EOSC Future

EOSC-IF

EOSC Security Operational Baseline 2022

The EOSC Future project is co-funded by the European Union Horizon Programme call INFRAEOSC-03-2020, Grant Agreement number 101017536

Version 1.0
September 2022

EOSC-IF / EOSC Security Operational Baseline 2022

Lead by **Nikhef (NWO-I)**
Authored by the EOSC Future Trust and Security Coordination team, David L. Groep, Alf Moens, Daniel Kouřil, Baptise Grenier, David Crooks, David Kelsey, Ian Neilson, Linda Cornwall, Matt Viljoen, Pinja Koskinen, Ralph Niederberger, Romain Wartel, Sven Gabriel, Urpo Kaila
Reviewed by EOSC Future TCB

Dissemination Level of the Document

Public

Abstract

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 aims to establish a sufficient level of trust between all Participants in the Infrastructure to enable reliable and secure Infrastructure operation.

Version History

Version	Date	Authors/Contributors	Description
V1.0	09/2022	David L. Groep, Alf Moens, Daniel Kouřil, Baptise Grenier, David Crooks, David Kelsey, Ian Neilson, Linda Cornwall, Matt Viljoen, Pinja Koskinen, Ralph Niederberger, Romain Wartel, Sven Gabriel, and Urpo Kaila	Consolidated version after public consultation
V1.0	09/2022	ibidem	Final Version endorsed by the TCB
	12/2022	David L. Groep	Assigned DOI https://doi.org/10.5281/zenodo.7396725

Copyright Notice

Table of Contents

Table of Tables

Glossary

EOSC Future project Glossary is incorporated by reference: https://wiki.eoscfuture.eu/x/JQCK

List of Abbreviations

Terminology in this document follows conventional IT service management vocabulary (such as ITIL and FitSM) and the RFC 2119 [2] key words.

Acronym	Definition
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 [1][1].
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

[1] AARC BPA 2019: https://aarc-community.org/guidelines/aarc-g045

1 Intended Audience

This Baseline is relevant for 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 SHALL apply in full to the EOSC Core services and the Infrastructure Proxy for the EOSC Core Services. It also applies to all participants in the EOSC authentication and authorization infrastructure (EOSC AAI) as per the AAI requirements. It is RECOMMENDED that all EOSC service providers follow these Baseline Requirements to achieve a sufficient level of security in the EOSC. 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.

Adherence to this policy is REQUIRED for EOSC Core services, based on the Core Provider Agreement. All other services should considered this the best practice and are RECOMMENDED to follow its guidance.

2 Description and main features

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 aims to establish a sufficient level of trust between all Participants in the Infrastructure to enable reliable and secure Infrastructure operation.

3 Licensing Information

4 Related Guidelines

Resource Type	Title	Short Description	relatedIdentifier
Guideline	AARC Policy Development Kit	Provided to support Research Infrastructures in adopting or enhancing a policy set that regulates the operation and use of an authentication and authorisation infrastructure in line with the AARC Blueprint Architecture.	https://aarc-community.org/policies/policy-development-kit/
Guideline	AARC Blueprint Architecture	The AARC Blueprint Architecture (BPA) is a set of software building blocks that can be used to implement federated access management solutions for international research collaborations. The Blueprint Architecture lets software architects and technical decision makers mix and match tried and tested components to build customised solutions for their requirements.	https://aarc-community.org/architecture/
Policy	IRIS Service Operations Security Policy	To reduce the likelihood of and impact from security incidents on the IRIS Infrastructure, its Participants and the wider Research community, this policy gives authority for actions to be taken by designated individuals and organisations and places responsibilities on IRIS Participants.	https://www.iris.ac.uk/security/

Table 1: Related Guidelines

5 Integration Options

Adherence to this policy is REQUIRED for EOSC Core services, based on the Core Provider Agreement. All other services should considered this the best practice and are RECOMMENDED to follow its guidance.

6 Interoperability Guidelines

The Security Operational Baseline Requirements state that

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>.

7 Examples of solutions implementing this specification

The Security Operational Baseline is accompanied by a continuously updated ancillary "Questions and Answers" resource that clarifies the Baseline and provides references to resources that facilitate the adoption and implementation of the Baseline [3].

This resource is available at

https://wiki.eoscfuture.eu/display/PUBLIC/EOSC+Security+Operational+Baseline+FAQ

References

[1] AARC BPA 2019: https://aarc-community.org/guidelines/aarc-g045

[2] RFC 2119, https://www.ietf.org/rfc/rfc2119.txt

[3] Baseline FAQ https://wiki.eoscfuture.eu/display/PUBLIC/EOSC+Security+Operational+Baseline+FAQ