IRIS Infrastructure Security Policy

This policy, the IRIS Infrastructure Security Policy, is effective from 5th November, 2020.

Introduction

To fulfil its mission, it is necessary for the IRIS Infrastructure (https://www.iris.ac.uk) to be protected from damage, disruption and unauthorised use. This document presents the policy regulating those activities of IRIS Participants related to the security of the IRIS Infrastructure.

Definitions

IRIS Infrastructure
All of the IT hardware, software, networks, data, facilities, processes and any other elements that together are required to develop, test, deliver, monitor, control or support IRIS Services.

IRIS Management
The IRIS Delivery Board [R1].

IRIS Participant
An entity providing, using, managing, operating, supporting or coordinating one or more IRIS service(s).

IRIS Service
An infrastructure component fulfilling a need of one or more IRIS Communities, such as computing, storage, networking or software systems.

IRIS Service Provider
An entity responsible for the management, deployment, operation and security of an IRIS service.

IRIS 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 User
A member of an IRIS Community authorised to access and use IRIS Services.

IRIS Security Officer
An individual, appointed by the IRIS Management, responsible for operational security of the IRIS Infrastructure.

In this document the key words ‘must’, ‘must not’, ‘required’, ‘shall’, ‘shall not’, ‘should’, ‘should not’, ‘recommended’, ‘may’, and ‘optional’ are to be interpreted as described in RFC 2119 [R2]

Objectives

To reduce the likelihood of and impact from security incidents on the IRIS Infrastructure, its Participants and the wider Research community, this policy gives authority for actions to be taken by designated individuals and organisations and places responsibilities on IRIS Participants.

Scope

This policy applies to all IRIS Participants. This policy augments IRIS Service Providers' local security policies by setting out additional IRIS Infrastructure specific requirements.

Approval and Maintenance

This policy is approved by IRIS Management and thereby endorsed and adopted by the IRIS Infrastructure as a whole.

The IRIS Management may delegate responsibility for maintenance and revision of this document as required. Substantive revisions must be submitted to IRIS Management prior to adoption.

The most recently approved version of this document is available at [R3].

Responsibilities

Responsibilities of the IRIS Management:

> The IRIS Management provides, through the adoption of this policy and through its representations on the various management bodies of the IRIS Infrastructure, the overall authority for the decisions and actions resulting from this policy including procedures for the resolution of disputes.
>
> The IRIS Management maintains the set of policies approved for use within the IRIS Infrastructure and ensures that IRIS Participants are aware of their roles and responsibilities.
>
> The IRIS Management must appoint the IRIS Security Officer.

Responsibilities of the IRIS Security Officer:

> The IRIS Security Officer coordinates the operational security capabilities of the IRIS Infrastructure, including the enabling of compliance with the Sirtfi framework [R4]. The IRIS Security Officer may, in consultation with IRIS Management and other appropriate persons, require actions by IRIS Participants as are deemed necessary to protect the IRIS Infrastructure from or contain the spread of IT security incidents. The IRIS Security Officer handles requests for exceptions to this policy as described below. The Security Officer is responsible for establishing and periodically testing a communications flow for use in security incidents. The IRIS Security Officer may delegate responsibilities to designated individuals or groups as necessary to provide operational coverage.

Responsibilities of IRIS Service Providers:

> Service providers must deploy security controls to protect the confidentiality, integrity and availability of their services and designate a security contact to collaborate with the IRIS Security Officer and affected IRIS Participants in the handling of security incidents. The security contact for the service provider shall promptly inform the IRIS Security Officer of any suspected or confirmed security incident that could impact IRIS.

Responsibilities of IRIS Users:

IRIS Users must abide by the terms of the IRIS Infrastructure Acceptable Use Policy (AUP)[R3] and must collaborate in timely reporting and resolution of security incidents affecting the IRIS Infrastructure.

Responsibilities of IRIS Communities:

IRIS Communities must collaborate with the IRIS Security Officer to proactively limit risk posed to IRIS from their use of the Infrastructure, including the reporting and resolution of suspected or confirmed security incidents and issues arising from Community members' use of the Infrastructure.

IRIS Communities must manage the lifecycle of their members (registration, renewal and removal) to ensure that membership is restricted to only bonafide individuals, and all members are made aware of their responsibilities as stated in the IRIS Infrastructure Acceptable Use Policy.

Physical and Network Security

All the requirements for the physical and network security of IRIS Services are expected to be adequately covered by each IRIS Service Provider’s local security policies and practices, and those of their underlying network provider(s).

To support specific IRIS Community workflows it may be necessary to permit inbound or outbound network traffic. It is the responsibility of the IRIS Service to accept or mitigate the risks associated with such traffic.

Exceptions to Compliance

Wherever possible, IRIS Infrastructure policies and procedures are designed to apply uniformly to all IRIS Participants. If this is not possible, for example due to legal or contractual obligations, exceptions may be made. Such exceptions should be time-limited and must be documented and submitted to the IRIS Infrastructure Security Officer for approval at the appropriate level of management.

In exceptional circumstances it may be necessary for IRIS Participants to take emergency action in response to some unforeseen situation which may violate some aspect of this policy. If such an action is necessary, the exception should be minimised, documented, time-limited and authorised at the highest level of local management commensurate with taking the emergency action promptly. Details of the action taken must be notified to the IRIS Security Officer at the earliest opportunity.

Sanctions

IRIS Service Providers that fail to comply with this policy in respect of a service they are operating may lose the right to have their services recognised by the IRIS Infrastructure until compliance has once more been satisfactorily demonstrated.

IRIS Communities who fail to comply with this policy may lose their members' right of access to and collaboration with the IRIS Infrastructure, and may lose the right to have their services recognised by the IRIS Infrastructure until compliance has once more been satisfactorily demonstrated.

IRIS Users who fail to comply with this policy may lose their right of access to the IRIS Infrastructure, and may have their activities reported to their IRIS Community or their home organisation.

Any activities thought to be illegal may be reported to appropriate law enforcement agencies.

Further Information and Guidance

The current version of this policy and additional documents, together with guidance for implementation of IRIS security policy, may be found at [R3].

References

[R1] https://www.iris.ac.uk/about-iris/structure/
[R2] https://tools.ietf.org/html/rfc2119
[R3] https://www.iris.ac.uk/security
[R4] https://refeds.org/sirtfi

Other Sources / Attribution / Acknowledgements: "EGI Top Level Security Policy", used under CC BY-NC-SA 4.0.The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).