EGI Foundation

Security coordination and security tools

OPERATIONAL LEVEL AGREEMENT

Customer	EGI Foundation
Provider	**STFC, FOM-Nikhef, CERN, CESNET, GRNET**
Start Date	1st January 2018
End Date	31st December 2020
Status	FINAL
Agreement Date	18th September 2018
OLA Link	https://documents.egi.eu/document/3254

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

TERMINOLOGY

The EGI glossary of terms is available at: https://wiki.egi.eu/wiki/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

The present Operational Level Agreement ("the Agreement') is made between **EGI Foundation (the Customer)** and **STFC, FOM-Nikhef, CERN, CESNET, GRNET (the Provider)** 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 2018** to **31st December 2020**.

The Agreement was discussed and approved by the Customer and the Provider **18th September 2018**.

The provider(s) is (are) bound by the terms and conditions of the Corporate-level EGI 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 oversees 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 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 infrastructure. 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 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 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.
	• **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 in Corporate-level EGI Operational Level Agreement.

3 Support

As defined in Corporate-level EGI Operational Level Agreement.

Support is provided via EGI Service Desk[2] Support Unit:

- Security tools: EGI Security Monitoring
- Security coordination: Security Management

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 organizations providing the service.

3.1 Incident handling

As defined in Corporate-level EGI Operational Level Agreement.

3.2 Service requests

As defined in Corporate-level EGI 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%

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

Monthly Reliability

- 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 in Corporate-level EGI 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.

Customer contact for the Provider	Alessandro Paolini operations@egi.eu
Provider contact for the Customer	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 service, 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	Every 9 months (first report covering the period Jan – Sep 2018)	Provider	Survey form prepared by EGI Foundation

	target performance achieved during reporting period			

6.3 Violations

As defined in Corporate-level EGI Operational Level Agreement.

6.4 Escalation and complaints

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

- In case of repeated violation of the Services targets for four consecutive 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 Provider contact who will promptly address these concerns. Should the Customer still feel dissatisfied, about either the result of the response or the behaviour of the Provider, EGI Foundation Director director@egi.eu should be informed.

7 Information security and data protection

As defined in Corporate-level EGI Operational Level Agreement

8 Responsibilities

8.1 Of the Provider

Additional responsibilities of the Provider are as follow:

- Adhere to all applicable operational and security policies and procedures[3] and to other policy documents referenced therein;
- Use communication channel defined in the agreement;
- Attend OMB[4] and other operations meeting when needed;
- Accept EGI monitoring services provided to measure fulfilment of agreed service level targets.

[3] https://www.egi.eu/about/policy/policies_procedures.html
[4] https://wiki.egi.eu/wiki/OMB

- Service with associated roles are registered in GOC DB[5] as site entity under EGI.eu Operations Centre hosting EGI central operations tools[6]

8.2 Of the Customer

The responsibilities of the customer are:

- Raise any issues deemed necessary to the attention of the Provider;
- Collect requirements from the Resource infrastructure Providers;
- Support coordination with other EGI services
- Provide monitoring to measure fulfilment of agreed service level targets.

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 Customer according to the following rules:

- Technical content of the agreement and targets will be reviewed on a yearly basis.

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