WISE SCI Working Group
Maintenance of the AARC Policy Development Kit

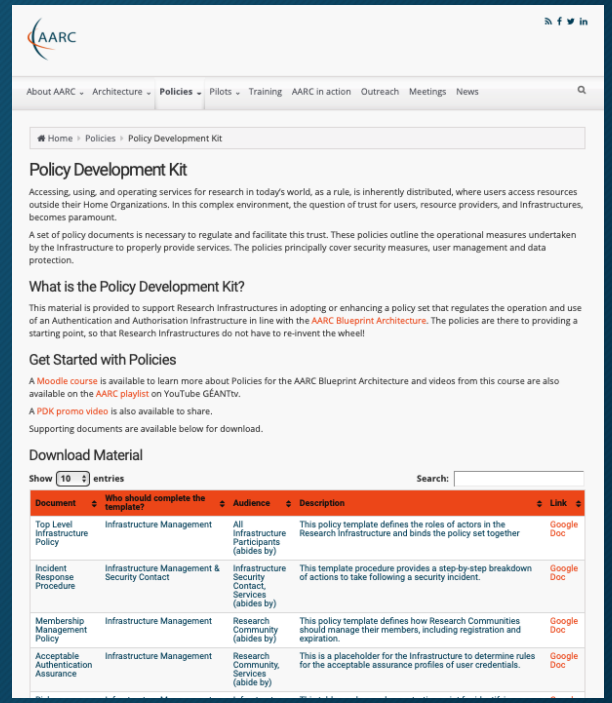
David Kelsey (UKRI-STFC)

WISE and SIG-ISM, Virtual, 21 April 2022

Policy Development Kit (reminder)
Many thanks to Hannah Short (CERN)
Slides shown by her at WISE in Oct 2021

Policy Development Kit - Background

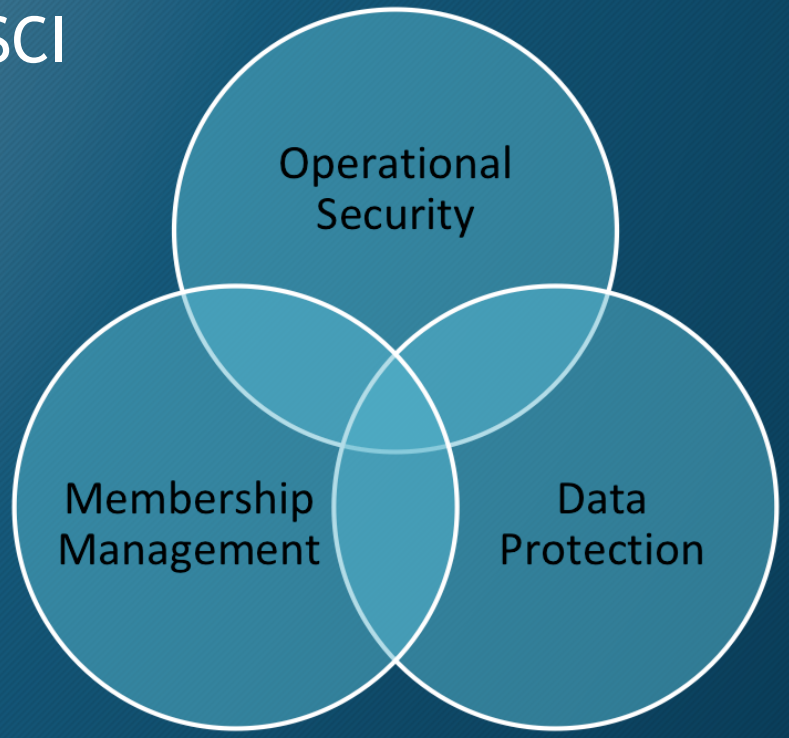
- In 2017 the AARC project highlighted Policy training as a priority, the AARC2 project tasked with providing it!
  - Interest from additional groups e.g. WISE, EUGridPMA
  - WISE SCI refers to the need for multiple policies but no concrete examples provided
  - Research Communities were asking for help getting started with policies and related documents (this has continued...)
- Since then
  - Published PDK https://aarc-community.org
  - Agreed to be maintained by WISE
  - Practical experience gathered



Policy Development Kit - Content

- Which policies? Work backwards from SCI
  - Top level policy
    - Operational Security
    - Membership Management
    - Data Protection

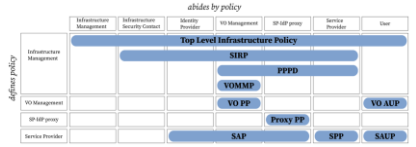
- Sources of inspiration?
  - EGI
  - CTSC
  - ELIXIR
  - …



Policy Development Kit - Content

		Management	Infrastructure Security Contact	User Community Management	Service Management	User
Top Level	Infrastructure Policy	Defines & Abides by	Abides by	Abides by	Abides by	
Data Protection	Privacy Statement	Defines			Defines	Views
	Policy on the Processing of Personal Data	Defines	Abides by	Abides by	Abides by	
Membership Management	Community Membership Management Policy	Defines		Abides by		
	Acceptable Use Policy	Defines		Defines		Abides by
	Acceptable Authentication Assurance	Defines		Abides by	Abides by	
Operational Security	Incident Response Procedure	Defines	Abides by		Abides by	

Evolution

Infrastructure	Changes	Comment	Link
HIFIS (previously HDF)	Initial users (and one of main contributors)		https://hifis.net/doc/helmholtz-aai/policies/
ELIXIR	Added Terms of Use	Focused on the AAI only rather than the entire Infra. Dropped Top Level	ToU https://docs.google.com/document/d/10DBkPr_zWpFJPWTav8SMw61IVExIU0349pUkBl9cLjw/edit#
IRIS	Significantly modified Top Level policy and Service Operations Security Policy	Emphasis on standalone, short policies	SOSP https://www.iris.ac.uk/wp-content/uploads/2021/05/IRIS-Service-Operations-Security-Policy.pdf
EOSC	Built from IRIS's Service Operations Security Policy	Much more loosely coupled infrastructure than anticipated by PDK	SOSP https://docs.google.com/document/d/1a8TQAfOnB0CADo_n5nn7-DQX6jV7Iz-2i90hBAzMgGY/edit#heading=h.eyau1431a74f

Comparison table

- Work done by Ian N to compare the Service Operations PDK version with IRIS and EOSC
- Key changes pulled out for discussion later :)
- https://wiki.geant.org/display/WISE/Policy+Development+Kit

AARC PDK – 7 + 3 sub clauses, 417 words	**IRIS** – 10 clauses, 336 words	**EOSC Baseline** (as of 30/09/2021) – 13 clauses, 444 words
By running a Service, you agree to the conditions laid down in this document and other referenced documents, which may be subject to revision. You shall comply with all relevant Infrastructure Policies [R1]	Each Service Provider must	All EOSC Service Providers, directly connected Identity Providers, and AAI Proxies, must
1. You shall provide and maintain accurate contact information, including at least one Security Contact who shall support Sirtfi [R2] on behalf of the service.	1. collaborate with others in the reporting and resolution of security events or incidents arising from their Service's participation in the Infrastructure and those affecting the Infrastructure as a whole [R3][R4].	1. comply with the SIRTFI security incident response framework for structured and coordinated incident response 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.

Maintenance of AARC PDK
(now rest of slides from Dave Kelsey)

AARC PDK - Current work

- WISE SCI working group has restarted
  - In Autumn 2021
  - Meeting roughly every 2 weeks
  - Chaired by Hannah Short (until December 2021)
    - Then by Dave Kelsey (from January 2022)
- Start with “Service Operations Security Policy”
  - Lots of interest in Infrastructures having clear policies about what is required for participating services
- Next topic – agreed by SCI-WG in January 2022
  - update AARC guidance on Data Protection

- https://wise-community.org/policy-development-kit/

Service Operations Security Policy

- Draft completed
- Next step - consultation of the WISE Community
  - Comments, suggestions, changes, feedback
  - Consultation starts here today!
- Then we can publish the updated version of this AARC PDK component

The WISE AARC Policy Development Kit

Service Operations Security Policy Template

Part of the generic WISE-AARC Policy Development Kit

Draft Version 0.93, 4 Apr 2022

Authors: Members of the WISE Community SCI Working Group, particularly:

Linda Cornwall (UKRI), David Crooks (UKRI), Thomas Dack (UKRI), Sven Gabriel (Nikhef), Baptiste Grenier (EGI Foundation), David Groep (Nikhef), David Kelsey (UKRI), Maarten Kremers (SURF), Alf Moens (GEANT), Ian Neilson (UKRI), Ralph Niederberger (FZJ), Hannah Short (CERN), Uros Stevanovic (KIT), Romain Wartel (CERN)

e-mail: sci@lists.wise-community.org

Other Sources / Attribution / Acknowledgements: "EGI Service Operations Security Policy", used under CC BY-NC-SA 3.0.The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

WISE SCI PDK policy template

Text still required to provide introduction to "What is the PDK?"

When using the policy template text below, Angle brackets "< >" and bold text indicates text which either needs to be replaced with the correct information or it is optional and should be deleted or replaced as indicated. Text in coloured boxes provides advice and guidance and should not be present in the final policy document.

Questions to ask yourself when defining the policy:

- Do you require a generic security contact from Services (e.g. security@site.com) or would individually identifiable contacts in addition be beneficial?
- How quickly do you require a response during a security incident? Is this on a best effort basis, or can a more specific timeframe be expected?
- For how long is a Service obliged to fulfil its obligations after announcing its retirement?
- Which security best practices must be followed/adopted by infrastructure Services? We recommend Sirtfi but there may be others.
- For how long should logs be kept?

The WISE AARC Policy Development Kit

Service Operations Security Policy

This policy, version **<X>**, is effective from **<insert date>**.

By running a Service, you agree to the conditions laid down in this document **<and other referenced documents>**. You acknowledge that your Service's connection to the Infrastructure may be regulated for administrative, operational and security purposes if you fail to comply with these conditions. Upon retirement of a Service, the obligations specified in this policy shall not lapse for a period **<of X months>**.

You shall:

The following security specific clauses are recommended for all infrastructures

1. Aim for the safe and secure operation of the Service, which shall not be detrimental to the Infrastructure nor to its Participants.

Service Operations – draft text (2)

You shall:

The following security specific clauses are recommended for all infrastructures

1. Aim for the safe and secure operation of the Service, which shall not be detrimental to the Infrastructure nor to its Participants.
2.

   We recommend including at least a generic contact point that ensures response regardless of individual personnel availability, and that does not expose personal data. However, you may wish to include additional individuals. Any contact is better than no contact.

   Provide and maintain accurate contact information, including at least one Security Contact. **<This contact SHOULD be responsive regardless of individual personnel availability.>**
3. Respond to requests for assistance with regards to a security incident **<or threat> <on an informal and best effort basis | within X business hours>,** when received from another Participant or the Infrastructure Security team. This includes participation in scheduled exercises to test Infrastructure resilience as a whole.
4.

   Note that a Service may be composed of many components or layers of infrastructure, logs from all of which may need to be combined. You may wish to include more precise guidance to ensure a global overview of service-level traceability.

Retain sufficient system/service generated information (logs), aggregated centrally wherever possible, and protected from unauthorised access or modification, for a minimum period of **<X>** days, to be used for traceability and forensics in the event of a security incident.

5. Follow IT security best practices, including pro-actively applying updates or configuration changes related to security. The following practices MUST be adopted:

   You may want to consider inserting a static copy, or a dated version, of the external practices in case they are updated.

   a. **<Support of the Sirtfi Framework [insert reference] on behalf of your Service>**
   b. **<Include any additional mandatory practices, such as ISO compliance>**
6. Inform users, where appropriate, when their access to your Service has been regulated, and do so only for administrative, operational or security purposes.
7. Promptly inform the Infrastructure Security Officer of any non-compliance with this policy.

Service Operations (3)

The following clauses are not security specific but are often included in the Service Operations Security Policy if no other suitable policy exists

8. Respect the legal rights of Infrastructure Users and others with regard to their personal data, and only use such data for administrative, operational, accounting, monitoring or security purposes.
9. Not hold Users or other Infrastructure participants responsible for any loss or damage incurred as a result of the provision or use of their Service in the Infrastructure, except to the extent specified by law or any licence or service level agreement.
10. Ensure that any information you provide regarding the suitability and properties of the Service is as accurate as possible.

Now to AARC PDK guidance on Data Protection

Guidance on Data Protection (e.g. for GDPR)

- The original AARC PDK and related guidance on this topic:
- Policy on the processing of personal data https://docs.google.com/document/d/1QseGQVzUQqvosqhjkF2qlHUI4Swlhgb8oDe8N6NWcqE/edit?usp=sharing
- Privacy Policy https://docs.google.com/document/d/1ZU7VjH3g7qcfWcz0Z8TTv-vQiVoRA_wOsuMyJaz28Og/edit?usp=sharing
- https://aarc-project.eu/wp-content/uploads/2016/12/AARC-DNA3.5_Recommendations-for-Processing-Personal-Data_2016_11_07_v4_DG.pdf
- https://aarc-project.eu/wp-content/uploads/2018/05/AARC-G042-Data-Protection-Impact-Assessment-initial-guidance-for-communities.pdf

Old AARC PDK policy templates (Personal Data) - just some parts

Policy on the Processing of Personal Data

Questions to ask yourself when defining this policy:
- Purpose of processing personal data?
- Who has access to these data and why?
- Are the data properly protected?
- Does the user have access to their personal data?

This policy is effective from <insert date>.

INTRODUCTION

This policy ensures that data collected as a result of the use of the Infrastructure is processed fairly and lawfully by Infrastructure participants. Some of this data, for example that relating to user registration, monitoring and accounting contains "personal data" as defined by the European Union (EU) [GDPR]. The collection and processing of personal data is subject to restrictions aimed at protecting the privacy of individuals.

DEFINITIONS

Infrastructure - The bounded collection of universities, laboratories, institutions or similar entities, which adhere to a common set of policies [<insert link>] and together offer data processing and data storage services to End Users.
Participant - Any entity providing, managing, operating, supporting or coordinating one or more Infrastructure service(s).
Personal Data - Any information relating to an identified or identifiable natural person [GDPR].
Processing (Processed) - Any operation or set of operations, including collection and storage, which is performed upon Personal Data [GDPR].
End User - An individual who by virtue of their membership of a recognised research community is authorized to use Infrastructure services.

Privacy Policy

Questions to ask yourself when defining this policy:
- Who or what is your Data Controller?
- Will your Research Community have a Data Protection Officer?
- Which information do you need to collect on the user? Is this minimised?
- Specific data collected by each service may vary. Can your Infrastructure provide a template statement for all services?

This policy is effective from <insert date>.

Name of the Service	SHOULD be the same as mdui:DisplayName
Description of the Service	SHOULD be the same as mdui:Description
Data controller and a contact person	You may wish to include the Data Controller defined for the Infrastructure, rather than per-service
Data controller's data protection officer (if applicable)	

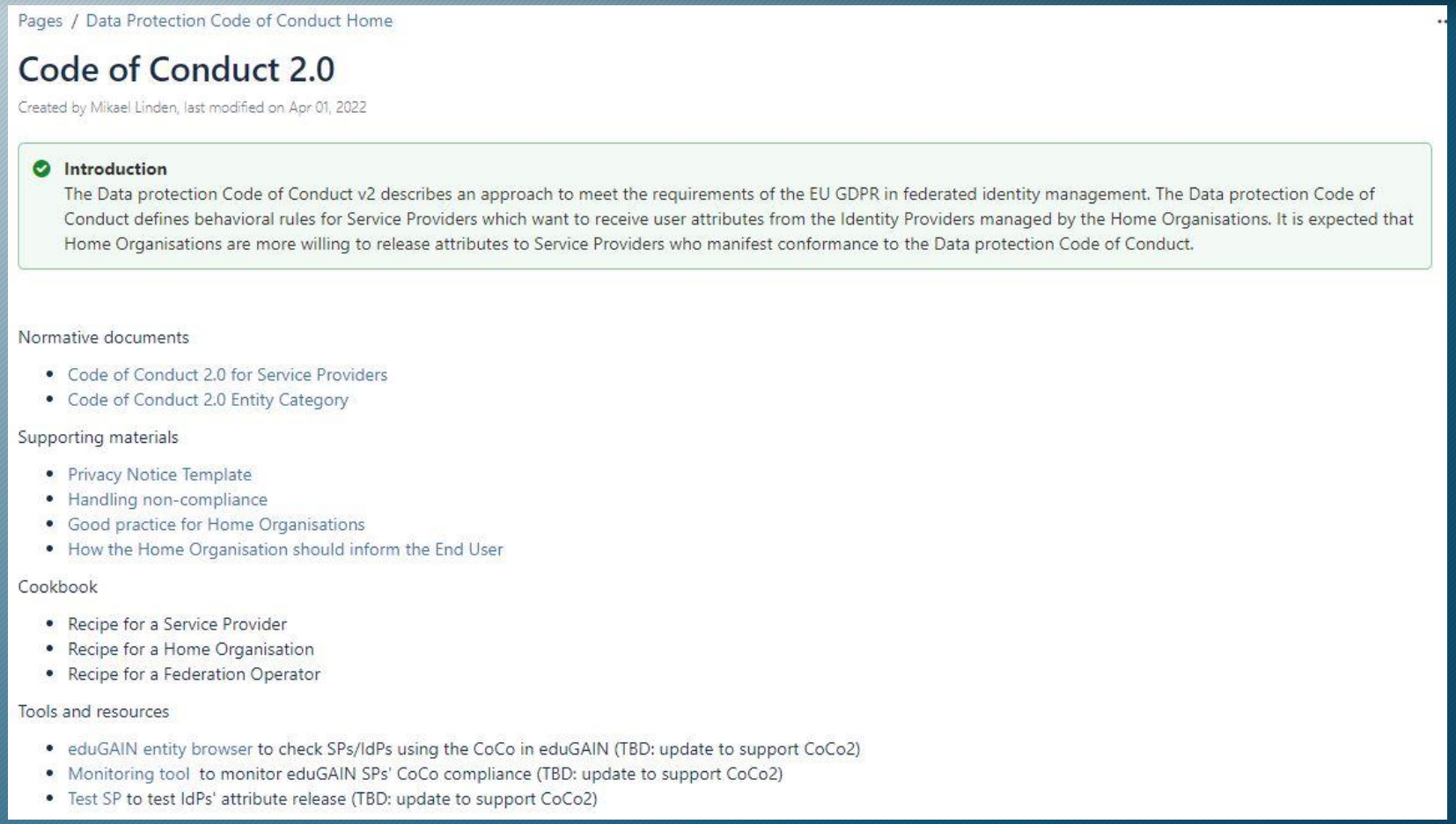
Life Science Login Service (input to SCI-WG)

- An AAI service which used the AARC PDK as templates for several of its policies https://lifescience-ri.eu/ls-login/
- The Life Science Login service has published (Jan22) its policies at:
- https://lifescience-ri.eu/ls-login/policy-on-the-processing-of-personal-data-of-the-ls-aai-service.html
- https://lifescience-ri.eu/ls-login/privacy-notice-for-life-science-login.html
- SCI-WG compared the LS Login documents with the AARC PDK versions
- Result of comparison
  - They used the AARC PDK templates with very few changes
    - Main difference – 10 years data retention (common practice in Life Sciences data)

REFEDS Data Protection Code of Conduct V2

- Update of old GEANT CoCo V1 – for GDPR
  - https://wiki.refeds.org/display/CODE/Code+of+Conduct+1.0
- Initially hoped for approval by EU authorities
- But not done – document is now guidance for best practice
- REFEDS V2 consultation has now ended
  - To be published (by REFEDS not GEANT)
  - https://wiki.refeds.org/display/CODE/Code+of+Conduct+2.0

REFEDS Code of Conduct V2



Pages / Data Protection Code of Conduct Home

Code of Conduct 2.0

Created by Mikael Linden, last modified on Apr 01, 2022

Introduction

The Data protection Code of Conduct v2 describes an approach to meet the requirements of the EU GDPR in federated identity management. The Data protection Code of Conduct defines behavioral rules for Service Providers which want to receive user attributes from the Identity Providers managed by the Home Organisations. It is expected that Home Organisations are more willing to release attributes to Service Providers who manifest conformance to the Data protection Code of Conduct.

Normative documents

- Code of Conduct 2.0 for Service Providers
- Code of Conduct 2.0 Entity Category

Supporting materials

- Privacy Notice Template
- Handling non-compliance
- Good practice for Home Organisations
- How the Home Organisation should inform the End User

Cookbook

- Recipe for a Service Provider
- Recipe for a Home Organisation
- Recipe for a Federation Operator

Tools and resources

- eduGAIN entity browser to check SPs/IdPs using the CoCo in eduGAIN (TBD: update to support CoCo2)
- Monitoring tool to monitor eduGAIN SPs' CoCo compliance (TBD: update to support CoCo2)
- Test SP to test IdPs' attribute release (TBD: update to support CoCo2)

SCI-WG work on AARC PDK – Data Protection

- We will (next) update the policy template and the template Privacy Notice
- May have multiple approaches based on what different Infrastructures currently do
- The updated AARC PDK guidance will also reference the new REFEDS Code of Conduct V2
- Aim to include input from outside of the EU (not just GDPR)
- Please join us - to help update the templates!

Questions & Feedback