

**Security Traceability
and Logging Policy**

|  |  |
| --- | --- |
| Document identifier | EGI-<GROUPID>-<KEYWORD>-V<VERSION> |
| Document Link | <https://documents.egi.eu/public/ShowDocument?docid=81>  |
| Last Modified | 11/10/2016 |
| Version | 1.1 |
| Policy Group Acronym | SPG |
| Policy Group Name | Security Policy Group |
| Contact Person | David Kelsey/STFC |
| Document Type | Policy/Procedure |
| Document Status | DRAFT |
| Approved by | TBD |
| Approved Date | TBD |

TABLE OF CONTENTS

1 INTRODUCTION 4

2 NOTATION 4

3 REQUIREMENTS FOR TRACEABILITY AND LOGGING 4

4 PRODUCTION AND RETENTION OF LOGGING DATA 5

5 IMPLEMENTATION 5

6 REFERENCES 5

**COPYRIGHT NOTICE**



This work by EGI.eu is licensed under a Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/).

**AUTHORS LIST**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Name** | **Partner/Activity/Organisation/Function** | **Date** |
| **From** |  |  |  |

**DELIVERY SLIP**

|  |  |  |
| --- | --- | --- |
|  | ***Body*** | ***Date*** |
| **Reviewed by:** |  |  |
| **Reviewed by:** |  |  |
| **Reviewed by:** |  |  |
| **Approved by:** |  |  |

**DOCUMENT LOG**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Issue*** | ***Date*** | ***Comment*** | ***Author/Partner*** |
| **v.1** |  |  |  |
| **...** |  |  |  |
| **...** |  |  |  |
| **v.n** |  |  |  |

**TERMINOLOGY**

A complete project glossary is provided at the following page: <http://www.egi.eu/about/glossary/>

**APPLICATION AREA**

This document is a formal EGI.eu policy or procedure applicable to all participants and associate participants, beneficiaries and Joint Research Unit members, as well as its collaborating projects.

**POLICY/PROCEDURE AMENDMENT PROCEDURE**

Reviews and amendments should be done in accordance with the EGI.eu “Policy Development Process” (<https://documents.egi.eu/document/169>).

# INTRODUCTION

This policy is effective from <DATE> and replaces an earlier version of this document [R1]. This policy is one of a set of documents that together define the Security Policy [R2]. This individual document must be considered in conjunction with all the policy documents in the set.

This policy defines the minimum requirements for traceability of actions on the e-Infrastucture Resources and Services as well as the production and retention of security related logging in the IT Infrastructure.

All terms are defined in the Glossary [R3].

# NOTATION

This document occasionally uses terms that appear in capital letters.

When the terms "MUST", "SHOULD", "MUST NOT", "SHOULD NOT", and "MAY" appear capitalized, they are being used to indicate particular requirements of this specification. A definition of the meanings of these terms may be found in IETF RFC 2119.

# REQUIREMENTS FOR TRACEABILITY AND LOGGING

The management of risk is fundamental to the operation of any e-Infrastructure. Identifying the cause of incidents is essential to prevent them from re-occurring. In addition, it is a goal to contain the impact of an incident while keeping services operational. For response to incidents to be acceptable this needs to be commensurate with the scale of the problem.

The minimum level of traceability for use of the IT Infrastructure is to be able to identify the source of all actions (executables, file transfers, pilot jobs, portal jobs, virtual machine management, image management etc) and the individual who initiated them. In addition, sufficiently fine-grained controls, such as blocking the originating user and monitoring to detect abnormal behaviour, are necessary for keeping services operational. It is essential to be able to understand the cause and to fix any problems before re-enabling access for the user.

The aim is to be able to answer the basic questions who, what, where, and when concerning any incident. This requires retaining all relevant information, including timestamps and the digital identity of the user, sufficient to identify, for each service instance, and for every security event including at least the following: connect, authenticate, authorize (including identity changes) and disconnect.

# PRODUCTION AND RETENTION OF LOGGING DATA

In order to satisfy the traceability requirements, software deployed in the IT Infrastructure MUST include the ability to produce sufficient and relevant logging, and to collect logs centrally at a Resource Centre. The software SHOULD follow any security guidelines on logging defined by the e-Infrastructure.

The level of the logging MUST be configured by all Service Providers, including but not limited to the Resource Centres, to produce the required information which MUST be retained for a minimum of 90 days. Security Operations MAY define longer periods of retention for specific services and/or operational requirements. The logs MUST be collected centrally at the service provider level.

# IMPLEMENTATION

The security architecture and software used in the IT Infrastructure is under constant change. Security Operations provides detailed requirements on the implementation of this policy. Participants MUST abide by the detailed implementation instructions.

# REFERENCES

|  |  |
| --- | --- |
| R 1 | (Old version) Grid Security Traceability and Logging Policy.<https://documents.egi.eu/document/81> |
| R 2 | Approved EGI Security Policies. [https://wiki.egi.eu/wiki/SPG:Documents](https://wiki.egi.eu/wiki/SPG%3ADocuments)  |
| R 3 | EGI Glossary. <https://wiki.egi.eu/wiki/Glossary_V1>SPG Security Policy Glossary of Terms. <https://documents.egi.eu/document/71> |