# The EOSC Security Baseline

*EOSC Future TCB, August 2022*

**David Groep – WP7.5 Security Operations and Policy lead**
*Nikhef Physics Data Processing programme*
*UM Department of Advanced Computing Sciences, Faculty of Science and Engineering*

# Keeping the EOSC secure

**“ensure confidentiality, integrity and availability”**

**“protecting data and services from threats and vulnerabilities”**

In our heterogeneous EOSC at large, founded on subsidiarity, this translates to

- *primum non nocere*: do no harm to interests & assets of others, including users
- not expose other service providers in the EOSC ecosystem to enlarged risk *as a result of their participation in EOSC*
- be transparent about infosec maturity and risk to its customers and suppliers

***baselining* is a true & tried approach to improve collective security posture**

# Applicability of ISM policies and processes

**EOSC ISM differentiates between Core and Exchange**

- both are in scope for all security policies
- **Core**: mandatory adherence (and pro-active support from the security team)
- **Exchange**: based on Interoperability Framework (& ‘RFC2119-RECOMMENDED’)

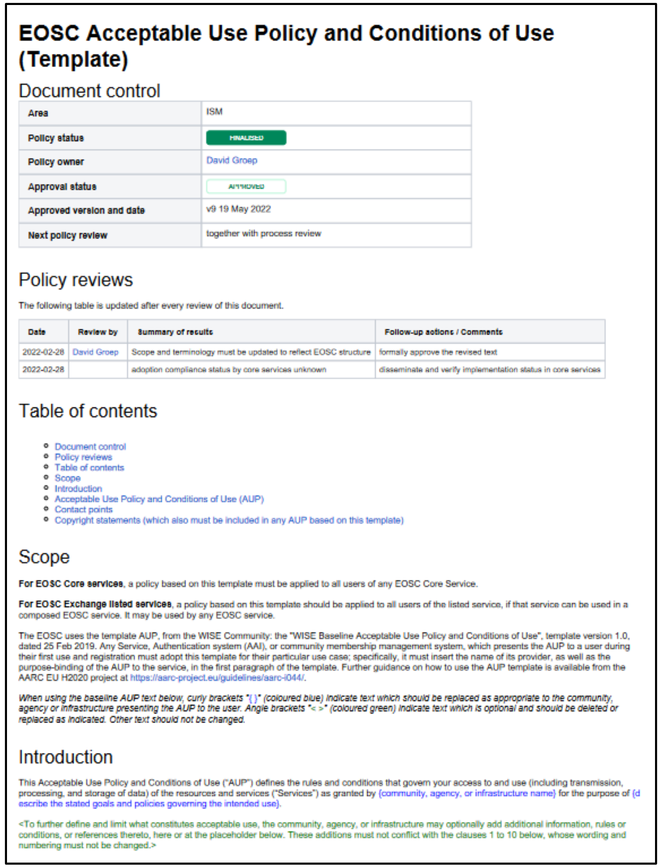
**Participants are autonomous**

- but subscribe to *shared commitment* of maintaining trustworthy & secure EOSC

**With everyone expected to participate in incident response and ‘drills’**

- for the Core services, expert forensics support is provided for if desired
- in the Exchange, coordination and liaison are the primary tasks of the CSIRT
  *but the EOSC CSIRT will of course help where it can!*

# Policy – a baselining approach for AUP and Operations



## EOSC Acceptable Use Policy and Conditions of Use (Template)

### Document control

| | |
|---|---|
| **Area** | ISM |
| **Policy status** | FINALISED |
| **Policy owner** | David Groep |
| **Approval status** | APPROVED |
| **Approved version and date** | v9 19 May 2022 |
| **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 |
|---|---|---|---|
| 2022-02-28 | David Groep | Scope and terminology must be updated to reflect EOSC structure | formally approve the revised text |
| 2022-02-28 | | adoption compliance status by core services unknown | disseminate and verify implementation status in core services |

### Table of contents

- Document control
- Policy reviews
- Table of contents
- Scope
- Introduction
- Acceptable Use Policy and Conditions of Use (AUP)
- Contact points
- Copyright statements (which also must be included in any AUP based on this template)

### Scope

**For EOSC Core services**, a policy based on this template must be applied to all users of any EOSC Core Service.

**For EOSC Exchange listed services**, a policy based on this template should be applied to all users of the listed service, if that service can be used in a composed EOSC service. It may be used by any EOSC service.

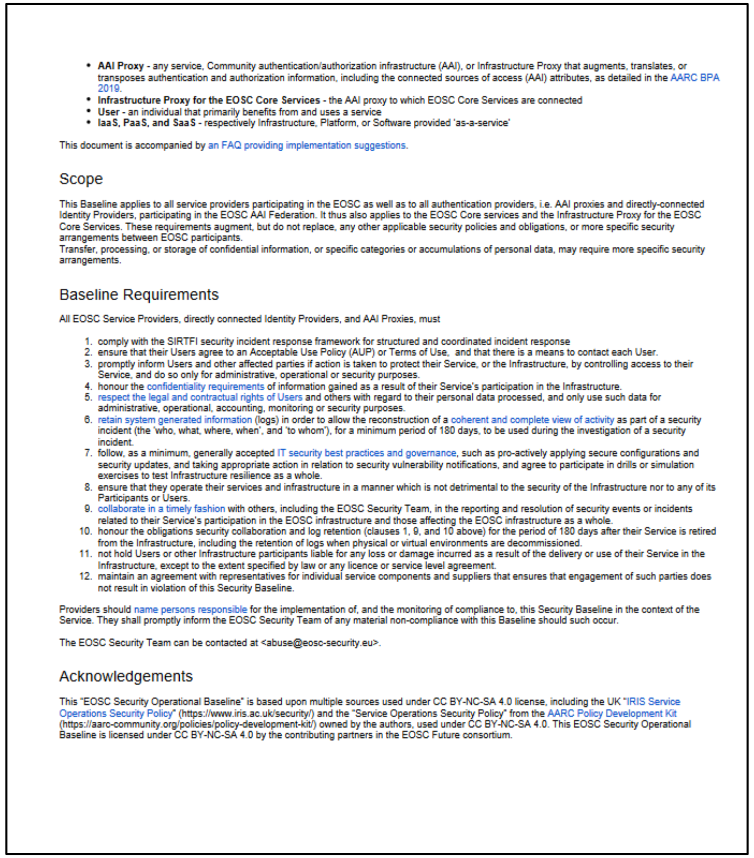
The EOSC uses the template AUP, from the WISE Community: the "WISE Baseline Acceptable Use Policy and Conditions of Use", template version 1.0, dated 25 Feb 2019. Any Service, Authentication system (AAI), or community membership management system, which presents the AUP to a user during their first use and registration must adopt this template for their particular use case; specifically, it must insert the name of its provider, as well as the purpose-binding of the AUP to the service, in the first paragraph of the template. Further guidance on how to use the AUP template is available from the AARC EU H2020 project at https://aarc-project.eu/guidelines/aarc-i044/.

*When using the baseline AUP text below, curly brackets "{ }" (coloured blue) indicate text which should be replaced as appropriate to the community, agency or infrastructure presenting the AUP to the user. Angle brackets "< >" (coloured green) indicate text which is optional and should be deleted or replaced as indicated. Other text should not be changed.*

### Introduction

This Acceptable Use Policy and Conditions of Use ("AUP") defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services ("Services") as granted by {community, agency, or infrastructure name} for the purpose of {describe the stated goals and policies governing the intended use}.

<To further define and limit what constitutes acceptable use, the community, agency, or infrastructure may optionally add additional information, rules or conditions, or references thereto, here or at the placeholder below. These additions must not conflict with the clauses 1 to 10 below, whose wording and numbering must not be changed.>



- **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, 9, and 10 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.

*Common AUP (based on WISE AUP) – required for core services to ensure consistency, strongly recommended for all services and for community AAI proxies*

*EOSC Security Operational Baseline*
*a **mere 12 points** that make you a trustworthy provider organisation towards your peers and the EOSC*

# EOSC Security Operational Baseline

Co-development of EOSC Future & AARC Policy Community

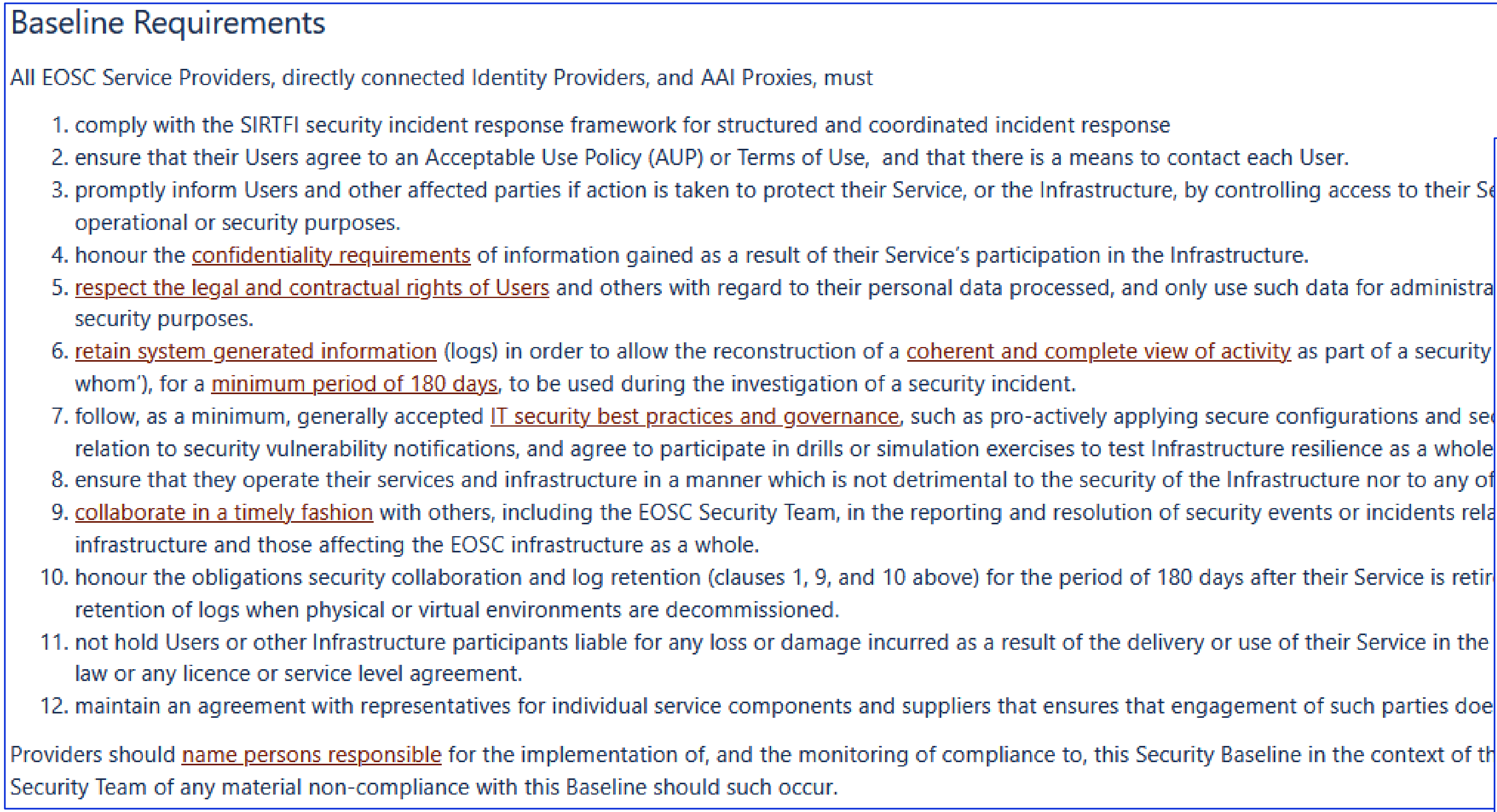
- version based on the AARC Policy Development Kit
- specifically geared towards the more heterogeneous EOSC ecosystem
- mindful of urgent need for *collective* and *coherent* response

EOSC consultation, together with AEGIS, AARC, and GEANT EnCo

- Baseline complemented by an ‘FAQ’ with guidance and references, but it defined *no new standards*: ‘there is enough good stuff out there’
- leverages REFEDS Sirtfi framework
- connects to the EOSC Core Security Team
- part of the EOSC SMS and Core Participation Agreement

Joint input to the new *WISE AARC Service Operational Policy* work in SCI

# EOSCSMS – EOSC Security Operational Baseline & FAQ

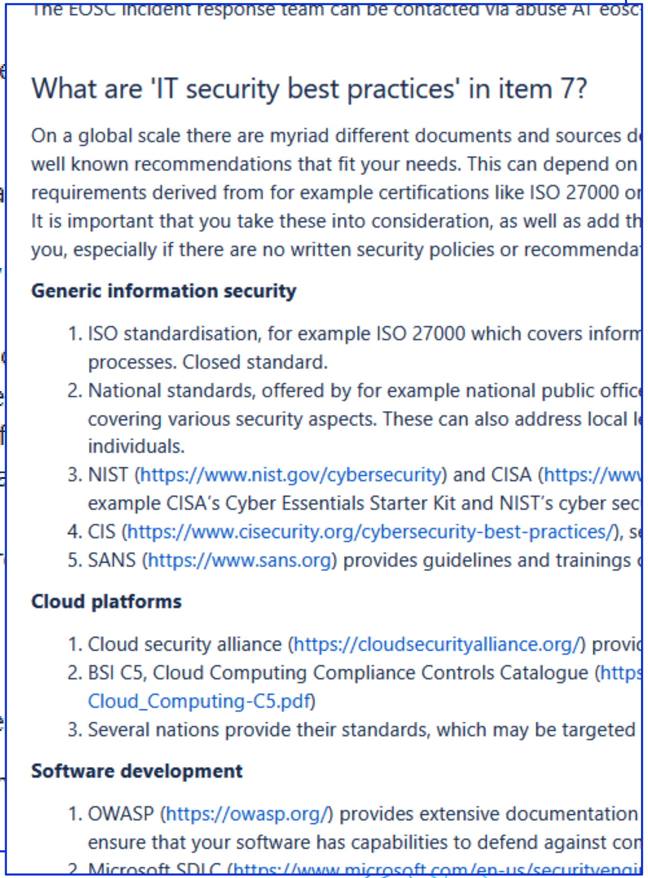


## Baseline Requirements

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 Se 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 administra 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 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 se 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
9. collaborate in a timely fashion with others, including the EOSC Security Team, in the reporting and resolution of security events or incidents rela infrastructure and those affecting the EOSC infrastructure as a whole.
10. honour the obligations security collaboration and log retention (clauses 1, 9, and 10 above) for the period of 180 days after their Service is retir 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 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 doe

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



The EOSC incident response team can be contacted via abuse AT eosc

### What are 'IT security best practices' in item 7?

On a global scale there are myriad different documents and sources d well known recommendations that fit your needs. This can depend on requirements derived from for example certifications like ISO 27000 or It is important that you take these into consideration, as well as add th you, especially if there are no written security policies or recommenda

**Generic information security**

1. ISO standardisation, for example ISO 27000 which covers inform processes. Closed standard.
2. National standards, offered by for example national public office covering various security aspects. These can also address local l individuals.
3. NIST (https://www.nist.gov/cybersecurity) and CISA (https://www example CISA's Cyber Essentials Starter Kit and NIST's cyber sec
4. CIS (https://www.cisecurity.org/cybersecurity-best-practices/), se
5. SANS (https://www.sans.org) provides guidelines and trainings

**Cloud platforms**

1. Cloud security alliance (https://cloudsecurityalliance.org/) provic
2. BSI C5, Cloud Computing Compliance Controls Catalogue (https Cloud_Computing-C5.pdf)
3. Several nations provide their standards, which may be targeted

**Software development**

1. OWASP (https://owasp.org/) provides extensive documentation ensure that your software has capabilities to defend against con
2. Microsoft SDLC (https://www.microsoft.com/en-us/securityengi

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

Thanks to the EOSC Future WP7.5 collaborators: Alf Moens, Daniel Kouřil, Baptise Grenier, David Crooks, David Groep, David Kelsey, Ian Neilson, Linda Cornwall, Matt Viljoen, Pinja Koskinen, Ralph Niederberger, Romain Wartel, Sven Gabriel, and Urpo Kaila.

EOSC Future

# Discussion time!

eoscfuture.eu

Nikhef Maastricht University

**David Groep**
**https://www.nikhef.nl/~davidg/presentations/**
**https://orcid.org/0000-0003-1026-6606**

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