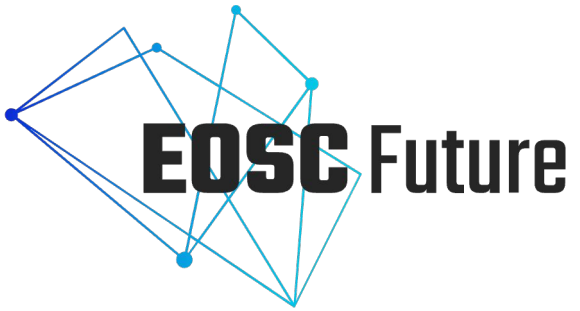


EOSC:
a secure and trusted place to reside

EOSC Symposium, November 2022

Nikhef

Maastricht University

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

Security is a means – a way to support the EOSC mission

“ensure confidentiality, integrity and availability”

“protecting our data and services from threats and vulnerabilities”

and in our interconnected EOSC, also security is a collective responsibility

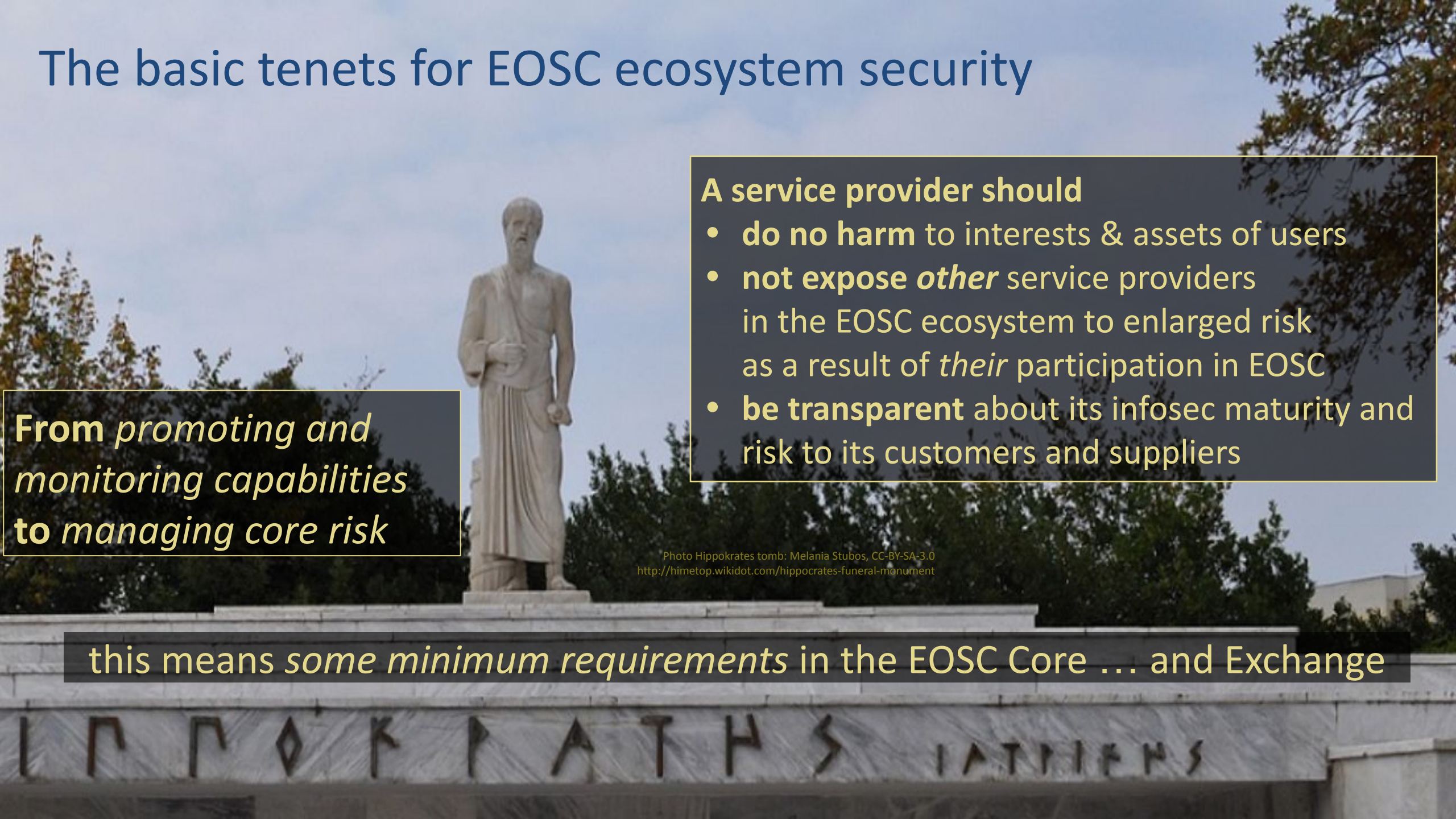
and also an opportunity to collaborate and improve our posture together

The basic tenets for EOSC ecosystem security

A service provider should

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

From *promoting and monitoring capabilities* **to** *managing core risk*



this means *some minimum requirements* in the EOSC Core … and Exchange

Keeping the EOSC secure

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

- minimum requirements to ensure a **collective response**
  and to prevent miscreants to hide in unmanaged corners of the system
- leverage collective knowledge and capabilities that each provider already has
  'baseline' is just that – only the provider really knows the inner sensitivities of each service or data set
- supported by expert fall-back in case incidents happen (and they do happen!)

How the security coordination team supports a trusted EOSC

Risk-centric self-assessment framework
- based on federated InfoSec guidance including WISE SCI

Baselining security policies & common assurance
- AARC, REFEDS, IGTF, PDK & practical implementation measures

An incident coordination hub and a trust posture
- spanning providers and core, based on experience & exercises

Actionable operational response to incidents
- EOSC core expertise to support resolution of cross-provider issues

Fostering trust through a known skills programme
- so that your peers may have confidence in service provider abilities

WISE SCI: wise-community.org/sci
AARC&c: aarc-community.org, refeds.org, igtf.net
PDK: aarc-community.org/policies/policy-development-kit

How the Information Security Process helps

EOSC ISM differentiates between Core and Exchange

- **Core**: mandatory adherence (and pro-active support from the security team) since the security of the Core services underpins the whole EOSC ecosystem
- **Exchange**: based on Interoperability Framework (& 'RFC2119 RECOMMENDED')

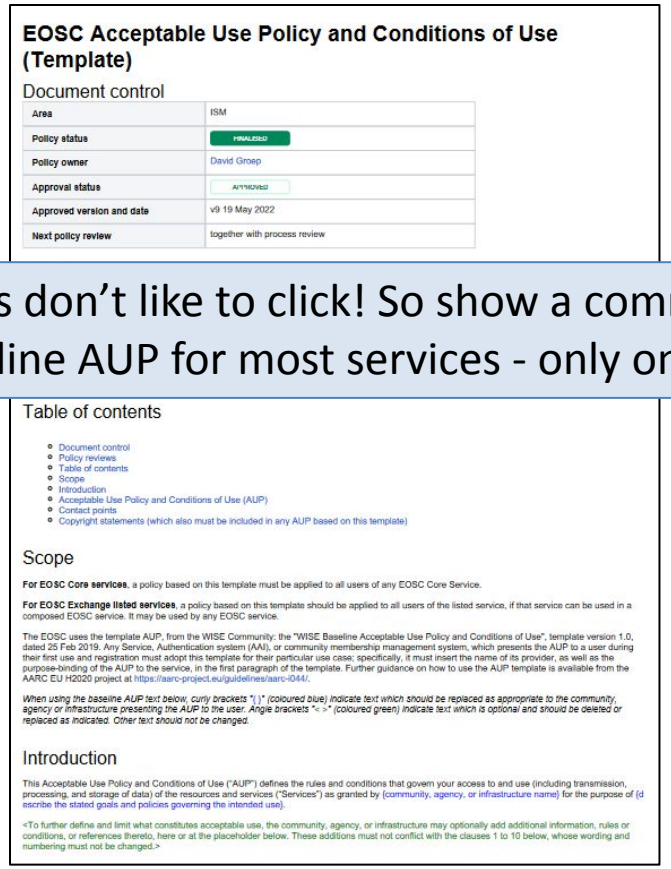
Participants are autonomous

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

We need everyone's help in incident response and 'drills' (that also a lot of fun!)

- 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

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.

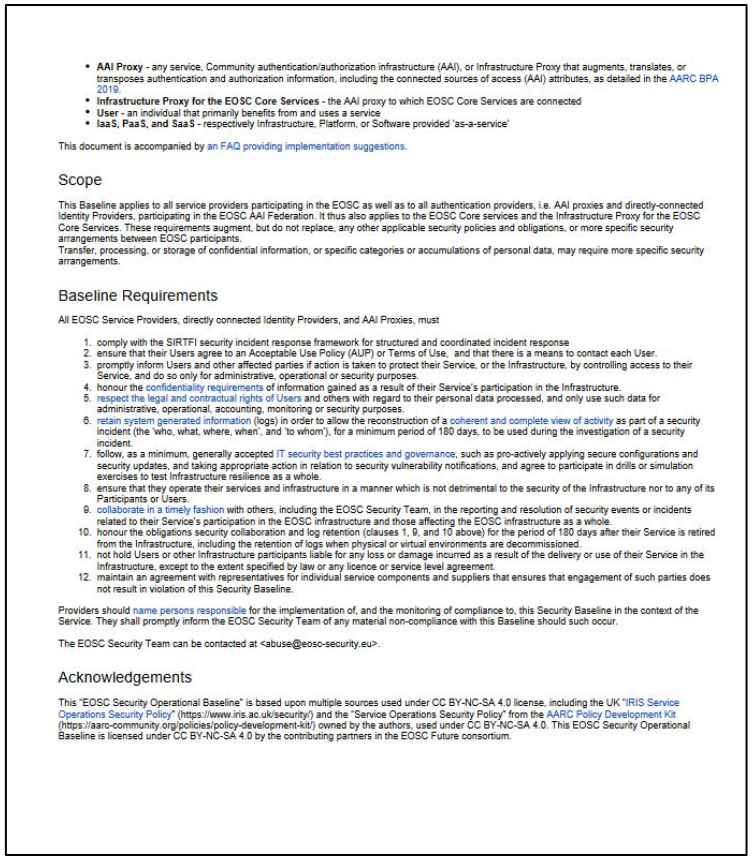
Introduction

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.>

Users don't like to click! So show a common baseline AUP for most services - only once

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



- **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.

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

EOSCSMS – EOSC Security Operational Baseline & FAQ

Baseline Requirements

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

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 Servic 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 securit 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 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 fr 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 no 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>.

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 o 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 offic covering various security aspects. These can also address local l individuals.
3. NIST (https://www.nist.gov/cybersecurity) and CISA (https://ww example CISA's Cyber Essentials Starter Kit and NIST's cyber sec
4. CIS (https://www.cisecurity.org/cybersecurity-best-practices/), s
5. SANS (https://www.sans.org) provides guidelines and trainings

Cloud platforms

1. Cloud security alliance (https://cloudsecurityalliance.org/) provi
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

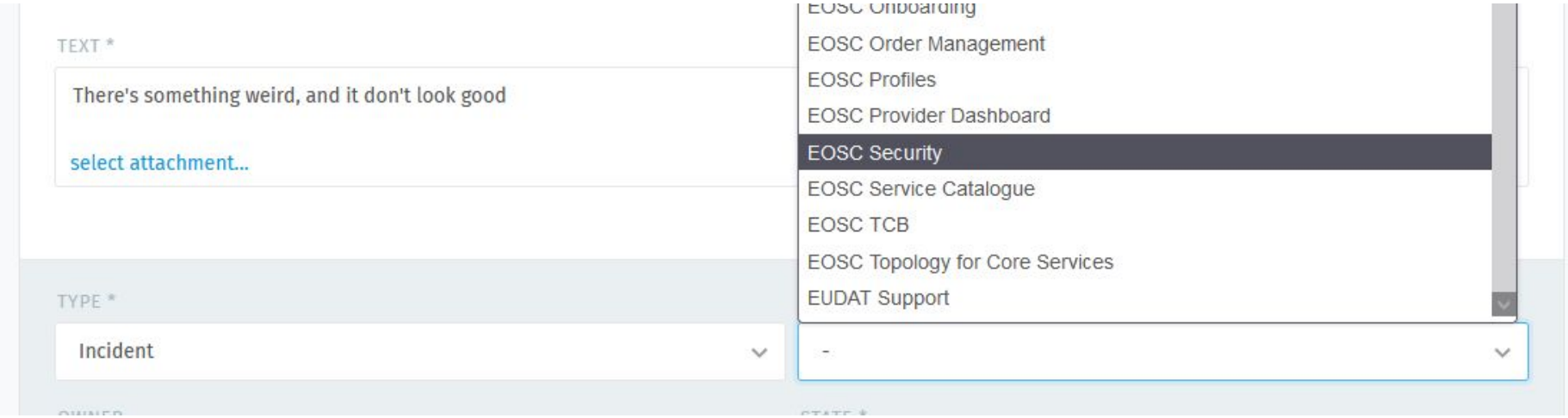
1. OWASP (https://owasp.org/) provides extensive documentation ensure that your software has capabilities to defend against co
2. Microsoft SDLC (https://www.microsoft.com/en-us/securityengi

Who you gonna call?

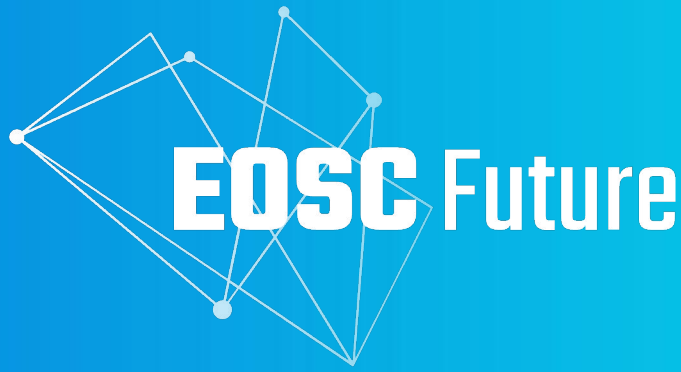
If there's something weird, and it don't look good?

abuse@eosc-security.eu

or select the EOSC Security group in the helpdesk



And of course there are real people there – your friendly CSIRT central team is:
Pau Cutrina, Daniel Kouřil, and David Crooks



Thank you

Questions

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

EOSC:
Change and Release, Capacity and Availability Management

EOSC Symposium, November 2022

Nikhef
Maastricht University

Joao Pina – WP7.2 Security Management lead
LIP

EOSC Change Management

- **The goal of this process** is to ensure that **any changes** that may have an impact on how the service is running are thoroughly *planned, approved, implemented and reviewed* in a controlled manner to avoid adverse impact of changes to services or the customers receiving services.

- **EOSC CHM implementation is a lightweight** one based on peer review of changes through Jira Tickets which helps to ensure:
  - changes are well thought through, planned and risks are understood (and mitigated against)

- **Benefits:**
  - Improve quality of service for end users
  - EOSC Continuous improvement
  - Helps coordination of dependent service delivery
  - Spreads know-how, prevents “islands of knowledge”
  - Collective responsibility of major decisions
  - a place to safe records about what was implemented and what is going on (for future deliverables and reports etc)

  - **What is not:**
  - CHM **is not about** approving what you do and/or controlling you!

- **EOSC Implementation**
  - Changes to Core technical services tracked with Jira tickets, raised for tickets and reviewed/approved by Change Advisory Board

EOSC Release and Deployment

- **The goal of this process** is to ensure that all releases are deployed into production in the most efficiently and effectively way. In order to achieve this it's necessary that every single release is build, tested and delivered according to the established EOSC-Future guidelines.

- **EOSC-Future guidelines** defined under the *Software and Quality Assurance guidelines*: services section (only one single document for all software and services best practices).
  - **Based on well established SQA** documents:
    - A set of Common Software Quality Assurance Baseline Criteria for Research Projects (DOI: 10.20350/digitalCSIC/12543)
    - A set of Common Service Quality Assurance Baseline Criteria for Research Projects (DOI 10.20350/DIGITALCSIC/12533)

EOSC Future

EOSC Release and Deployment Management

- **EOSC Release and Deployment main focus:**
  - **Automated Integration, Deployment and Testing** all EOSC Core services should be deployed with the minimal human interaction in order to avoid human errors and ensure consistency of a deployment process.
  - **Documentation** Service documentation MUST follow the FAIR principles;
  - **Security** make sure service they have defined security tests;
  - **Operational** make sure all services follow the EOSC operations guidelines;
  - **Observability**

- **Status:**
  - **EOSC Services** have very different architecture and complexity so individual services have different release and deployment implementations according to service.
  - **Integration testing** are tests required when there is a dependency between services. This type of tests are a challenge due the interaction between services in EOSC. In order to improve the adoption and reliability of this tests, it was created a dedicate working group. This work group it's not under EOSC SMS authority. The SMS only establishes process and policies for monitoring services it does not interfere on the EOSC development.

EOSC Future

EOSC Capacity Management

- **Goal of this process:** to ensure that a service has the *capacity* to meet the *agreed requirements* (CPA), and are able to adequate the service continuity in case of **exceptional situations**

- **EOSC Implementation:**
  - The process considers all resources required to deliver the IT service, and plans for short, medium, and long-term business for capacity requirements.
  - Dedicated plan for each individual service is created.
  - The **definition of Capacity plan are not easy** for many of the EOSC Core services due to there complexity, interoperability and also by the fact that some have multiple providers.

EOSC Capacity Management

- Each of the individual per Core service/activity - Capacity plan contains the following sections:
  - **Service Level Indicators:** Definition of measurable quantitative parameters relevant for understanding the capacity of the service.
    - Hardware, human resources and software
  - **Capacity strategy and adjustment models :** Description on how to modify the capacity of a service as a consequence of a change in demand together with adopted models with strategies for an increase of demand.
    - hardware, architecture, human resources
  - **Capacity Risks:** defined and rated in terms of likelihood and impact for all the above. For example: do we have enough people to operate the service? and in case of staff shortages?

EOSC Availability and Continuity

- **Goal of this process:** to ensure that a service can meet the *agreed uptime* (CPA), and are able to adequate the service continuity in case of **exceptional situations**

- **EOSC Implementation:**
  - The process considers all resources required to deliver the IT service, and plans for short, medium, and long-term business for availability and continuity requirements.
  - Dedicated plan for each individual service is created.
  - Risks affecting availability/continuity are created, mitigated against and regularly reviewed

Thank you

Questions

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