

**EGI.eu**

**Security coordination and security tools**

**OPERATIONAL LEVEL AGREEMENT**

|  |  |
| --- | --- |
| **Customer** | EGI.eu |
| **Provider** | **STFC, FOM-Nikhef, CERN, CESNET, GRNET** |
| **Start Date** | 1 May 2016 |
| **End Date** | 31 December 2017 |
| **Status** | DRAFT |
| **Agreement Date** | [date of final agreement] |
| **OLA Link** | <https://documents.egi.eu/document/2770>  |

**DOCUMENT LOG**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Issue*** | ***Date*** | ***Comment*** | ***Author*** |
|  |  |  | Małgorzata Krakowian |

**TERMINOLOGY**

The EGI glossary of terms is available at: [https://wiki.egi.eu/wiki/Glossary](https://wiki.egi.eu/wiki/Glossary%20)

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](#_Toc443560631)

[2 Service hours and exceptions 4](#_Toc443560632)

[3 Support 5](#_Toc443560633)

[3.1 Incident handling 5](#_Toc443560634)

[3.2 Service requests 6](#_Toc443560635)

[4 Service level targets 6](#_Toc443560636)

[5 Limitations and constraints 7](#_Toc443560637)

[6 Communication, reporting and escalation 7](#_Toc443560638)

[6.1 General communication 7](#_Toc443560639)

[6.2 Regular reporting 8](#_Toc443560640)

[6.3 Violations 8](#_Toc443560641)

[6.4 Escalation and complaints 9](#_Toc443560642)

[7 Information security and data protection 9](#_Toc443560643)

[8 Responsibilities 9](#_Toc443560644)

[8.1 Of the Provider 9](#_Toc443560645)

[8.2 Of the Customer 10](#_Toc443560646)

[9 Review, extensions and termination 10](#_Toc443560647)

The present Operational Level Agreement (“the Agreement’) is made between **EGI.eu (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 **1 May 2016** to **31 December 2017**.

The Agreement was discussed and approved by the Customer and the Provider **[date]**.

The Agreement extends the Corporate-level EGI Operational Level Agreement[[1]](#footnote-1) with following information:

# 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, 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.
 |
| Operation  | The provisioning of this activity includes the operations and maintenance of the operational tools that support security, namely:* Security Nagios - A Security Nagios service is provided to monitor a range security relevant assets like CRLs, file system permissions, vulnerable file permissions etc. Ad-hoc probes need to be deployed to support incident management, to assess the vulnerability of the infrastructure with regard to specific security issues and for proactive security management. The results produced are available to the EGI Security dashboard for visualization.
* Pakiti - Pakiti is monitoring and notification service which is responsible for checking the patching status of systems. The results produced are available to the EGI Security dashboard for visualization.
* Incident Reporting Tool - RTIR 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. The tools include a web portal used by the SSC operators to control the run, an extension of RTIR for evaluations of sites, and customized Pakiti used in SSC preparation phases.
 |

# Service hours and exceptions

As defined in Corporate-level EGI Operational Level Agreement.

# Support

As defined in Corporate-level EGI Operational Level Agreement.

Support is provided via EGI Service Desk[[2]](#footnote-2) Support Unit:

* Security tools: EGI Security Monitoring
* Security coordination: Security Management

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.

## Incident handling

As defined in Corporate-level EGI Operational Level Agreement.

## Service requests

As defined in Corporate-level EGI Operational Level Agreement.

# 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**

* 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)

# Limitations and constraints

As defined in Corporate-level EGI Operational Level Agreement.

# Communication, reporting and escalation

## 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** | Peter Solagnaoperations@egi.eu  |
| **Provider contact for the Customer** |  [name][email] [title] |
| **Service Support contact** | See Section 3 |

## 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** | **Delivery** |
| Service Performance Report | The document provides the overall assessment of service performance (per month) and OLA target performance achieved during reporting  | May-Aug 2016: 4 Months reportSept-Dec 2016: 4 Months reportJan-June 2017: 6 Months reportJuly-Dec 2017: 6 Months report3 | At least one page document submitted to the Executive Board for assessment and made publicly available at EGI Document server[[3]](#footnote-3) bythe Customer contact |

## Violations

As defined in Corporate-level EGI Operational Level Agreement.

## 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.eu Director [director@egi.eu](http://director@egi.eu) should be informed.

# Information security and data protection

As defined in Corporate-level EGI Operational Level Agreement

# Responsibilities

## Of the Provider

Additional responsibilities of the Provider are as follow:

* Adhere to all applicable operational and security policies and procedures[[4]](#footnote-4) and to other policy documents referenced therein;
* Use communication channel defined in the agreement;
* Attend OMB[[5]](#footnote-5) and other operations meeting when needed;
* Accept EGI monitoring services provided to measure fulfilment of agreed service level targets.
* Service with associated roles are registered in GOC DB[[6]](#footnote-6) as site entity under EGI.eu Operations Centre hosting EGI central operations tools[[7]](#footnote-7)

## 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.

# 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.
1. <https://documents.egi.eu/document/2752> [↑](#footnote-ref-1)
2. <http://helpdesk.egi.eu/> [↑](#footnote-ref-2)
3. <https://documents.egi.eu> [↑](#footnote-ref-3)
4. <https://www.egi.eu/about/policy/policies_procedures.html> [↑](#footnote-ref-4)
5. <https://wiki.egi.eu/wiki/OMB> [↑](#footnote-ref-5)
6. <http://goc.egi.eu/> [↑](#footnote-ref-6)
7. <https://goc.egi.eu/portal/index.php?Page_Type=NGI&id=4> [↑](#footnote-ref-7)