EOSC Security Baseline

Aims of the EOSC Security Baseline

To fulfil its mission, it is necessary for the European Open Science Cloud (EOSC) to be protected from damage, disruption, and unauthorized 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 also 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 (*preliminary*)

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 and Authorization Infrastructure (Community AAI), or Infrastructure Proxy that augments, translates, or transposes authentication and authorization information, including the connected sources of access (AAI) attributes [ref: 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

This document will be 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) that includes a means to contact the User.
3. 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.
4. 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.
5. 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.
6. honour the confidentiality requirements of information gained as a result of their Service's participation in the Infrastructure.
7. respect the legal and contractual rights of Users and others with regard to their personal data processed as part of service delivery, and only use such data for administrative, operational, accounting, monitoring or security purposes.
8. retain system generated information (logs) in order to be able to answer the basic questions who, what, where, when, and to whom, aggregated centrally wherever possible, and protected from unauthorised access or modification, for a minimum period of 180 days, to be used during the investigation of a security incident.
9. honour the obligations as specified in clauses 1, 3, and 8 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.
10. 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.
11. 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.
12. maintain an agreement with representatives for individual service components and suppliers confirming that they also agree to this Security Baseline, to allow a coherent and complete view of the activity involved with a security incident, including situations where the service acts as part of a layered technology stack
13. promptly inform the EOSC Security Team of any material non-compliance with this Baseline.

Providers should name persons responsible for implementation and monitoring of this Security Baseline in the context of the Service.

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

Acknowledgements