



Authentication and Authorisation for Research and Collaboration

Policy Starter Pack

Authentication and Authorisation for Research and Collaboration

Hannah Short (CERN), Uros Stevanovic (KIT)

AARC NA3

With much input from Irina Mikhailava and the rest of NA3

EUGridPMA

May 24th 2018

Agenda

Brief outline

- Motivation
- Policy Starter Pack
 - Definition
 - Content
- Continuation

Motivation

- Last AARC AHM highlighted Policy as a priority
- Interest from additional groups e.g. WISE
- Snctfi framework refers to the need for multiple policies but no concrete examples provided
- Research Communities are asking for help getting started with policies and related documents

Training support

Andrea Biancini (**Reti**), leader of the training activity, presented the modular approach being taken to **AARC training**. Priorities for the next 6 months were defined based on feedback from the meeting participants. The following areas were highlighted as high priorities:

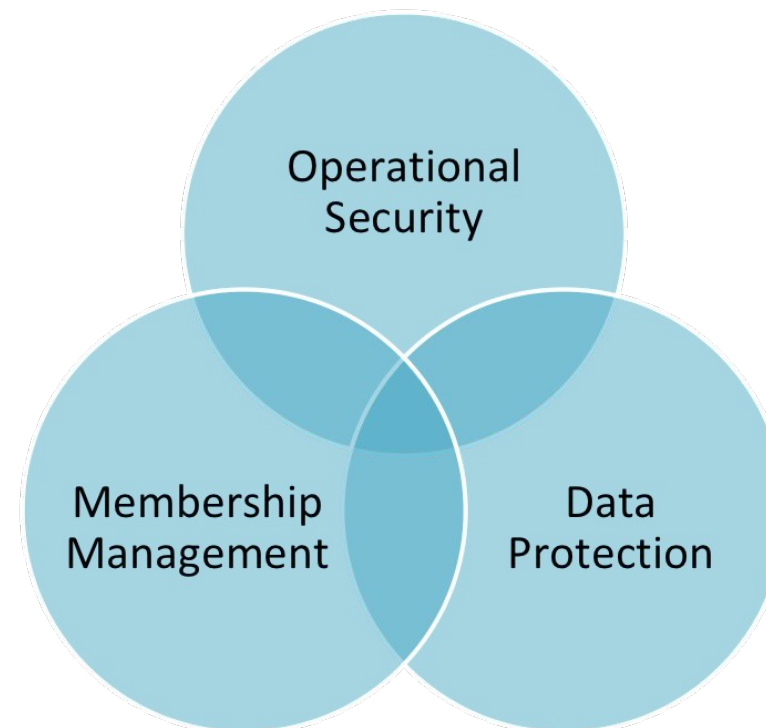
- › Training for the life sciences community following the first pilot results expected in January 2018;
- › Training for the EPOS community resource providers, explaining how to enable federated access, and a more general training about how **EPOS** can deploy an AAI based on the AARC blueprint architecture.
- › General training on **AARC policies**;
- › Training modules to support service providers in research collaborations.

In parallel the training team will continue to work on a 'handbook' for service providers that will be made available via e- and research-infrastructures. This will provide information on how to enable federated access and how to connect to infrastructure proxies.

AARC2 AHM November 2017 Highlights

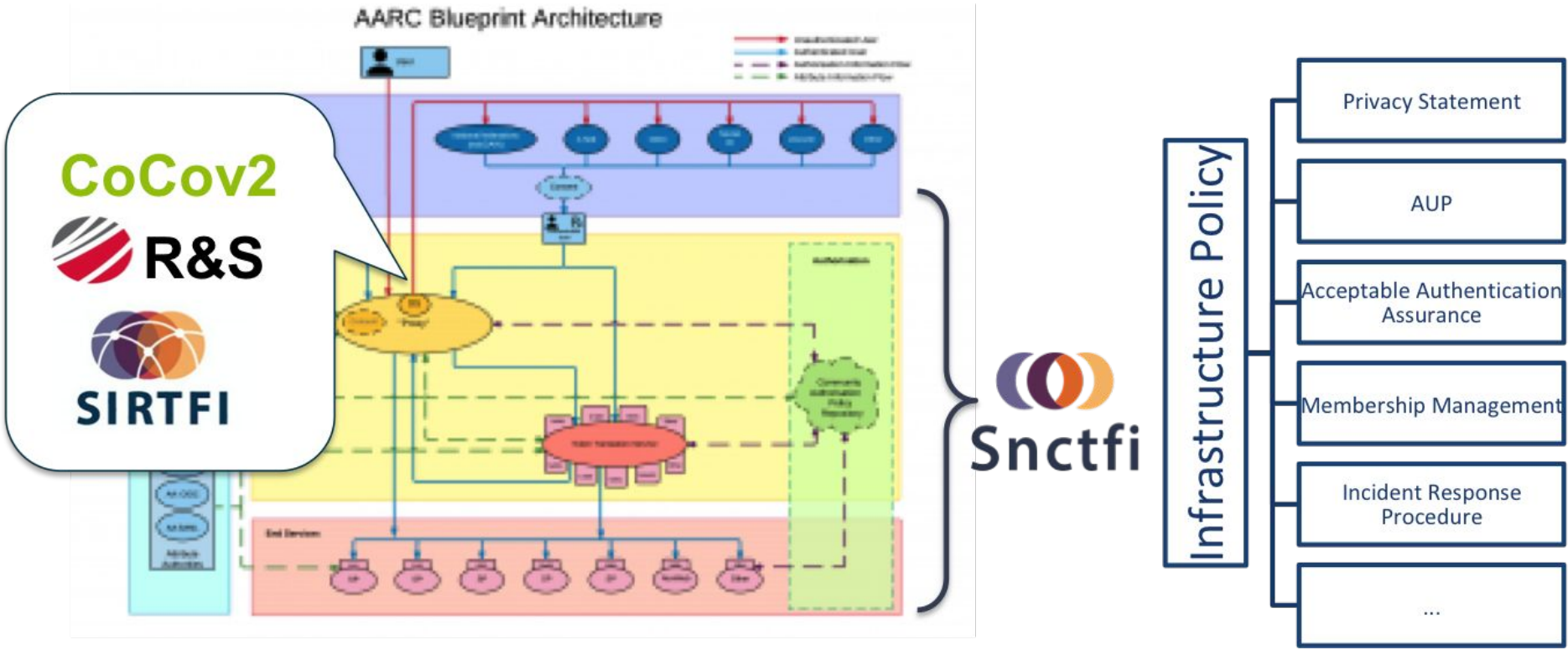
Policy Starter Pack

- Which policies? Start from Snctfi and work downwards
 - Top level policy
 - Operational Security
 - Membership Management
 - Data Protection
- Which frameworks?
 - Best practice community frameworks
- Sources of inspiration?
 - EGI
 - CTSC
 - ELIXIR
 - ...



*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 Starter Pack



		Management	Infrastructure Security Contact	User Community Management	Service Management	User
Top Level	Infrastructure Policy	Defines & Abides by	Abides by	Abides by	Abides by	Abides by
Data Protection	Privacy Statement	Defines			Defines	Views
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 Starter Pack

Policy pack must be:

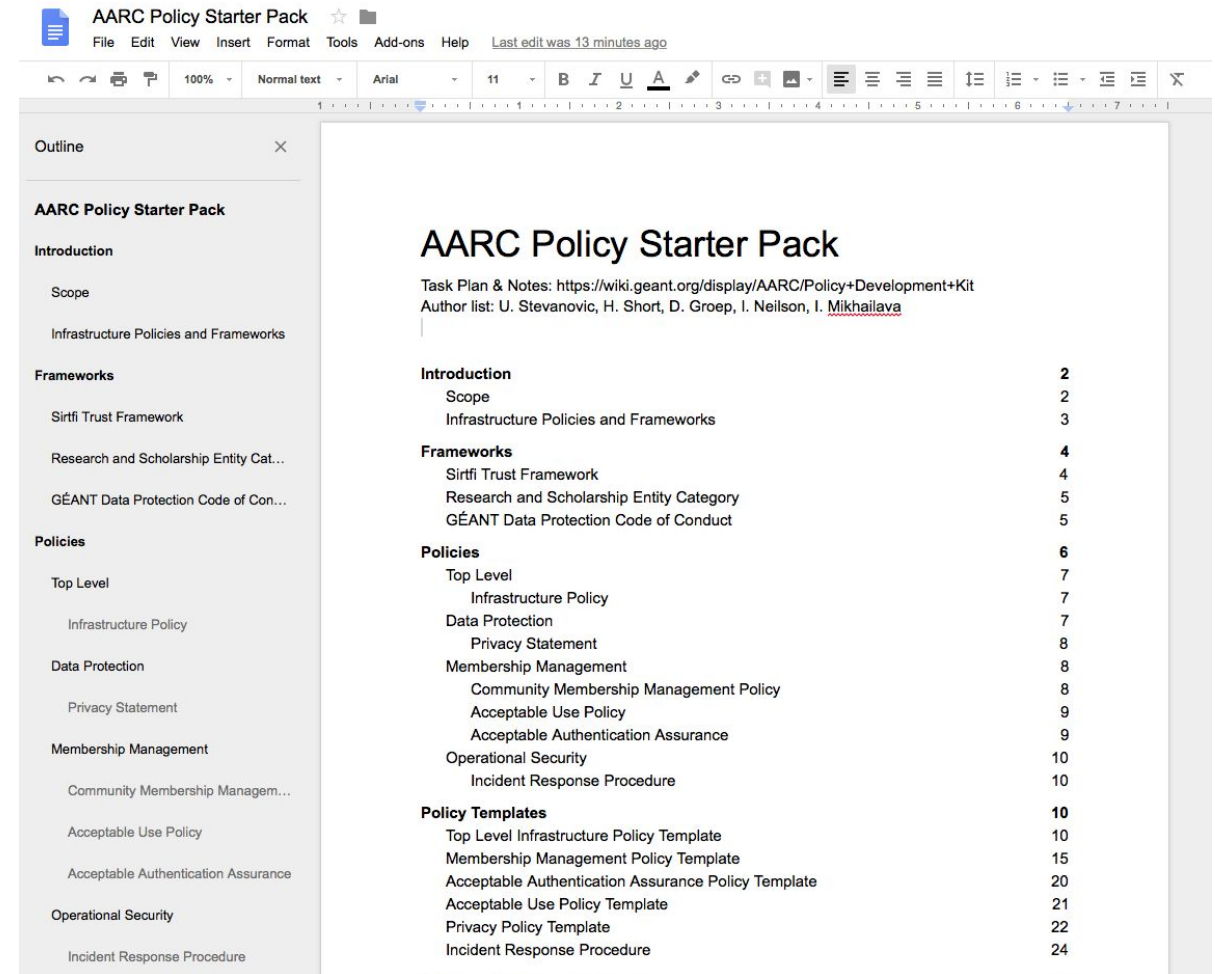
- Modular
- Widely applicable
- Modifiable
- Simple

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 Starter Pack

- Collaborative effort between NA2 and NA3
- Input from wider community through WISE and IGTF



AARC Policy Starter Pack

File Edit View Insert Format Tools Add-ons Help Last edit was 13 minutes ago

100% Normal text Arial 11 B I U A

Outline

AARC Policy Starter Pack

Introduction

- Scope
- Infrastructure Policies and Frameworks

Frameworks

- Sirtfi Trust Framework
- Research and Scholarship Entity Cat...
- GÉANT Data Protection Code of Con...

Policies

- Top Level
 - Infrastructure Policy
- Data Protection
 - Privacy Statement
- Membership Management
 - Community Membership Managem...
 - Acceptable Use Policy
 - Acceptable Authentication Assurance
- Operational Security
 - Incident Response Procedure

AARC Policy Starter Pack

Task Plan & Notes: <https://wiki.geant.org/display/AARC/Policy+Development+Kit>
 Author list: U. Stevanovic, H. Short, D. Groep, I. Neilson, I. Mikhailava

Introduction	2
Scope	2
Infrastructure Policies and Frameworks	3
Frameworks	4
Sirtfi Trust Framework	4
Research and Scholarship Entity Category	5
GÉANT Data Protection Code of Conduct	5
Policies	6
Top Level	7
Infrastructure Policy	7
Data Protection	7
Privacy Statement	8
Membership Management	8
Community Membership Management Policy	8
Acceptable Use Policy	9
Acceptable Authentication Assurance	9
Operational Security	10
Incident Response Procedure	10
Policy Templates	10
Top Level Infrastructure Policy Template	10
Membership Management Policy Template	15
Acceptable Authentication Assurance Policy Template	20
Acceptable Use Policy Template	21
Privacy Policy Template	22
Incident Response Procedure	24

Top Level Infrastructure Policy

- Top policy regulating activities and duties with all participants (with other policies..)
- EGI Top Policy served as an input
- Binds additional policies together

Content:

- Definitions
 - Objectives
 - Scope
- Roles and Responsibilities
 - Management
 - Security contacts
- Security
- Sanctions
- Exceptions

INTRODUCTION AND DEFINITIONS

To fulfil its mission, it is necessary for the Infrastructure to protect its assets. This document presents the *policy* regulating those activities of *participants* related to the security of the Infrastructure.

Definitions

The phrase Infrastructure when italicised in this document, means all of the people and organisations, hardware, software, networks, facilities, etc. that are required to develop, test, deliver, monitor, control or support IT services.

The other italicised words used in this document are defined as follows:

- *Policy* is interpreted to include rules, responsibilities and procedures specified in this document together with all those in other documents which are required to exist by stipulations in this document.
- A *participant* is any entity providing, using, managing, operating, supporting or coordinating one or more IT *service(s)*.
- A *service* is any computing or software system accessible by *Users* of the Infrastructure.
- ...

Membership Management Policy Template

- Management of community users
- EGI as a source

Content

- Definitions
- Users (meaning and obligations)
- Community manager and other roles
- Community
 - Aims and purposes
 - Membership
 - Membership Life Cycle
- Data protection
- Traceability
- Registry and registration data

INTRODUCTION

This policy is designed to establish trust between a Community and other Communities, Infrastructures, and the R&E federations. The behaviour of the Community and its users must be appropriate and facilitate the Community's compliance with the requirements of the Sncf document [ref]. The identifiers of requirements from the Sncf document are provided herein for ease of reference. This Policy applies to the Community Manager and other designated Community management personnel. It places requirements on Communities regarding eligibility, obligations and rights of their Users, and it governs their relationships with all Infrastructures with which they have a usage agreement. ...

DEFINITIONS

A Community is a set of one or more groups of persons (Users), organised with a common purpose, with a Community Management willing to take responsibility for all sub-groups, jointly granted access to one or more Infrastructures. It may serve as an entity which acts as the interface between the individual Users and an Infrastructure. In general, the members of the Community will not need to separately negotiate access with Service Providers or Infrastructures (hereafter jointly called Infrastructures).

...

Acceptable Authentication Assurance Policy

- Defining the required form and values for assurance
- R&S, IGTF, REFEDS

Content:

- Defining approved authentication sources
- Operational matters
- More specific policies (if necessary)

INTRODUCTION

In order to protect its assets, the Infrastructure needs to authenticate, identify, and trace Users granted access to its Services. The authentication and identification must be sufficient to meet the requirements of the Security Policy and any ancillary Specific Policies, bearing in mind the nature of data stored within the Infrastructure and the heterogeneous authentication options.

DEFINITION OF APPROVED AUTHENTICATION ASSURANCE SOURCES

<Define your own approved Authentication Assurance sources. Options to consider include

IGTF profiles

Combinations of REFEDS profiles, such as Sirfti + RAF

>

OPERATIONAL MATTERS

<Authentication Assurance will be propagated with the user's authentication token for relying services to include in Authorisation decisions.>|<Only users conforming to one of the approved authentication assurance profiles shall be granted access to the Infrastructure.>

...

Acceptable Use Policy (AUP)

- Presented to the user
- User must accept it before accessing the services
- Defining the goal and purpose of the community/infrastructure

Content:

- User declaration
 - Mostly expectations and obligations that user is taking on itself when using the resources

RESEARCH COMMUNITY AIMS AND PURPOSES

This Research Community is operated for the purpose of <insert a brief description>. Individual services within the Infrastructure may present additional Acceptable Use Policies.

USER DECLARATION

By registering as a user you declare that you have read, understood and will abide by the following conditions of use:

1. You shall only use the resources/services to perform work, or transmit or store data consistent with the stated goals, policies and conditions of use as defined by the body or bodies granting you access.
2. You shall provide appropriate acknowledgement of support or citation for your use of the resources/services provided as required by the body or bodies granting you access.
3. You shall not use the resources/services for any purpose that is unlawful and not (attempt to) breach or circumvent any administrative or security controls.
4. You shall respect intellectual property and confidentiality agreements.
5. You shall protect your access credentials (e.g. private keys or passwords).
6. ...

Privacy Policy

- Privacy policy presented to the user
- Info about processing of the user's personal data
- Per service (including Main Privacy Policy)

Content:

- Which data are collected?
- For what purpose?
- DPO? Contact?
- Jurisdiction?
- Legal basis?
- Disclosure of data?
- Access, remedies
- Retention
- DP CoCo

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)	

Incident Response Procedure

- Description of the procedure how to handle an incident response
- Duties and responsibilities

Content:

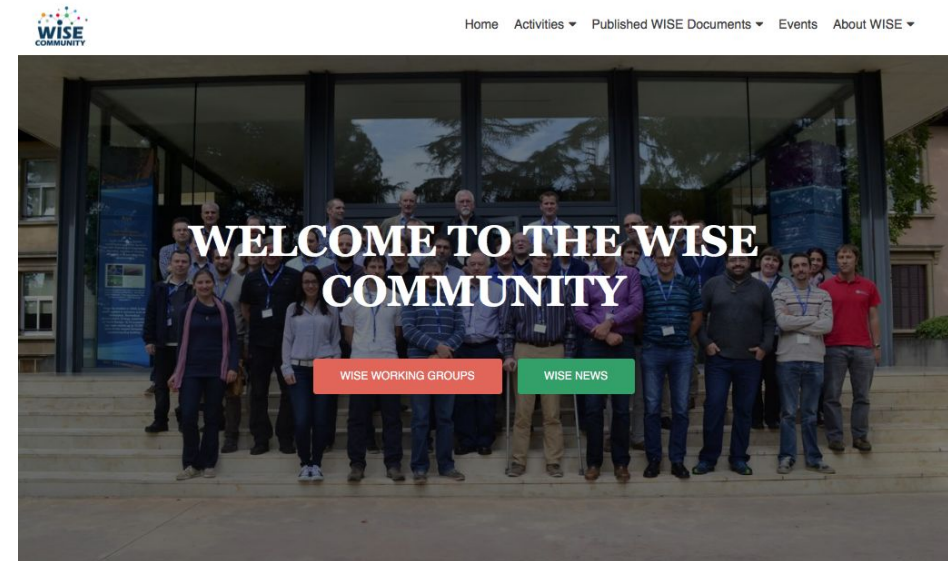
- Procedure for Infrastructure Services:
 - Timely reporting
 - Suspension, investigation
 - Sharing of necessary info
- Procedure for the Infrastructure Security Contact:
 - Assisting the participants
 - Reporting the incident, notifications
 - Suspension, investigation
 - Corrective actions

Security Incident Response Procedure for Infrastructure Participants

1. Contain the security incident to avoid further propagation whilst aiming at carefully preserving evidence and logs. Record all actions taken, along with an accurate timestamp.
2. Report the security incident to the Infrastructure Security Contact point within one local working day of the initial discovery or notification of the security incident.
3. In collaboration with the Security Incident Response Coordinator (identified by the Infrastructure Security Contact), ensure all affected participants in the infrastructure and federation (and, if applicable, in other federations), are notified via their security contact with a “heads-up” and can take action.
4. Announce suspension of service (if applicable) in accordance with infrastructure, federation and interfederation practices.
5. Perform appropriate investigation, system analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. Identifying the cause of security incidents is essential to prevent them from reoccurring. The time and effort needs to be commensurate with the scale of the problem and with the potential damage and risks faced by affected participants....

Continuation

- Phase 1
 - (This is now!)
 - Necessary policies for Snctfi compliance
- Phase 2
 - Continue through the WISE Community
 - An extended set of policy templates for Infrastructures



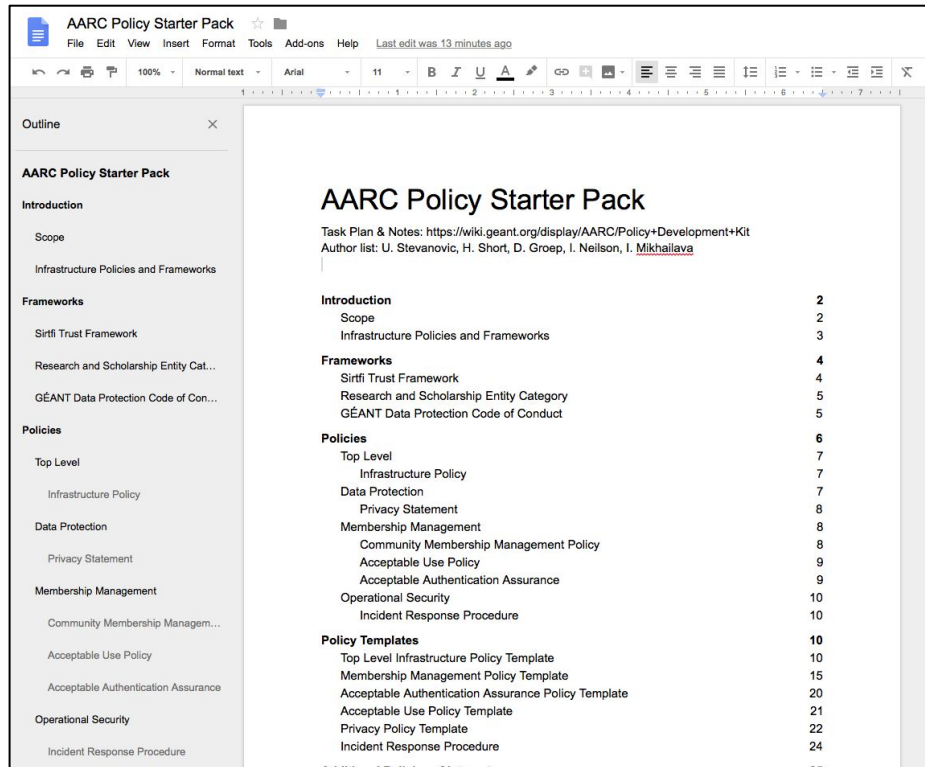
ACTIVITIES

JOIN A WISE WORKING GROUP TO CONTRIBUTE TO OUR GOALS



Dissemination

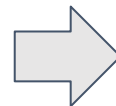
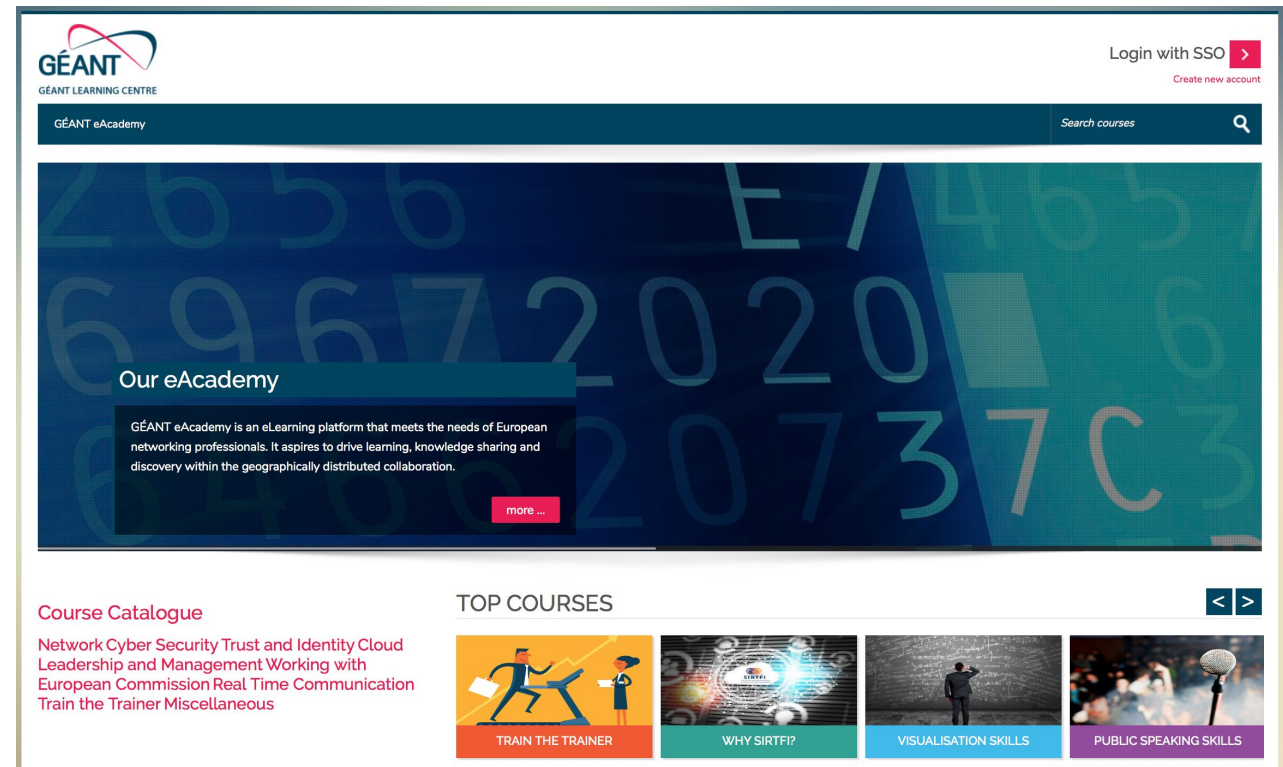
Material currently in Google Doc to be transformed into Moodle Course



AARC Policy Starter Pack

Task Plan & Notes: <https://wiki.geant.org/display/AARC/Policy+Development+Kit>
 Author list: U. Stevanovic, H. Short, D. Groep, I. Neilson, I. Mikhailava

Introduction	
Scope	2
Infrastructure Policies and Frameworks	3
Frameworks	4
Sirtfi Trust Framework	4
Research and Scholarship Entity Category	5
GÉANT Data Protection Code of Conduct	5
Policies	6
Top Level	7
Infrastructure Policy	7
Data Protection	7
Privacy Statement	8
Membership Management	8
Community Membership Management Policy	8
Acceptable Use Policy	9
Acceptable Authentication Assurance	9
Operational Security	10
Incident Response Procedure	10
Policy Templates	10
Top Level Infrastructure Policy Template	10
Membership Management Policy Template	15
Acceptable Authentication Assurance Policy Template	20
Acceptable Use Policy Template	21
Privacy Policy Template	22
Incident Response Procedure	24

GÉANT
GÉANT LEARNING CENTRE

Login with SSO [Create new account](#)

GÉANT eAcademy Search courses

Our eAcademy

GÉANT eAcademy is an eLearning platform that meets the needs of European networking professionals. It aspires to drive learning, knowledge sharing and discovery within the geographically distributed collaboration.

[more ...](#)

Course Catalogue

TOP COURSES

- Train the Trainer
- Why Sirtfi?
- Visualisation Skills
- Public Speaking Skills

Proposed Next Steps

1. AARC
 - a. Put Training Material Online
 - b. Targeted discussion with Research Communities
 - c. Webinars or in-person training as needed
 - d. An open training session at a FIM4R Workshop or DI4R
2. Extension
 - a. Use work to bootstrap wider discussion with IGTF, WISE (and any other interested parties)

Further Reading

Wiki space:

<https://wiki.geant.org/display/AARC/Policy+Development+Kit>

Draft Content:

https://docs.google.com/document/d/176vzNaoK6KvKTMp8Glk2n1NaM6bxiS1QgH8M3_mu7NI/edit?usp=sharing

Thank you
Any Questions?



<https://aarc-project.eu>



© GÉANT on behalf of the AARC project.

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).