IRIS Community Security Policy

This policy, the IRIS Community Security Policy, is effective from 11/05/2023.[1]

Introduction

The IRIS Infrastructure Security Policy[2] defines an IRIS Community as *"A group of individuals (members), organised with a common purpose, and jointly granted access to the IRIS infrastructure".* Access to IRIS resources is commonly authorised and facilitated through an individual's membership of such a Community. To help protect those resources from damage or misuse, a Community has responsibilities in the manner it manages its membership and the way it behaves towards the Infrastructure. This policy, by defining the relationship between a Community and the supporting Infrastructure, aims to establish a sufficient level of trust to enable reliable and secure Infrastructure operation.

Support structures and procedures, necessary for an implementation of this policy, should be created as a collaboration between a Community and the Infrastructure. Guidance on this implementation is available in the References and Notes section provided below, which may be updated from time to time, and does not form part of the effective policy.

Definitions

Entities identified by a leading capital letter in this document are defined in the IRIS Infrastructure Security Policy[2], omitting the IRIS prefix for brevity.

Scope

This policy applies to each Community that makes use of the Infrastructure and to those who, on behalf of that Community, operate or manage services which interact with the Infrastructure.

Policy

Each Community must

1. agree a name with the Infrastructure to be used to uniquely identify the Community in the Infrastructure [R3],

[1] The current approved version of this policy can be found at https://www.iris.ac.uk/security/

[2] The IRIS Infrastructure Security Policy - https://www.iris.ac.uk/wp-content/uploads/2021/02/IRIS-Infrastructure-Security-Policy.pdf

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. [R4, R2],
3. actively manage its membership to restrict it to qualifying individuals [R5],
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 when acting as such to use Infrastructure resources exclusively for those purposes and
    c. does not conflict with the IRIS AUP[3]

    [R6],
5. control by policy, by technical means or by both, each member's access to and use of resources allocated to the Community by the Infrastructure so that only work within the scope of the Community AUP is carried out. In addition
    a. the ability to trace the member's actions on the Infrastructure must be preserved and
    b. where policy is used, without technical means, the member must agree to be bound by the terms of the Infrastructure AUP,

    [R7],
6. promptly suspend an individual's authorisation to use Infrastructure resources at the request of the Infrastructure Security Officer [R5],
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[4],
8. honour the confidentiality requirements of operational information gained as a result of the Community's use of the Infrastructure [R8],
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 [R9],
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,

[3] https://www.iris.ac.uk/wp-content/uploads/2022/05/IRIS-Acceptable-Use-Policy.pdf

[4] https://www.iris.ac.uk/wp-content/uploads/2021/05/IRIS-Service-Operations-Security-Policy.pdf

11. review its compliance with this Policy at least once per year, promptly inform the Infrastructure Security Officer of any non-compliance with this policy, and endeavour to correct violations[5] in a timely manner.

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.

References and Notes

R1. Many of the requirements in this document derive from the WISE Community 'Security for Collaborating Infrastructures Trust Framework' document: https://wise community.org/sci/.

R2. 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.

R3. Communities should register globally unique names. 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.

R4. To assist in the resolution of operational issues, including with the investigation of security incidents, the Infrastructure 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.

R5. The membership of a community should be managed in a way which is appropriate for the scale and organisation of the community, the resources to which its members have access, and in accordance with any relevant Infrastructure requirements. Consideration should be given to the adequacy of processes involved in the full membership lifecycle, including registration, periodic renewal (where appropriate), timely removal when membership terminates, and the maintenance of accurate contact information throughout. Suspension of a member's access may be important as a precaution during an ongoing security investigation.

[5] Exceptions to compliance are dealt with in the IRIS Infrastructure Security Policy$^{\text{Error! Bookmark not defined.}}$

R6. By a community member’s explicit agreement to abide by the terms and conditions of an AUP, they are made aware of their responsibilities and expectations regarding appropriate behaviour. Members must agree to abide by the community AUP at initial registration and thereafter renew this agreement in accordance with the requirements of the community and the Infrastructure.

A ‘layered’ approach, where the community AUP, references the infrastructure AUP, is acceptable. A template for such a community AUP is provided in Appendix 1. Where reference is not made to the infrastructure AUP (see “Resource Usage Control: Technical controls” scenario below) it is recommended that the community AUP be based on the WISE Baseline AUP template (https://wise-community.org/wise-baseline-aup/).

R7. Access to resources can be limited by both technical and policy controls. The implementation of such controls may be a shared responsibility between the community and the infrastructure, or other third party, providing a service (such as membership management, authentication or other access control facility) on which the community is reliant. Such divisions of responsibility should be clearly understood and agreed before use of the service begins.

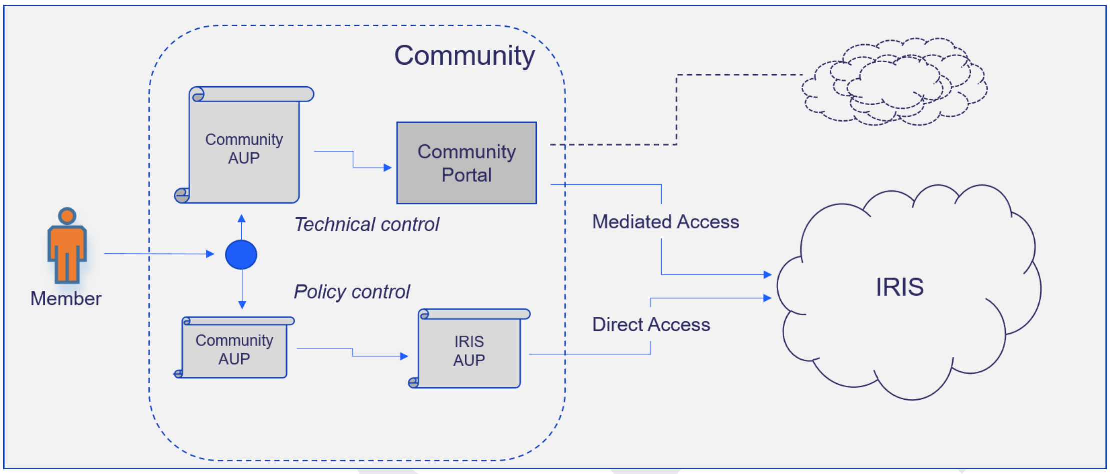
- Technical controls: processing capabilities available to a user are limited by the design of the system that is used to access a resource. The system must be operated in such a way that the security requirements of the Infrastructure are satisfied (e.g. log retention for use in the event of a security incident). Where a community makes use of a service operated by the infrastructure or other third party, responsibility for fulfilling these requirements may, of necessity, be shared with the service operator (e.g. traceability of user actions through a job submission service).

  Example: A community member accesses resources via a community-run portal (workflow manager, job submission interface etc.) on which they have a community-managed account enabling them to construct workflows (jobs) for submission to remote resources. The user does not have an account on the target resources and the operations and datastores available to the user as part of the job are restricted to those made available by the administrators of the portal. The portal administrators are able to trace back to the identity of the originating users, through system logs or otherwise, all jobs submitted to the Infrastructure.

- Policy controls: the user agrees to be bound by the conditions of a usage agreement governing their use of Infrastructure resources.

  Example: The user may have an account on a resource which, in theory, would enable arbitrary work to be performed but they agree only to use it for work related to their community's objectives. Appropriate sanctions are in place should the agreement be broken.

Policy control will typically apply to community managers who implement the technical controls on community members i.e. the administrators of the community portal described above.



Resource Usage Control by Policy or Technical Means

R8. 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).

R9. Community management must familiarise itself with the requirements of relevant local data privacy legislation (e.g. GDPR in the EU, UK GDPR and DPA 2018 in the UK), such as regarding the processing of personal data during registration and ongoing management of the lifecycle of its membership. These may include the use of a Privacy Notice presented to its members, and the creation of a policy covering the processing of personal data. Where the membership registration and lifecycle processing is delegated to an infrastructure or third party service, it is expected that such service operators would largely fulfil the technical requirements (display of privacy notices, security of data etc.) but the community may still be responsible as data controller. The AARC Community published a guideline on privacy risk assessment (AARC-G042) together with template policy and privacy notices (AARC Policy Development Kit). The REFEDS Data Protection Code of Conduct provides a best practice guidance framework for Service Providers regarding the EU GDPR, including a template Privacy Notice (Code of Conduct 2.0 documents). The UK Information Commissioner also publishes guidance on this and other Data Protection topics (What privacy information should we provide?).

Appendix 1 - Template Community AUP

Clause 3 should be omitted if there are no additions.

<Insert community name> Acceptable Use Policy and Conditions of Use

This policy, the <insert community name> Acceptable Use Policy and Conditions of Use <insert version as v.0x>, is effective from <insert date>. The currently effective version of this policy is available at <insert url>.

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>.

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 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>

<insert text of IRIS Infrastructure AUP>

Other Sources / Attribution / Acknowledgements: ‘EGI Community Membership Management Policy’ and ‘EGI Community Operations Security Policy’ used under CC BY 4.0. The research leading to these results received funding from the European Community’s Horizon2020 Programme under Grant Agreement No. 730941 (AARC2)