# EGI TECHNOLOGY PROVIDER DPM/DMLITE UNDERPINNING AGREEMENT

| | |
|---|---|
| **Service Provider** | EGI Foundation |
| **Technology Provider** | CESNET/CVUT |
| **Technology** | Support of DPM/DMLite |
| **First day of service delivery** | 1st January 2021 |
| **Last day of service delivery** | 30th June 2023 |
| **Status** | Final |
| **Agreement Link:** | https://documents.egi.eu/document/3672 |

## DOCUMENT LOG

| *Issue* | *Date* | *Comment* | *Author* |
|---|---|---|---|
| **v0.1** | 2021-10-06 | first draft; added sections about regular reporting, ownership of results, software compliance. | Alessandro Paolini, Baptiste Grenier, |
| **v1.0** | 2021-10-08 | updated the milestones section; document finalised | Alessandro Paolini |
| **v1.1** | 2022-10-26 | Yearly review; updated some links | 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://go.egi.eu/glossary).

# Contents

## Contents

# 1 Introduction

This agreement is made between **CESNET/CVUT** (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 **1st January 2021** to **30th June 2023**. It was discussed and approved by the EGI Foundation and the Lead Beneficiary on **8th October 2021**.

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 to the EGI Foundation contact given to the Technology Provider (see section 6.1).

# 2 Scope of the services

This agreement is focussed on the following goals:

- Support and maintain the DPM/DMLite technology product.
- Support the Resource Centres when migrating to a different storage solution.

## 2.1 Milestones

In order to achieve the aforementioned goals, the following milestone was agreed:

- Regular release of DPM/DMLite software, including bug fixes and new features
- Release of scripts to support the migration to dCache

# 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 organised 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: **DPM Development**.

Service communication support is available:

- between Monday and 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[1]. 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[2]
- 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): **Medium**.

## 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 Technology Provider will be handled accordingly to the Vulnerability Issue Handling Procedure[3].

The software addressing 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.
- 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

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

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

[3] https://documents.egi.eu/document/3867

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<br>EGI Foundation Service Delivery and Information Security Lead[4]<br><br>Alessandro Paolini operations@egi.eu<br>EGI Foundation Service Delivery and Information Security Officer and EGI-ACE WP7 leader |
| **Technology Provider contact** | Petr Vokac petr.vokac@cern.ch |
| **Contact for service users** | According to defined support channels |

## 6.2 Regular reporting

As part of the fulfilment of this Agreement, the Technology Provider is requested to periodically report over the activities conducted in the related period. The frequency of the reports is 10 months (first report covering the period Jan – Oct 2021).

The reports are collected in a form of a survey that EGI Foundation will circulate and the Technology Provider will fill in.

## 6.3 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.

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

## 6.4 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.

# 7 Ownership of Results

The EGI Federation asks in return of its investment permanent free non-exclusive usage rights for the EGI Foundation and its participants and proper credit for the funding in the licence distributed with the project. The EGI Strategic & Innovation Fund, through the EGI Foundation and its participants, also has the rights to extend, modify and evolve any software or any other IP generated as part of the projects. A licence compatible with the open source principles and with the unlimited reuse by EGI should be selected. Publication of results in scientific papers, conferences or other means is welcome.

# 8 Information security & data protection

The following rules for Information Security and data protection must be enforced by the Technology Provider:

- 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)[5] can be used as a basis.
- The Provider must enforce the EGI WISE Acceptable Usage Policies[6].
- The Provider shall comply with all principles set out by the GÉANT Data Protection Code of Conduct[7] 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[8] 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

[5] https://aarc-project.eu/policies/policy-development-kit/
[6] https://documents.egi.eu/public/ShowDocument?docid=3600
[7] https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home
[8] https://confluence.egi.eu/display/EGIPP/EGI+Federation+Operations

- 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

# 9 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[9].
- Attend EGI-ACE and other operations/technical meetings when needed.

## 9.1 Software compliance

Unless explicitly agreed between EGI Foundation and the Technology Provider, software being used and developed to provide the service should:

- Be licensed under an open source and permissive licence (like MIT, BSD, Apache 2.0,...).
- The licence should provide unlimited access rights to the EGI community.
- Have source code publicly available via a public source code repository (if needed a mirror can be put in place under the EGI organisation in GitHub[10].) All releases should be appropriately tagged.
- Taking security aspects into consideration from the start
- Adopt best practices (more information on those topics is available on our documentation site[11]):
    - Defining and enforcing code style guidelines.
    - Using Semantic Versioning.
    - Using a Configuration Management frameworks such as Ansible.
    - Follow security best practices
    - Having automated testing in place.
    - Using code reviewing.
    - Treating documentation as code.

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

[10] https://github.com/EGI-Foundation

[11] https://docs.egi.eu/internal/guidelines-software-development/

- Documentation should be available for Developers, administrators and end users.

# 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[12] 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[13] 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[14] to the Technology Provider in order to develop and contribute corrections necessary to the maintained software components.

# 11 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.

[12] https://confluence.egi.eu/display/EGIBG/Software+Provisioning+Process

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

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