Science and Technology Facilities Council

Scientific Computing

iris

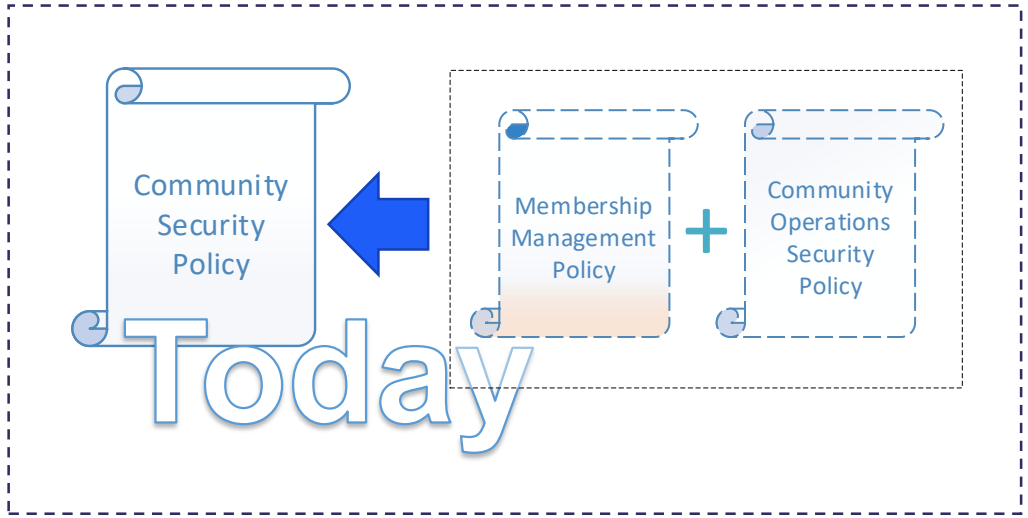
IRIS Community Security Policy

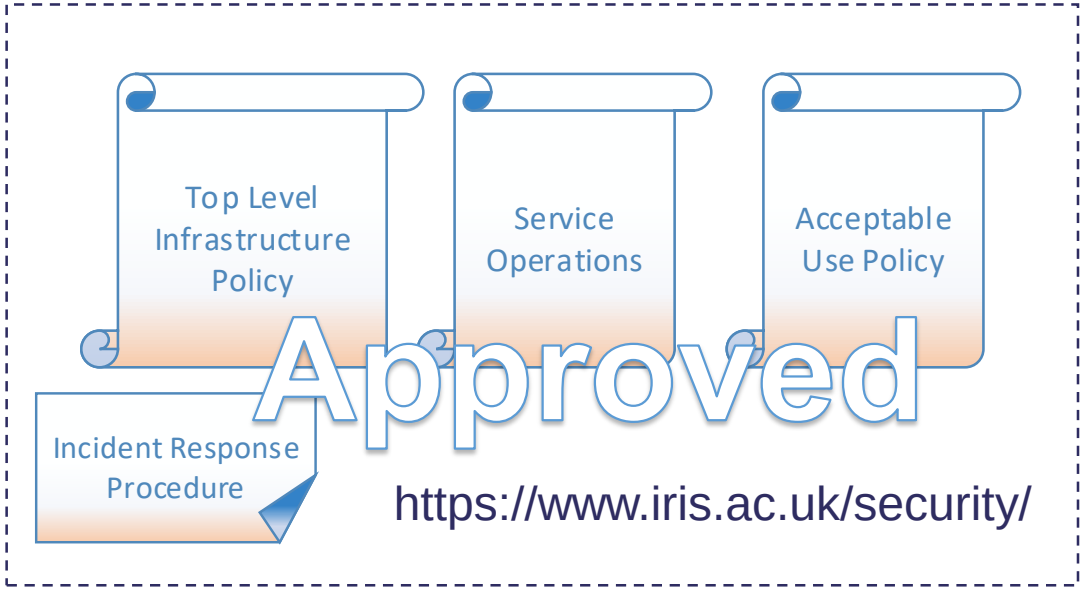
Second DRAFT for comments

Ian Neilson, David Crooks, Dave Kelsey

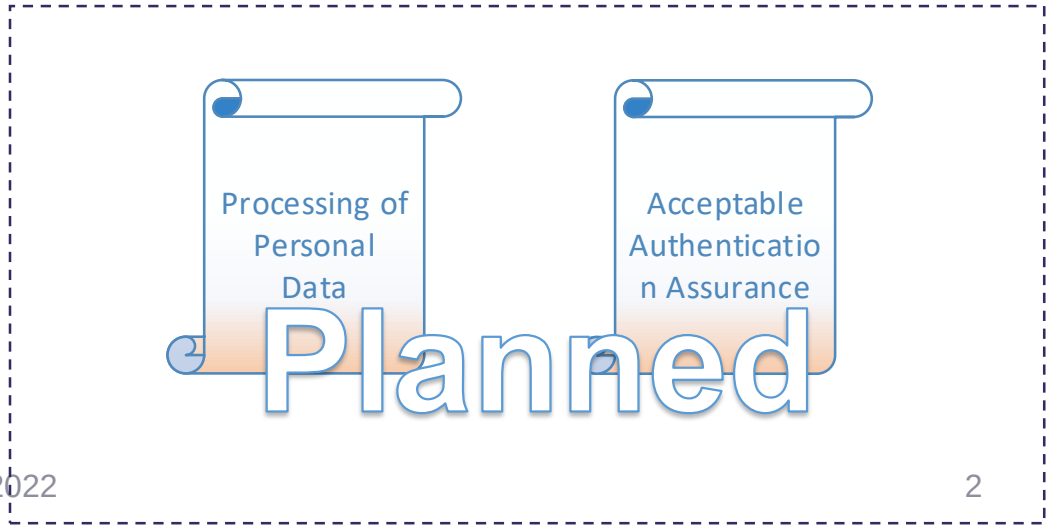
ian.neilson@stfc.ac.uk

Context: IRIS Policies to date





AARC Policy Development Kit
https://aarc-community.org/



Science and Technology Facilities Council
Scientific Computing

Policy Scope

- What is a “Community”?

  “A group of individuals (members), organised with a common purpose, and jointly granted access to the IRIS infrastructure. An IRIS Community may act as the interface between individual members and the IRIS Infrastructure.” – IRIS Infrastructure Security Policy

  - Sometimes “Virtual Organisation”, “Collections of Users”, …

- Who does this policy apply to?

  “… to the Community and those operating and managing services on behalf of the Community.”

Policy Objectives

- What does the policy aim to achieve?

  "To help protect [IRIS] resources from damage or misuse …"

- How does it do this?

  1. **Asserts** that a Community has "*responsibilities in the manner [the Community] manages its membership and the way it behaves towards the Infrastructure.*"
  2. **Requires** a set of actions and behaviours "*defining the relationship between a Community and a supporting Infrastructure, aims to establish a sufficient level of trust to enable reliable and secure Infrastructure operation.*"
  3. **Declares** that *"Communities that fail to comply with this policy may have their access to the Infrastructure restricted or suspended by the Infrastructure until compliance has once more been satisfactorily demonstrated."*

This Policy isn't ..

- A set of contractual obligations
  - Does provide a set of (minimum) "expectations"
- A cookbook of operational procedures
  - Does include (non-normative) guidance
  - Assumes that as IRIS continues to evolve –

    "Support structures and procedures, necessary for an implementation of this policy, should be created as a collaboration between a Community and the Infrastructure with which it has a usage agreement. Guidance on this implementation is available in the References and Notes section …"

A note on Policy Style

- It tries to be -
  - Concise
    - Short clauses addressing single requirements
  - Understandable
    - Not a legal document, SLA, …
- Sometimes it must be “fuzzy” -
  - A lot depends on context, Community scale, organisation, maturity …
  - Guidance notes given for further explanation and references
  - Implementation procedures handled separately
    - On-boarding, incident response, decommissioning, …

Policy clauses ~ incident handling

Each Community must -

1. agree a name with the Infrastructure to be used to uniquely identify the Community in the Infrastructure [Naming]

2. collaborate with others in the reporting and resolution of security events or incidents arising from their Community's participation in the Infrastructure and those affecting the Infrastructure as a whole [Contact Information, Sirtfi]

Policy clauses ~ incident handling

Guidance and Notes:

1. agree a name w
identify the Commu

2. collaborate with
security events or
participation in th
Infrastructure as a v

R3. Sirtfi: Those organising a Community, particularly in the case where Community-specific services are delegated to a third-party service operator, should be aware of the recommendations of the REFEDS Sirtfi framework - A Security Incident Response Trust Framework for Federated Identity (https://refeds.org/sirtfi), with which a number of the requirements and recommendations in this document align.

R4. Naming: It is strongly recommended that Infrastructures require Communities to register globally unique names. These should be either a URN prefix that is persistently assigned to the Community or a fully-qualified domain name from the global domain name system assigned to the Community by the relevant naming authority.

R5. Contact Information: To assist in the resolution of operational issues, including with the investigation of security incidents, an Infrastructure hosting a Community will register Community contacts. Such contacts should be authoritative for management, security and operational decisions relating to the Community's use of the Infrastructure, and any services operated by or on behalf of the Community that interact with the Infrastructure. It is recommended that, to provide redundancy, at least two individuals are identified within the community, including one to act as a primary security contact point.

Policy Clauses ~ membership management

3. actively manage its membership to restrict it to qualifying individuals

4. define a Community Acceptable Use Policy (AUP) which, as a minimum:
   - a. defines the science purposes (goals, aims etc.) of the Community,
   - b. binds members of the Community to use Infrastructure resources exclusively for those purposes,
   - c. does not conflict with the IRIS AUP
   - ~~d. binds members of the Community to the Infrastructure AUP~~

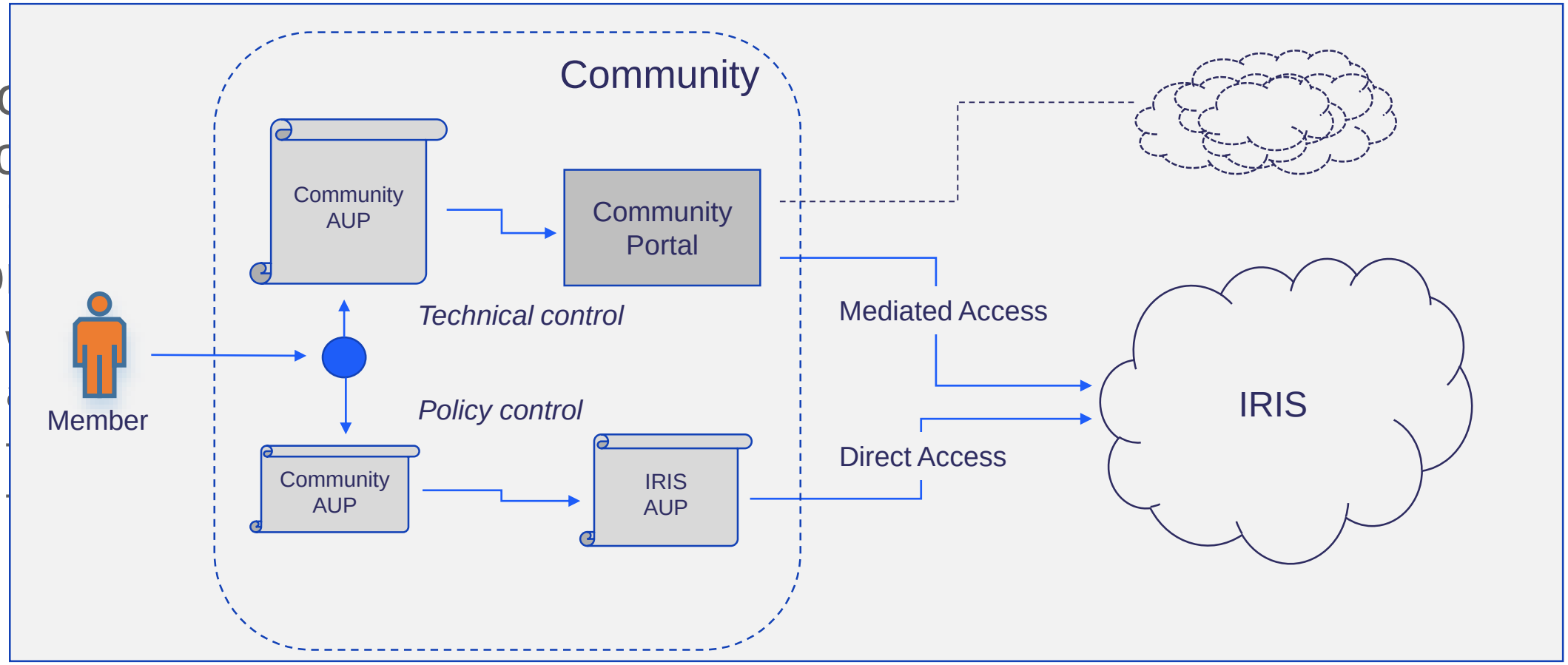
Text removed from first draft

Policy Clauses ~ authorisation

- 5. control by policy, technical means or both, each member's access to and use of the resources allocated to the Community by the Infrastructure so that only work within the scope of the Community AUP is carried out. In addition:
  - where policy is used, without technical means, the member must agree to be bound by the terms of the Infrastructure AUP and
  - technical means must preserve the ability to trace the actions of individual users on the Infrastructure.

Policy Clauses ~ authorisation

- 5. c
  acc
  by
  Co
  - v
  - t



Policy Clauses ~ operations

6. promptly suspend an individual's authorisation to use Infrastructure resources on request of the Infrastructure Security Officer

7. ensure that services managed by, or on behalf of, the Community are operated in accordance with the requirements of the IRIS Service Operations Security Policy

Policy Clauses ~ confidentiality and privacy

8. honour the confidentiality requirements of information gained as a result of the Community’s use of the Infrastructure

9. define a Privacy Notice, or use other appropriate means, to provide all legally required information to those members whose personal data is processed as a result of the Community's use of the Infrastructure, and only use such data for administrative, operational, accounting, monitoring and security purposes

Policy Clauses ~ confidentiality and privacy

8. honour the confidentiality requirements of information gained as a result of the Community's use of the Infrastructure

R9. Information Management: Information such as names, email and telephone contact numbers, network addresses and associated configuration information and non-public security (CSIRT) contact data and threat intelligence may be exchanged as part of normal activities or during a security incident investigation. Any obligations restricting the sharing or publication of such information must be honoured (see also policy clause 8).

se
e of

Policy Clauses *~ Shhh! liability and compliance*

10. not hold Service Providers or other Infrastructure participants responsible for any loss or damage incurred as a result of their members' use of or participation in the Infrastructure, except to the extent specified by law or any licence or service level agreement

11. promptly inform the Infrastructure Security Officer of any non-compliance with this policy, assess its compliance with this Policy at least once per year, and endeavour to correct violations in a timely manner

Community AUP template

Leveraging IRIS AUP for policy controlled access use-case

Define purposes

This Acceptable Use Policy and Conditions of Use ("AUP") defines the rules that govern your access to and use (including transmission, processing, and storage of data) of the resources and services ("Services") as enabled by virtue of your membership of the <insert community name> for the purpose of <insert objectives/purposes of the community>.

Binds members

1. You shall only use the Services in a manner consistent with the purposes and limitations described above.
2. You shall abide by limitations and conditions of use as given in the IRIS IRIS Acceptable Use Policy and Conditions of Use reproduced below, and as updated from time to time available at https://www.iris.ac.uk/security/.
3. <Insert additional community-specific clauses.>

The administrative contact for this AUP is: <insert email address>
The security contact for this AUP is: <insert email address>

The privacy statements (e.g. Privacy Notices) are located at: <insert url>

Base on IRIS AUP

<insert text of infrastructure AUP>

Use WISE Baseline AUP template for technical controls use case

https://wise-community.org/wise-baseline-aup/

Science and Technology Facilities Council

Scientific Computing

Thank you

ian.neilson@stfc.ac.uk