SECURITY TRACEABILITY AND LOGGING POLICY

Document identifier	EGI-SPG-Traceability-Logging_V2
Document Link	https://documents.egi.eu/document/2934
Last Modified	11/10/2016
Version	2
Policy Group Acronym	SPG
Policy Group Name	Security Policy Group
Contact Person	David Kelsey/STFC
Document Type	Security Policy
Document Status	Ready for Approval
Approved by	EGI Foundation Executive Board
Approved Date	14/11/2016

TABLE OF CONTENTS

COPYRIGHT NOTICE

AUTHORS LIST

	Name	Partner/Activity/Organisation/Function	Date
From	David Kelsey on behalf of EGI SPG	STFC/SPG Chair	14/11/2016

DELIVERY SLIP

	Body	***Date***
Reviewed by:	EGI Foundation Executive Board	14/11/2016
Approved by:	EGI Foundation Executive Board	14/11/2016

DOCUMENT LOG

Issue	***Date***	***Comment***	***Author/Partner***
V1.1	23/10/2016	Full draft	Vincenzo Spinoso/EGI Foundation; David Kelsey/STFC
V2	14/11/2016	Review and approval by EGI Foundation Executive Board	

TERMINOLOGY

A complete project glossary is provided at the following page: https://wiki.egi.eu/wiki/Glossary_V3

APPLICATION AREA

This document is a formal EGI 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 "Policy Development Process" (https://documents.egi.eu/document/169).

1 INTRODUCTION

This policy is effective from 14/11/2016 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-Infrastructure Resources and Services as well as the production and retention of security related logging in the IT Infrastructure.

Additional SPG terms are defined in the Glossary [R3].

2 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.

3 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.

4 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.

5 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.

6 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
R 3	SPG Security Policy Glossary of Terms. https://documents.egi.eu/document/71