EGI Foundation

Security coordination and security tools

OPERATIONAL LEVEL AGREEMENT

Service Provider	EGI Foundation
Service Suppliers	**UKRI, FOM-Nikhef, CERN, CESNET, GRNET, IJS**
Start Date	1st January 2021
End Date	30st June 2023
Status	FINAL
Agreement Date	25th November 2020
OLA Link	https://documents.egi.eu/document/3672

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
FINAL	22/03/2016	Final version	Małgorzata Krakowian
2.0	17/11/2017	New OLA covering 2018, 2019, 2020	Alessandro Paolini
2.1	07/10/2019	yearly review, introduced the roles Service Provider and Component Provider, updated sections on Violations, Escalations, and Complaints	Alessandro Paolini
3.0	06/11/2020, 22/02/2021	Corporate EGI OLA renamed into EGI Default OLA. Updated to cover EGI ACE: added IJS as Component Provider, added Software and ITSM compliance, updated the support unit names. Added in section 9 the requirement about periodic supplier process audits conducted by EGI Foundation;	Baptiste Grenier, Alessandro Paolini, Dave Kelsey
3.1	15/12/2021, 23/02/2022	yearly review; introduced the term Service Supplier; updated section 7 and section 8.	Alessandro Paolini
3.2	09/03/2023	yearly review; updated some links	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

1 The Services **4**
2 Service hours and exceptions 6
3 Support 6
3.1 Incident handling 7
3.2 Service requests 7
4 Service level targets 7
5 Limitations and constraints 7
6 Communication, reporting, and escalation 7
6.1 General communication 7
6.2 Regular reporting 8
6.3 Violations 8
6.4 Escalation and complaints 9
7 Information security and data protection 9
8 Responsibilities 10
8.1 Of the Service Suppliers 10
8.1.1 Software compliance 10
8.1.2 IT Service Management compliance 11
8.2 Of the EGI Foundation 11
9 Review, extensions, and termination 11

The present Agreement ("the Agreement') is made between **EGI Foundation (the Service Provider)** and **UKRI, FOM-Nikhef, CERN, CESNET, GRNET, IJS (the Service Suppliers)** to define the provision and support of the provided services as described hereafter. Representatives and contact information are defined in Section 6.

This Agreement is valid from **1st January 2021** to **30th June 2023**.

The Agreement was discussed and approved by the EGI Foundation and the Service Suppliers **25th November 2020.**

The Service Suppliers are bound by the terms and conditions of the EGI Default Operational Level Agreement[1] supplemented by the terms and conditions of this specific Agreement:

1 The Services

The Services are defined by the following properties:

Technical	The security coordination activities must liaise with the resource providers (~40 among NGIs and EIROS) the resource centres (~350) and oversee the technologies used in the production infrastructure, for example: O.S. Platforms, HTC, Cloud, Storage, AAI capabilities.
Coordination	• **Security Operations Coordination** - Central coordination of the security activities ensures that policies, operational security, and maintenance are compatible amongst all partners, improving availability and lowering access barriers for use of the infrastructure. This coordination ensures that incidents are promptly and efficiently handled, that common policies are followed by providing services such as security monitoring, and by training and dissemination with the goal of improving the response to incidents. This includes liaison with external security organisations, coordination of security training, of security service challenges and of security threat risk assessment. • **Security Policy Coordination** - Security policy development covers diverse aspects, including operational policies (agreements on vulnerability management, intrusion detection and prevention, regulation of access, and enforcement), incident response policies (governing the exchange of information and expected actions), participant responsibilities (including acceptable use policies,

[1] https://documents.egi.eu/document/2752

identifying users and managing user communities), traceability, legal aspects, and the protection of personal data. Since research is global, such policies must be coordinated with peer infrastructures in Europe and elsewhere, such as PRACE, Open Science Grid, XSEDE, and like efforts in the Asia Pacific. Coordination mechanisms such as the FIM4R group, TERENA REFEDS, SCI, Open Grid Forum and the IGTF will need to be employed.

- **Security Incident Response Coordination** - Coordination of incident response activities in collaboration with the Incident Response Task Force. The primary responsibility for basic incident response and forensics still lies with each NGI, while the EGI Global IRTF will coordinate incident response and information exchange. For complex multi-site incidents and in cases where advanced forensics is needed, the EGI Global IRTF will step in and take an active part, to protect the continued integrity of the EGI infrastructure as a whole. Validation of EGI Global incident response capability is done by coordinating security service challenges that both assess readiness of infrastructure operations and verify adequate traceability features in the software used. This task will also liaise with other CSIRTs via for example TF-CSIRTS and FIRST.
- **Software Vulnerability Group Coordination** - The Software Vulnerability Group aims to eliminate existing software vulnerabilities from the deployed infrastructure and prevent the introduction of new ones, and runs a process for handling software vulnerabilities reported. This depends on investigation and risk assessment by a collaborative team drawn from technology providers and other security groups, known as the Risk Assessment Team (RAT).
- **International Grid Trust Federation (IGTF) and EUGridPMA** - A common authentication trust domain is required to persistently identify all EGI participants. This task is about the representation of EGI in IGTF and EUGridPMA. This representation will bring operational and policy needs of EGI to the attention of the PMA, bring issues raised by the PMA to the attention of the appropriate groups within EGI, and keep the EGI Council informed of progress and policies of the EUGridPMA. This task is also responsible for the coordination of the provision of EGI versions of the IGTF Certification Authority distributions as required by the EGI Council.

In particular the activity will have to liaise with the following entities:

	• NGI and EIROs security teams. In the hierarchical operational structure of EGI most of the communications go from EGI to the Operations Centres, and then from the Operations Centres to the Resource Centres. • Resource Centres security teams. To ensure prompt reaction and support in case of security incident or critical violation of security policies. • Other European and international e-infrastructures and research infrastructures. The liaison must be direct peer to peer and in the context of security initiatives such as WISE as an example, respectively to tackle specific topics or to develop a collaboration framework for security. • Cross infrastructure policy groups, such as for example WISE, SIG-ISM, AARC AEGIS, FIM4R and REFEDS.

Operation	The provisioning of this activity includes the operations and maintenance of the operational tools that support security, namely:
	
	• **Security Monitoring** - the activity should provide monitoring services to check for security vulnerabilities and other security-related problems in the EGI production infrastructure. Monitoring uses ad-hoc probes implemented to address specific security issues as well as generic probes used to gather security-related information. The main features are:
	  • Monitor a range of security relevant assets like for example: CRLs, file system permissions and vulnerable file permissions
	  • Monitor and check the software packages deployed in the services of the production infrastructure and the status of patching security vulnerability by deploying relevant software updates.
	  • 2 different monitoring boxes are operated:
	  ▪ pakiti (by CESNET)
	  ▪ secmon (by GRNET)
	• **Incident Reporting Tool** - ticketing system for tracking of incident reporting activities.
	• **Tools for Security Service Challenge support** - Security challenges are a mechanism to check the compliance of sites/NGIs/EGI with security requirements. Runs of Security Service Challenges need a set of tools that are used during various stages of the runs.

2 Service hours and exceptions

As defined by the EGI Default Operational Level Agreement.

3 Support

As defined by the EGI Default Operational Level Agreement.

Support is provided via EGI Helpdesk[2] Support Units:

- Security tools:
  - pakiti: Security Monitoring
  - secmon: Monitoring (ARGO)
- Security coordination: Security Coordination

Support is also provided through abuse@egi.eu for the security incident handling.

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.

3.1 Incident handling

As defined by the EGI Default Operational Level Agreement.

3.2 Service requests

As defined by the EGI Default Operational Level Agreement.

4 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): 90%

Monthly Reliability

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

- 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): 90%

Quality of Support level

- Medium (Section 3)

5 Limitations and constraints

As defined by the EGI Default Operational Level Agreement.

6 Communication, reporting, and 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	Alessandro Paolini operations@egi.eu
Service Suppliers contact	David Kelsey david.kelsey@stfc.ac.uk
Service Support contact	See Section 3

6.2 Regular reporting

As part of the fulfilment of this Agreement and provisioning of the Services, the following reports will be provided:

Report title	Contents	Frequency	Produced by	Delivery
Service Performance Report	The document provides the overall assessment of service performance (per month) and OLA target performance achieved during the reference reporting period	10 months (first report covering the period Jan – Oct 2021)	Service Suppliers	Survey form prepared by EGI Foundation

6.3 Violations

The Service Suppliers commits to inform the EGI Foundation, 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 violations of the Services targets, the Service Suppliers will provide justifications and a plan for Services enhancement to the EGI Foundation. The Service Suppliers 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 EGI Foundation will notify the supporting Resource Centres in case of suspected violation via the EGI Service Desk. The case will be analysed to identify the cause and verify the violation.

6.4 Escalation and complaints

For escalation and complaints, the Service Suppliers contact point shall be used, and the following rules apply.

- In case of repeated violation of the Services targets for two consecutive months or four months over a period of 12 months, a review of the Agreement and of the Services enhancement plan will take place involving the parties of the Agreement.
- Complaints or concerns about the Services provided should be directed to the Service Suppliers contact who will promptly address these concerns. Should the EGI Foundation still feel dissatisfied, about either the result of the response or the behaviour of the Service Suppliers, EGI Foundation Director director@egi.eu should be informed.

7 Information security and data protection

The following rules for Information Security and data protection should be enforced when they are applicable:

- The Service Suppliers agrees to make every effort to maximise security level of users' data and minimise possible harm in the event of an incident.
- EGI Foundation holds the role of the Data Controller while the Service Suppliers holds the role of Data Processor. When applicable Data Processing Agreements must be signed between EGI Foundation (the Data Controller) and Service Suppliers (the Data Processor).
- The Service Suppliers must comply with the EGI Policy on the Processing of Personal Data[3] and provide a Privacy Notice. This privacy Notice must be agreed with EGI Foundation and must be based on the Privacy Policy template provided by the AARC Policy Development Kit (PDK)[4].

[3] https://documents.egi.eu/public/ShowDocument?docid=2732

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

- The Service Suppliers must enforce the EGI WISE Acceptable Usage Policies[5].
- The Service Suppliers shall comply with all principles set out by the GÉANT Data Protection Code of Conduct[6] in its most current version, which will be made available to the Service Suppliers by EGI Foundation upon request.
- Security incidents affecting the services described in Section 1 must be reported to abuse@egi.eu within 4 hours after their discovery and handled according to SEC01 procedure.
- The Service Suppliers must meet all requirements of any relevant EGI policies or procedures[7] 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
    - EGI-doc-710: Security Incident Handling Procedure

8 Responsibilities

8.1 Of the Service Suppliers

Additional responsibilities of the Component Providers include:

- Using communication channels defined in this Agreement.
- Attending OMB[8] and other operations meetings when needed.
- Accepting EGI monitoring services provided to measure fulfilment of agreed service level targets.
- The Services with associated roles are registered in GOC DB[9] as a site entity under EGI.eu.
- Operations Centre hosting EGI central operations tools[10]

8.1.1 Software compliance

Unless explicitly agreed, software being used and developed to provide the service should:

- Be licensed under an open source and permissive licence (e.g. MIT, BSD, Apache 2.0,...).
- Unless otherwise agreed, be licensed to provide unlimited access and exploitation rights to the EGI Federation.

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

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

[7] https://confluence.egi.eu/display/EGIPP/EGI+Policies+and+Procedures+Home

[8] https://confluence.egi.eu/display/EGIBG/Operations+Management+Board

[9] http://goc.egi.eu/

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

- 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[11].) All releases should be appropriately tagged.
- Adopt best practices:
    - Defining and enforcing code style guidelines.
    - Using Semantic Versioning.
    - Using a Configuration Management frameworks such as Ansible.
    - Taking security aspects into consideration at every point in time.
    - Having automated testing in place.
    - Using code reviewing.
    - Treating documentation as code.
    - Documentation should be available for Developers, administrators and end users.

8.1.2 IT Service Management compliance

- Key staff who deliver services should have foundation or basic level ITSM training and certification
    - ITSM training and certification could include standards and best practices such as FitSM, ITIL, ISO 20000 etc.
- Key staff and service owners should have advanced/professional training and certification covering the key service management processes for their services.
- Component Providers should have clear interfaces with the EGI Service Management System processes and provide the required information.
- Component Providers should commit to improving their management system used to support the services they provide.

8.2 Of the EGI Foundation

The responsibilities of the Service Provider are:

- Delivering and planning the Services according to an ISO 20000 compliant manner.
- Raising any issues deemed necessary to the attention of the Service Suppliers.
- Collecting requirements from the Resource infrastructure Providers.
- Supporting coordination and integration with other EGI services.
- Providing monitoring to measure fulfilment of agreed service level targets.
- Providing clear interfaces to the EGI SMS processes.

[11] https://github.com/EGI-Federation

9 Review, extensions, and termination

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

- Technical content of this Agreement and targets will be reviewed on a yearly basis.
- EGI Foundation shall be entitled to conduct audits or mandate external auditors to conduct audits of suppliers and federation members. These will aim at evaluating the effective provision of the agreed service or service component and execution of activities related to providing and managing the service prior to the commencement of this Agreement and then on a regular basis. EGI Foundation will announce audits at least one month in advance. The Component Provider / supplier shall support EGI Foundation and all auditors acting on behalf of EGI Foundation to the best of their ability in carrying out the audits. The Component Provider / supplier is obliged to provide the auditors, upon request, with the information and evidence necessary. Efforts connected to supporting these audits by the provider / federation member will not be reimbursed.