



SECURITY INCIDENT RESPONSE POLICY

Document identifier	EGI-SPG-Security-Incident-Response_V2
Document Link	https://documents.egi.eu/document/2935
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

1 SECURITY INCIDENT RESPONSE POLICY.....	4
2 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	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	11/10/2016	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 SECURITY INCIDENT RESPONSE POLICY

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

A security incident is the act of violating an explicit or implied security policy (for example, a Resource Centre security policy or an e-Infrastructure security policy). Nothing in this policy is meant to restrict the flow of information from a Resource Centre to incident response teams or other organisations to which the participant is required to report incidents.

The objective of this policy is to ensure that all incidents are investigated as fully as possible and that Resource Centres promptly report intrusions. In particular, security incidents are to be treated as serious matters and their investigation must be resourced appropriately.

Effective security incident response depends on the maintenance of e-Infrastructure security contact information as defined by the e-Infrastructure, including in the Service Operations Security Policy [R4] and the Virtual Organisation Registration Security Policy [R5].

The e-Infrastructure will appoint an incident coordinator for each suspected incident, in order to promote the cooperation across the Resource Centres and collaboration with peer e-Infrastructures, and assign a unique identifier to each incident, which is considered public information. The coordinator may share incident information as appropriate with other organisations, in particular peer e-Infrastructures, which have adopted this policy.

As an e-Infrastructure participant, you agree to the conditions laid down in this document and other referenced documents that may be revised from time to time.

1. *You shall promptly report suspected security incidents to your local organization's incident response team.*
2. *You shall promptly report suspected security incidents (or your involvement therein) that have known or potential impact or relationship to the e-Infrastructure resources, services, or identities, via the incident response channels defined by the e-Infrastructure.*
3. *You shall follow the incident response procedure defined by the e-Infrastructure.*
4. *You shall promptly respond to and investigate incident reports regarding resources, services, or identities for which you are responsible.*
5. *You shall perform appropriate investigations and forensics and share the results with the incident coordinator.*
6. *You shall aim at preserving the privacy of involved participants and identities, and ensure that information shared with you is not publicly archived or published at your end without prior agreement from both the sender and the incident coordinator appointed by the e-Infrastructure for each incident. Public disclosure of information regarding security events should be handled through the Resource Centre Public Relations contacts.*

2 REFERENCES

R 1	(Old version: V1) Security Incident Response Policy. https://documents.egi.eu/document/82
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
R 4	Service Operations Security Policy. https://documents.egi.eu/document/1475
R 5	Virtual Organisation Registration Security Policy. https://documents.egi.eu/document/78