AARC Authentication and Authorisation for Research and Collaboration

The Security Baseline – in EOSC and the AARC PDK

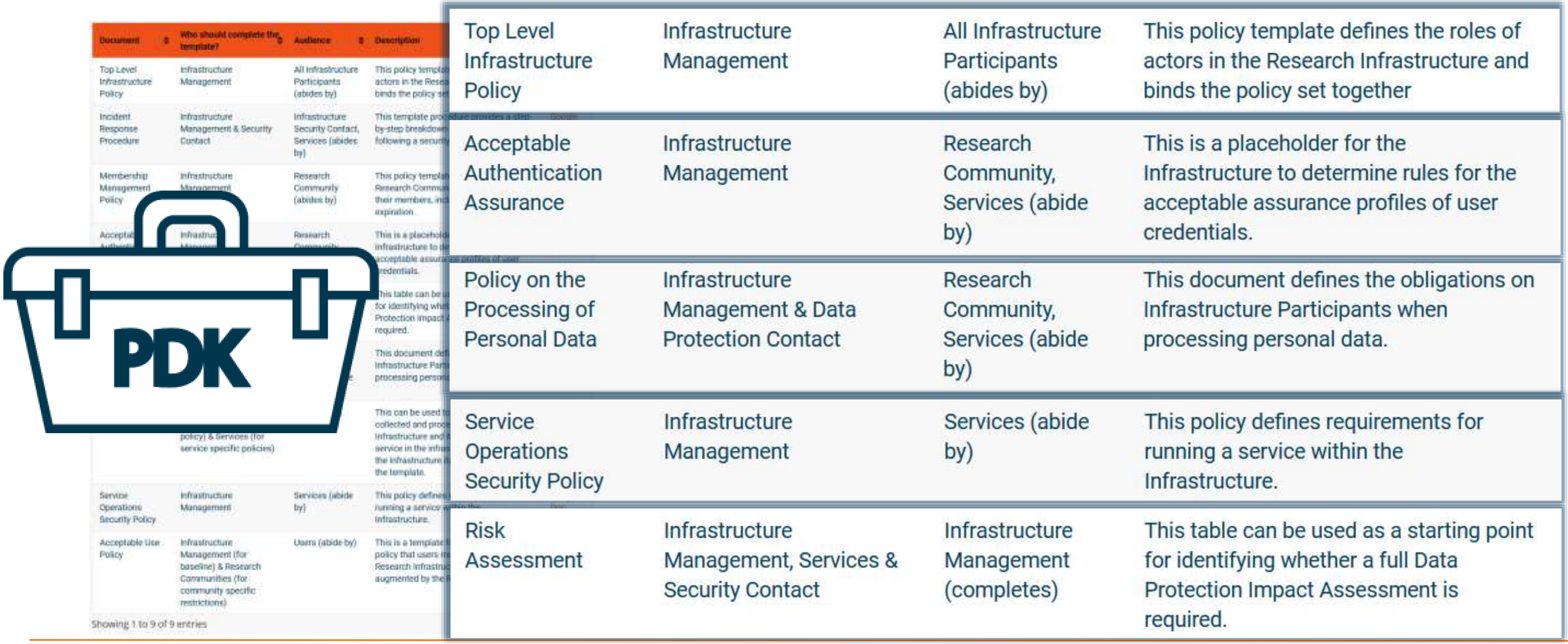
‘for loosely connected services and infrastructure’

David Groep
AARC Policy Area coordinator
Nikhef Physics Data Processing (PDP) programme

Nikhef

EUGridPMA 53
2021.09.27

AARC Policy Development Kit - Service-centric policies



Document	Who should complete the template?	Audience	Description
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the acceptable assurance profiles of user credentials.
Policy on the Processing of Personal Data	Infrastructure Management & Data Protection Contact	Research Community, Services (abide by)	This document defines the obligations on Infrastructure Participants when processing personal data.
Service Operations Security Policy	Infrastructure Management	Services (abide by)	This policy defines requirements for running a service within the Infrastructure.
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.

Showing 1 to 9 of 9 entries

https://aarc-project.eu/policies/policy-development-kit/

PDK “Service Operations” development

AARC Policy Development Kit “Service Operations” policy was rather specific

- addressed also some ‘service-internal’ operations and software
- embedded in the PDK ecosystem and did not work well as a ‘stand-alone’ document
- had a built-in assumption of a coherent and coordinated infrastructure

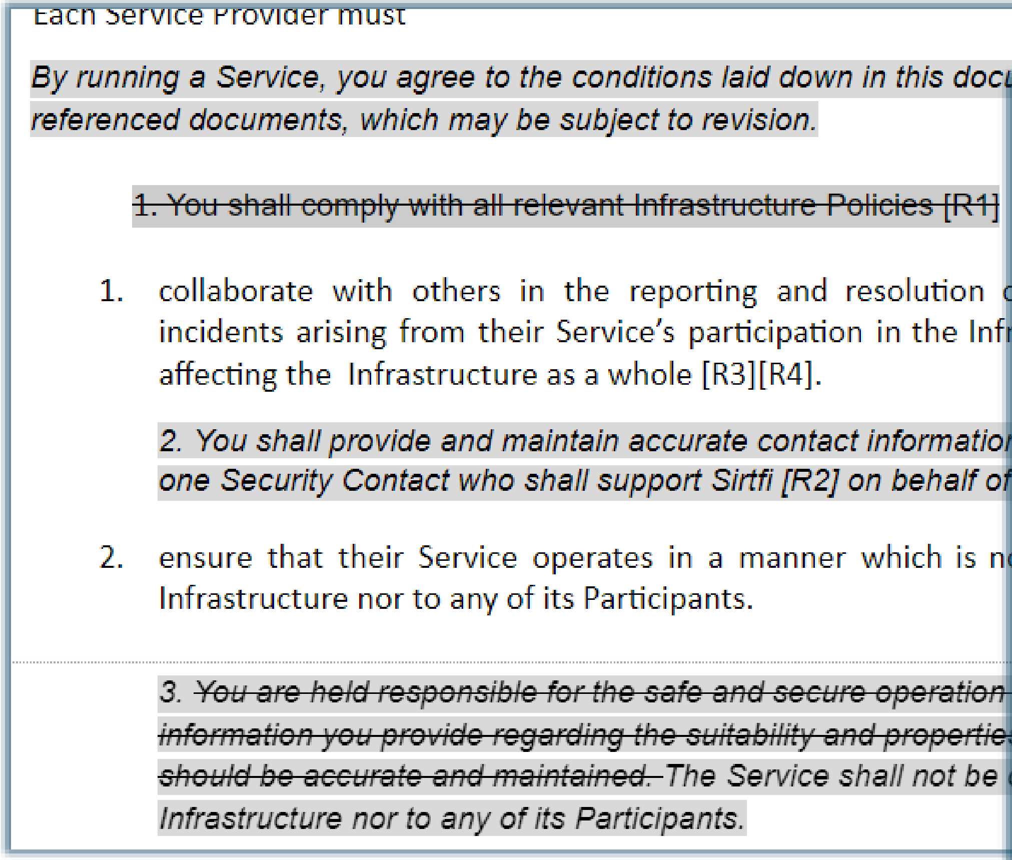
Developed by UK-IRIS to be

- more stand-alone
- better implementable by adding references and notes (‘best practice’, or an ‘FAQ’)

In the EOSC ecosystem, original assumptions also no longer hold

- services provided are less coherent, and much more autonomous then every before
- need to accommodate providers with varying maturity levels - and different intentions!

The UK IRIS improvements



Each Service Provider must

By running a Service, you agree to the conditions laid down in this docu~~ment and other~~ referenced documents, which may be subject to revision.

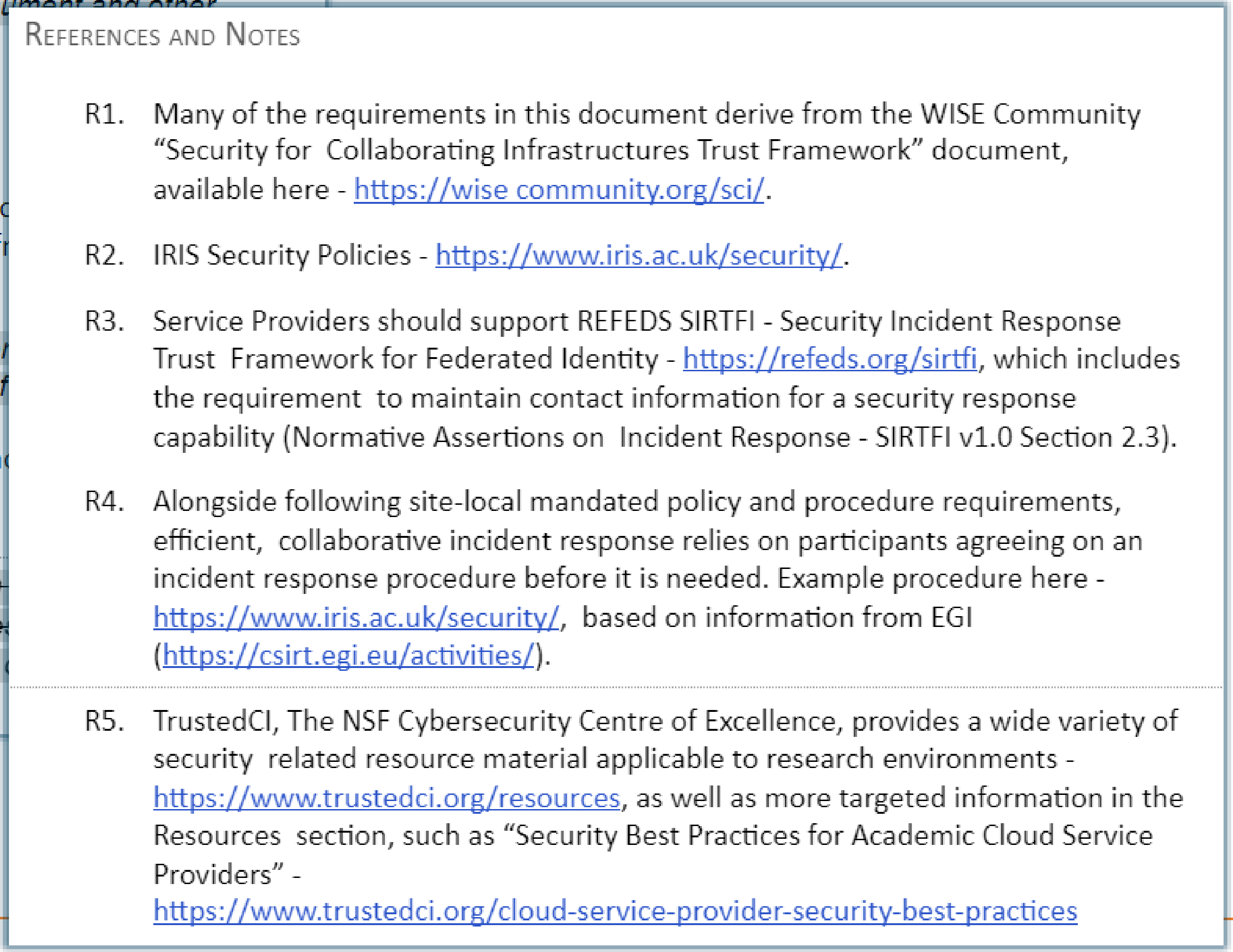
~~1. You shall comply with all relevant Infrastructure Policies [R1]~~

1. collaborate with others in the reporting and resolution o incidents arising from their Service's participation in the Infr affecting the Infrastructure as a whole [R3][R4].

2. You shall provide and maintain accurate contact informatio one Security Contact who shall support Sirtfi [R2] on behalf of

2. ensure that their Service operates in a manner which is no Infrastructure nor to any of its Participants.

~~3. You are held responsible for the safe and secure operation information you provide regarding the suitability and propertie should be accurate and maintained.~~ The Service shall not be Infrastructure nor to any of its Participants.



References and Notes

R1. Many of the requirements in this document derive from the WISE Community "Security for Collaborating Infrastructures Trust Framework" document, available here - https://wise community.org/sci/.

R2. IRIS Security Policies - https://www.iris.ac.uk/security/.

R3. Service Providers should support REFEDS SIRTFI - Security Incident Response Trust Framework for Federated Identity - https://refeds.org/sirtfi, which includes the requirement to maintain contact information for a security response capability (Normative Assertions on Incident Response - SIRTFI v1.0 Section 2.3).

R4. Alongside following site-local mandated policy and procedure requirements, efficient, collaborative incident response relies on participants agreeing on an incident response procedure before it is needed. Example procedure here - https://www.iris.ac.uk/security/, based on information from EGI (https://csirt.egi.eu/activities/).

R5. TrustedCI, The NSF Cybersecurity Centre of Excellence, provides a wide variety of security related resource material applicable to research environments - https://www.trustedci.org/resources, as well as more targeted information in the Resources section, such as "Security Best Practices for Academic Cloud Service Providers" - https://www.trustedci.org/cloud-service-provider-security-best-practices

Towards a Baseline instead of a single policy

Not all services are created equal

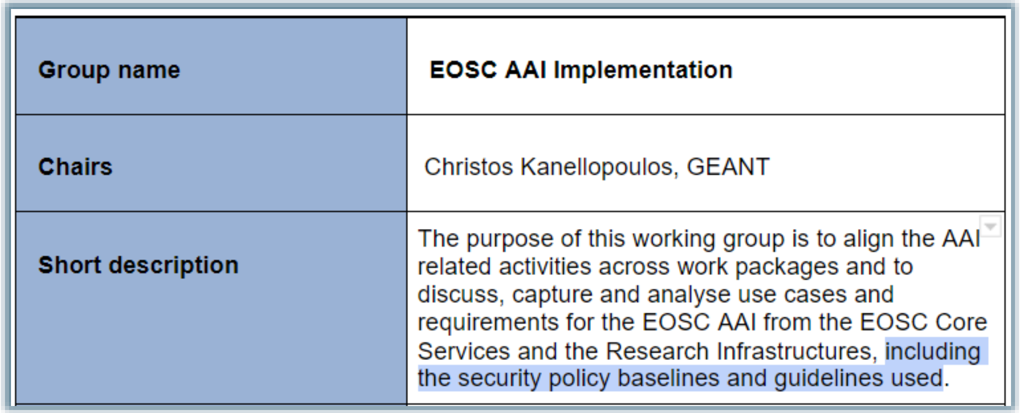
- EOSC primarily about user experience & research success: security there to support this goal
- Services are composable – and thus interdependent
- Premise: *do no harm*!

Security *Baseline*

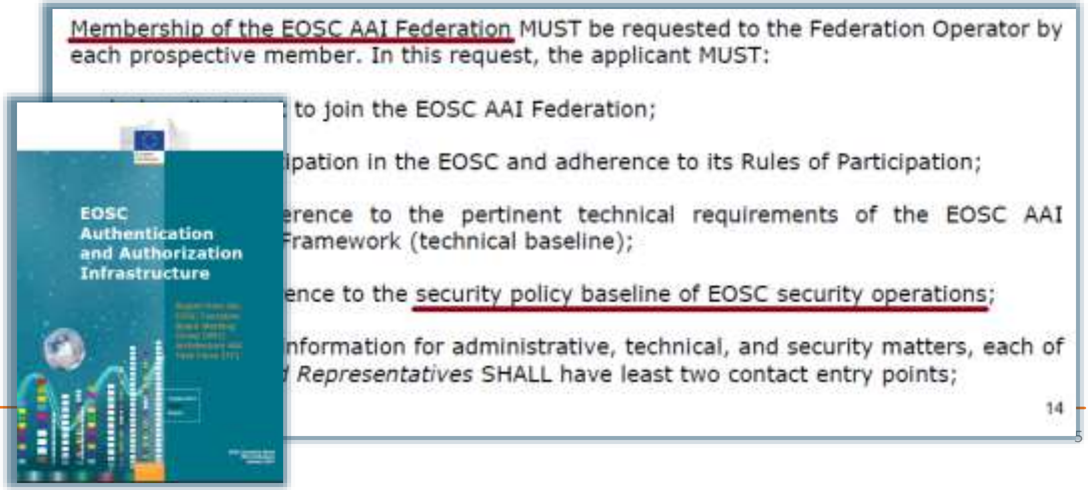
- prerequisite for connecting to the Core Infra Proxy
- connection requirement for the EOSC AAI
- may evolve over time

Additional elements can be added to augment trust

- through service level agreements
- by maturity grading (‘WISE SCI’ peer assessments)



Group name	**EOSC AAI Implementation**
Chairs	Christos Kanellopoulos, GEANT
Short description	The purpose of this working group is to align the AAI related activities across work packages and to discuss, capture and analyse use cases and requirements for the EOSC AAI from the EOSC Core Services and the Research Infrastructures, including the security policy baselines and guidelines used.



Membership of the EOSC AAI Federation MUST be requested to the Federation Operator by each prospective member. In this request, the applicant MUST:

to join the EOSC AAI Federation;

ipation in the EOSC and adherence to its Rules of Participation;

erence to the pertinent technical requirements of the EOSC AAI Framework (technical baseline);

ence to the security policy baseline of EOSC security operations;

nformation for administrative, technical, and security matters, each of *Representatives* SHALL have least two contact entry points;

14

EOSC Authentication and Authorization Infrastructure

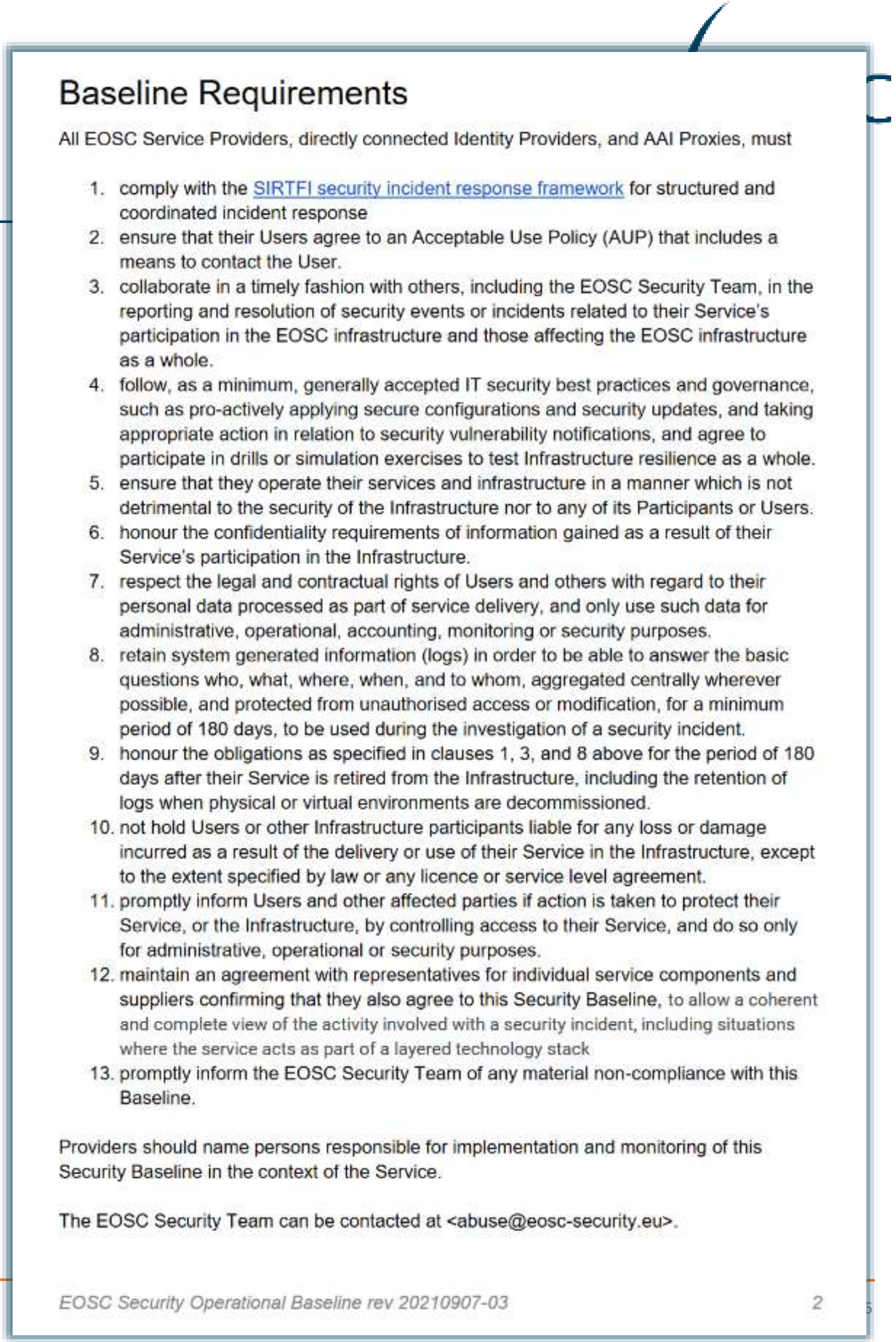
Baseline Process

Co-development of EOSC Future & AARC Policy Community

- version based on UK-IRIS evolution of the AARC PDK
- specifically geared towards the looser EOSC ecosystem
- mindful of urgent need for collective coherent response

AARC Policy team consultation – 1st round just finished

- 13 itemised points - https://edu.nl/avfv4
- complemented by an ‘FAQ’ with guidance and refs
  (no new standards, there is enough good stuff out there)
- leverages *Sirtfi* framework
- connects to the Core Security Team



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.

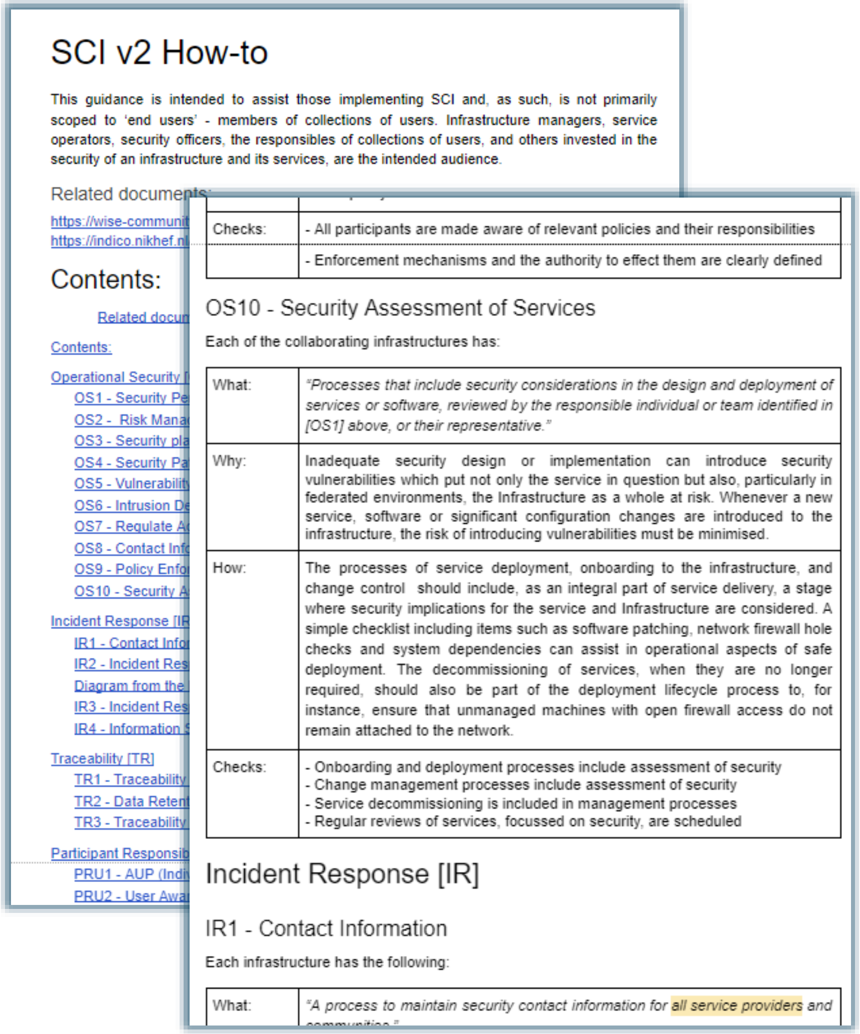
The EOSC Security Team can be contacted at <abuse@eosc-security.eu>.

EOSC Security Operational Baseline rev 20210907-03 2

https://wiki.eoscfuture.eu/x/Q4sb

Complementing elements

- SCI maturity assessment model
- WISE Risk Assessment Templates
- EOSC Future Core Security Team
- Contact information
- Response processes and guidance
- …



SCI v2 How-to

This guidance is intended to assist those implementing SCI and, as such, is not primarily scoped to ‘end users’ - members of collections of users. Infrastructure managers, service operators, security officers, the responsibles of collections of users, and others invested in the security of an infrastructure and its services, are the intended audience.

Related documents:

https://wise-communit
https://indico.nikhef.nl

Contents:

Checks:	- All participants are made aware of relevant policies and their responsibilities
	- Enforcement mechanisms and the authority to effect them are clearly defined

OS10 - Security Assessment of Services

Each of the collaborating infrastructures has:

What:	*“Processes that include security considerations in the design and deployment of services or software, reviewed by the responsible individual or team identified in [OS1] above, or their representative.”*
Why:	Inadequate security design or implementation can introduce security vulnerabilities which put not only the service in question but also, particularly in federated environments, the Infrastructure as a whole at risk. Whenever a new service, software or significant configuration changes are introduced to the infrastructure, the risk of introducing vulnerabilities must be minimised.
How:	The processes of service deployment, onboarding to the infrastructure, and change control should include, as an integral part of service delivery, a stage where security implications for the service and Infrastructure are considered. A simple checklist including items such as software patching, network firewall hole checks and system dependencies can assist in operational aspects of safe deployment. The decommissioning of services, when they are no longer required, should also be part of the deployment lifecycle process to, for instance, ensure that unmanaged machines with open firewall access do not remain attached to the network.
Checks:	- Onboarding and deployment processes include assessment of security - Change management processes include assessment of security - Service decommissioning is included in management processes - Regular reviews of services, focussed on security, are scheduled

Incident Response [IR]

IR1 - Contact Information

Each infrastructure has the following:

What:	*“A process to maintain security contact information for all service providers and communities.”*

EOSC Security Operational Baseline (rev 20210908-03)

- https://docs.google.com/document/d/1a8TQAfOnB0CADo_n5nn7-DQX6jV7Iz-2i90hBAzMgGY
- Development location(s): *to be discussed now*
- FAQ for now at https://wiki.eoscfuture.eu/display/EOSCF/EOSC+Security+Operational+Annotated+Baseline

Thank you

Any Questions?

davidg@nikhef.nl

AARC

https://aarc-community.org

The work leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme and other sources.

this work is co-supported by the EOSC-Future project, the GN4-3 project, EGI-ACE, UK-IRIS, and SURF