# EOSC-hub Security Policy

# Document control

|  |  |
| --- | --- |
| **Area** | ISM |
| **Policy status** | DRAFT (1 March 2019) |
| **Owner** | David Kelsey |
| **Approval status** | APPROVAL REQUIRED |
| **Approved version and date** |  |
| **Next policy review** | together with process review |

# Policy reviews

The following table is updated after every review of this document.

Click here to expand...

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Review by** | **Summary of results** | **Follow-up actions / Comments** |
|  |  |  |  |
|  |  |  |  |

# Table of contents

* [Document control](#EOSC-hubSecurityPolicy-Documentcontrol)
* [Policy reviews](#EOSC-hubSecurityPolicy-Policyreviews)
* [Table of contents](#EOSC-hubSecurityPolicy-Tableofcontents)
* [Introduction](#EOSC-hubSecurityPolicy-Introduction)
* [Scope](#EOSC-hubSecurityPolicy-Scope)
* [Definitions](#EOSC-hubSecurityPolicy-Definitions)
* [Objectives](#EOSC-hubSecurityPolicy-Objectives)
* [Additional Policy Documents](#EOSC-hubSecurityPolicy-AdditionalPolicy)
* [Approval and Maintenance](#EOSC-hubSecurityPolicy-ApprovalandMaint)
* [EOSC-hub Security Policy Statements](#EOSC-hubSecurityPolicy-EOSC-hubSecurity)
* [ROLES AND RESPONSIBILITIES](#EOSC-hubSecurityPolicy-ROLESANDRESPONSI)
	+ [The Collaborating Infrastructure Security Officers](#EOSC-hubSecurityPolicy-TheCollaborating)
	+ [Service Management](#EOSC-hubSecurityPolicy-ServiceManagemen)
* [PHYSICAL SECURITY](#EOSC-hubSecurityPolicy-PHYSICALSECURITY)
* [NETWORK SECURITY](#EOSC-hubSecurityPolicy-NETWORKSECURITY)
* [EXCEPTIONS TO COMPLIANCE](#EOSC-hubSecurityPolicy-EXCEPTIONSTOCOMP)
* [SANCTIONS](#EOSC-hubSecurityPolicy-SANCTIONS)
* [REFERENCES](#EOSC-hubSecurityPolicy-REFERENCES)
* [Copyright](#EOSC-hubSecurityPolicy-Copyright)

# ****Introduction****

To fulfil its mission, it is necessary for the EOSC-hub project and its Collaborating Infrastructures, hereafter jointly called the "Collaborating Infrastructures", to protect their assets. This document presents the policy regulating those activities of participants related to the security of the Collaborating Infrastructures.

This security policy is aimed to be compliant with WISE Security for Collaborating Infrastructures (SCI) version 2 [R1].

# ****Scope****

This policy applies to all participants involved in providing, using, managing, operating, supporting or coordinating one or more EOSC-hub registered Service(s) with Integration level High, hereafter called the "Services". This policy augments local Service policies by setting out additional Infrastructure specific requirements.

# ****Definitions****

The words Collaborating Infrastructure when italicised in this document, means all of the people and organisations, hardware, software, networks, facilities, etc. that are required to develop, test, deliver, monitor, control or support the Services.

The other italicised words used in this document are defined as follows:

* Policy is interpreted to include rules, responsibilities and procedures specified in this document together with all those in other documents which are required to exist by stipulations in this document.
* A participant is any entity providing, using, managing, operating, supporting or coordinating one or more  service(s).
* A service is any computing or software system accessible by Users of the Infrastructure.
* The Management is the collection of the various boards, committees, groups and individuals mandated to oversee and control the Infrastructure.
* A User is an individual who has been given authority to access and use one or more Services and Infrastructure  resources.
* A User Community is a grouping of Users, usually not bound to a single institution, which, by reason of their common membership and in sharing a common goal, are given authority to use a set of services.
	+ Included in the definition of a User Community are cases where services are offered to individual Users who are not members of an explicitly organised User Community.
* The User Community Management is the collection of various individuals and groups mandated to oversee and control a User Community.

Other terms are defined in the Glossary [R2].

In this document the key words `must', `must not', `required', `shall', `shall not', `recommended', `may', and `optional' are to be interpreted as described in RFC 2119 [R3]

# ****Objectives****

This policy gives authority for actions which may be carried out by designated individuals and organisations, and places responsibilities on all participants.

# ****Additional Policy Documents****

Additional policy documents required for a proper implementation of this policy are to be found in [R4].

# ****Approval and Maintenance****

(note: This section is still being discussed - not yet sure which body will formally "approve")

This policy is approved by the EOSC-hub AMB and the implementation of the policy's requirements by the Collaborating Infrastructures is the responsibility of the SMB. This policy will be maintained and revised by the EOSC-hub security teams as required by the SMB and resubmitted for formal re-approval by the AMB whenever strategic changes are needed.

# ****EOSC-hub Security Policy Statements****

# ****ROLES AND RESPONSIBILITIES****

This section defines the roles and responsibilities of participants.

**The EOSC-hub Activity Management Board (AMB) and Service Management Board (SMB)**

(note: This section is still being discussed - not yet sure which body will formally "approve")

The Management of EOSC-hub includes the AMB and SMB. Collaborating Infrastructures have their own management structures. Collectively these are all referred to as The Management.

The AMB provides the overall authority for the decisions and actions resulting from this policy including procedures for the resolution of disputes. The AMB is also responsible for the approval of strategic changes to this policy.

The SMB is responsible for requiring the compliance of the Collaborating Infrastructures with, as well as approval of non-strategic changes to, this policy.

The AMB is responsible for providing and maintaining a Privacy Notice for EOSC-hub and the SMB is responsible for maintain a registry of Privacy Statements of Services in relation to personal data processed by the Services.

The SMB is responsible for ensuring that any identity management proxy facing the Research & Education identity federations complies with the Snctfi Trust Framework [R5].

## ****The**** CollaboratingInfrastructure ****Security Officers****

The Security Officers from EGI and EUDAT jointly coordinate the operational security capabilities of the project, including the implementation of the Sirtfi framework [R6] by the Collaborating infrastructures.

The Security Officers may, in consultation with the Management and other appropriate persons, require actions by participants as are deemed necessary to protect the Collaborating Infrastructures from, or contain the spread of, IT security incidents.

The Security Officers handle requests for exceptions to this policy as described below.

The Security Officers are responsible for establishing and periodically testing a communications flow for use in security incidents ~~and for reporting any potential personal data breaches to the appropriate Data Protection authority (note: this is the responsibility of the Data Controller)~~. (note: this text left in place, even though with strikethrough - to remind that someone has to take responsibility for Data Controller obligations - this is not a job for the Security Officer)

## Service ****Management****

The Service must designate a Security contact point (person or team) that is willing and able to collaborate with affected participants in the management of security incidents and to take prompt action as necessary to safeguard services and resources during an incident.

Services must abide by the Infrastructure Services Security Operations Policy [R4] and the Sirtfi framework [R6].

Services acknowledge that participating in the Infrastructure and allowing related inbound and outbound network traffic increases their IT security risk. Services are responsible for accepting or mitigating this risk.

Services must produce and maintain a list of their information assets. They must identify threats to their Service and assets and must perform regular security risk assessments. To mitigate the identified risks Services must deploy effective security controls to protect the confidentiality, integrity and availability of their services and resources.

For Services processing personal data, a Privacy Notice must be made available to the Management for the registry of Privacy Notices and presented to Users before or upon first access to the Service.

# ****PHYSICAL SECURITY****

All the requirements for the physical security of the equipment used to provide a Service are expected to be adequately covered by each Service’s local security policies and practices. These should, as a minimum, reduce the risks from intruders, fire, flood, power failure, equipment failure and environmental hazards. Stronger physical security may be required for equipment used to provide certain critical services such as User Community membership services, Identity Management Proxies, or credential repositories.

# ****NETWORK SECURITY****

All the requirements for the networking security of Services are expected to be adequately covered by each Service’s local security policies and practices.

To support specific User Community workflows it may be necessary to permit inbound or outbound network traffic. It is the responsibility of the Service to assess and appropriately mitigate the risks associated with such traffic.

# ****EXCEPTIONS TO COMPLIANCE****

Wherever possible, Infrastructure policies and procedures are designed to apply uniformly to all participants. If this is not possible, for example due to legal or contractual obligations or due to compelling operational difficulties, exceptions may be made. Such exceptions should be time-limited and must be documented and authorised by an Infrastructure Security Officer and, if required, approved at the appropriate level of the Management. Such exceptions must not unduly compromise the integrity or trustworthiness of the Infrastructure.

In exceptional circumstances it may be necessary for participants to take emergency action in response to some unforeseen situation which may violate some aspect of this policy for the greater good of pursuing or preserving legitimate Infrastructure objectives. If such a policy violation is necessary, the exception should be minimised, documented, time-limited and authorised at the highest level of the Management commensurate with taking the emergency action promptly, and the details notified to the Infrastructure Security Officers at the earliest opportunity.

# ****SANCTIONS****

Services that fail to comply with this policy may lose the right to be recognised by the Infrastructure until compliance has been satisfactorily demonstrated again.

User Communities who fail to comply with this policy may lose their right of access to and collaboration with the Infrastructure and may lose the right to have their services recognised by the Infrastructure until compliance has been satisfactorily demonstrated again.

Users who fail to comply with this policy may lose their right of access to the Infrastructure, and may have their activities reported to their User Community or their home organisation.

Any activities thought to be illegal may be reported to appropriate law enforcement agencies.

# ****REFERENCES****

|  |  |  |
| --- | --- | --- |
| R1 | WISE Security for Collaborating Infrastructures SCI V2 (31 May 2017) | <https://wise-community.org/sci/> |
| R2 | EOSC-hub Glossary | [https://confluence.egi.eu/display/EOSC/EOSC-hub+Glossary](file:///C%3A%5Cdisplay%5CEOSC%5CEOSC-hub%2BGlossary) |
| R3 | IETF RFC2119 | <https://www.ietf.org/rfc/rfc2119.txt> |
| R4 | ISM PoliciesEOSC-hub Security PolicyEOSC-hub Service Operations Security PolicyEOSC-hub Acceptable Use Policy and Conditions of Use | [https://confluence.egi.eu/display/EOSC/ISM+Policies](file:///C%3A%5Cdisplay%5CEOSC%5CISM%2BPolicies)[https://confluence.egi.eu/display/EOSC/EOSC-hub+Security+Policy](https://confluence.egi.eu/display/EOSC/EOSC-hub%2BSecurity%2BPolicy)[https://confluence.egi.eu/display/EOSC/EOSC-hub+Service+Operations+Security+Policy](https://confluence.egi.eu/display/EOSC/EOSC-hub%2BService%2BOperations%2BSecurity%2BPolicy)[https://confluence.egi.eu/display/EOSC/EOSC-hub+Acceptable+Use+Policy+and+Conditions+of+Use](https://confluence.egi.eu/display/EOSC/EOSC-hub%2BAcceptable%2BUse%2BPolicy%2Band%2BConditions%2Bof%2BUse) |
| R5 | Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (Snctfi) version 1.0 | <https://www.igtf.net/snctfi/igtf-snctfi-1.0-20170723.pdf> |
| R6 | The Security Incident Response Trust Framework for Federated Identity (Sirtfi) version 1.0 | <https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf> |

# ****Copyright****

Copyright owned by EOSC-hub and the authors. This document is licensed under [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/)

The policy is based on a template (Policy Development Kit) from the AARC2 EU H2020 project licensed under CC-BY-NC-SA 4.0 <https://aarc-project.eu/policies/policy-development-kit/> and that template is itself based on earlier work by EGI.eu, licensed under a Creative Commons Attribution 4.0 International License. <https://documents.egi.eu/document/3015>

Other Sources / Attribution / Acknowledgements: SCI version 2 from the WISE Community, used under CC BY-NC-SA 4.0.