[5] https://docs.egi.eu/internal/helpdesk/features/ticket-priority/

[6] https://docs.egi.eu/internal/helpdesk/features/quality-of-support-levels/

[7] https://confluence.egi.eu/display/EGIBG/SVG

[8] https://documents.egi.eu/document/2538

- Failures in the normal operation of the service caused by failures in Federated Operations service components (e.g. 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. Severe examples include:
  - fire, flood, earthquake or other natural phenomena,
  - war, embargo, riot, civil disorder, rebellion, revolution.

6 Communication, reporting & escalation

6.1 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 EGI Foundation Service Delivery and Information Security Lead[9]
Technology Provider contact	Documented on the Technology Provider catalogue pages.
Contact for service users	According to defined support channels.

6.2 Agreement violations

The Provider commits to informing 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 two consecutive months, the Provider 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.

6.3 Escalation & complaints

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

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

- In case of violating the service targets for four consecutive months, a review of the Agreement will be taken up 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.

7 Information security & data protection

A series of guidelines[10] 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[11] and Software Security Checklist[12].
- 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.

8 Additional responsibilities of the provider

Additional responsibilities of the Provider are as follows:

- Adhere to all applicable operational and security policies and procedures and to other policy documents referenced therein.
- Use communication channels defined in the agreement (see section 6.1).
- Accept EGI monitoring services provided to measure fulfilment of service level targets agreed between EGI and the Provider, as defined in section 4..
- Handle security issues in a timely manner.
- Deliver service components according to EGI Software Component Delivery procedure[13].

[10] A list of suggested material and references: https://docs.egi.eu/internal/guidelines-software-development/
[11] https://confluence.egi.eu/display/EGIBG/Secure+Coding
[12] https://confluence.egi.eu/display/EGIBG/Software+Security+Checklist
[13] https://wiki.egi.eu/wiki/EGI_Software_Component_Delivery

9 EGI Foundation responsibilities

The responsibilities of the EGI Foundation are:

- Raise any issues deemed necessary to the attention of the 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 having successfully passed through the UMD or CMD Software Provisioning Process[14] and facilitating software deployment on the EGI production e-infrastructure.
- Provide the UMD or CMD software provisioning infrastructure composed of:
    - UMD or CMD repositories, supporting the agreed operating systems;
    - Community repositories - through AppDB[15] the Provider has access to a repository-as-a-service platform to upload their software releases;
    - Web front-end – containing information about UMD or CMD releases (release notes, lists of components, configuration information).
- Communicate collected and prioritised requirements and use cases from EGI communities.
- Define generic and specific acceptance criteria related to all software components contributed to EGI.
- Involve the Provider in the triaging of the issues mentioned above through the EGI second level support team.
- Provide access to boards, processes and knowledge of the EGI Software Vulnerability Group[16] to aid the Provider in developing and contributing corrections necessary to the maintained software components.

10 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.

[14] https://confluence.egi.eu/x/aYILCQ

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

[16] https://confluence.egi.eu/x/zAXpB