Science and Technology Facilities Council

Building an IRIS trust framework

David Crooks
David Kelsey
Ian Neilson
Ian Collier

WISE COMMUNITY

Overview

- Introduction to IRIS
- Requirements & process
- Current status
- Next steps
- Observations

Science and Technology Facilities Council

WISE COMMUNITY

IRIS Background

- e**I**nfrastructure for **R**esearch and **I**nnovation for **S**TFC
- Loose collaboration of **Science Activities** and **Provider Entities**
  - Primarily driven by the physics communities supported by STFC
- Does not run infrastructure **directly**
  - Not a project in that sense
  - Commissions deployment of resources available to all of its science activities
- IRIS 4x4 is a capital project coordinated by IRIS
  - £4 million per year for 4 years
  - No money for operations
  - Can issue grants for equipment and grants to make things
    - Such as the trust framework

UKRI Science and Technology Facilities Council

WISE COMMUNITY

IRIS Background

Science Activities

- ALMA
- ATLAS
- CCFE
- CLF
- CMS
- CTA
- DLS
- DUNE
- eMERLIN
- EUCLID
- GAIA
- ISIS
- LHCb
- LIGO
- LSST
- Lux-Zeplin
- SKA

Provider Entities

- The Ada Lovelace Centre (ALC)
- DiRAC [HPC]
- GridPP [HTC]
- The Hartree Centre
- STFC Scientific Computing Department
- The DLS Computing Department
- CCFE computing

UKRI Science and Technology Facilities Council

WISE COMMUNITY

The IRIS environment

- Mixture of HTC/HPC resources
  - HTC (GridPP) mixture of X509 and FIM (in the future)
  - HPC largely SSH key based Authn
  - Varying levels of existing use of federated identity management
- Very varied user base
  - HEP + Astro + Photonics…
  - Part of large experiments and quasi-independent researchers

IRIS Background

- If we want these communities to work together, need some common elements
  - Policy and Trust Framework
  - Identity Management
  - Resource Accounting
  - Monitoring

Requirements for trust framework

- IRIS contains a range of resource providers with existing policy frameworks
  - Need to develop a framework that sits alongside these and satisfies the wider need
- Some providers are already connected within the wider federated world
  - Particularly GridPP/WLCG
- However: it does represent a new community in its own right
  - And exists within a distributed, federated infrastructure landscape
- Requirement to establish the necessary policies to allow interoperation between resource providers, services and user groups
  - And relationships to existing policy

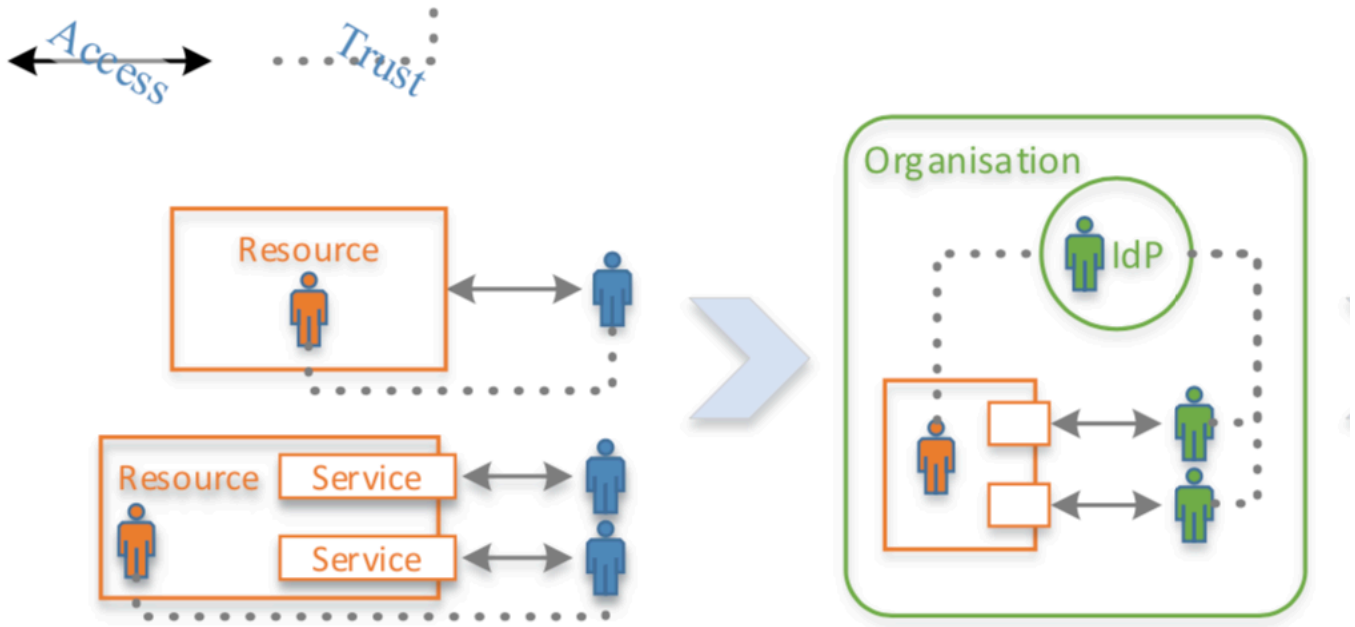
IRIS Trust Framework

- The IRIS Trust Framework is intended to build the security policy required by IRIS
  - Start with foundational and user-facing policies
  - Roadmap for the future
- Security Incident Response
  - Clear roles and basic policy framework

Process

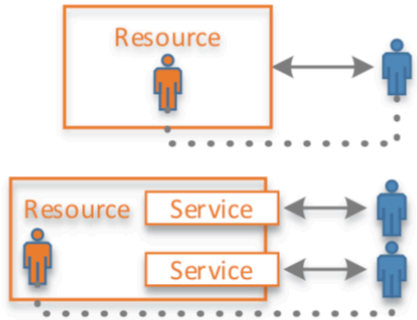
- Build on extensive existing experience developing policy within existing communities
  - GridPP/WLCG, UK Access Management Federation, EGI, …
  - Extend to new resource providers and user communities
- Identify key stakeholders and develop trust relationships
- Coordinated work is ongoing to deploy an IAM identity proxy for IRIS
  - See talk at mini-FIM4R at Fermilab
  - Use this as driver
  - See also talk by Andrea Ceccanti at CHEP 2018 on Token-based Authentication and Authorization for HEP

Trust relationship scenarios

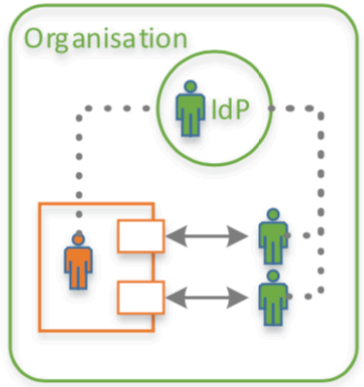


Access provisioned by resource manager. Explicit trust between the manager and the users.

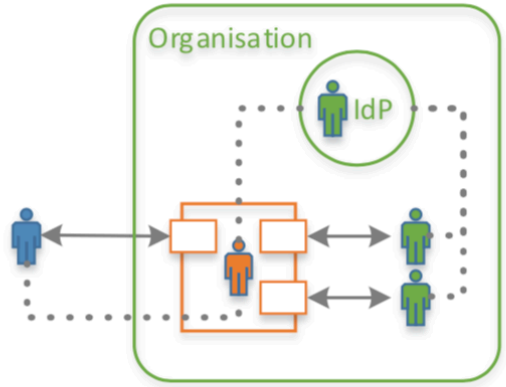
Authentication delegated to Organisation's Identity Provider. Explicit trust between the manager and the IdP.



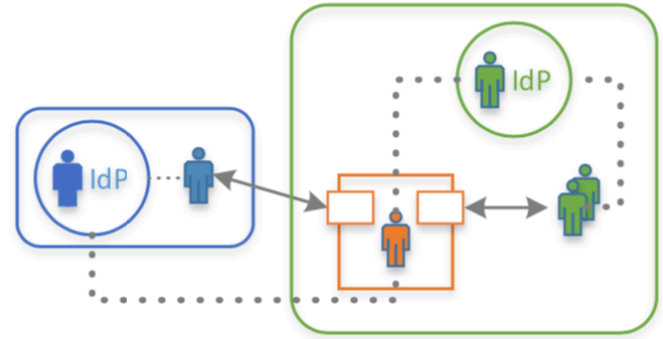
Access provisioned by resource manager. Explicit trust between the manager and the users.



Authentication delegated to Organisation's Identity Provider. Explicit trust between the manager and the IdP.

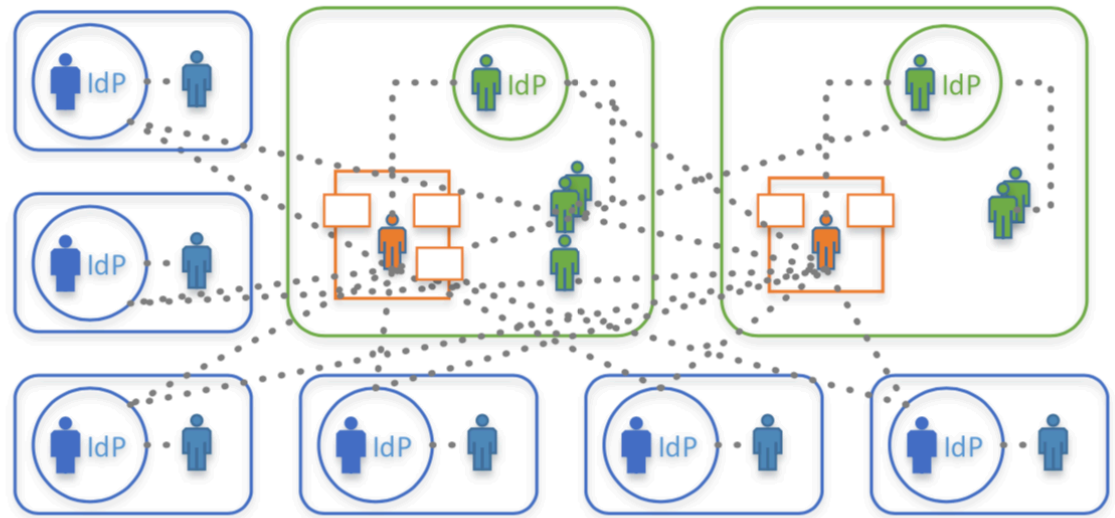


Hybrid trust model

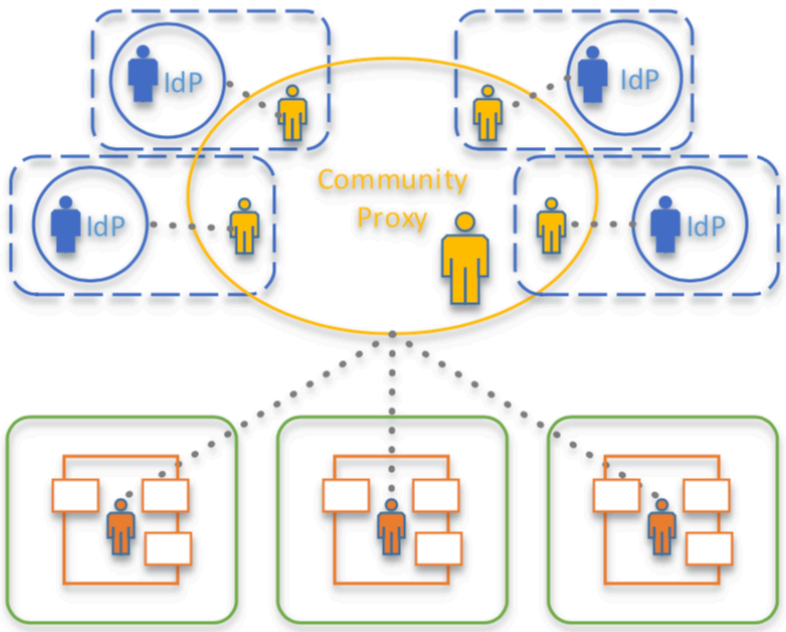


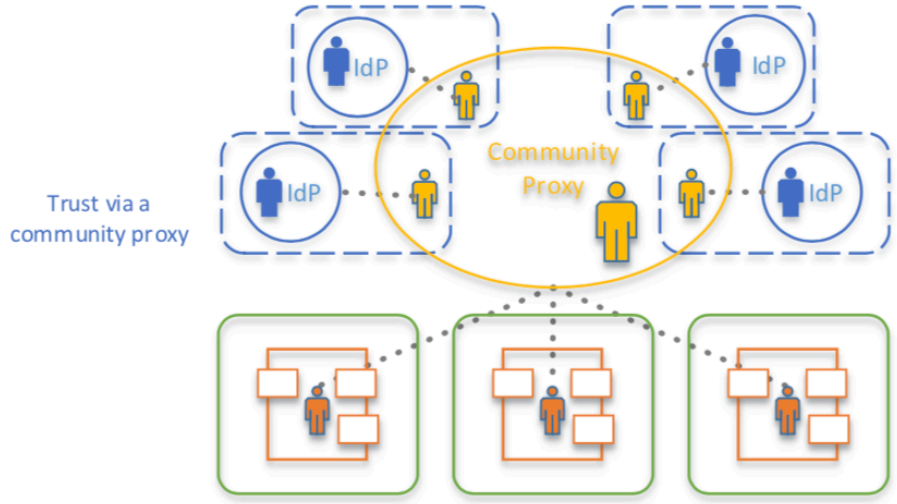
Explicit trust of 'external' IdP

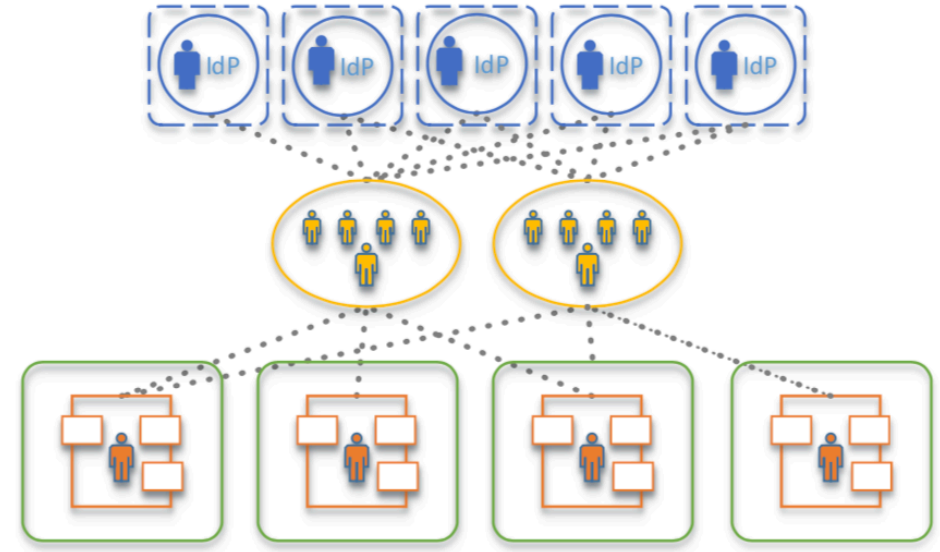
Trust scaling problems.
(User interaction with resource omitted)

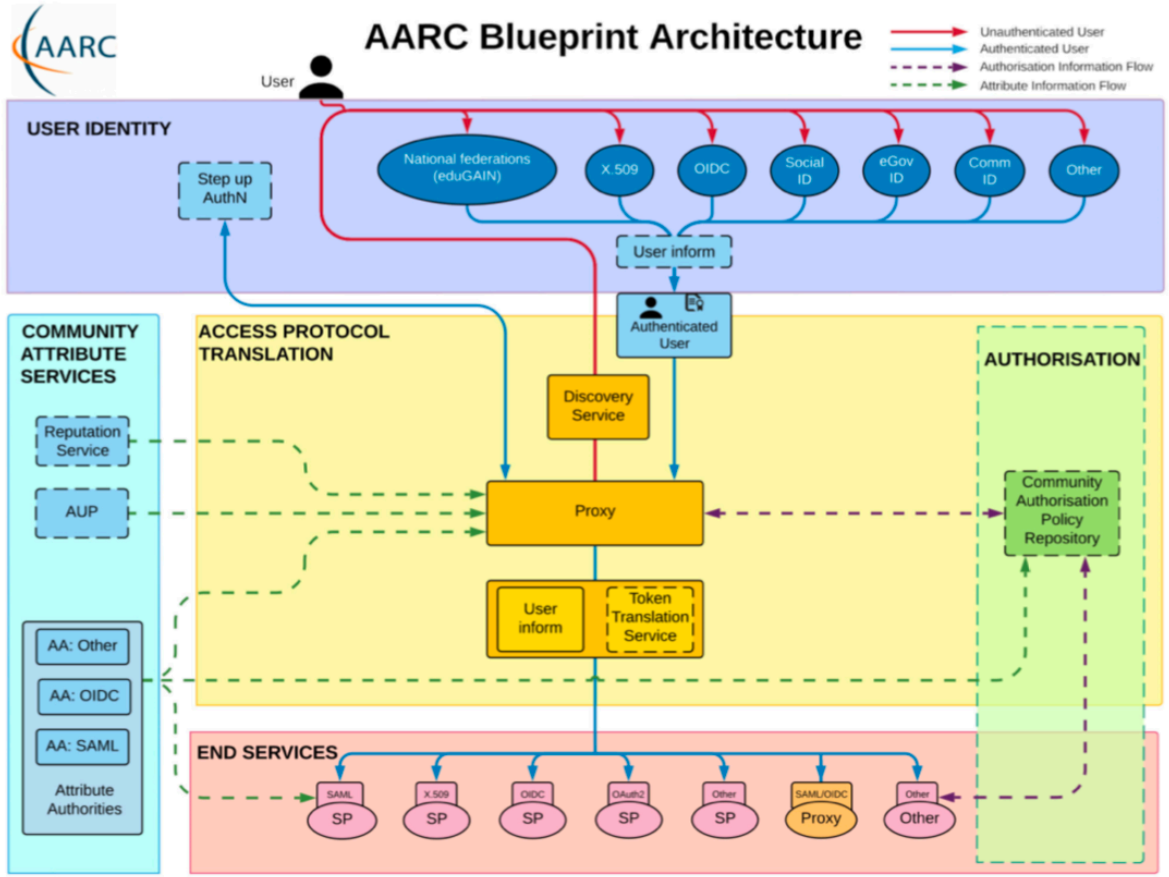


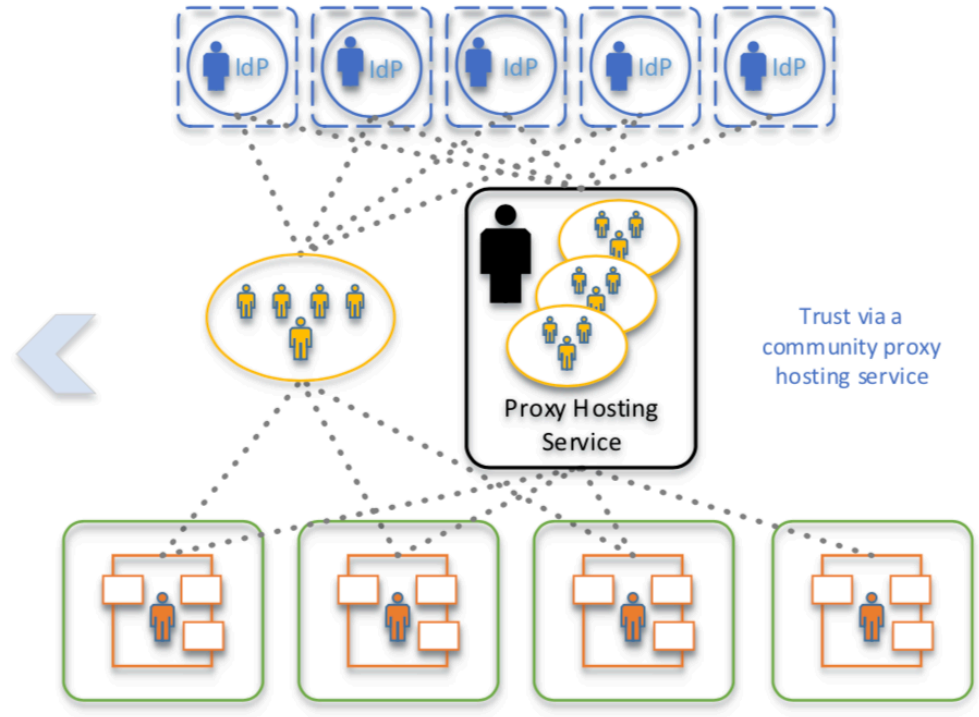
Trust via a community proxy




Trust via a community proxy
IdP
IdP
IdP
IdP
Community Proxy


IdP
IdP
IdP
IdP
IdP


AARC
AARC Blueprint Architecture
Unauthenticated User
Authenticated User
Authorisation Information Flow
Attribute Information Flow
User
USER IDENTITY
Step up AuthN
National federations (eduGAIN)
X.509
OIDC
Social ID
eGov ID
Comm ID
Other
User inform
Authenticated User
COMMUNITY ATTRIBUTE SERVICES
ACCESS PROTOCOL TRANSLATION
AUTHORISATION
Reputation Service
AUP
Discovery Service
Proxy
Community Authorisation Policy Repository
User inform
Token Translation Service
AA: Other
AA: OIDC
AA: SAML
Attribute Authorities
END SERVICES
SAML SP
X.509 SP
OIDC SP
OAuth2 SP
Other SP
SAML/OIDC Proxy
Other Other


IdP
IdP
IdP
IdP
IdP
Proxy Hosting Service
Trust via a community proxy hosting service

Roadmap

- AARC Policy Development Kit
  - Authentication and Authorisation for Research Collaboration
  - Recently completed EU projects
- 9 documents aimed at best practice bootstrap for infrastructures & communities deploying the AARC Blueprint Architecture
  - Federated IDPs with services/resources ‘behind’ an AAI Proxy
- Policies intended to co-exist with local policies where applicable

WISE

- Wise Information Security for Collaborating e-Infrastructures
  - https://wise-community.org/about-wise/
- Global collaborative community of security experts
- IRIS work takes place under aegis of WISE
  - Benefit to IRIS of considerable experience
  - Benefit to WISE and wider community of new requirements and context

AARC Policy Development Kit

Document	Who should complete the template?	Audience	Description
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
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.
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.
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.
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.
Policy on the Processing of Personal Data	Infrastructure Management & Data Protection Contact	Research Community, Services (abide by)	This document defines the obligations on Infrastructure Participants when processing personal data.
Privacy Policy	Infrastructure Management (for general policy) & Services (for service specific policies)	Users (view)	This can be used to document the data collected and processed by the Infrastructure and its participants. Each service in the infrastructure, as well as the infrastructure itself, should complete the template.
Service Operations Security Policy	Infrastructure Management	Services (abide by)	This policy defines requirements for running a service within the Infrastructure.
Acceptable Use Policy	Infrastructure Management (for baseline) & Research Communities (for community specific restrictions)	Users (abide by)	This is a template for the acceptable use policy that users must accept to use the Research Infrastructure. It should be augmented by the Research Community.

AARC Policy Development Kit

Document	Who should complete the template?	Audience	Description
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**
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.
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.
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.
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.
Policy on the Processing of Personal Data	Infrastructure Management & Data Protection Contact	Research Community, Services (abide by)	This document defines the obligations on Infrastructure Participants when processing personal data.
Privacy Policy	**Infrastructure Management (for general policy) & Services (for service specific policies)**	**Users (view)**	**This can be used to document the data collected and processed by the Infrastructure and its participants. Each service in the infrastructure, as well as the infrastructure itself, should complete the template.**
Service Operations Security Policy	Infrastructure Management	Services (abide by)	This policy defines requirements for running a service within the Infrastructure.
Acceptable Use Policy	**Infrastructure Management (for baseline) & Research Communities (for community specific restrictions)**	**Users (abide by)**	**This is a template for the acceptable use policy that users must accept to use the Research Infrastructure. It should be augmented by the Research Community.**

Draft UK IRIS AUP

- Use of a common, baseline AUP
  - Based on the WISE Baseline AUP template
    - Promotes trust in users' behaviour across infrastructures
    - Reduce need to agree to multiple different AUPs
  - Allows for consistent presentation of necessary Privacy Notices
  - Allows for augmentation with additional local / community requirements
    - 10 immutable clauses + scope to add specific additional ones
  - Easier bootstrapping – don't reinvent the wheel

Draft UK IRIS Privacy Notice

- Presented to user at time of registration alongside AUP
- Assumes GDPR legal basis of “legitimate interest” for processing
  - i.e. not consent – due to imbalance of power (employer – employee)
- To be taken from (final) deployment context
  - Personal data gathered / processed
  - Data retention period
  - Use of ‘common policy framework’ for processing

Draft UK IRIS Infrastructure Security Policy

- Provides high-level framework for other subordinate policies
  - Approved/adopted by infrastructure management body to give
  - **"…authority for actions which may be carried out by designated individuals and organisations and places responsibilities on all participants."**
  - Roles and Responsibilities of Management
  - Roles and Responsibilities of Security Contact
  - Physical and Network Security
    - Delegated to local/service policies, but scoped.
  - Exceptions to Compliance and Sanctions

Incident response

- GridPP has distributed incident response capability through EGI CSIRT, supported by NGI UK Security Team
- Initial proposal for IRIS is to expand NGI UK Security Team to include new IRIS resource providers
  - Focus in the beginning on sharing experience and building trust
  - Understand the boundaries between incident response for **IRIS**, **existing infrastructures**, and **local institutions**
- Specify security contacts for resource providers

Observations

- Using a technology deployment (such as IRIS-IAM) can be helpful in developing a policy timeline
  - And crystalising use cases
- Requirements setting is a critical component in developing policy
- Developing policy is an excellent way for a community to introspect itself
  - What are the relationships between entities and use cases?
  - What defines a ‘User’? ...
- This provides both a challenge and an opportunity
- There is a benefit to working on policies in the light of groups such as WISE
  - Enhances interoperability from the outset

The IRIS trust challenge

- Generate the minimum policy set to enable this environment
- Identify critical workflows and responsible parties to support take-up of these policies in the community
- Service operators as well as community managers and users are key stakeholders
- At all levels, emphasise that IRIS policy sits alongside local policy
  - Need to communicate that concept to stakeholders
  - Key point: this is the model that scales!

Next steps

- In progress
  - Gather feedback on drafts
  - Membership Management Policy/Acceptable Assurance
- Ongoing discussion framing policies in the context of IRIS structure
- Use scenarios & use cases to explore mapping policies to stakeholder responsibilities

UKRI Science and Technology Facilities Council

Questions?

UKRI Science and Technology Facilities Council

Thank you

Science and Technology Facilities Council @STFC_Matters Science and Technology Facilities Council