AARC Policy Starter Pack

Objective: Provide new or evolving Research Communities and Infrastructures with the guidance they need to develop a complete policy suite supporting Federated Identity Management

Audience: Operational Management of Research Communities and their respective infrastructures

Relevant questions:

- *We're worried that we will have legal issues receiving federated identities, which policies do we need?*
- *What is a reasonable expectation of assurance of incoming identities?*
- *How can I ensure that all my users are covered by an incident response capability?*
- *What checks and measures should I put in place when managing the users of my community services, or members of virtual organisations?*

Introductory Content:

- Make clear why these policies should be adopted, where they have come from and examples of how they help
-

Policy Areas:

(Would be good to have actionable points as well as dry document examples)
(Can we encourage people to be in the right mindset to make their own decisions about timelines for policy decisions etc)

Snctfi (top level) -- for scalable, bounded communities https://aarc-project.eu/policies/snctfi/

Data Protection

- CoCo (&v2)
- AARC deliverable template
- Risk Assessment (due to the GDPR) -> WISE https://wise-community.org/risk-assessment-template/

Membership management

- Can cover Users, Communities and contributing services
- Attribute request/release
- AUP - Acceptable Use Policy

Security Incident Response

- Sirtfi (Able to assert for RC? Require it for incoming federated users? Is step up required?)
- AARC deliverable template
- Security policies e.g. EGI

LoA (What is the acceptable level? Is step up required?)

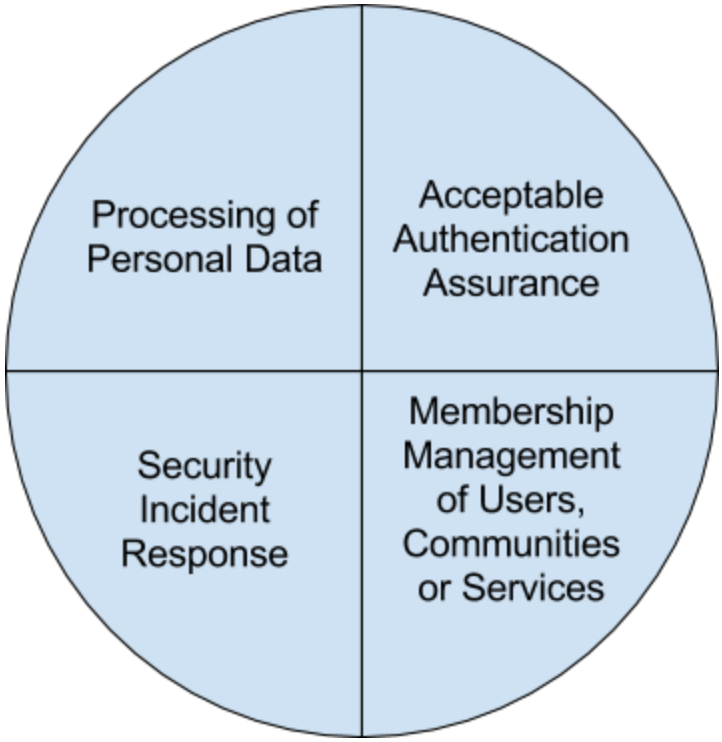
- REFEDS LoA
- AARC minimum LoA https://aarc-project.eu/wp-content/uploads/2015/11/MNA31-Minimum-LoA-level.pdf
- MFA

Sources of input:

- EGI security and community policies
- AARC templates
- CoCo work

Crazy ideas for how this could work...

- Moodle course walking people through decisions for each policy aspect
- Website static pages (bit dull)
- Recorded video snippets for each aspect (Uros and Hannah can do a double act of questions and answers!)
- “Click in” style website
- Road show
- Face-to-face session where we split the room into sections and ask for questions on specific policies
- Recorded interviews with experts on specific topics, e.g. GDPR, Security Incident Response



Key Ideas for each topic:

- What is this policy for?
- Sub policies
- Does my RC/Infrastructure need it?
- What do I need to do?
- Who needs to agree to the policy and where should it live?
- Template

Could group as:

- General Policies
- Audience Specific

See e.g.
https://edms.cern.ch/ui/#!master/navigator/project?P:1412060393:1412060393:subDocs
And https://wiki.egi.eu/wiki/SPG:Documents

Task Plan:

Task	*Who?*
Introduction	Hannah
Introduction to Snctfi	Uros

Data Protection - **Example policy** - **CoCo**	Uros
Membership Management & LoA - **EGI policy** - **AUP**	Both
Operational Security	Hannah
Example Template Set	Both

Actions:

- Uros share plan with David and Dave

Contents

Introduction

This material provides new or evolving Research Communities and Infrastructures with the guidance they need to develop a complete policy suite supporting Federated Identity Management. As Research Communities seek to increase their interaction with external identities, such as those from identity federations or social providers, certain provisions should be made for Data Protection, Membership Management and Security Incident Response. The policies presented here aim to take trust, assurance and governance aspects into account whilst providing a coherent set of documents to be adopted by interested parties.

Policies are essential for setting expectations for participants in a Research Community, stretching from the Infrastructure management to the researchers themselves. Conversely, a violation of policy may be classified as an incident and may warrant and give grounds for investigation to protect the Community. Policy decisions may or may not be enforced on a technical level; the Research Community themselves will be best placed to define the permitted usage of their resources through a combination of technology and documentation.

When incorporating external identities into their ecosystem, Research Communities are faced with new questions, including but not limited to:

- We're worried that we will have legal issues receiving federated identities, which policies do we need?
- What is a reasonable expectation of the level of assurance of incoming identities?
- How can I ensure that all my users are covered by an incident response capability?
- What checks and measures should I put in place when managing the users of my community services, or members of virtual organisations?