# EOSC-hub Service Operations 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

## Scope

This security policy applies to Service Providers that operate any EOSC-hub registered service with Integration level High.

# Definitions

All terms are defined in the EOSC-hub Glossary [R3].

# EOSC-hub Service Operations Security Policy

By running a Service on an EOSC-hub Infrastructure (the "Infrastructure"), by providing a Service that is part of the Infrastructure, or retaining state that is related to the Infrastructure, you agree to the conditions below.

1. You shall comply with all pertinent Information Security Management (ISM) policies [R1] as approved by the Infrastructure Management.
2. You shall provide and maintain accurate contact information, including at least one Security Contact who shall support Sirtfi [R2] on behalf of the service.
3. You are held responsible for the safe and secure operation of the Service. Any information you provide regarding the suitability and properties of the Service should be accurate and maintained. The Service shall not be detrimental to the Infrastructure nor to any of its Participants.
4. You should follow IT security best practices including pro-actively applying updates or configuration changes related to security. You shall respond appropriately, and within the specified time period, on receipt of security notices from the Infrastructure or any of its participants.
5. You shall document your processing of personal data in a Privacy Notice that is displayed to the User and made available to the Infrastructure.
    a. You shall apply due diligence in maintaining the confidentiality of user credentials and of any data you hold where there is a reasonable expectation of privacy.
    b. You shall collect and retain sufficient auditing information to be able to assist the Infrastructure in security incident response.
    c. You shall use logged information, including personal data, only for administrative, operational, accounting, monitoring and security purposes. You shall apply due diligence in maintaining the confidentiality of logged information.
6. Provisioning of Services is at your own risk. Any software provided by the Infrastructure is provided on an as-is basis only, and subject to its own license conditions. There is no guarantee that any procedure applied by the Infrastructure is correct or sufficient for any particular purpose. The Infrastructure and any other participants acting as service hosting

providers are not liable for any loss or damage in connection with your participation in the Infrastructure.

7. You may control access to your Service for administrative, operational and security purposes and shall inform the affected users where appropriate.
8. Your Service's connection to the Infrastructure may be controlled for administrative, operational and security purposes if you fail to comply with these conditions.

Upon retirement of your Service, the obligations specified in clauses 1, 2, 5 and 6 shall not lapse for the retention period agreed with the Infrastructure.

# References

| | | |
|---|---|---|
| R1 | ISM Policies | https://confluence.egi.eu/display/EOSC/ISM+Policies |
| R2 | The Security Incident Response Trust Framework for Federated Identity (Sirtfi) v1.0 | https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf |
| R3 | EOSC-hub Glossary | https://confluence.egi.eu/display/EOSC/EOSC-hub+Glossary |

# Copyright Statement

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, "Service Operations Security Policy" by EGI.eu, licensed under a Creative Commons Attribution 4.0 International License.