Policy Starter Pack

Authentication and Authorisation for Research and Collaboration

Hannah Short (CERN), Uros Stevanovic (KIT)

NA3

With much input from Irina Mikhailava and the rest of NA3

AARC AHM, Athens

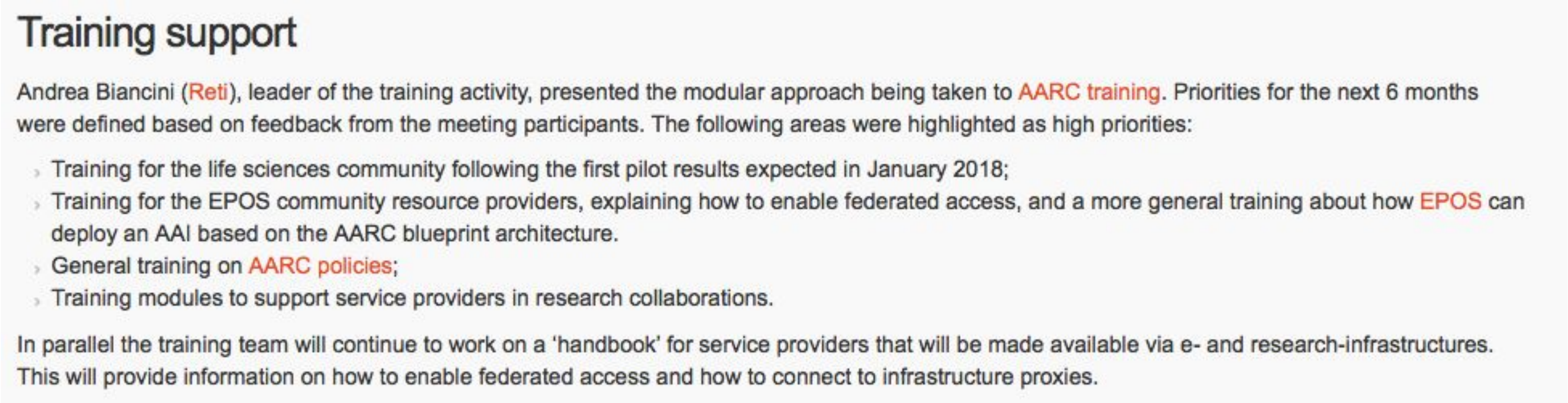
April 13th 2018

Agenda
Brief outline

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

Motivation

- Last AARC AHM highlighted Policy as a priority
- 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:

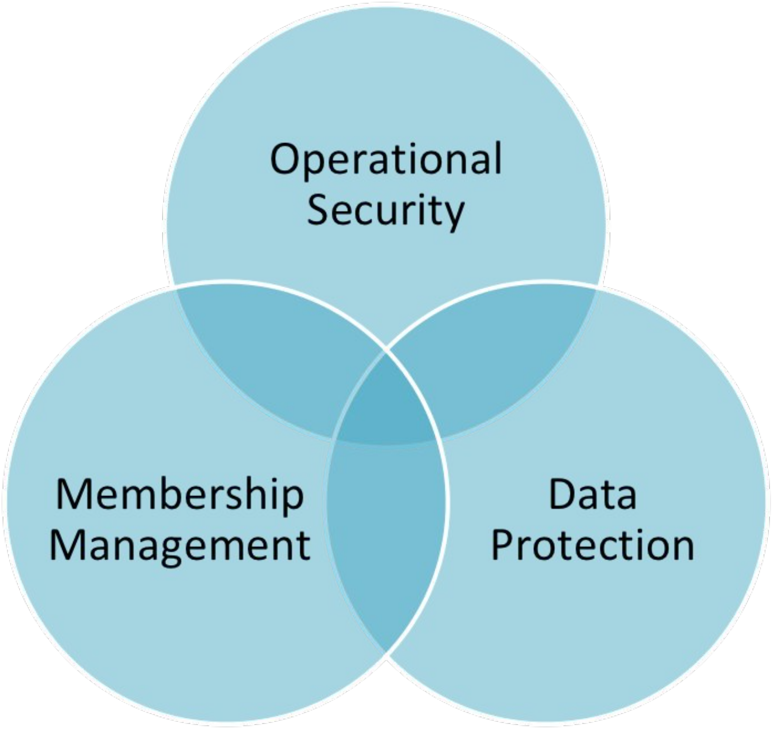
- Training for the life sciences community following the first pilot results expected in January 2018;
- Training for the EPOS community resource providers, explaining how to enable federated access, and a more general training about how EPOS can deploy an AAI based on the AARC blueprint architecture.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

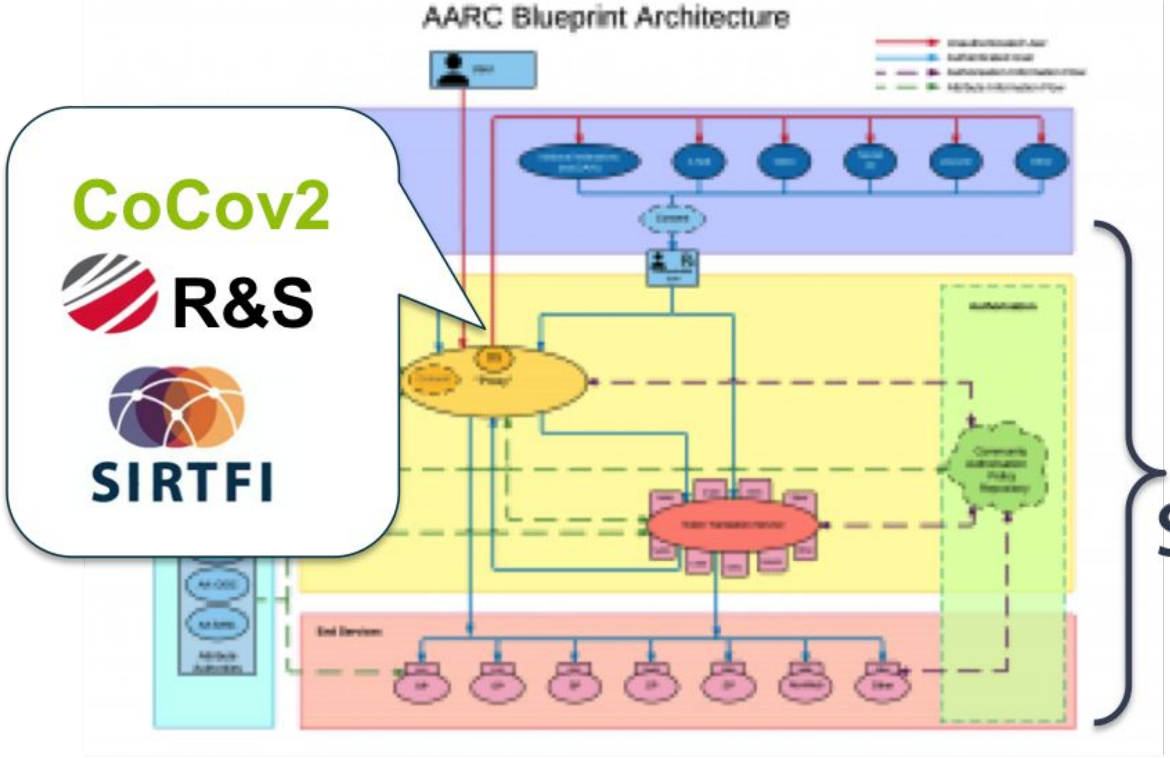
- Which policies? Start from Snctfi and work downwards
  - Top level policy
    - Operational Security
    - Membership Management
    - Data Protection
- Which frameworks?
  - Best practice community frameworks
- Sources of inspiration?
  - EGI
  - CTSC
  - ELIXIR
  - ...



Policy Starter Pack

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



Snctfi

Infrastructure Policy

- Privacy Statement
- AUP
- Acceptable Authentication Assurance
- Membership Management
- Incident Response Procedure
- …

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:

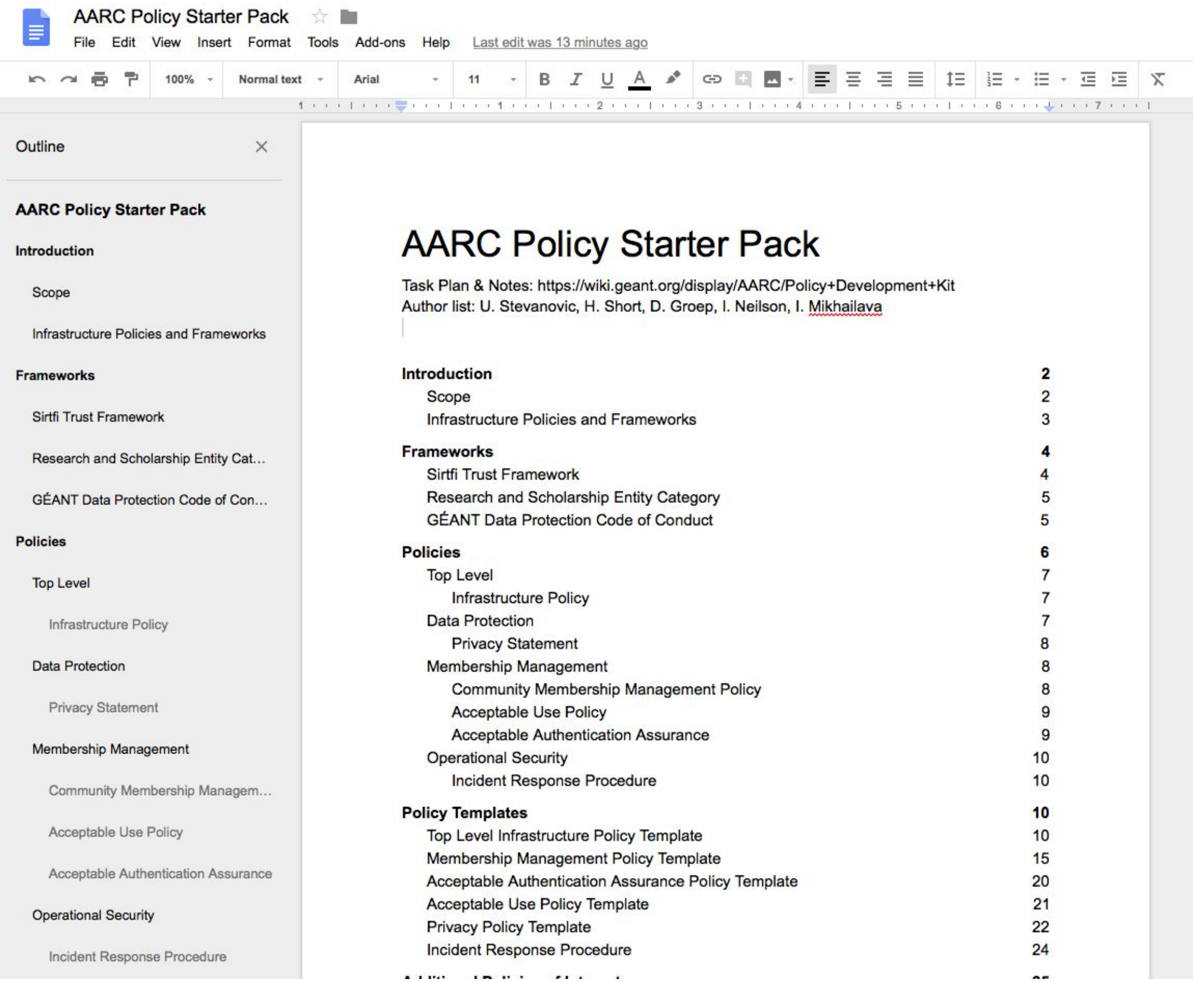
- Modular
- Widely applicable
- Modifiable
- Simple

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
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

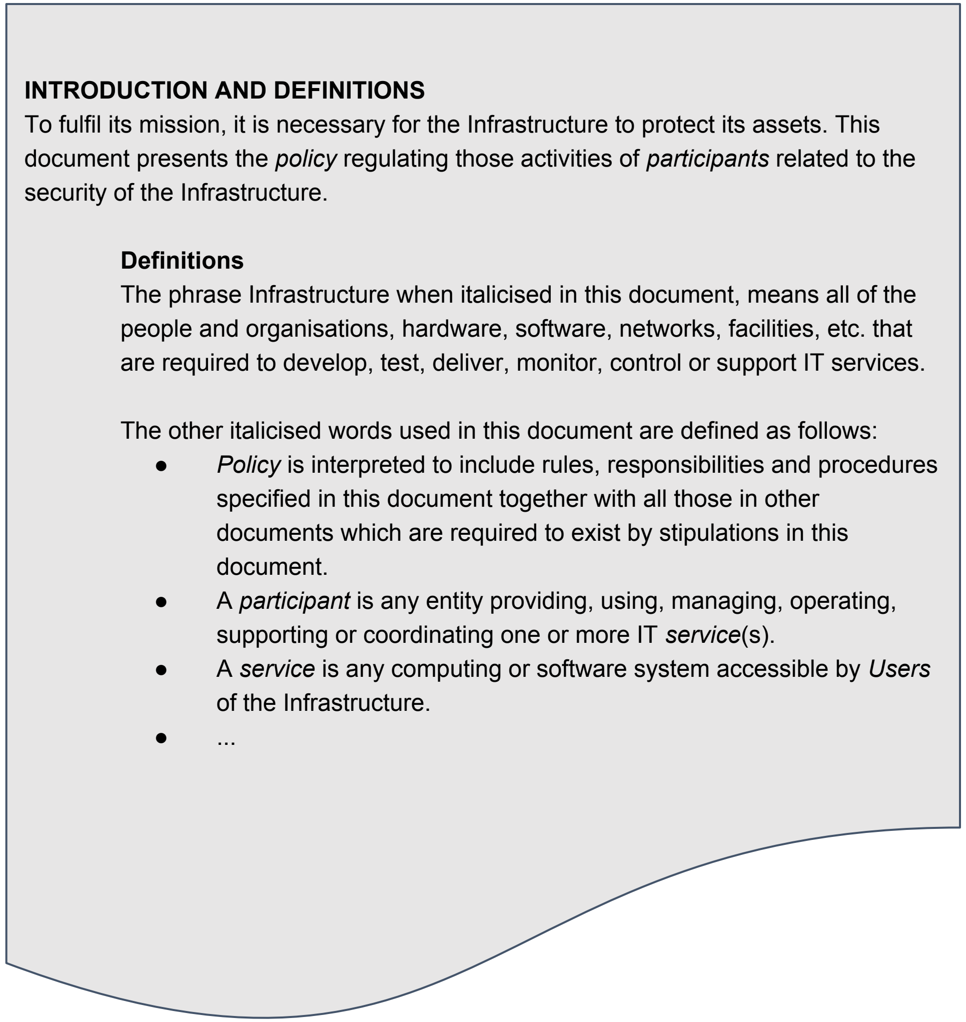
Introduction **2**
Scope 2
Infrastructure Policies and Frameworks 3
Frameworks **4**
Sirtfi Trust Framework 4
Research and Scholarship Entity Category 5
GÉANT Data Protection Code of Conduct 5
Policies **6**
Top Level 7
Infrastructure Policy 7
Data Protection 7
Privacy Statement 8
Membership Management 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

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:

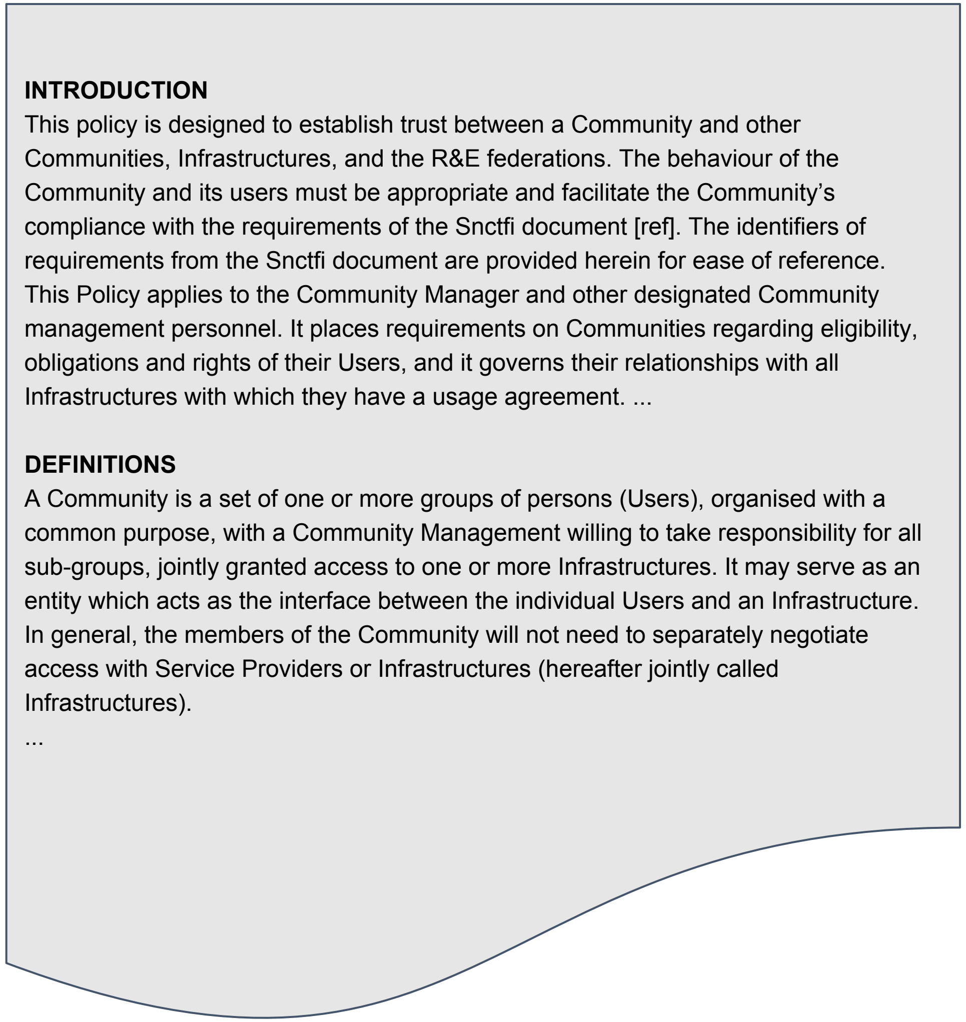
- *Policy* is interpreted to include rules, responsibilities and procedures specified in this document together with all those in other documents which are required to exist by stipulations in this document.
- A *participant* is any entity providing, using, managing, operating, supporting or coordinating 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 Snctfi document [ref]. The identifiers of requirements from the Snctfi 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).

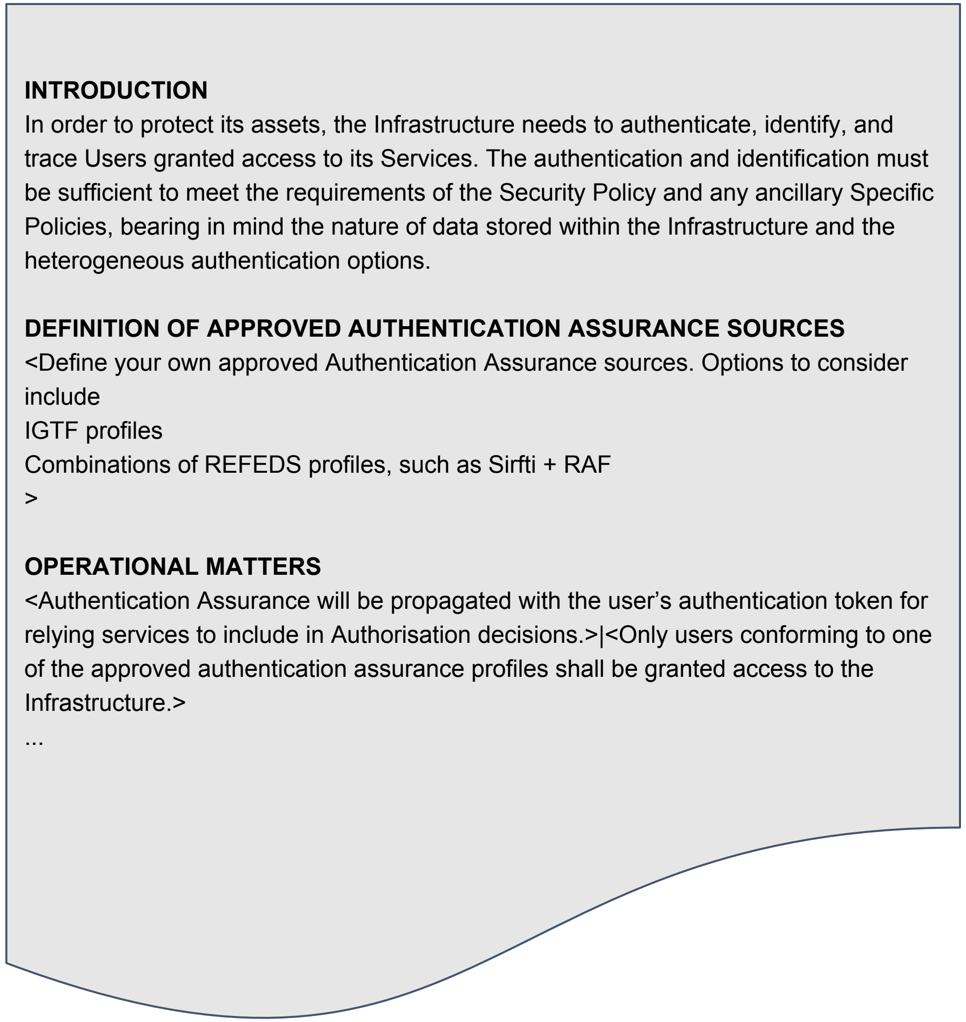
...

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

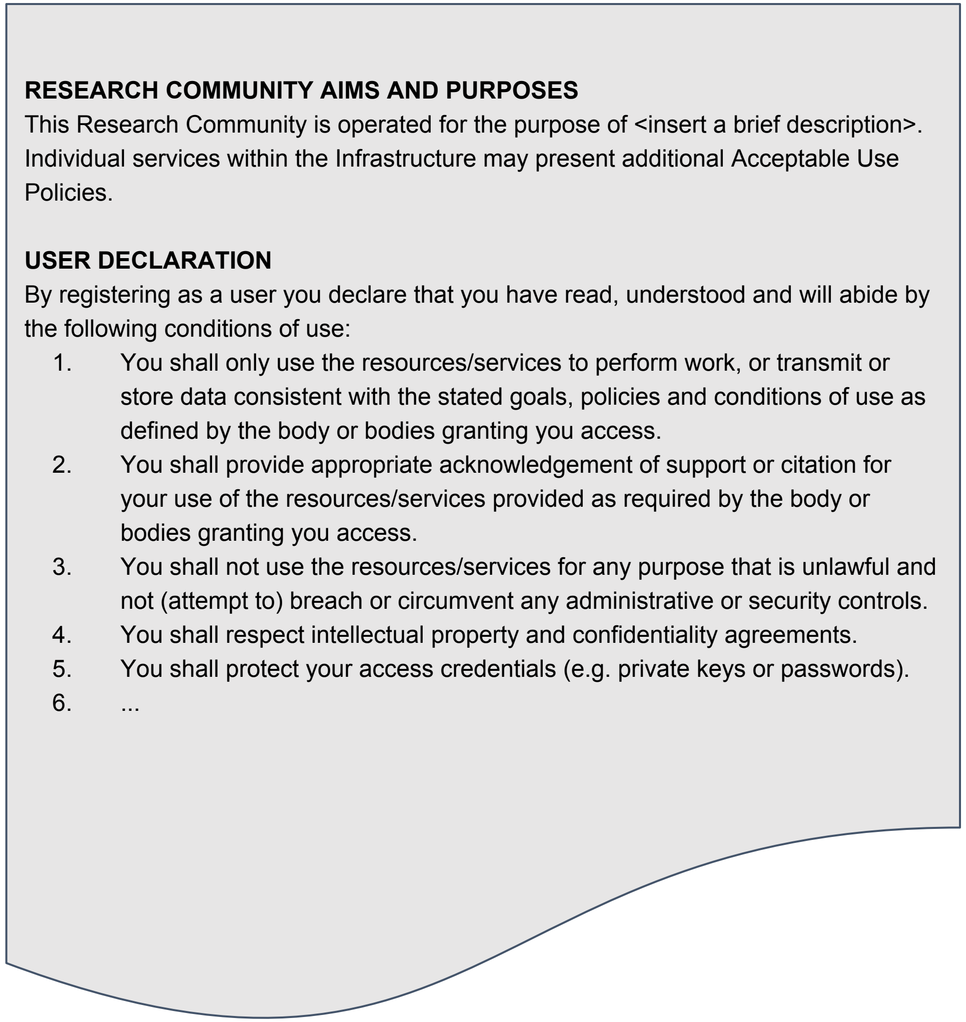
<Authentication Assurance will be propagated with the user's authentication token for relying services to include in Authorisation decisions.>|<Only users conforming to one of the approved authentication assurance profiles shall be granted access to the Infrastructure.>
...

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:

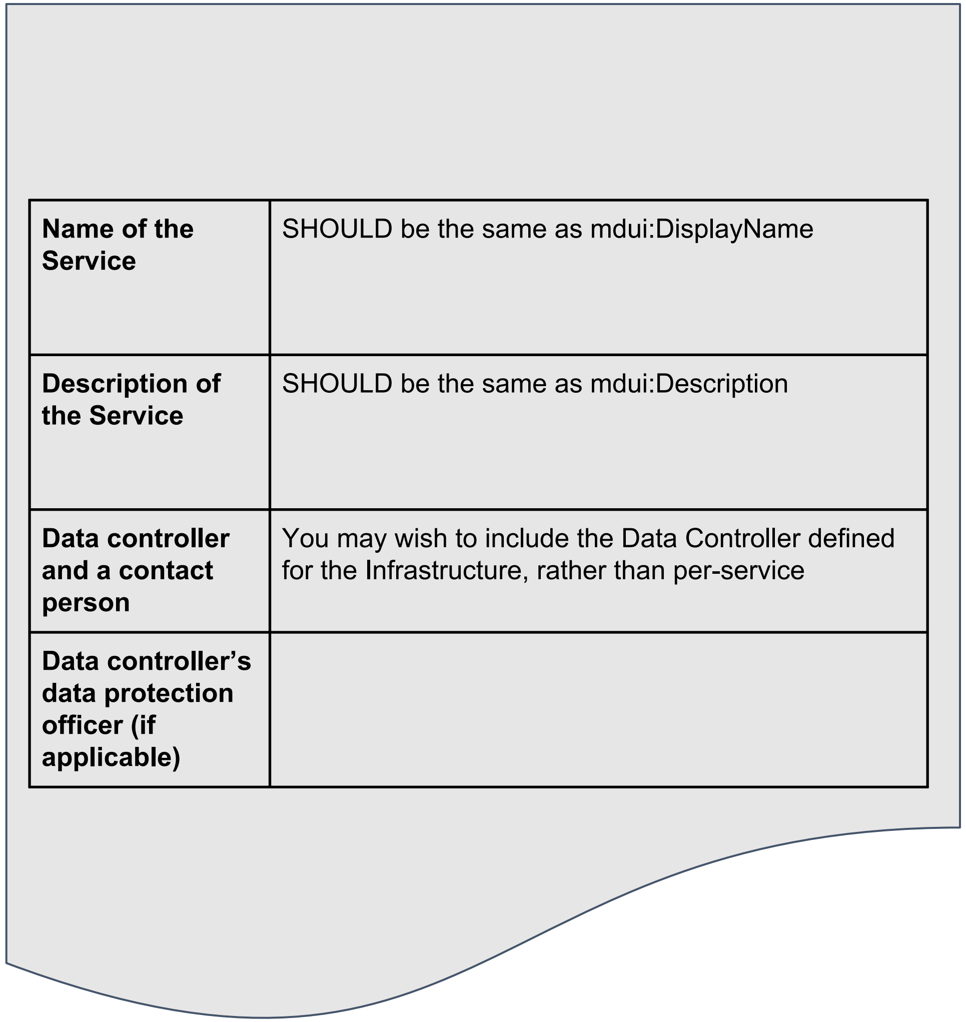
1. You shall only use the resources/services to perform work, or transmit or store data consistent with the stated goals, policies and conditions of use as defined by the body or bodies granting you access.
2. You shall provide appropriate acknowledgement of support or citation for your use of the resources/services 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



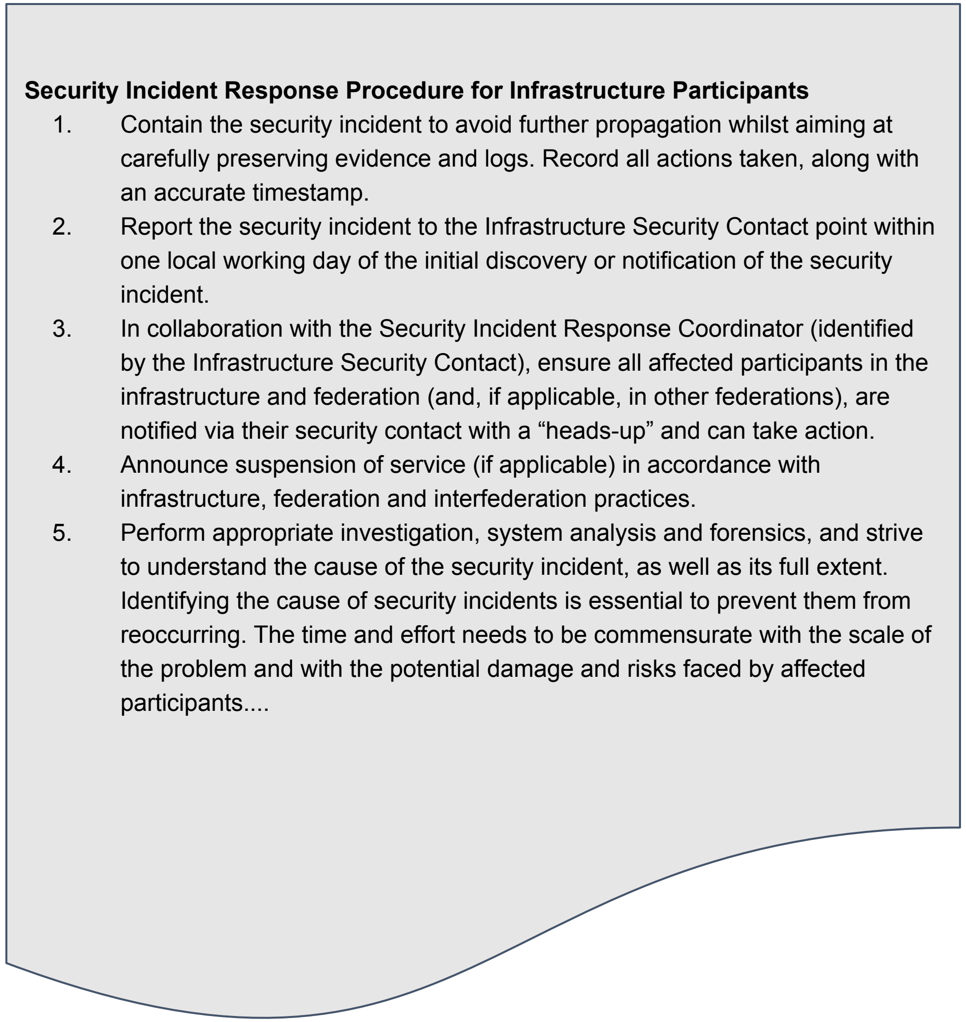
Name of the Service	SHOULD be the same as mdui:DisplayName
Description of the Service	SHOULD be the same as mdui:Description
Data controller and a contact person	You may wish to include the Data Controller defined for the Infrastructure, rather than per-service
Data controller’s data protection officer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

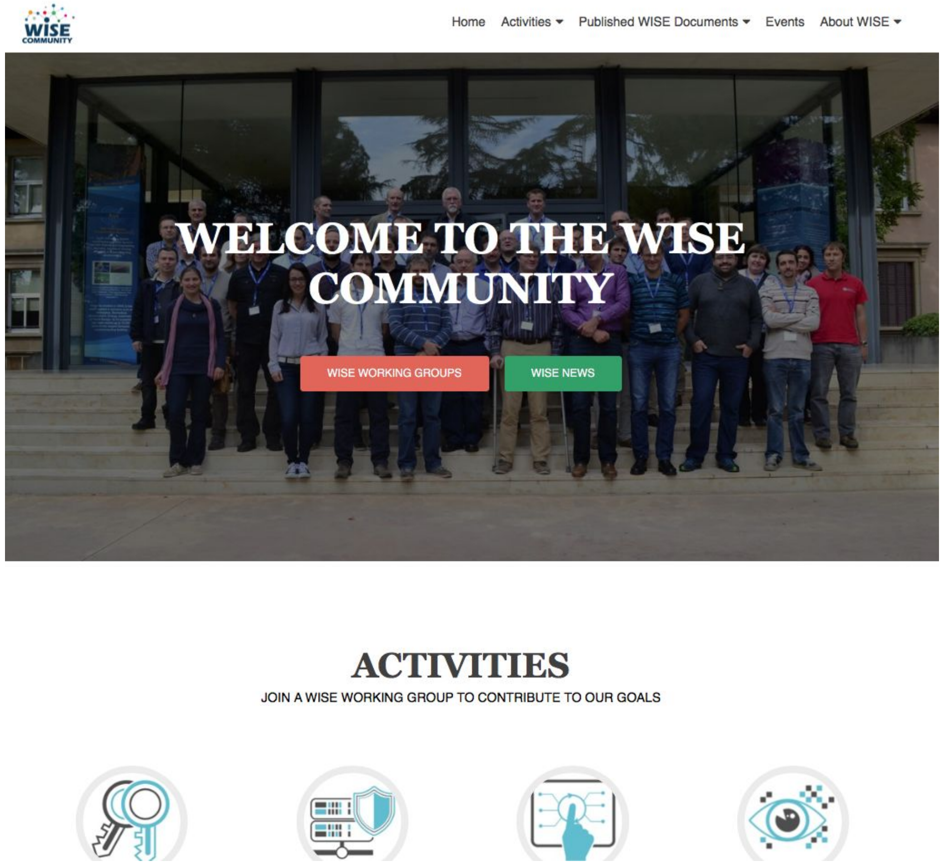


Security Incident Response Procedure for Infrastructure Participants

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

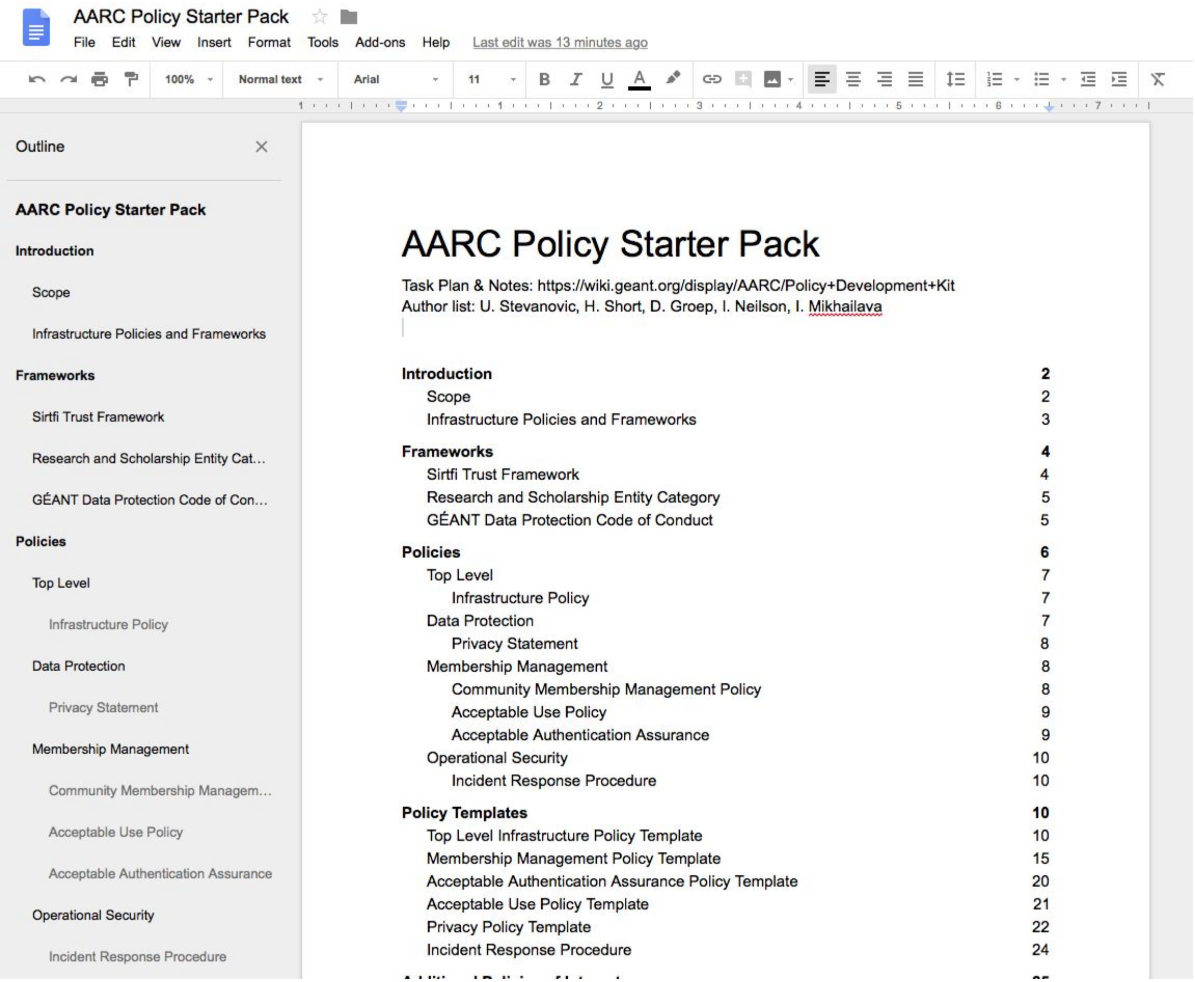
- Phase 1
  - (This is now!)
  - Necessary policies for Snctfi compliance
- Phase 2
  - Continue through the WISE Community
  - An extended set of policy templates for Infrastructures



Training - Online

Material currently in Google Doc to be transformed into

- Website content
- Slides
- Moodle Course (?)
- Video
- …



AARC Policy Starter Pack

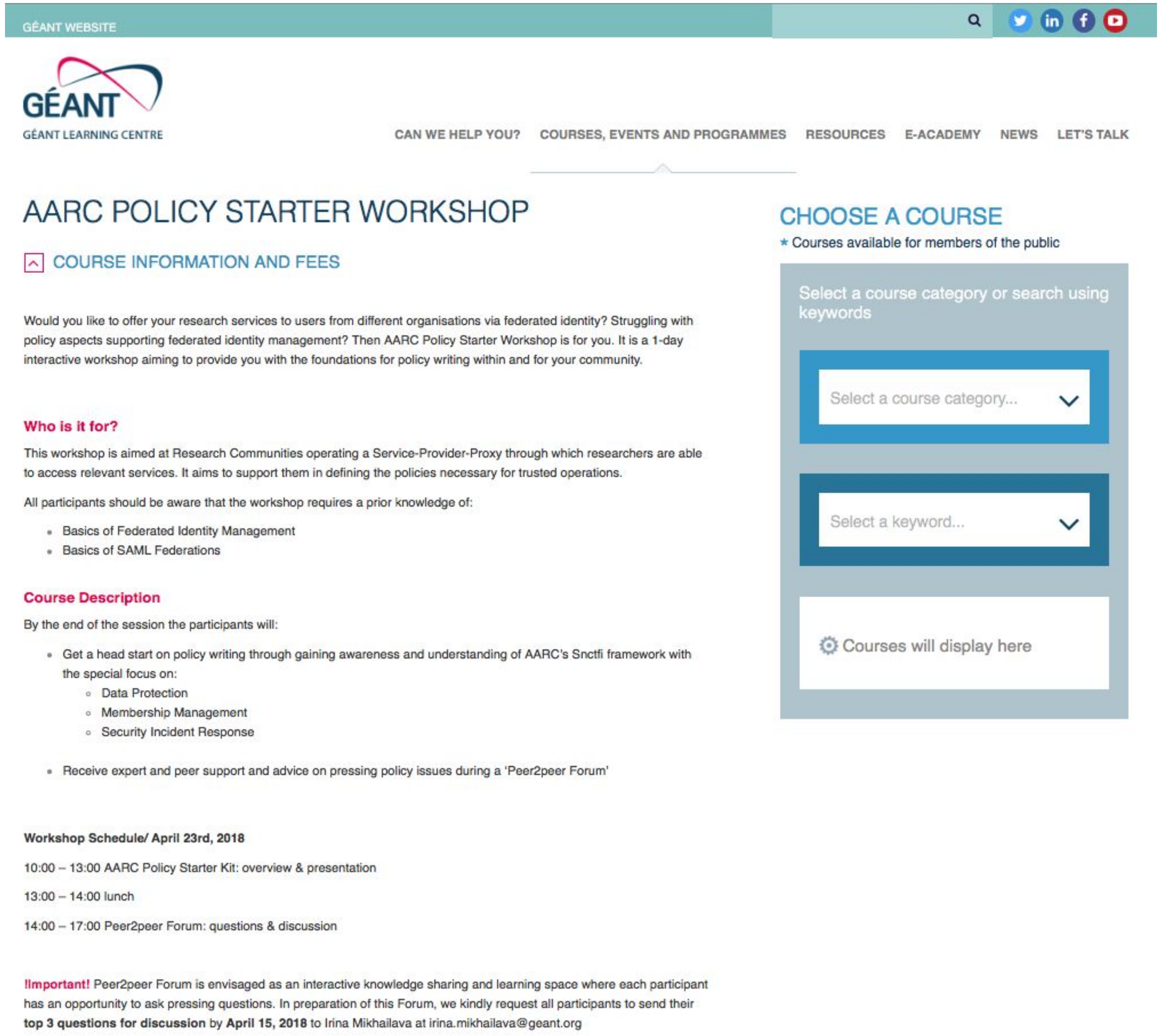
Task Plan & Notes: https://wiki.geant.org/display/AARC/Policy+Development+Kit
Author list: U. Stevanovic, H. Short, D. Groep, I. Neilson, I. Mikhailava

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

Training - Face to Face

- April 23rd
- GÉANT Office, Amsterdam
- Audience
  - Proxy providers
  - Single or multiple Research Communities
- Full day
  - Introduction to policy documents
  - Peer2peer Forum

CANCELLED


GÉANT WEBSITE
GÉANT
GÉANT LEARNING CENTRE
CAN WE HELP YOU?
COURSES, EVENTS AND PROGRAMMES
RESOURCES
E-ACADEMY
NEWS
LET'S TALK
CHOOSE A COURSE
* Courses available for members of the public
Select a course category or search using keywords
Select a course category...
Select a keyword...
Courses will display here

AARC POLICY STARTER WORKSHOP

COURSE INFORMATION AND FEES

Would you like to offer your research services to users from different organisations via federated identity? Struggling with policy aspects supporting federated identity management? Then AARC Policy Starter Workshop is for you. It is a 1-day interactive workshop aiming to provide you with the foundations for policy writing within and for your community.

Who is it for?

This workshop is aimed at Research Communities operating a Service-Provider-Proxy through which researchers are able to access relevant services. It aims to support them in defining the policies necessary for trusted operations.

All participants should be aware that the workshop requires a prior knowledge of:

- Basics of Federated Identity Management
- Basics of SAML Federations

Course Description

By the end of the session the participants will:

- Get a head start on policy writing through gaining awareness and understanding of AARC's Snctfi framework with the special focus on:
  - Data Protection
  - Membership Management
  - Security Incident Response
- Receive expert and peer support and advice on pressing policy issues during a 'Peer2peer Forum'

Workshop Schedule/ April 23rd, 2018

10:00 – 13:00 AARC Policy Starter Kit: overview & presentation

13:00 – 14:00 lunch

14:00 – 17:00 Peer2peer Forum: questions & discussion

!Important! Peer2peer Forum is envisaged as an interactive knowledge sharing and learning space where each participant has an opportunity to ask pressing questions. In preparation of this Forum, we kindly request all participants to send their **top 3 questions for discussion** by **April 15, 2018** to Irina Mikhailava at irina.mikhailava@geant.org

What went wrong?

We only had 3 people register…

- Is this an advertising issue?
- Is it because policy sounds “a bit dry”?
- Is it a bad time?
- Have we misunderstood the need for policy training?

Proposed Next Steps

1. Put Training Material Online
2. Targeted discussion with Research Communities
3. Webinars or in-person training as needed
4. An open training session at a FIM4R Workshop or DI4R

Further Reading

Wiki space:

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

Draft Content:
https://docs.google.com/document/d/176vzNaoK6KvKTMp8Glk2n1NaM6bxiS1QqH8M3_mu7NI/edit?usp=sharing

Thank you

Any Questions?

AARC

https://aarc-project.eu

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).