**EGI.eu**

EGI Federated Cloud Security Questionnaire for sites deploying Cloud technology

|  |  |
| --- | --- |
| Document identifier | EGI\_CSIRT\_SVG\_FederatedCloud-Sites |
| Document Link | https://documents.egi.eu/document/<DOCID> |
| Last Modified | 14/02/2014 |
| Version | 0.1 |
| Policy Group Acronym | CSIRT |
| Policy Group Name | Computer Security Incident Response Team |
| Contact Person | Linda Cornwall, Sven Gabriel |
| Document Type | Procedure/Questionnaire |
| Document Status | Draft |
| Approved by | Body who approved the doc |
| Approved Date | DD/MM/YYYY |

|  |
| --- |
| Policy Statement  This is a checklist for sites, which must be answered by sites to provide the minimum information which CSIRT requires to consider whether to recommend Site Certification from a security point of view in order to be part of the EGI infrastructure, in particular the EGI Federated Cloud. |

Copyright notice

This work by EGI.eu is licensed under a Creative Commons Attribution 3.0 Unported License (see a copy of the license at <http://creativecommons.org/licenses/by/3.0>). This license let you remix, tweak, and build upon this work, and although your new works must acknowledge EGI.eu, you do not have to license your derivative works on the same terms. Reproductions or derivative works must be attributed by attaching the following reference to the copied elements: “Based on work by EGI.eu used with permission under a CC-BY 3.0 license (source work URL: specify if known)”.

.

1. Authors list

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Name** | **CSIRT** | **Date** |
| **From** | Linda Cornwall, Sven Gabriel, Daniel Kouril, Maarten Litmaath |  | 10th February 2014 |

1. Delivery Slip

|  |  |  |
| --- | --- | --- |
|  | **Body** | **Date** |
| Reviewed by | TCB | DD/MM/YYYY |
| Reviewed by | OMB | DD/MM/YYYY |
| Reviewed by | UCB | DD/MM/YYYY |
| Approved by | EGI.eu Director | DD/MM/YYYY |
| Approved by | EGI.eu Executive Board | DD/MM/YYYY |

1. Document Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Comment** | **Author/Organization** |
| 0.1 | 14th Feb 2014 | First Draft after various e-mail discussions | Linda Cornwall/STFC |
| 1.0 |  |  |  |
| 2.0 |  |  |  |
| 3.0 |  |  |  |
| 4.0 |  |  |  |

1. Application area

This document is a formal EGI.eu policy or procedure applicable to all participants and associate participants, beneficiaries and Joint Research Unit members, as well as its collaborating projects.

1. POLICY/procedure amendment procedure

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

1. ORGANISATION SUMMARY

To support science and innovation, a lasting operational model for e-Infrastructure is needed − both for coordinating the infrastructure and for delivering integrated services that cross national borders. The objective of EGI.eu (a foundation established under Dutch law) is to create and maintain a pan-European Grid Infrastructure in collaboration with National Grid Initiatives (NGIs) in order to guarantee the long-term availability of a generic e-infrastructure for all European research communities and their international collaborators.

In its role of coordinating grid activities between European NGIs, EGI.eu will:

* Operate a secure integrated production grid infrastructure that seamlessly federates resources from providers around Europe
* Coordinate the support of the research communities using the European infrastructure coordinated by EGI.eu
* Work with software providers within Europe and worldwide to provide high-quality innovative software solutions that deliver the capability required by our user communities
* Ensure the development of EGI.eu through the coordination and participation in collaborative research projects that bring innovation to European Distributed Computing Infrastructures (DCIs)

The EGI.eu is supporting ‘grids’ of high-performance computing (HPC) and high-throughput computing (HTC) resources. EGI.eu 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 will collect user requirements and provide support for the current and emerging user communities. 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 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, 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 Introduction 7

1.1 EGI Security Policies apply in the Cloud 7

1.2 Security principles continue in the cloud 7

1.3 Security is evolving 7

1.4 Caveats 7

2 Checklist for Certification of sites 8

2.1 About the Cloud Resource Providers Infrastructure 8

2.1.1 Check that Site-security-contact and csirt email are set in the GOCDB, and that they work, and provide a response 8

2.1.2 State the Cloud enabling technology used 8

2.1.3 What is the process for keeping the service(s) and OS patched and up-to-date, especially with respect to security patches? 8

2.1.4 Provider network separation 8

2.1.5 Policies 8

2.1.6 What processes exist to maintain audit logs (e.g. for use during an incident)? 8

2.2 About the Cloud Service itself 9

2.2.1 Who is allowed access to the machine(s) on which the service(s) run, and how do they obtain access? 9

2.2.2 State whether identity providers other than EGI approved are enabled 9

2.2.3 What mechanism(s) are in place to suspend a user or user group 9

2.3 About the Virtual Machines instantiated in the Cloud 9

2.3.1 Image sources and the EGI FedCloud model 9

2.3.2 What mechanism is in place to ensure only endorsed VMs are executed on the infrastructure? 9

2.3.3 Differentiating operators and users 9

2.3.4 Network monitoring 9

2.3.5 Incident response and investigations 10

2.3.6 Are any non-standard configuration(s) in place? 10

2.4 About EGI and non-EGI co-tenancy 10

2.4.1 Customer identification 10

2.4.2 Policies 10

2.4.3 VM execution 10

2.4.4 What is the process for keeping the service(s) and OS patched and up-to-date, especially with respect to security patches? 11

2.4.5 What mechanism(s) are in place to suspend customers or customer groups? 11

2.4.6 How long are identity and audit records for customers retained? 11

3 References 12

Appendix A – Checklist Form 13

# Introduction

The EGI infrastructure has been based on Grid Technology for more than a decade, and the Grid based technology is very mature from a security point of view. The various EGI security teams, Computer Security Incident Response Team (CSIRT), the Software Vulnerability Group (SVG), and the Security Policy Group (SPG) have been working to develop policies and techniques to allow the secure sharing of computing resources across a global infrastructure. It is important that this experience is applied and adapted to newer technologies, and at present this in particular means ‘Cloud’ technology.

## EGI Security Policies apply in the Cloud

Sites deploying Cloud technology should be aware that the security policies developed by the EGI Security Policy Group (SPG) apply to any technology, including Cloud technology, which is deployed in the EGI infrastructure. These policies are listed at [R 1]. These policies may require some adaptation to cope with changing technology, and changing responsibilities of the various participants in the infrastructure.

## Security principles continue in the cloud

Just because technology is changing, does not mean that security principles change. It is still necessary to ensure that sites are run in a secure manner, and that data access is properly authorized, credentials are protected, and that it is possible to carry out incident response and suspend a user or identity which is involved in a security incident. This means suitable traceability of users and contacts for the sites are in place.

## Security is evolving

Any checklists or recommendations produced will evolve over time, as experience with new technology develops and becomes better understood and as technology changes.

## Caveats

This is the minimum requirements concerning Federated Cloud Services which the EGI CSIRT team considers necessary to recommend site certification. This is the first version, and it defines the minimum we have identified as being necessary at the present time. It is subject to revision, future sites seeking certification may be asked for more by the security team and service providers already certified may be asked to put more controls in place in the future.

# Checklist for Certification of sites

This lists the basic checks which must be carried out with Cloud Resource providers (CRP) offering “Infrastructure-as-a-Service” clouds based on the execution of virtual machine images, in order for EGI CSIRT to be satisfied that the site is suitable for inclusion in the EGI Federated Cloud. This does not include checks that other required mechanisms are in place, such as for accounting, which are also necessary for the Certification of Federated cloud site.

.

## About the Cloud Resource Providers Infrastructure

### Check that Site-security-contact and csirt email are set in the GOCDB, and that they work, and provide a response

### State the Cloud enabling technology used

The software stack(s) used to provide the federated cloud service must be described. This may be, for example, OpenStack or OpenNebula.

Where proprietary software is used, it is RECOMMENDED to ask for a security assessment thereof to be provided. The CRP MUST agree to discontinue products that are known to pose a security threat to the Infrastructure, as determined by the EGI Security Teams – or at its options withdraw from the infrastructure.

### What is the process for keeping the service(s) and OS patched and up-to-date, especially with respect to security patches?

### Provider network separation

The network separation of management and service traffic should be documented. This includes aspects such as: presence of a separate network for management of physical hosts and the (virtual) network(s) to which customer VMs can be connected; whether that is a physically separated network; what are the (network) security controls separating the management network from the systems running the cloud enabling software; can customer traffic be separately monitored?

*There are probably no ‘right’ or ‘wrong’ answers, but it should allow for containment of incidents, and monitoring of traffic in a way that preserves confidentiality of non-affected customers, &c.*

### Policies

Does the CRP agree to be bound by the EGI security and other policies?

### 

ese mechanismsdIn general, o (EGI may provides)

## About the Cloud Service itself

### 

The CRP should describe if this is a shared service (EGI shares this cloud service with other customers that are not covered by the EGI security policies) or a EGI-proprietary one.

Are the cloud enabling services run on a dedicated system to which only cloud customers have access, or are cloud services (also) offered through other interfaces?

If the cloud service to EGI is offered in a multi-tenancy system, how (if so) are EGI and non-EGI customers separated? How (if applicable) are EGI customers protected from other tenants?

### State whether identity providers other than EGI approved are enabled

For identifying users, EGI maintains a policy regarding the trusted Certification Authorities for use in EGI[R2]. If you support authenticating VM operators with other types of identity than those approved by EGI in this document, please state both their type and identity assurance level Describe how appropriate traceability to the end-entities involved is retained through these identity mechanisms (one may take the classification of the EGI VO Portal [R3] as an example).

If you allow external third parties to manage system entities other than VM images (and image store etc.), describe how they are authenticated.

### What mechanism(s) are in place to suspend a user or user group

Describe the mechanisms available, and how the site takes into account information provided centrally by the EGI security teams regarding suspended users.

Describe how suspensions are effectuated with regard to currently executing VMs.

## About the Virtual Machines instantiated in the Cloud

### Image sources and the EGI FedCloud model

Does the CRP follow exclusively the EGI Federated Cloud model of running ‘endorsed’ virtual machines from a trusted EGI market place?

### 

Which controls are used to ensure this is applied for all VMs? Which mechanisms are used to ensure VMs in the local image store are all endorsed and no non-endorsed VMs are executed?

### Differentiating operators and users

Can and does your cloud management framework separate operators (those who has start, stop, copy, clone or destroy VMs) and users (those who can view a running system)? If so, do you apply different controls for each of these groups?

### Network monitoring

Describe how network monitoring is implemented for customer VMs. Describe how all network traffic can be traced to a specific VM instance and its associated operator.

### Incident response and investigations

Describe your ability to participate in incident response and investigation.

Are you capable of preserving point-in-time snapshots of the state of virtual machine executing in your infrastructure? Are you allowed and willing to share the images related to EGI FedCloud users and user communities with the EGI security incident response team(s)? Do you have any preconditions related to investigations and incident response?

### Are any non-standard configuration(s) in place?

***If the answers above are “yes, only EGI FedCloud VMs are used”, the following questions are no longer relevant. Many of the questions below should then be addressed by the VM endorsers and/or the VM operators, who are subject to their own policy sets.***

## About EGI and non-EGI co-tenancy

You (also) run customer VMs from customers that are not controlled through EGI security policies. This could potentially pose a risk to the EGI FedCloud infrastructure, other CRPs, VM operators, or end-users (e.g. because actions are ascribed to EGI users who are not involved in an incident, or because data integrity or conficentiality of EGI users is compromised). For the EGI security teams, it is important to be able to assess the associated risks.

### Customer identification

How are your non-EGI customers identified? Can these users be authenticated and positively distinguished from EGI users? What mechanisms are in place to ensure actions are not inadvertently associated with identified EGI users?

### Policies

Do you require that all customers abide by a set of security policies and/or do you have an acceptable use policy (AUP)? Are your terms and conditions publicly available (and if so, where)?

Describe what communications mechanisms are in place to ensure your customers are aware of these policies, terms and conditions.

Do your terms and conditions protect customers from each other?

Does your AUP include clauses that permit participating in incident response by, e.g., providing network and systems information? Would you consider the EGI security incident response task force forensics expert(s) as an appropriate third party in such investigations, when they pertain to incidents involving EGI users, VM operators, and/or VM endorsers?

### VM execution

Are all customers able to execute VM images?

This could be which VM operators do you allow? Do you allow only VM operators approved by EGI?

(Requires discussion.)

### What is the process for keeping the service(s) and OS patched and up-to-date, especially with respect to security patches?

Describe your mechanisms and policies for ensuing acceptable use.

Do your terms and conditions or AUP put requirements on the VM images with regards to vulnerability patching?

Do your terms and conditions or AUP put requirements on the external behaviour of the VMs executing (such as: no security violations, no network abuse nor spoofing, no email or message abuse, &c)?

## Do you have systems in place for the enforcement or monitoring of these policies?

### What mechanism(s) are in place to suspend customers or customer groups?

### How long are identity and audit records for customers retained?

# References

|  |  |
| --- | --- |
| R 1 | The EGI Security Policy Group https://wiki.egi.eu/wiki/SPG:Documents |
| R 2 | https://documents.egi.eu/document/83 |
| R 3 | https://documents.egi.eu/document/80 |
| R 4 |  |
| R 5 |  |

1. – Checklist Form