EGI-InSPIRE

INCIDENT RESPONSE PROCEDURE

Document identifier:	EGI-Procedure-CSIRT-693-V2.doc
Date:	**28/07/2011**
Activity:	**SA1**
Lead Partner:	
Document Status:	**DRAFT**
Dissemination Level:	**PUBLIC**
Document Link:	https://documents.egi.eu/document/693

Abstract

This procedure is aimed at minimising the impact of security incidents by encouraging post-mortem analysis and promoting cooperation between grid sites. It is based on the EGI Incident Response policy [R1].



I. COPYRIGHT NOTICE

II. DELIVERY SLIP

	Name	Partner/Activity	Date
From			
Reviewed by	**Moderator:** **Reviewers:**		
Approved by			

III. DOCUMENT LOG

Issue	Date	Comment	Author/Partner
1	28/06/2011	First Draft based on MS405, a few minor update, added appendix C and appendix D	Mingchao Ma/STFC
2	28/07/2011	Addressed comments from Dorine	Mingchao Ma/STFC
3	11/10/2011	Corrected a reference in the incident response check list (appendix D)	Mingchao Ma/STFC

IV. 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.

V. 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

VI. TERMINOLOGY

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

VII. 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.

VIII. EXECUTIVE SUMMARY

This procedure is aimed at minimising the impact of security incidents by encouraging post-mortem analysis and promoting cooperation between grid sites. It is based on the Grid Incident Response policy [R1] and is essentially the well-established Incident Response Procedure in EGEE.

This grid incident response procedure is aiming at complementing local security procedures. Unless specified otherwise in separate service level agreements, all times in this document refer to normal local working hours.

This document is intended for grid site security contacts and site administrators and is primarily aimed at reporting security incidents.

TABLE OF CONTENTS

1 INTRODUCTION

Grid sites are tightly interconnected, both in a technical fashion through various middlewares and in a human fashion through shared staff and users. This is basically a good thing, and a prerequisite for building a cohesive e-Infrastructure. However, this also means that security incidents can very quickly spread between sites. Incident response must be proportionally strong and decisive.

This document describes the procedure for incident response in the European Grid Infrastructure. It aims at minimizing the impact of security incidents by encouraging post-mortem analysis and promoting cooperation between grid sites. It is based on the EGI security Incident Response policy [R1]. To assist the audience to make better use of this document, a flow chart and check list are also provided in appendix C and D respectively

The intended audience of this document is grid site security contacts and site. Unless specified otherwise in separate service level agreements, all times in this document refer to normal local working hours.

2 DEFINITIONS

A security incident is the act of violating an explicit or implied security policy (ex: local security policy, EGI Acceptable Use Policy).

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

3 CONTACT POINTS

Contact e-mail addresses used in this document:

abuse@egi.eu – this address reaches the Incident Response Task Force within the EGI CSIRT and is the main contact point for reporting security incidents.

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

4 SITE RESPONSIBILITIES

When a security incident potentially affecting grid users, services or operations is suspected, the following procedure MUST be followed:

1. Immediately inform your local security team, your NGI Security Officer and the EGI CSIRT via abuse@egi.eu. **This step MUST be completed within 4 hours after the suspected incident has been discovered.** You are encouraged to use the templates in Appendix B.
2. Do NOT reboot or power off the host. In case no support is shortly available, whenever feasible and, if admitted by your local security procedure and if you are sufficiently familiar with the host/service to take responsibility for this action, try to contain the incident. For instance by unplugging all connections (network, storage, etc) to the host. Please note down carefully what actions you take with a timestamp; that would be very important for later analysis as well as if the incident ends up in a legal case. **This step SHOULD be completed as soon as possible, and MUST be completed within one working day after the suspected incident has been discovered**.
3. Confirm the incident, with assistance from your local security team and the EGI CSIRT.
4. If applicable, announce downtime for the affected hosts in accordance with the EGI operational procedures [R2], with "Security operations in progress" as the reason. **If applicable, this step MUST be completed within one working day after the suspected incident has been discovered.**
5. Perform appropriate analysis and take necessary corrective actions as per Appendix A. Logging information such as IP addresses, timestamps and identities involved etc., concerning the source of any suspicious successful connection, must meet the minimal requirements specified in Appendix A. The objective is to understand the source and the cause of the incident, the affected credentials and services, and the possible implications for the infrastructure. **Throughout step 5, requests from the EGI CSIRT MUST be followed-up within 4 hours.**
6. Coordinate with your local security team and the EGI CSIRT to **send an incident closure report within 1 month** following the incident to all the sites via site-security-contacts@mailman.egi.eu, including lessons learnt and resolution. This report should be labelled AMBER or higher, according to the Traffic Light Protocol [R3].
7. Restore the service and, if needed, update the service documentation and procedures to prevent recurrence as necessary.

5 INCIDENT COORDINATOR RESPONSIBILITIES

The EGI CSIRT appoints a security incident coordinator for each incident. This may be the Duty Contact or another CSIRT member. The tasks of the incident coordinator include:

1. Evaluate the initial incident report and determine whether it appears to be part of a multi-site incident. That is, whether it is related to a previously known incident (e.g. do the same attacking IP addresses appear, are the attacker's tools and methodology strongly similar).
2. If this is a new, unrelated incident, assign an identifying tag (of the format "[EGI-20100101]", or, if multiple incidents occur on the same date, "[EGI-20100101-01]") to the incident and announce it to all sites via site-security-contacts@mailman.egi.eu – see e-mail templates in Appendix B. **This step MUST be completed within 4 hours after the suspected incident is reported by the site.**
3. If the incident is part of a multi-site incident, the incident coordinator MAY choose not to announce each incident separately, but instead issue regular updates on the overall multi-site incident.
4. Whenever and as often as necessary, send updated summary reports to all sites (site-security-contacts@mailman.egi.eu), containing the status of the incident and possibly details needed to search locally for signs of malicious activity. Never send sensitive information without prior agreement of the originating site.
5. Whenever and as often as necessary, send updated detailed reports to the sites directly involved and affected by the incident, containing interesting findings or possible leads that could be used to resolve the incident
6. Actively stimulate and probe the affected parties to obtain accurate information at an appropriate level of detail and in a timely manner.
7. Aim at understanding the exact cause and extent of the incident, what assets have been compromised (credentials etc.), and how to resolve the incident.
8. Help involved sites resolve the incident by providing recommendations, promoting collaboration with other sites and periodically checking their status.
9. Maintain communications with any other involved parties inside and outside EGI.
10. When suspended accounts or identities no longer represent a threat, typically when the incident is resolved and compromised credentials have been re-issued, inform the sites that access from these accounts or identities can be restored.

6 REFERENCES

R 1	The EGI Incident Response Policy; https://documents.egi.eu/document/82
R 2	EGI Operational Procedures; https://documents.egi.eu/document/15
R 3	Traffic Light Protocol; https://wiki.egi.eu/wiki/EGI_CSIRT:TLP

APPENDIX A: INCIDENT ANALYSIS

As part of the security incident resolution process, sites are expected to produce the following information:

- Host(s) affected (ex: compromised hosts, hosts running suspicious user code)
- Host(s) used as a local entry point to the site (ex: UI or WMS IP address)
- Remote IP address(es) of the attacker
- Evidence of the compromise, including timestamps (ex: suspicious files or log entry)
- What was lost, details of the attack (ex: compromised credentials, (root) compromised host)
- If available and relevant, the list of other sites possibly affected
- If available and relevant, possible vulnerabilities exploited by the attacker
- The actions taken to resolve the incident
- Identify and kill suspicious process(es) as appropriate, but aim at preserving the information they could have generated, both in memory and on disk.
- If it is suspected that some grid credentials have been abused or compromised, you MUST ensure the relevant accounts have been suspended
- If it is suspected that some grid credentials have been abused, you MUST ensure that the relevant VO manager(s) have been informed. VO contacts are available from: https://cic.gridops.org/index.php?section=vo
- If it is suspected that some grid credentials have been compromised, you MUST ensure that the relevant CA has been informed. CA contacts are available from: https://www.eugridpma.org/showca
- If needed, seek help from your local security team, from your NGI Security Officer or from the EGI CSIRT
- If relevant, additional reports containing suspicious patterns, IP addresses, files or evidence that may be of use to other Grid parties SHOULD be sent to the EGI CSIRT.

As part of the investigations, sites MUST be able to provide the relevant logging information produced by local services. Logging information such as IP addresses, timestamps and identities involved etc., concerning the source of any suspicious successful connection, must meet the following minimal requirements:

- 6 months prior to the discovery of the incident for successful SSH connections against grid services, and for the originating submission host for grid jobs
- 3 months prior to the discovery of the incident for all other grid related services.

For example, should an incident be detected and reported on 1st of September, it is expected that sites can produce the relevant logging information for suspicious SSH connections from 1st of March.

APPENDIX B: TEMPLATES FOR REPORTING A SECURITY INCIDENT

Should a security incident be suspected, the use of the following email templates is encouraged. They can be used both by the site security officer to communicate with the EGI CSIRT and by the incident coordinator to broadcast information to the sites. Normally, they should be labelled AMBER or higher, according to the Traffic Light Protocol [R3].

The first template is aimed at notifying the grid participants soon after the incident has been discovered (heads-up), as described in Step 2 of the procedure above.

FROM: <you>
TO: <site-security-contacts@mailman.egi.eu/abuse@egi.eu>
SUBJECT: Security incident suspected at <site> [EGI-<DATE>] TLP: AMBER
*** AMBER Information – Limited Distribution ***
*** This may be shared with trusted security teams on a need-to-know basis ***
*** see https://wiki.egi.eu/wiki/EGI_CSIRT:TLP for distribution restrictions ***
Dear security contacts,

A suspected security incident has been detected at <site>.

Summary of the information available so far:

<Ex: A malicious SSH connection was detected from 012.012.012.012. The extent of the incident is unclear for now, and more information will be published in the coming hours as forensics are progressing at our site. However, all sites should check for successful SSH connection from 012.012.012.012 as a precautionary measure.>

The second template can be used to provide a detailed view of the incident, and may be completed and reposted as the investigation progresses.

FROM: <you>
TO: <site-security-contacts@mailman.egi.eu/abuse@egi.eu>
SUBJECT: Security incident suspected at <site> [EGI-<DATE>] TLP:AMBER
*** AMBER Information – Limited Distribution ***
*** This may be shared with trusted security teams on a need-to-know basis ***
*** see https://wiki.egi.eu/wiki/EGI_CSIRT:TLP for distribution restrictions ***
Dear security contacts,

A security incident has been detected at <site>.

- Short summary of the incident
<Provide a high-level overview of the incident>

- Host(s) affected
<List of compromised hosts and/or hosts running suspicious user code.
ex: grid-worker-node-124.mysite.org (123.123.123.123)>

- Host(s) used as a local entry point to the site (ex: UI or WMS IP address)
<The host that the attacker is likely to have used to access the site.
ex: grid-ui-101.mysite.org (123.123.123.124)>

- Remote IP address(es) of the attacker
<The remote host from where the attacker is likely to have connected from.
ex: 123.adsl.somecorp.com (012.012.012.012)>

- Evidence of the compromise, including timestamps (ex: suspicious files or log entry)
<Ex: the attacker logged in has root from 123.adsl.somecorp.com. Times are UTC:
Mar 24 12:00:09 grid-ui-101 sshd[13896]: Accepted password for root from 012.012.012.012>

- What was lost, details of the attack
<Provide available details on the extent of the compromise. Ex:
System logs revealed the attacker guessed the root password of grid-ui-101 on Mar 24 12:00:09 (UTC) after hundreds of attempts. Then, the attacker [...] etc.>

- If available and relevant, the list of other sites possibly affected
<Ex: firewall logs reveal suspicious SSH connections from the compromised node to grid-ui.friendlysite.org on Mar 24 13:01:03 (UTC). friendlysite.org has been contacted.>

- Possible vulnerabilities exploited by the attacker
<Ex: the attacker exploited a weak root password and gained further access by exploiting CVE-2009-1234 against [...] etc.>

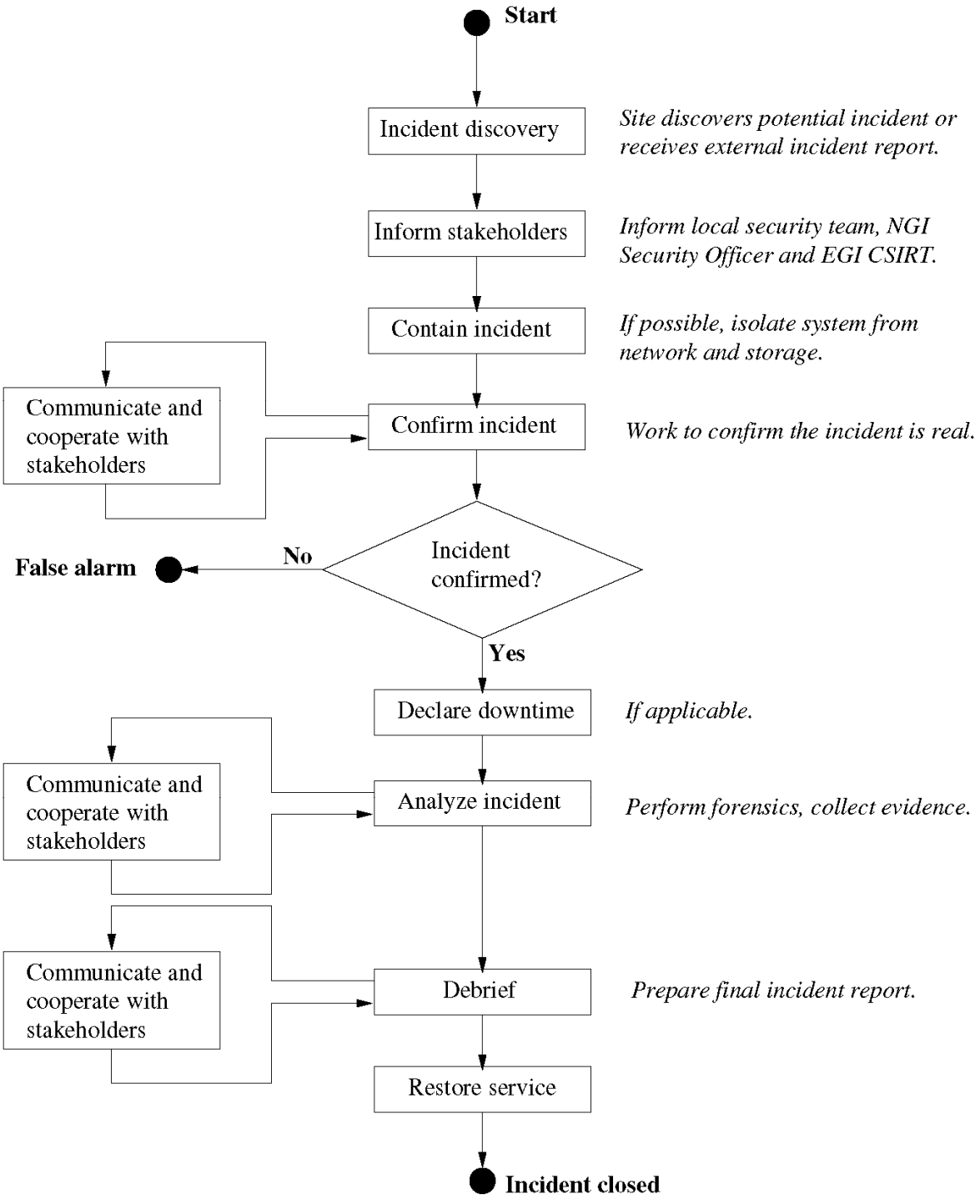
- Actions taken to resolve the incident
<Ex: Disk images have been saved, hosts have been reinstalled from scratch with new, strong root passwords, and SSH has been configured to prevent "root" logins with password.>

- Recommendations for other sites, actions suggested
<Ex: Sites should check and report any successful SSH connection from grid-ui-101 between Mar 24 12:00:09 (UTC) and Mar 24 17:00:00 (UTC).
It is also recommended to avoid direct SSH access, and to configure sshd with "PermitRootLogin without-password".>

- Timeline of the incident
<Ex:
2009-03-24 09:12:43 UTC Multiple SSH connection attempts from 012.012.012.012
2009-03-24 12:00:09 UTC Attacker connects as root on grid-ui-101.mysite.org from 012.012.012.012
2009-03-24 13:01:03 UTC SSH scan from grid-ui-101 against grid-ui.friendlysite.org

[...]
2009-03-24 15:00:00 UTC Site security team investigating
2009-03-24 15:34:00 UTC EGI security contacts informed [...]>

APPENDIX C: FLOW CHART FOR INCIDENT RESPONSE



APPENDIX D: INCIDENT RESPONSE CHECK LIST

EGI Incident Response Procedure — Site Checklist

Revision 1744 (2011-10-10)

1 – (Suspected) Discovery

1. ☐ Local Security Team — *If applicable: INFORM **WITHIN 4 HOURS**.*
2. ☐ NGI Security Officer — *INFORM **WITHIN 4 HOURS**.*
3. ☐ EGI CSIRT Duty Contact — *INFORM via "abuse@egi.eu" **WITHIN 4 HOURS**.*

2 – Containment

1. ☐ Affected Hosts — *If feasible: ISOLATE as soon as possible **WITHIN 1 WORKING DAY**.*

3 – Confirmation

1. ☐ Incident — *CONFIRM WITH YOUR LOCAL SECURITY TEAM AND/OR EGI CSIRT.*

4 – Downtime Announcement

1. ☐ Service Downtime — *If applicable: ANNOUNCE WITH REASON "SECURITY OPERATIONS IN PROGRESS" **WITHIN 1 WORKING DAY**.*

5 – Analysis

1. ☐ Evidence — *COLLECT AS APPROPRIATE.*
2. ☐ Incident Analysis — *PERFORM AS APPROPRIATE.*
3. ☐ Requests From EGI CSIRT — *FOLLOW UP **WITHIN 4 HOURS**.*

6 – Debriefing

1. ☐ Post-Mortem Incident Report — *PREPARE AND DISTRIBUTE via "site-security-contacts@mailman.egi.eu" **WITHIN 1 MONTH**.*

7 – Normal Operation Restoration

1. ☐ Normal Service Operation — *RESTORE AS PER SITE STANDARDS **AFTER INCIDENT HANDLING IS COMPLETE**.*
2. ☐ Procedures and Documentation — *UPDATE as appropriate to reflect analysis results.*

References

- EGI Incident Response Procedure — *https://documents.egi.eu/document/710*
- EGI CSIRT Wiki — *https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page*
- EGI Security Team Contacts — *https://wiki.egi.eu/wiki/EGI_CSIRT:Contacts*
- EGI CSIRT Abuse Report E-Mail Address — *abuse@egi.eu*