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

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://wiki.egi.eu/wiki/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. until the Provider is registered in the Technology Provider wiki[2],[3].

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 at Technology Provider wiki page.

Service communication support is available:

- between Monday and Friday

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

[2] https://wiki.egi.eu/wiki/Technology_Providers

[3] https://wiki.egi.eu/wiki/EGI_Cloud_Middleware_Distribution_products

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

- 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[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 at Technology Provider wiki page.

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 Security Vulnerability Group. Requests for fixing security vulnerabilities affecting the software provided by the Provider will be handled accordingly to the Vulnerability Issue Handling Procedure[7].

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

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 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.

[5] https://wiki.egi.eu/wiki/FAQ_GGUS-Ticket-Priority

[6] https://wiki.egi.eu/wiki/FAQ_GGUS-QoS-Levels

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

- 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

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[8]
Technology Provider contact	Documented at Technology Provider wiki page.
Contact for service users	According to defined support channels

6.2 Agreement violations

The 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 two 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.

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:

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

- 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.

7 Information security & data protection

The following rules for information security and data protection apply:

- The Provider must define and abide by an information security and data protection policy related to the service being provided. The templates provided by the AARC Policy Development Kit (PDK)[9] can be used as a basis.
- The Provider must enforce the EGI WISE Acceptable Usage Policies[10].
- The Provider shall comply with all principles set out by the GÉANT Data Protection Code of Conduct[11] in its most current version, which will be made available to the RP by EGI Foundation upon request.
- This Information Security and Data Protection policy must meet all requirements of any relevant EGI policies or procedures[12] and also must be compliant with the relevant national legislation. Regarding the 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 Additional responsibilities of the provider

Additional responsibilities of the 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;

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

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

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

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

- Handle security issues in timely manner;
- Deliver service components according to EGI Software Component Delivery procedure[13].

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 successfully passed through the UMD or CMD Software Provisioning Process[14] 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 AppDB[15] 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 EGI community.
- 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 appointed EGI second level support team.
- Provide access to boards, process and knowledge of EGI's Software Vulnerability Group[16] to the Provider in order to develop and contribute 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.

[13] https://wiki.egi.eu/wiki/EGI_Software_Component_Delivery

[14] https://wiki.egi.eu/wiki/EGI_Software_Provisioning

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

[16] https://wiki.egi.eu/wiki/SVG:SVG