



EGI-InSPIRE

CSIRT CRITICAL SECURITY OPERATIONAL PROCEDURE

EU MILESTONE:NONE

Document identifier:	EGI-CSIRT-CriticalSecurity-V5
Date:	14/02/2011
Activity:	SA1
Lead Partner:	EGI.eu
Document Status:	DRAFT
Dissemination Level:	PUBLIC
Document Link:	https://documents.egi.eu/document/283

Abstract

This is a brief document describing the procedure for dealing with Critical Security Issues where action needs to be taken by a single site or multiple sites. Failure of sites to act on this or respond may lead to site suspension, as in such a situation the site is not considered secure enough to remain as part of the EGI infrastructure. Site suspension actually means removing the site from resource information systems. Approval from the OMB is sought for this procedure.



COPYRIGHT NOTICE

Copyright © Members of the EGI-InSPIRE Collaboration, 2010. See www.egi.eu for details of the EGI-InSPIRE project and the collaboration. EGI-InSPIRE (“European Grid Initiative: Integrated Sustainable Pan-European Infrastructure for Researchers in Europe”) is a project co-funded by the European Commission as an Integrated Infrastructure Initiative within the 7th Framework Programme. EGI-InSPIRE began in May 2010 and will run for 4 years. This work is licensed under the Creative Commons Attribution-Noncommercial 3.0 License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc/3.0/> or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, and USA. The work must be attributed by attaching the following reference to the copied elements: “Copyright © Members of the EGI-InSPIRE Collaboration, 2010. See www.egi.eu for details of the EGI-InSPIRE project and the collaboration”. Using this document in a way and/or for purposes not foreseen in the license, requires the prior written permission of the copyright holders. The information contained in this document represents the views of the copyright holders as of the date such views are published.

I. DELIVERY SLIP

	Name	Partner/Activity	Date
From	The CSIRT Team		
Reviewed by	Moderator: Reviewers: <<To be completed by project office on submission to AMB/PMB>>		
Approved by	AMB & PMB <<To be completed by project office on submission to EC>>		

II. DOCUMENT LOG

Issue	Date	Comment	Author/Partner
1	15 th Dec 2010	First draft	
2	20 th Dec 2010	Second draft, after Mingchao + Sven comments	
3	5th Jan 2010	Third draft, after discussion during CSIRT EVO meeting	
4	17 th Jan 2010	Forth draft, after comments from Tobias Dussa, Mingchao Ma, Giuseppe Misurelli, and Ricardo Brunetti and discussion with Mingchao Ma	

III. APPLICATION AREA



This document is a formal deliverable for the European Commission, applicable to all members of the EGI-InSPIRE project, beneficiaries and Joint Research Unit members, as well as its collaborating projects.

IV. DOCUMENT AMENDMENT PROCEDURE

Amendments, comments and suggestions should be sent to the authors. The procedures documented in the EGI-InSPIRE “Document Management Procedure” will be followed:

<https://wiki.egi.eu/wiki/Procedures>

V. TERMINOLOGY

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



VI. 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 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 within the ESFRI projects. Additional 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 (VRCs) – structured international user communities – that are grouped into specific research domains. VRCs are formally represented within EGI at both a technical and strategic level.

VII. EXECUTIVE SUMMARY

Overview

In order to prevent incidents, it is important to ensure that operational action is taken in a timely manner when a security problem has been found and a solution identified. A critical security problem is one where it is considered that urgent action needs to be taken, in order for both individual sites and the infrastructure as a whole to be secure. The most common type of critical security problem is where a software vulnerability has been found, and assessed as ‘critical’.

After a problem has been assessed as critical, and a solution is available then sites are required to take action. This document primarily defines the procedure from this time, where sites are asked to take action, and what steps are taken if they do not respond or do not take action.

If a site fails to take action, this may lead to site suspension by removing the site from the resource information system as defined in appropriate policy documents.

Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

"SHOULD", "SHOULD NOT", are to be interpreted as in the EU GridPMA IGTF as “do it this way or explain to the group why you are not doing it this way and gain mutual agreement”.

Intended Audience

This document is intended for grid site security contacts and site administrators in order to inform them what to expect and what is expected of them when they are asked to carry out an action to deal with a critical security problem. It is also intended to ensure that CSIRT members and the Security Officer on duty know what is expected of them. This document is also intended for Operations Management in order to give them visibility of the process, so that they may approve it.

Contact Points

Contact e-mail addresses used in this document:

site-security-contacts@mailman.egi.eu this address reaches the security contacts at all grid sites. The mailing list is automatically populated from GOCDB

ngi-security-contacts@mailman.egi.eu This is the National Grid Infrastructure security contacts list – again automatically populated from the GOCDB

noc-managers@mailman.egi.eu This is how to contact the National Operation Centre managers. Note that this mailing list is also used to contact the Operations Management Board (OMB) as all OMB members are on the NOC managers mailing list and no OMB specific mailing list is currently available.



Chief Operations Officer – COO is on the noc-managers list and need not be contacted separately.



TABLE OF CONTENTS

Overview.....	5
Definitions.....	5
Intended Audience.....	5
Contact Points.....	5
1 INTRODUCTION.....	9
2 CSIRT ACTIONS AND RESPONSIBILITIES – NEW CRITICAL SECURITY OPERATIONAL PROBLEM.....	10
2.1 Heads up issued.....	10
2.2 Find solution to problem.....	10
2.3 Send advisory with 7 day deadline.....	10
2.4 3 days before the deadline.....	10
2.5 For each vulnerable site.....	11
2.6 24 hours before deadline.....	11
2.7 Respond to any request and communicate with sites.....	11
3 CSIRT ACTION AND REONSIBILITIES - RE-INTRODUCTION OF CRITICAL SECURITY PROBLEM.....	12
3.1 CSIRT must open a ticket in EGI tracker.....	12
3.2 24 hours before deadline.....	12
3.3 Respond to any requests communication with sites.....	12
4 PROCEDURE FOR SITE SUSPENSION.....	13
4.1 24 hours before Site Suspension.....	13
4.1.1 Final reminder.....	13
4.1.2 Inform NOC managers and the OMB.....	13
4.2 On the Site suspension deadline.....	13
4.3 Allowing more time for some specific sites.....	14
4.4 Not carrying out site suspension.....	14
4.5 Carry out Site suspension.....	14
4.6 Getting suspended sites back into the infrastructure.....	14
5 SITES VIEW AND RESPONSIBILITIES.....	15
5.1 Site security is the responsibility of the site.....	15
5.2 Sites will be informed of critical security problems, and given time to act.....	15
5.3 Sites should contact CSIRT or their NGI security contact if they cannot carry out the recommended action.....	15
5.4 Sites will receive at least 3 notifications before site suspension is invoked.....	15
5.4.1 New problems.....	15
5.4.2 Old problems, and unsafe configuration problems.....	15
5.5 Sites will receive a final warning at least 24 hours before site suspension.....	16
6 NOC MANAGERS AND OMB VIEW.....	17
6.1 NOC managers and the OMB will be informed when action is requested to resolve a critical security problem.....	17
6.2 NOC managers and the OMB will be informed at least 24 hours before site suspension.....	17



6.3 The OMB and/or the COO may take the decision that sites are not suspended.... 17

6.4 NOC managers and the OMB will be informed if any sites get suspended..... 17

7 APPENDIX 1 - NOTES ON ACCEPTABLE ACTIONS BY SITES 18

7.1 Prior to CSIRT recommendations..... 18

7.2 After CSIRT recommendations 18

7.3 Actions which CSIRT is unlikely to see as acceptable..... 18

8 REFERENCES 19



1 INTRODUCTION

The procedure for handling of incidents by the EGI Computer Security Incident Response Team (CSIRT) is described in the EGI Incident handling procedure [R 1]. The procedure for handling software vulnerabilities (particularly in Grid Middleware which is part of the EGI UMD) by the EGI Software Vulnerability Group (SVG) is described in the Vulnerability issue handling process [R 2]. These two procedures have been approved together as Milestone MS405. However, a gap has been identified, in that after serious software vulnerabilities have been resolved it is important to ensure that all systems in the EGI infrastructure install an updated version of the software in a timely manner, and that any other serious operational security problem is resolved in a timely manner. This describes the procedure for ensuring that critical security operational issues are addressed in a timely manner and for giving sites adequate warning before removing from the EGI resource information system if they fail to make their sites secure.

The procedure is written to be agnostic relative to the systems used to establish site status, find information on sites, or track progress. This document focuses on affects on sites and CSIRT interaction with sites. Details of actual systems and what to do are maintained on the CSIRT private Wiki. More details of the procedure carried out by CSIRT including work carried out prior to establishing what action(s) should be taken by CSIRT is available in [R 3].

The CSIRT Team seeks agreement and approval of this process from the Operations Management Board (OMB). In particular approval is needed that the steps taken are acceptable leading up to site suspension if sites fail to act to deal with a critical operational security problem.



2 CSIRT ACTIONS AND RESPONSIBILITIES – NEW CRITICAL SECURITY OPERATIONAL PROBLEM

Note that actions that fall outside of working hours are on a ‘best efforts’ basis. CSIRT actions may be carried out by the EGI CSIRT Security Officer on Duty, or by any member of the CSIRT team as agreed within the team.

2.1 Heads up issued

When a critical vulnerability has been identified, CSIRT may send a ‘Heads Up’ to sites. This is to inform sites of the problem and that urgent action may be requested in the coming hours or days.

This is OPTIONAL.

If sent, it SHOULD refer to any public information on the vulnerability, and why it is a problem in the EGI environment.

2.2 Find solution to problem

CSIRT MUST define what actions should be taken. This may be to install new versions of software which does not contain the vulnerability or make a configuration change that mitigates or removes the vulnerability. In exceptional circumstances when no solution is found in a reasonable timescale this may be to suspend or stop running certain software or services. If such action results in severe service interruption, an explicit authorization from senior management must be obtained prior to recommending that sites take such action.

2.3 Send advisory with 7 day deadline

The EGI-CSIRT Security-Officer-On-Duty MUST send an advisory, this advisory MUST state what action is to be taken by sites in order to eliminate the critical security problem.

The covering letter MUST include the deadline for carrying out the action.

The deadline MUST be at least 7 days after the advisory is issued. If the deadline falls on a Friday, weekend, or common public holiday the deadline SHOULD be set to the first working day after allowing 7 days. It MUST also be clear that if sites do not carry out this action, and do not respond, then site suspension is likely.

It should be clear that CSIRT will help if necessary, and that if sites do not understand what to do or need any help they should contact CSIRT.

For widespread problems, the letter and advisory MUST be sent to site-security-contacts@mailman.egi.eu and ngi-security-contacts@mailman.egi.eu and copied to noc-managers@mailman.egi.eu

For problems which only affect a small number of individual sites, the sites can be informed individually of the problem.

2.4 3 days before the deadline

For each site that is still vulnerable, 3 days before the deadline, CSIRT MUST open a ticket in the EGI tracker. This MUST be sent to the site administrator, site security contact, and NGI security contact.



Tickets will include information that all sites might need to handle the issue. The Security-Officer-On-Duty then might add dedicated information for sites needing additional information during the follow up.

It MUST be clear that failure to act will lead to site suspension shortly after the deadline.

2.5 For each vulnerable site

Check daily whether the site has acted. If it has, CSIRT SHOULD close the ticket and include 'Thank you for addressing this problem'. If not, CSIRT MUST send a reminder.

2.6 24 hours before deadline

CSIRT SHOULD produce a list of which sites have not updated, and send this to noc-managers@mailman.egi.eu. The site will also receive a final warning as the first step of the site suspension process as described in section 4

If all sites have updated, CSIRT SHOULD inform noc-managers@mailman.egi.eu, and there is no need for further action.

2.7 Respond to any request and communicate with sites

CSIRT MUST respond to any request for more information or help from sites, and do all they can to help individual sites remove the critical security problem. Alternative solutions other than that may be agreed between the site and CSIRT – some notes on this are in section 7.



3 CSIRT ACTION AND REPONSIBILITIES - RE-INTRODUCTION OF CRITICAL SECURITY PROBLEM

Sometimes an 'old' critical security problem may apparently re-appear from the monitoring of site security. Sometimes a site that does not register as vulnerable as defined in section 2.4 may appear vulnerable later in the run up to the 7 day deadline. It is not expected that this will be a widespread problem. In both these cases, sites are given a minimum of 48 hours to respond and resolve the problem before the site is suspended. A similar procedure may also be used to deal with any other serious security problem at an individual site.

3.1 CSIRT must open a ticket in EGI tracker

CSIRT MUST open a ticket in the EGI tracker. This MUST be sent to the site administrator, site security contact, and NGI security contact. This ticket MUST include a reference to the previous advisory, SHOULD have the previous advisory appended, and allow the site a minimum of 48 hours to act or respond.

3.2 24 hours before deadline

After 24 hours, check whether the site has acted. If it has, CSIRT SHOULD close the ticket and include 'Thank you for addressing this problem'. If not, CSIRT MUST send a reminder.

If the site has not acted CSIRT SHOULD inform noc-managers@mailman.egi.eu of the problem. The site will also receive a final warning as the first step of the site suspension process as described in section 4.

3.3 Respond to any requests communication with sites

CSIRT MUST respond to any request for more information or help from sites, and do all they can to help individual sites remove the critical security problem. Alternative solutions other than that may be agreed between the site and CSIRT – some notes on this are in section 7.

4 PROCEDURE FOR SITE SUSPENSION

In the case where sites fail to act on a critical security problem the site suspension procedure MAY be invoked at the discretion of CSIRT. The EGI Grid Site Operations [R 4] allows sites to be suspended by removing the site from the resource information system. This procedure implements the policy. Also note that a specific site suspension policy document is also going to be written by the EGI SPG.

Normally this procedure will be invoked in parallel to the steps in section 2 or 3 to handle a critical security problem. In extreme circumstances (e.g. where an individual site has behaved in a reckless manner) it may be invoked independently.

4.1 24 hours before Site Suspension

The following 2 steps MUST be carried out at approximately the same time, but may be an hour or two apart. They MUST be carried out at least 24 hours before site suspension is carried out.

4.1.1 Final reminder

The EGI CSIRT MUST notify the affected site's security contact and NGI security officers that unless they carry out the recommended action by the deadline the site will be suspended. Clearly state that failure to comply with the recommendations/advisories sent earlier will lead to site suspension. State that this is a final reminder.

It MUST be made clear that if there is a problem carrying out the recommended action CSIRT will try and help to find a solution. Attempts MUST be made to find a solution with the site if at all possible, and site suspension should only be invoked in the case of no response or failure to find a way to prevent it.

4.1.2 Inform NOC managers and the OMB

CSIRT MUST send a summary to NGI-Management and the OMB (noc-managers@mailman.egi.eu) with the following information:

- Which steps were taken by EGI-CSIRT.
- For each site which is still vulnerable
 - The name of the site
 - If the site has simply not responded, state this.
 - If the site has stated why the recommendations could not be followed, include this.
 - Include any relevant information on plans/alternative mitigation for the site.
 - Include whether CSIRT is recommending suspension for the site.
- State that if the situation does not change CSIRT plans to suspend the site on the deadline.

4.2 On the Site suspension deadline

If EGI CSIRT takes the decision to suspend a site, CSIRT MUST inform NGI management and the OMB (noc-managers@mailman.egi.eu) and COO about the decision including which sites are being suspended and why.

Send all these sites a notification that site suspension is about to be carried out and why.

4.3 Allowing more time for some specific sites

In some circumstances the deadline for specific sites may be delayed to allow more time to carry out suitable actions. This will be at the discretion of CSIRT. CSIRT will always work with the sites to try and prevent site suspension, and find an acceptable solution that can be carried out in the near future so that there is no need for site suspension.

Site may also be given more time on the request of the COO and/or OMB.

4.4 Not carrying out site suspension

Site suspension will not be carried out if the COO states that it is not to be carried out.

Site suspension will not be carried out if the majority of OMB members state it should not be carried out.

Note that it is up to the COO and/or OMB members to act if when they are informed as in section 4.1.2 if they do not wish site suspension to happen. Approval of the procedure will imply that site suspension will happen according to the procedure unless the COO and/or OMB acts to prevent it.

Site suspension is seen as a last resort, and if CSIRT can find a solution with the site then site suspension will not be carried out.

4.5 Carry out Site suspension

Site suspension may be carried out by the EGI CSIRT co-ordinator or deputy may suspend a site by changing the status of the site in the GOCDB to 'suspended'.

All sites which are suspended must be recorded at https://wiki.egi.eu/wiki/Underperforming_sites_and_suspensions.

4.6 Getting suspended sites back into the infrastructure

If a suspended site wishes to become part of the Grid again they should indicate to CSIRT that they have taken appropriate action, if CSIRT is satisfied then the CSIRT co-ordinator or deputy will certify the site and reverse the suspension in the GOCDB.

Alternative (TBD)

If a suspended site wishes to become part of the Grid again they should indicate to their ROD that they want to be part of the Grid again. The ROD then sets the site to 'Uncertified' and then the site certification procedure takes place.

5 SITES VIEW AND RESPONSIBILITIES

5.1 Site security is the responsibility of the site

Sites are responsible for their own security. CSIRT and other security groups in EGI exist to help keep sites to be as secure as possible. Sites **MUST** carry out some actions recommended by CSIRT in order for the site to remain part of the Grid, i.e. the site information being in the resource information system.

5.2 Sites will be informed of critical security problems, and given time to act

If a critical security problem has been identified, sites will be informed of what they need to do. Normally initially this will be a general e-mail and advisory given to all sites

Sites **SHOULD** act to eliminate critical security problems as quickly as possible.

Sites **MUST** act before the deadline, which will be at least 7 days away for any new problem.

Individual sites will always be given at least 48 hours to act, if an old problem is re-introduced or an unsafe configuration is found.

One possible exception is if an incident occurs at a site; particularly if it is adversely affecting other sites.

5.3 Sites should contact CSIRT or their NGI security contact if they cannot carry out the recommended action

If sites do not understand the advisory, or have problems acting on it, sites **SHOULD** contact CSIRT or their NGI security contact for help.

If a site wishes to carry out a different action to that recommended by CSIRT, the site **MUST** contact CSIRT or their NGI security contact. CSIRT must agree that the alternative action by the site is satisfactory.

If a site is unable to act or needs more time, the site **MUST** contact CSIRT or their NGI security contact and attempt to agree a solution.

CSIRT and the NGI security contacts are available to help sites find a satisfactory solution.

5.4 Sites will receive at least 3 notifications before site suspension is invoked

5.4.1 New problems

Sites will at least receive an initial 7 day deadline notification and at least 2 further individual reminders including a final warning as stated in section 5.5 before site suspension is invoked. Sites will normally receive a reminder 3 days before the deadline and daily until the deadline, if they do not carry out the appropriate action. They will also receive a final notification that site suspension is about to proceed.

5.4.2 Old problems, and unsafe configuration problems

For the re-introduction of old problems, or unsafe site configurations, sites will receive an initial notification giving them at least 48 hours to act, a reminder 24 hours later, and a final notification that site suspension is about to proceed.



5.5 Sites will receive a final warning at least 24 hours before site suspension

If a site fails to carry out appropriate action, sites will receive a warning at least 24 hours before site suspension.



6 NOC MANAGERS AND OMB VIEW

6.1 NOC managers and the OMB will be informed when action is requested to resolve a critical security problem

The notification and advisory, along with the deadline, will be copied to the NOC managers and the COO as in section 2.3

6.2 NOC managers and the OMB will be informed at least 24 hours before site suspension

At least 24 hours before the deadline, NOC managers, the OMB and the COO will be informed of how many sites have failed to carry out the requested action as in section 2.6 or in 3.2 and that the site suspension will result if appropriate action is not carried out.

6.3 The OMB and/or the COO may take the decision that sites are not suspended

A majority decision of the OMB and/or the COO may overrule site suspension.

6.4 NOC managers and the OMB will be informed if any sites get suspended.

NOC managers, the OMB and the COO will be informed if any sites actually get suspended. This should include the name(s) of sites, the date and time they are suspended, and why.

7 APPENDIX 1 - NOTES ON ACCEPTABLE ACTIONS BY SITES

This is not extensive, but is intended to provide some guidelines on which types of actions are acceptable to resolve a critical security problem and which are not.

7.1 *Prior to CSIRT recommendations*

Sites may take any reasonable action they wish when a critical security problem has been identified but no action has yet been recommended by the CSIRT team.

This may include:

- Install a version of software which has been re-compiled using own patch
- Suspending services
- Closing the site
- Configuration changes that mitigate the problem

Different sites may be affected in different ways by a critical security problem, depending on their own situation, and are allowed to make their own judgements on what action to take prior to a recommended solution being available.

7.2 *After CSIRT recommendations*

Sites must take action, acceptable actions include:

- The action recommended by CSIRT
- For a critical software vulnerability,
 - Update to a version which does not contain the vulnerability
 - Carry out their own re-build with the vendors patch to resolve the vulnerability
 - Carry out other vendor recommended action
- Action agreed with CSIRT
- An explanation of why the site is not vulnerable which is satisfactory to CSIRT

Note that if a site thinks they have taken appropriate action yet CSIRT considers them vulnerable they **MUST** explain why they think they are not vulnerable. A solution **MUST** be found that is acceptable to CSIRT.

7.3 *Actions which CSIRT is unlikely to see as acceptable*

- If monitoring suggests the site is vulnerable and the site has acted
 - Fail to respond
 - Fail to explain why they do not think their system is vulnerable
 - Fail to explain what alternative actions have been carried out to deal with the critical security problem



8 REFERENCES

R 1	The EGI Security incident handling procedure MS405 https://documents.egi.eu/public/ShowDocument?docid=47
R 2	The EGI Software Vulnerability Issue handling process MS405 https://documents.egi.eu/public/ShowDocument?docid=47
R 3	The EGI Critical Vulnerability Handling procedure https:// documents.egi.eu/public/ShowDocument?docid=282
R 4	EGI Grid Site Operations Policy https://documents.egi.eu/secure/ShowDocument?docid=75
R 5	