EOSC Security Operational Baseline

Applicability

Adherence to this policy is required for EOSC Core services, based on the Core Provider Agreement.

All other services: this policy is part of the EOSC Interoperability Framework and as such is binding for Exchange services for which it is relevant.

Note that the public facing copy of this policy is available here: EOSC Security Operational Baseline

Document control

Area	ISM
Policy status	FINALISED
Policy owner	David Groep
Approval status	APPROVED
Approved version and date	13 Sep 2022 v10
Next policy review	together with process review

Policy reviews

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

Date	Review by	Summary of results	Follow-up actions / Comments
28 Feb 2022	David Groep	Replace the service operations security policy since it was superseded by this version	consultation and endorsement
26 Sep 2022	Matthew Viljoen	Approved by TCB on 13 Sep 2022 (EOSC Future: PUBLIC /EOSC+Security+Operational+Baseline)	
02 May 2023	David Groep	Policy is confirmed in the publishing queue of the EOSC Interoperability framework	track EOSC I/F release with Michelle Williams
15 Jun 2023	David Groep	Identified as included as part of the EOSC I/F guidelines	https://search.marketplace.eosc-portal.eu/search/guideline?q=*&sort_ui=dlr&fq=status:(%22ir_status%5C-operating%22)

Table of contents

- Document control
- Policy reviews
- Table of contents
- Scope
    - Definitions
    - Scope
    - Baseline Requirements
    - Acknowledgements

Scope

To fulfil its mission, it is necessary for the European Open Science Cloud (EOSC) to be protected from damage, disruption, and unauthorised use. This Security Baseline supports these goals by defining minimum expectations and requirements of the behaviour of those offering services to users and communities connected to the EOSC, and of those providing access to services or assembling service components through the EOSC. It thereby applies to all participants in the EOSC authentication and authorization infrastructure (EOSC AAI). It aims to establish a sufficient level of trust between all Participants in the Infrastructure to enable reliable and secure Infrastructure operation.

Definitions

Terminology in this document follows conventional IT service management vocabulary (such as ITIL and FitSM) and the RFC 2119 key words:

- **Service Provider** - an organisation (or part of an organisation) that manages and delivers a service or services to customers
- **Identity Provider** - a service that creates, maintains, and manages identity information for principals and provides authentication services to relying parties
- **AAI Proxy** - any service, Community authentication/authorization infrastructure (AAI), or Infrastructure Proxy that augments, translates, or transposes authentication and authorization information, including the connected sources of access (AAI) attributes, as detailed in the AARC BPA 2019.
- **Infrastructure Proxy for the EOSC Core Services** - the AAI proxy to which EOSC Core Services are connected
- **User** - an individual that primarily benefits from and uses a service
- **IaaS, PaaS, and SaaS** - respectively Infrastructure, Platform, or Software provided ‘as-a-service’

This document is accompanied by an FAQ providing implementation suggestions.

Scope

This Baseline applies to all service providers participating in the EOSC as well as to all authentication providers, i.e. AAI proxies and directly-connected Identity Providers, participating in the EOSC AAI Federation. It thus also applies to the EOSC Core services and the Infrastructure Proxy for the EOSC Core Services. These requirements augment, but do not replace, any other applicable security policies and obligations, or more specific security arrangements between EOSC participants.
Transfer, processing, or storage of confidential information, or specific categories or accumulations of personal data, may require more specific security arrangements.

Baseline Requirements

All EOSC Service Providers, directly connected Identity Providers, and AAI Proxies, must

1. comply with the SIRTFI security incident response framework for structured and coordinated incident response
2. ensure that their Users agree to an Acceptable Use Policy (AUP) or Terms of Use, and that there is a means to contact each User.
3. promptly inform Users and other affected parties if action is taken to protect their Service, or the Infrastructure, by controlling access to their Service, and do so only for administrative, operational or security purposes.
4. honour the confidentiality requirements of information gained as a result of their Service’s participation in the Infrastructure.
5. respect the legal and contractual rights of Users and others with regard to their personal data processed, and only use such data for administrative, operational, accounting, monitoring or security purposes.
6. retain system generated information (logs) in order to allow the reconstruction of a coherent and complete view of activity as part of a security incident (the ‘who, what, where, when’, and ‘to whom’), for a minimum period of 180 days, to be used during the investigation of a security incident.
7. follow, as a minimum, generally accepted IT security best practices and governance, such as pro-actively applying secure configurations and security updates, and taking appropriate action in relation to security vulnerability notifications, and agree to participate in drills or simulation exercises to test Infrastructure resilience as a whole.
8. ensure that they operate their services and infrastructure in a manner which is not detrimental to the security of the Infrastructure nor to any of its Participants or Users.
9. collaborate in a timely fashion with others, including the EOSC Security Team, in the reporting and resolution of security events or incidents related to their Service’s participation in the EOSC infrastructure and those affecting the EOSC infrastructure as a whole.
10. honour the obligations security collaboration and log retention (clauses 1, 6, and 9 above) for the period of 180 days after their Service is retired from the Infrastructure, including the retention of logs when physical or virtual environments are decommissioned.
11. not hold Users or other Infrastructure participants liable for any loss or damage incurred as a result of the delivery or use of their Service in the Infrastructure, except to the extent specified by law or any licence or service level agreement.
12. maintain an agreement with representatives for individual service components and suppliers that ensures that engagement of such parties does not result in violation of this Security Baseline.

Providers should name persons responsible for the implementation of, and the monitoring of compliance to, this Security Baseline in the context of the Service. They shall promptly inform the EOSC Security Team of any material non-compliance with this Baseline should such occur.

The EOSC Security Team can be contacted at <abuse@eosc-security.eu>.

Acknowledgements

This “EOSC Security Operational Baseline” is based upon multiple sources used under CC BY-NC-SA 4.0 license, including the UK “IRIS Service Operations Security Policy” (https://www.iris.ac.uk/security/) and the “Service Operations Security Policy” from the AARC Policy Development Kit (https://aarc-community.org/policies/policy-development-kit/) owned by the authors, used under CC BY-NC-SA 4.0. This EOSC Security Operational Baseline is licensed under CC BY-NC-SA 4.0 by the contributing partners in the EOSC Future consortium.