

Policy Development Kit

Hannah Short (CERN)
WISE and SIG-ISM, Virtual 2021



Today



- Intro to the Policy Development Kit
- Evolution
- Feedback & Questions
- Working Session

Introduction



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
 - 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

A screenshot of the AARC website's "Policy Development Kit" page. The page includes a navigation menu, a breadcrumb trail, and introductory text about the kit's purpose. It also features a "Download Material" section with a table of documents.

Policy Development Kit

Accessing, using, and operating services for research in today's world, as a rule, is inherently distributed, where users access resources outside their Home Organizations. In this complex environment, the question of trust for users, resource providers, and Infrastructures, becomes paramount.

A set of policy documents is necessary to regulate and facilitate this trust. These policies outline the operational measures undertaken by the Infrastructure to properly provide services. The policies principally cover security measures, user management and data protection.

What is the Policy Development Kit?

This material is provided to support Research Infrastructures in adopting or enhancing a policy set that regulates the operation and use of an Authentication and Authorisation Infrastructure in line with the [AARC Blueprint Architecture](#). The policies are there to providing a starting point, so that Research Infrastructures do not have to re-invent the wheel!

Get Started with Policies

A Moodle course is available to learn more about Policies for the AARC Blueprint Architecture and videos from this course are also available on the [AARC playlist](#) on YouTube GEANTtv.

A [PDK promo video](#) is also available to share.

Supporting documents are available below for download.

Download Material

Show entries

Document	Who should complete the template?	Audience	Description	Link
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	Google Doc
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)	This template procedure provides a step-by-step breakdown of actions to take following a security incident.	Google Doc
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.	Google Doc
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.	Google Doc

Policy Development Kit - Process



- Majority of structuring and editing by AARC participants
- Input from wider community through WISE and IGTF
- Members of EOSC-Hub policy task were “volunteered” to review individual policy templates

A screenshot of a document editor window titled "AARC Policy Development Kit". The window shows a table of contents on the right side of the page. The table lists various sections and their corresponding page numbers. The sections are: Abstract (2), Introduction (2), Scope (3), Policy Impact on Infrastructure Operation (3), Infrastructure Policies and Frameworks (4), Frameworks (5), Sirtfi Trust Framework (5), Research and Scholarship Entity Category (5), GÉANT Data Protection Code of Conduct (6), Policies (7), Top Level (7), Infrastructure Policy (7), Data Protection (8), Privacy Statement (8), Risk Assessment (9), Membership Management (9), Community Membership Management Policy (10), Acceptable Use Policy (10), Acceptable Authentication Assurance (10), Operational Security (12), Incident Response Procedure (12), Policy Templates (12), Top Level Infrastructure Policy Template (12), Membership Management Policy Template (17), Acceptable Authentication Assurance Policy Template (22), and Acceptable Use Policy Template (23). The document is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License and builds on work from EGI. The author list includes U. Stevanovic, H. Short, D. Groep, I. Neilson, and I. Mikhailava. The document is also linked to a task plan and notes on the GEANT wiki.

Policy Development Kit - Considerations



Policy pack must be:

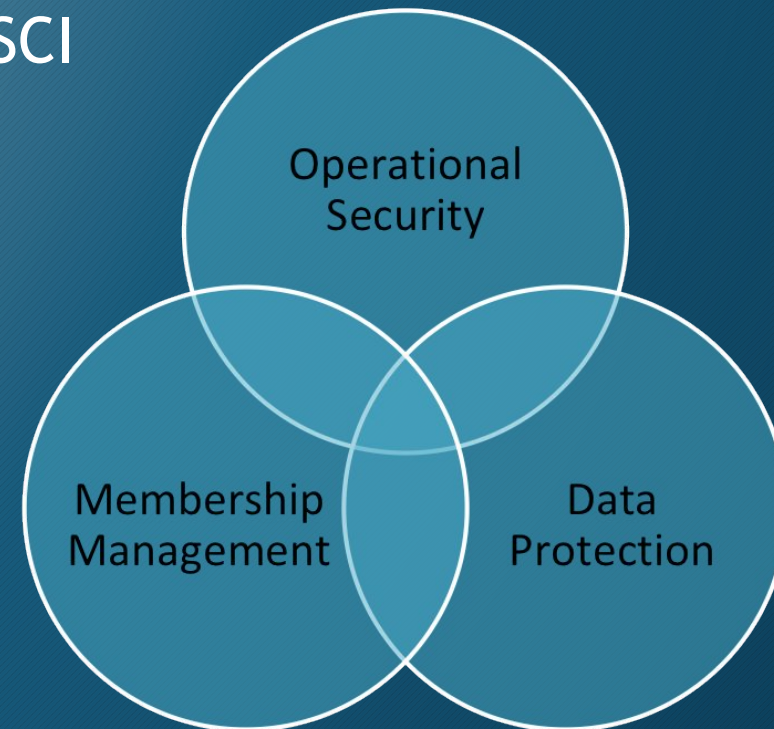
- Modular
- Coherent
- Widely applicable
- Modifiable
- Simple

Implications:

- Cannot assume that an infrastructure will have certain bodies, e.g. a CERT
- Terms must be defined as jargon varies, e.g. PI (Principal Investigator) vs VO (Virtual Organisation) Manager
- ...

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
 - ...



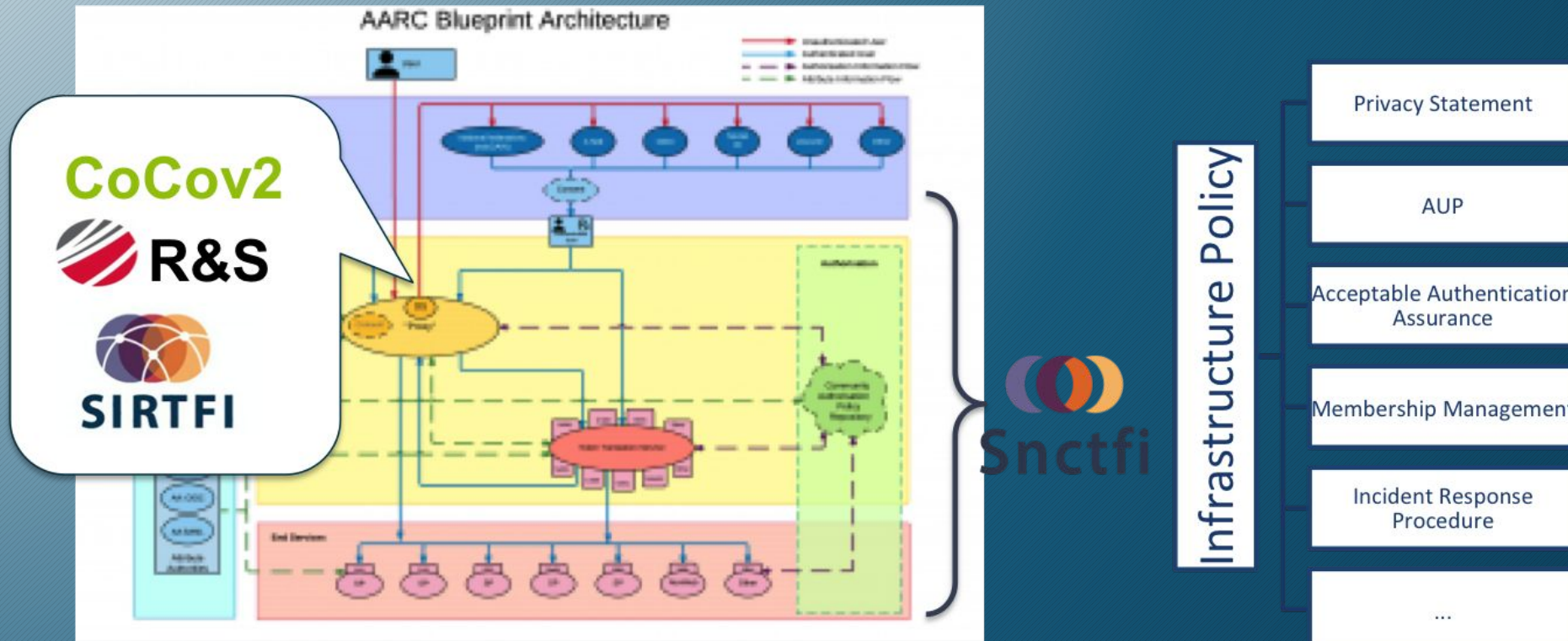
Policy Development Kit - Content



Actually, the policies can be applied much more broadly as we will see...

*The policies presented are relevant for an **Infrastructure operating a Service Provider Proxy** that represents the bound set of services in an identity federation. The policies are to be adopted by the Infrastructure itself and, where appropriate, additional policies are suggested for Infrastructure participants such as Services, User Community Management or Users. The Infrastructure may be for the sole use of a single **Research Community**, or may provide computing services to multiple Research Communities; the policies presented are designed to be **flexible**.*

Policy Development Kit - Content



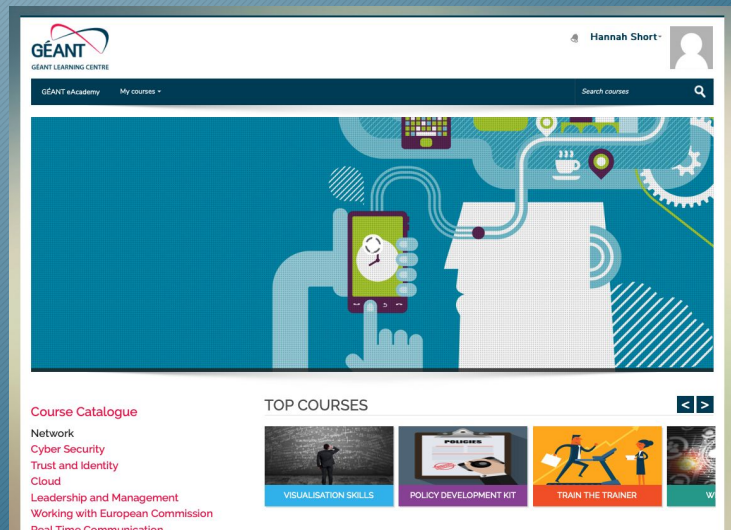
Policy Development Kit - Content



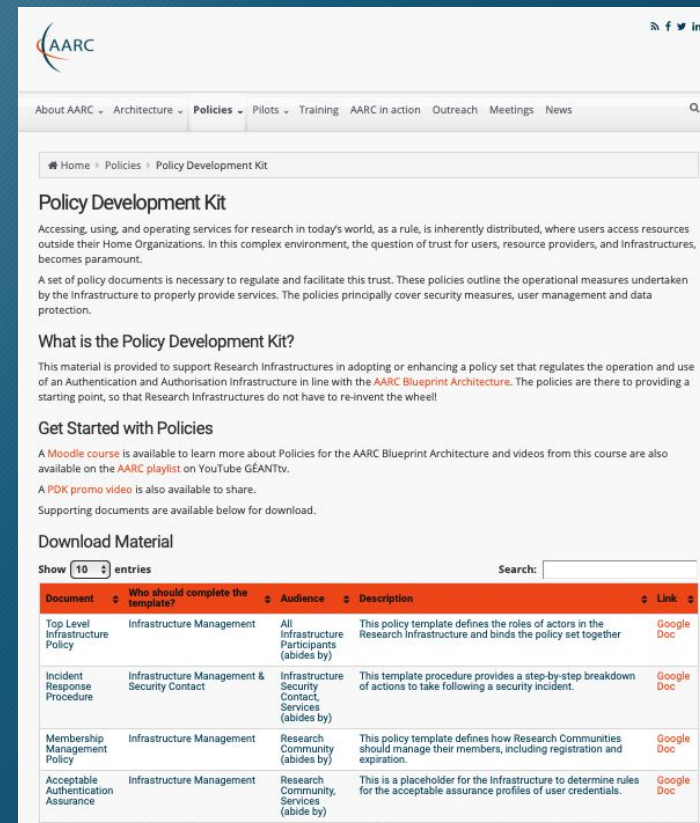
		Management	Infrastructure Security Contact	User Community Management	Service Management	User
Top Level	Infrastructure Policy	Defines & Abides by	Abides by	Abides by	Abides by	
Data Protection	Privacy Statement	Defines			Defines	Views
	Policy on the Processing of Personal Data	Defines	Abides by	Abides 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	

Policy Development Kit - Use

- Training course on the GEANT e-Academy
- Templates available directly from the AARC Website



The screenshot shows the GEANT e-Academy website. At the top, there is a user profile for Hannah Short. Below that is a search bar and a large graphic illustration of a hand holding a smartphone connected to various icons representing technology and education. On the left, there is a 'Course Catalogue' with links for Network, Cyber Security, Trust and Identity, Cloud, Leadership and Management, Working with European Commission, and Real Time Communication. In the center, there is a 'TOP COURSES' section with a carousel of course thumbnails, including 'VISUALISATION SKILLS', 'POLICY DEVELOPMENT KIT', and 'TRAIN THE TRAINER'.



The screenshot shows the AARC website page for the Policy Development Kit. The page has a navigation menu with options like About AARC, Architecture, Policies, Pilots, Training, AARC in action, Outreach, Meetings, and News. The main content area is titled 'Policy Development Kit' and includes an introduction, a definition of the kit, and a list of documents available for download.

Policy Development Kit

Accessing, using, and operating services for research in today's world, as a rule, is inherently distributed, where users access resources outside their Home Organizations. In this complex environment, the question of trust for users, resource providers, and Infrastructures, becomes paramount.

A set of policy documents is necessary to regulate and facilitate this trust. These policies outline the operational measures undertaken by the Infrastructure to properly provide services. The policies principally cover security measures, user management and data protection.

What is the Policy Development Kit?

This material is provided to support Research Infrastructures in adopting or enhancing a policy set that regulates the operation and use of an Authentication and Authorisation Infrastructure in line with the AARC Blueprint Architecture. The policies are there to providing a starting point, so that Research Infrastructures do not have to re-invent the wheel!

Get Started with Policies

A Moodle course is available to learn more about Policies for the AARC Blueprint Architecture and videos from this course are also available on the AARC playlist on YouTube GEANTtv.

A PDK promo video is also available to share.

Supporting documents are available below for download.

Download Material

Show 10 entries

Document	Who should complete the template?	Audience	Description	Link
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	Google Doc
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)	This template procedure provides a step-by-step breakdown of actions to take following a security incident.	Google Doc
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.	Google Doc
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.	Google Doc

Evolution



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_zWpFJPWTav8SMw61IVExIU0349pUkBI9cLjw/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 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.

Current work



- WISE SCI working group has restarted
- Meeting roughly every 2 weeks
- Partially triggered by CS3MESH who would like help before Christmas (thanks for being here!)
- Focusing on Service Operations Security Policy
 - Lots of interest in Infrastructures having clear policies about what is required for participating services
- <https://wise-community.org/policy-development-kit/>

Questions & Feedback



Working Session



Today, focus on the Secure Service Operations Policy

<https://docs.google.com/document/d/1oO2OsBG99Wf3ecvjU28qma4ubyzpBJgMIB93eRpz6Ck/edit?usp=sharing>