Security Policy for the Endorsement and Operation of Virtual Machine Images

Document identifier	EGI-SPG-VMEndorsementOperation-V4
Document Link	https://documents.egi.eu/document/2729
Last Modified	04/03/2016
Version	4
Policy Group Acronym	SPG
Policy Group Name	Security Policy Group
Contact Person	David Kelsey / STFC
Document Type	Security Policy
Document Status	Approved
Approved by	EGI Foundation Executive Board
Approved Date	10/10/2016

TABLE OF CONTENTS

1 Security Policy for the Endorsement and Operation of Virtual Machine Images 4
1.1 Introduction 4
1.2 Definitions 4
1.3 Use case classification 4
1.3.1 Endorser: resource centre, VM operator: resource centre 5
1.3.2 Endorser: Third party, VM operator: resource centre 5
1.3.3 Endorser: Third party, VM operator: Third Party 5
1.4 Policy Requirements on the VM Operator 5
1.5 Policy Requirements on the Endorser 6
2 References 8

COPYRIGHT NOTICE

AUTHORS LIST

	Name	Partner/Activity/Organisation/Function	Date
From	David Kelsey on behalf of EGI SPG	STFC / SPG Chair	04/03/2016

DELIVERY SLIP

	Body	***Date***
Reviewed by:	EGI Foundation Executive Board	10/10/2016
Approved by:	EGI Foundation Executive Board	10/10/2016

DOCUMENT LOG

Issue	***Date***	***Comment***	***Author/Partner***
V 3.9	08/01/2016	New version (draft of V4) of this policy to replace document #771. This addresses the new requirements of the EGI Federated Cloud as developed in EGI-Engage. The new document number is #2729.	David Kelsey/STFC
V3.91	17/02/2016	Address comments from Hannah Short, Peter Solagna and Linda Cornwall. Also detailed discussion at the EGI CSIRT F2F meeting in Prague 27/01/2016	David Kelsey/STFC
V3.92	04/03/2016	Produced during SPG meeting on this day. Takes all previous comments into account and those made during the meeting	David Kelsey/STFC
V4	10/10/2016	Review and approval by EGI Foundation Executive Board	

TERMINOLOGY

A complete project glossary is provided at the following page: https://wiki.egi.eu/wiki/Glossary_V2

APPLICATION AREA

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

POLICY/PROCEDURE AMENDMENT PROCEDURE

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

1 SECURITY POLICY FOR THE ENDORSEMENT AND OPERATION OF VIRTUAL MACHINE IMAGES

This policy is effective from 10/10/2016 and replaces an earlier version of this document [R1]. This policy is one of a set of documents that together define the Security Policy [R2]. This individual document must be considered in conjunction with all the policy documents in the set.

1.1 Introduction

This document describes the security-related policy requirements for the generation, distribution and operation of virtual machine (VM) images, as part of a trusted computing environment of the Infrastructure.

The aim is to enable VM images to be generated according to best practices and to be both trusted and operated elsewhere.

This policy does not compel resource centres to instantiate images endorsed in accordance with this policy. Should a resource centre decide to instantiate a VM image generated by any other non-compliant procedures, that resource centre is still bound by all applicable security policies and is required to consider the security implications of such an action on other participants.

1.2 Definitions

The following terms are defined:

- **Endorser**: A role, held either by an individual or a team, who is responsible for confirming that a particular VM image has been produced according to the requirements of this policy and states that the image can be trusted. An Endorser should be one of a limited number of authorised and trusted individuals appointed either by the infrastructure, a VO or a resource centre. The appointing body must assume responsibility for the actions of the Endorser and must ensure that he/she is aware of the requirements of this policy.
- **VM operator**: A role, held either by an individual or a team, who is responsible for the security of the VM during its operation phase, from the time it is instantiated, until it is terminated. Typically this addresses individuals with root access on the VM.
- **VM consumer**: A role held by an individual who consumes with no level of management privilege the services operated on or by a VM.
- **Third party**: An external entity other than the resource centre where the VM is operated.

1.3 Use case classification

The current policy document addresses the following use cases.

1.3.1 Endorser: resource centre, VM operator: resource centre

In this class virtualisation is not directly accessible by users. It includes, for example, the use of virtual worker nodes that act in a similar way to real worker nodes.

The resource centre is both the Endorser and the VM operator and is responsible to ensure the compliance of the VM with existing security policies.

1.3.2 Endorser: Third party, VM operator: resource centre

In this class, the resource centre is the VM operator, and the trust relationship is established between the resource centre and the Endorser.

1.3.3 Endorser: Third party, VM operator: Third Party

In this class, the resource centre runs the VM but is not the VM operator, and the trust relationship is established between the:

- Resource centre and the VM operator
- VM operator and the Endorser (both roles can be combined)

The resource centre is responsible to ensure sufficient traceability in order to enable malicious network activity to be linked with any VM and its VM operator, as defined in the Security Traceability and Logging policy.

The resource centre may decide to apply specific restrictions to control the access of the VM to other resources, including network services.

1.4 Policy Requirements on the VM Operator

By acting as a VM Operator you agree to the conditions laid down in this document and other referenced documents, which may be revised from time to time.

1. You are responsible to fulfil all the operational security and incident response requirements expressed in other policies.
2. You are responsible to ensure that any VM you operate is compliant with existing security policies, including but not limited to security patching, vulnerability management, incident response, data protection, and where applicable, logging and traceability.
3. You are responsible for handling all problems related to the execution of any licensed software in a VM image. You shall ensure that any software run in a VM, complies with applicable license conditions and you shall hold the resource centre running the image free and harmless from any liability with respect thereto.
4. If the VM image is endorsed then the instantiation may be considered to be trustworthy up to the point of contextualisation.

5. You are responsible for the consequences of contextualisation of any instantiated VM image, including credentials and certificates and for the operation of the VM from that point on.
6. You are responsible to ensure that the VM consumer has seen and accepted the "AUP and Conditions of Use" and for all actions of the VM consumer compliant with the AUP.
7. You recognise that the Infrastructure Organisation, the resource centres and the VOs reserve the right to block any endorsed image or terminate any instance of a virtual machine and associated user workload for administrative, operational or security reasons.

1.5 Policy Requirements on the Endorser

By acting as an Endorser you agree to the conditions laid down in this document and other referenced documents, which may be revised from time to time.

1. You are held responsible by all interested parties for checking and confirming that a VM image has been produced according to the requirements of this policy and that there is no known reason, security-related or otherwise, why it should not be trusted.
2. You recognise that the VM image must be generated according to current best practice, the details of which may be documented elsewhere by the infrastructure. These include but are not limited to:
    a) any image generation tool used must be fully patched and up to date;
    b) all operating system and other installed software security patches must be applied to all images and be up to date;
    c) images are assumed to be world-readable and as such must not contain any confidential information;
    d) images must not contain any installed accessible accounts or any other means of access;
    e) images must not contain any form of credential, such as passwords or private keys.
3. You must disclose to any appropriate stakeholder on request the procedures and practices you use for checking and endorsing images.
4. You must either provide and maintain an up to date list of your currently endorsed images together with the metadata relating to each VM image, or ensure that any application/VM image database provided by a third party and used by you for this purpose is capable of similar functionality.
5. Either the list or each individual image's metadata must be digitally signed by the endorser or the application/VM image database must be configured to support non-repudiation.
6. You, or the application/VM image database, must keep an auditable history of every image endorsed including the identity of the Endorser (individual not team), and all of the

information available to you on installed software and version numbers but at least the operating system and version number, and the date/time of generation. This must be made available to appropriate stakeholders on demand.

7. You, or the application/VM image database, must implement a removal or revocation procedure to allow the VM operators to exclude those images which are no longer endorsed. This procedure must be implemented whenever a relevant security update is required. This removal must also be recorded locally in your auditable history. Your responsibility for this revoked VM image ends at this point.
8. You are responsible for handling all issues related to the distribution of any licensed software in a VM image. You shall ensure that any software distributed in a VM image, complies with applicable license conditions and you shall hold the resource centre running the image free and harmless from any liability with respect thereto.
9. You must assist in security incident response.

2 REFERENCES

R 1	(Old version) Security Policy for the Endorsement and Operation of Virtual Machine Images: https://documents.egi.eu/document/771
R 2	Approved EGI Security Policies: https://wiki.egi.eu/wiki/SPG:Documents