EGI-InSPIRE

SECURITY INCIDENT RESPONSE POLICY

Document identifier	EGI-SPG-IncidentResponse-V1_0
Document Link	https://documents.egi.eu/document/82
Last Modified	**14/07/2010**
Version	**1.0**
Policy Group Acronym	**SPG**
Policy Group Name	**Security Policy Group**
Contact Person	**David Kelsey/STFC, UK**
Document Status	**Submitted**
Approved by	**Body who approved the doc**
Approved Date	**DD/MM/YYYY**

Policy Statement

This document describes the policy and responsibilities for handling security incidents affecting the Grid.

I. COPYRIGHT NOTICE

II. DELIVERY SLIP

	Body	Date
Approved by	EGI.eu Executive Board	DD/MM/YYYY

III. DOCUMENT LOG

Issue	Date	Comment	Author/Organization
1.0	14/07/2010	Imported from JSPG policy document with the same title. The only change to wording made was to update links to other documents. See https://edms.cern.ch/document/428035 (V3.2a, dated 6 Aug 2009) for the old JSPG document.	David Kelsey/STFC
2.0			
3.0			
4.0			

IV. PROJECT SUMMARY

To support science and innovation, a lasting operational model for e-Science is needed − both for coordinating the infrastructure and for delivering integrated services that cross national borders.

The EGI-InSPIRE project will support the transition from a project-based system to a sustainable pan-European e-Infrastructure, by supporting 'grids' of high-performance computing (HPC) and high-throughput computing (HTC) resources. EGI-InSPIRE will also be ideally placed to integrate new Distributed Computing Infrastructures (DCIs) such as clouds, supercomputing networks and desktop grids, to benefit the user communities within the European Research Area.

EGI-InSPIRE will collect user requirements and provide support for the current and potential new user communities, for example the ESFRI projects. Support will also be given to the current heavy users of the infrastructure, such as high energy physics, computational chemistry and life sciences, as they move their critical services and tools from a centralised support model to one driven by their own individual communities.

The objectives of the project are:

1. The continued operation and expansion of today's production infrastructure by transitioning to a governance model and operational infrastructure that can be increasingly sustained outside of specific project funding.
2. The continued support of researchers within Europe and their international collaborators that are using the current production infrastructure.
3. The support for current heavy users of the infrastructure in earth science, astronomy and astrophysics, fusion, computational chemistry and materials science technology, life sciences and high energy physics as they move to sustainable support models for their own communities.
4. Interfaces that expand access to new user communities including new potential heavy users of the infrastructure from the ESFRI projects.
5. Mechanisms to integrate existing infrastructure providers in Europe and around the world into the production infrastructure, so as to provide transparent access to all authorised users.
6. Establish processes and procedures to allow the integration of new DCI technologies (e.g. clouds, volunteer desktop grids) and heterogeneous resources (e.g. HTC and HPC) into a seamless production infrastructure as they mature and demonstrate value to the EGI community.

The EGI community is a federation of independent national and community resource providers, whose resources support specific research communities and international collaborators both within Europe and worldwide. EGI.eu, coordinator of EGI-InSPIRE, brings together partner institutions established within the community to provide a set of essential human and technical services that enable secure integrated access to distributed resources on behalf of the community.

The production infrastructure supports Virtual Research Communities − structured international user communities − that are grouped into specific research domains. VRCs are formally represented within EGI at both a technical and strategic level.

TABLE OF CONTENTS

1 SECURITY INCIDENT RESPONSE POLICY

A security incident is the act of violating an explicit or implied security policy (for example, a local security policy or a grid security policy). Nothing in this policy is meant to restrict the flow of information from a site to incident response teams or other organizations 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 sites 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 grid security contact information as defined by the Grid, including the Site Registration Security Policy (https://documents.egi.eu/document/76) and the Virtual Organisation Registration Security Policy (https://documents.egi.eu/document/78).

The Grid will appoint an incident coordinator for each suspected incident, in order to promote the cooperation across the sites and collaboration with peer-grids, 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 Grids which have adopted this policy.

As a grid 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 grid resources, services, or identities, via the incident response channels defined by the Grid.*
3. *You shall follow the incident response procedure defined by the Grid.*
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 Grid for each incident. Public disclosure of information regarding security events should be handled through the site Public Relations contacts.*