COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT) TERMS OF REFERENCE (TOR)

Document identifier	EGI-CSIRT-TOR-385-V2
Document Link	https://documents.egi.eu/document/385
Last Modified	19/08/2019
Version	2
Policy Group Acronym	CSIRT
Policy Group Name	Computer Security Incident Response Team
Contact Person	Sven Gabriel/Nikhef, NL
Document Type	Terms of Reference (ToR)
Document Status	For Approval by EGI Foundation Executive Board
Approved by	EGI.eu
Approved Date	19/08/2019

Purpose of this Document

The purpose of this document is to set out the Terms of Reference, composition and operating arrangements of the EGI Computer Security Incident Response Team (EGI CSIRT).

COPYRIGHT NOTICE

AUTHORS LIST

	Name	Partner/Activity/ Organisation/Function	Date
From	Sven Gabriel on behalf of EGI CSIRT	Nikhef/CSIRT Chair	30/11/2016

DELIVERY SLIP

	Body	***Date***
Reviewed by:	EGI Operations Management Board	24/11/2016
Approved by:	EGI Foundation Executive Board	

DOCUMENT LOG

Issue	***Date***	***Comment***	***Author/Partner***
V1	11/10/2011	Initial approved version	Mingchao Ma / STFC
V2	24/11/2016	Reviewed version from OMB for EGI Foundation Executive Board approval	Sven Gabriel / Nikhef

TERMINOLOGY

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

AMENDMENT PROCEDURE

Reviews and amendments should be done in accordance with the EGI “Policy Development Process” (https://documents.egi.eu/document/169). See also Section 9.

TABLE OF CONTENTS

1 Title....4

2 Definitions....4

3 Purpose and Responsibilities....4

3.1 Constituency....5

3.2 Service Description....5

3.2.1 Assessment of security vulnerabilities....5

3.2.2 Advisories....5

3.2.3 Security Monitoring....5

3.2.4 Incident Response Task Force (IRTF)....5

3.2.5 Training and Dissemination....5

3.2.6 Security Drills Group (SDG)....6

3.3 Service Level Description....6

4 AUTHORITY....6

5 Composition....6

5.1 Membership....6

5.2 Chair....7

5.2.1 Duties....7

5.2.2 Term of Office....7

5.2.3 Method of Appointment....7

6 OPERATING PROCEDURES....8

6.1 Communications and Meetings....8

6.2 Decision Making....8

6.3 Communication Channels....9

6.4 Reports....9

7 Evaluation....9

8 Related Material....9

9 Amendment....10

1 TITLE

The name of the group is EGI Computer Security Incident Response Team ("EGI CSIRT", hereafter also refer as "The Team" or "The Group").

2 DEFINITIONS

Word/Term	Definition
CSIRT	Computer Security Incident Response Team
VO	Virtual Organisation
IRTF	Incident Response Task Force
TI TF-CSIRT	Trusted Introducer Task-Force CSIRT[1]
SDG	Security Drills Group
SMG	Security Monitoring Group
TDG	Training and Dissemination Group
OMB	Operations Management Board
SOM	Senior Operations Manager
NREN	National Research and Education Network
NGI	National e-Infrastructure represented within EGI
EIRO	European International Research Organization
RC	Resource Centre

3 PURPOSE AND RESPONSIBILITIES

The EGI Computer Security and Incident Response Team (EGI-CSIRT) provides operational security for the EGI Infrastructure. This includes responding to computer security incidents affecting the infrastructure, which is carried out by co-ordinating the incident handling activities in the NGIs/EIROs, RCs, VOs, and where applicable interacting with partner Infrastructures CSIRTs and CSIRT communities with which EGI-CSIRT has a trust relationship.

If needed RCs are provided with expert level forensics support for the incident resolution.

EGI-CSIRT also provides preventive and educational services such as security monitoring, vulnerability assessment, advisories to mitigate risks due to vulnerabilities, and security training.

To improve collaboration in the field of IT-Security EGI-CSIRT actively reaches out to CSIRT communities and is an active member of TI TF-CSIRT.

The EGI CSIRT is led and coordinated by the EGI Security Officer.

[1] http://www.terena.org/activities/tf-csirt/

3.1 Constituency

EGI-CSIRT provides operational security (see "Purpose and Responsibilities") for all Resource Centres that have a signed OLA with EGI and for all partner infrastructures (NGIs) that have a signed operational MoU with EGI.

3.2 Service Description

Members of EGI CSIRT provide or assist in providing the following services.

3.2.1 Assessment of security vulnerabilities

Assist the Software Vulnerability Group in assessing the risk posed to the EGI Infrastructure by reported software vulnerabilities.

The course of further vulnerability handling is based on the agreed Criticality (CRITICAL, HIGH, MEDIUM, LOW).

For details see: Software Vulnerability Group (SVG) - Terms of Reference[2]

3.2.2 Advisories

Issue advisories concerning vulnerabilities in hardware or software running on the infrastructure assessed as having a 'High' or 'Critical' risk to the EGI infrastructure. These define mitigating actions that should be carried out. In the case of 'Critical' risk vulnerabilities members of the infrastructure are required to act or risk suspension from the infrastructure according to current policy.

3.2.3 Security Monitoring

Develop, deploy and maintain security monitoring tools. This includes monitoring of software versions and the configuration status of services running in the infrastructure with regard to the mitigations described in the advisories on ‘High’ or ‘Critical’ risk vulnerabilities.

3.2.4 Incident Response Task Force (IRTF)

Provide the Security Officer on Duty role on a weekly rota basis. The duty officer handles the day-to-day operational security issues and coordinates Computer Security Incident Response across the EGI infrastructure. The duty officer also follows up on monitoring alarms raised on detected CRITICAL software vulnerabilities. Sites not reacting to requests risk suspension from the infrastructure according to current policy. Current security issues and the status of open incidents and vulnerability handling tickets are discussed by IRTF members in weekly handover meetings.

3.2.5 Training and Dissemination

Raise awareness of security issues and improve security skills for participants in the infrastructure, particularly for system administrators and security contacts.

This is carried out by providing best practice training in secure service operation. For security experts, incident response and forensics training is provided.

[2] https://documents.egi.eu/public/ShowDocument?docid=108

This training is organised several times per year during conferences and meetings.

3.2.6 Security Drills Group (SDG)

The aim is to improve the incident response capabilities of participants in the project. Realistic simulation of security incidents is designed and implemented to assess the efficiency of EGI's incident response procedures and the particular set up at Resource Centres in the context of security operations. Improvements will be recommended where identified.

3.3 Service Level Description

The Services described above are provided where applicable at a service level defined in the Operation Level Agreement between EGI-CSIRT and EGI[3].

4 AUTHORITY

EGI CSIRT is authorised by the EGI Council through the EGI Foundation Executive Board to investigate any activity within its Terms of Reference and take controlling actions as defined in the Grid Security Policy and further policies and procedures referred to in that document[4]. In particular EGI-CSIRT may:

- Control the access of users to the infrastructure for security reasons
- Control RCs access to the Grid for security purposes and remove RCs resource information from resource information systems if they fail to act on a communicated critical security problem.

The EGI Council and the EGI Foundation Executive Board are the governing bodies of the Group.

5 COMPOSITION

5.1 Membership

EGI CSIRT consists of:

- NGI security officers and their deputies
- The NGI security officer is the voting member, their deputies can only vote if the full member is not available
- EGI Directorate and EGI Chief Operations Manager
- When members join EGI CSIRT they agree not to disclose confidential information concerning EGI CSIRT operation to which they have access outside of the confines of the team, without the agreement of the team
- When members join EGI CSIRT they acknowledge that they have read and understood the CSIRT Code of Practice document[5] and that they will

[3] https://documents.egi.eu/document/2170

[4] https://documents.egi.eu/document/86

[5] https://www.trusted-introducer.org/CCoPv21.pdf

comply with the MUST principles that are stated within it, and give proper attention to the SHOULD principles
- At any time any 3 voting members can together invite external experts to be temporary members as deemed necessary for the purposes of assisting in incident response. Such temporary membership will expire after 3 months unless converted to permanent membership by a majority vote and in any case shall be renewed annually.

5.2 Chair

Leadership of and Chair of EGI CSIRT is an EGI core activity. The Chair does not represent his/her own organisation; the organisation(s) responsible for this activity is able to nominate its own representative subject to the agreement of the EGI Foundation Managing Director. A Deputy Chair will be appointed subject to the agreement of the EGI Foundation Director.

5.2.1 Duties

The duties of the Chair include:

- Scheduling and running EGI CSIRT meetings and ensuring that minutes are taken and published
- Ensuring all discussion items end with a decision, action or definite outcome
- Inviting specialists to attend meetings when required according to the EGI CSIRT agenda
- Acting as general point of contact for EGI CSIRT
- Ensuring that documents produced are presented for approval and adoption and that once approved these are published and made available in the document repository
- Ensuring that EGI CSIRT meets the various demands placed on it to produce and maintain policy, procedure and best practice. This will include negotiation with EGI management, members of the Group and other stakeholders to agree priorities and timelines commensurate with the effort available to the Group
- Reporting to the EGI Chief Operations Manager when requested and as required.

5.2.2 Term of Office

The Term of Office is unlimited.

5.2.3 Method of Appointment

The EGI Foundation participant(s) responsible for performing the duties of the EGI CSIRT core activity appoint the Chair and Deputy Chair subject to the approval of the EGI Foundation Managing Director.

6 OPERATING PROCEDURES

The operation of EGI CSIRT will obey the EGI security policies and follow the procedures approved by EGI management. Any stakeholder of EGI also has the right to suggest new policies and procedures or revision of old policies and procedures, which in their opinion need revision. These requests should be submitted to the Chair of EGI CSIRT who will discuss it with EGI CSIRT during a subsequent meeting of the Group. The decision whether to accept this request or not will be recorded in the minutes of the meeting and feedback will be provided to the original requestor.

6.1 Communications and Meetings

All the members of the Group must subscribe to the EGI CSIRT mailing list (csirt@Egi.eu) and should use it as the primary written communication channel.

To allow for low latency communications, a secure instant messaging service is available to the team via EGI-SSO.

The Group deliberations happen at face-to-face meetings, phone/video conferences or via the Group mailing list.

The Group will meet face to face at least once per year; ideally three times per year and one of them will be at one of the bi-annual EGI Forums where practicable. The team will meet virtually (online/phone/video) once per month where practicable.

To enable consideration, where practicable, the draft agenda together with reports and documents that relate to the Group will be forwarded to members three working days prior to scheduled meetings.

Accurate minutes will be kept of each meeting of the Group. The minutes of a meeting shall be submitted to Group members for ratification at the next subsequent meeting of the Group.

The Group's public wiki and private wiki are listed in section 6.3. Due to the nature of EGI CSIRT operation and sensitivity of issues discussed at meetings, all minutes are posted on group's private wiki and only accessible by EGI CSIRT members.

6.2 Decision Making

- Wherever possible, the Group will arrive at proposed draft recommendations documents and/or advice by clear consensus, as determined by the Chair
- A voting process will only start if consensus cannot be reached after two consecutive group meetings or if at least one third of voting members of the Group call for a vote
- A decision is adopted if more than 50% of the voting members present cast their vote for the proposed decision
- If the Group's recommendations are adopted by majority vote, minority positions will be recorded and reported

- The Group may, by majority decision, refer matters for decision to the Director on issues where a consensus cannot be achieved.

6.3 Communication Channels

Communication Channel	Reference
EGI CSIRT team mailing list	csirt@mailman.egi.eu
Reporting a security incident	abuse@egi.eu, csirt@egi.eu, security@egi.eu
EGI CSIRT Main wiki	https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page
EGI CSIRT Private wiki (members only)	https://wiki.egi.eu/csirt/index.php/Main_Page
NGI security officers mailing list	ngi-security-contacts@mailman.egi.eu
EGI sites CSIRT mailing list	site-security-contacts@mailman.egi.eu
Jabber server (instant messaging using XMPP protocol)	https://www.egi.eu/about/intranet/jabber-howto.html

6.4 Reports

EGI CSIRT provides input about current operational security activities to the monthly OMB meeting. Reports of EGI CSIRT activities will be made available every six months to the EGI Foundation and its Executive Board and, where possible, annually to the wider EGI community at the bi-annual EGI Forums or similar event.

7 EVALUATION

EGI CSIRT will produce a report to the EGI Foundation every six months, in line with the reporting procedure defined in the respective OLA. The minutes of the group will be formally recorded and available to the EGI Foundation and the EGI OMB.

8 RELATED MATERIAL

Name	Location
EGI Policy Development Process	https://documents.egi.eu/document/169
Security Policy Group (SPG) - Terms of Reference	https://documents.egi.eu/public/ShowDocument?docid=64
Grid Security Policy	https://documents.egi.eu/document/86
Security Incident handling	https://documents.egi.eu/document/47

procedure	
Software Vulnerability Group (SVG) - Terms of Reference	https://documents.egi.eu/document/108
EGI-CSIRT Critical Vulnerability Operational Procedure	https://documents.egi.eu/document/283
EGI OLA Security Coordination	https://documents.egi.eu/document/2170

9 AMENDMENT

These Terms of Reference can be amended by mutual agreement of the Group Members through consultation and consensus. The amendments must be approved by the EGI Foundation Managing Director and EGI Foundation Executive Board.

The Group will review its Terms of Reference on an annual basis as a minimum.

The present Terms of Reference enters into force with immediate effect.

Yannick Legré
EGI Foundation Managing Director