IRIS Service Operations Security Policy

This policy, the IRIS Service Operations Security Policy, is effective from 20th May, 2021.

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 policy, by defining expectations of the behaviour of those offering Services to Communities using the Infrastructure, and to the operators of other supporting Infrastructure services, aims to establish a sufficient level of trust between all Participants in the Infrastructure to enable reliable and secure Infrastructure operation.

Support structures and procedures, necessary for the implementation of this policy, should be created as a collaboration between Service and Infrastructure management. The References and Notes section below contains information which may be helpful in the process of implementing this policy.

Definitions

Entities identified by a leading capital letter in this document are defined in the "IRIS Infrastructure Security Policy" [R2], omitting the IRIS prefix for brevity.

Scope

This policy applies to all IRIS Service Providers, including those managing, deploying, operating and securing Services on behalf of the Infrastructure as a whole.

Policy

Each Service Provider must

1. collaborate with others in the reporting and resolution of security events or incidents arising from their Service's participation in the Infrastructure and those affecting the Infrastructure as a whole [R3][R4].
2. ensure that their Service operates in a manner which is not detrimental to the Infrastructure nor to any of its Participants.
3. follow, as a minimum, common IT security best practices[R5][R6][R7], such as pro-actively applying security updates and taking appropriate action in relation to security vulnerability notifications, and participate in drills or simulation exercises to test Infrastructure resilience as a whole.
4. respect the confidentiality of information gained as a result of their Service's participation in the Infrastructure [R8].

5. respect the legal rights of Infrastructure Users and others with regard to their personal data, and only use such data for administrative, operational, accounting, monitoring or security purposes [R9][R10].

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

7. promptly inform Users and other affected parties if they take action to protect their Service, or the Infrastructure, by controlling access to their Service, and do so only for administrative, operational or security purposes.

8. retain sufficient system generated information (logs), aggregated centrally wherever possible [R11], and protected from unauthorised access or modification, for a minimum period of 90 days, to be used in the event of a security incident [R12].

9. honour the obligations as specified in clauses 1 and 8 above for a period of 90 days after their Service is retired from the Infrastructure, including the retention of logs when physical or virtual environments are decommissioned.

10. promptly inform the Infrastructure Security Officer of any non-compliance with this policy.

Service Providers that fail to comply with this policy may lose the right to have their services recognised 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, available here - https://wise community.org/sci/.

R2. IRIS Security Policies - https://www.iris.ac.uk/security/.

R3. Service Providers should support REFEDS SIRTFI - Security Incident Response Trust Framework for Federated Identity - https://refeds.org/sirtfi, which includes the requirement to maintain contact information for a security response capability (Normative Assertions on Incident Response - SIRTFI v1.0 Section 2.3).

R4. Alongside following site-local mandated policy and procedure requirements, efficient, collaborative incident response relies on participants agreeing on an incident response procedure before it is needed. Example procedure here - https://www.iris.ac.uk/security/, based on information from EGI (https://csirt.egi.eu/activities/).

R5. TrustedCI, The NSF Cybersecurity Centre of Excellence, provides a wide variety of security related resource material applicable to research environments - https://www.trustedci.org/resources, as well as more targeted information in the Resources section, such as "Security Best Practices for Academic Cloud Service Providers" - https://www.trustedci.org/cloud-service-provider-security-best-practices

R6. NCSC, the UK National Cyber Security Centre, provides general guidance covering current best practice for a broad range of IT security topics, including Access Control, Configuration Management, Logging and Vulnerabilities - https://www.ncsc.gov.uk/section/advice guidance/all-topics

R7. ISO 27000 series standards and the NIST Cyber Security Framework are foundational resources for the implementation of comprehensive information security management systems - https://www.iso.org/standard/73906.html, https://www.nist.gov/cybersecurity

R8. Information essential for the secure operation of a Service, such as names, email and telephone contact numbers of service operators, network addresses and associated configuration information and non-public security (CSIRT) contact data may be exchanged as part of normal service operation or during a security incident investigation. Any obligations governing the sharing or publication of such information must be honoured.

R9. The UK Information Commissioner's Office maintains up-to-date guidance on data protection issues, including the rights of individuals - https://ico.org.uk/for organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation gdpr/individual-rights/.

R10. The AARC projects created a number of guidelines relating to the handling of personal data relevant for infrastructure operators - https://aarc-community.org/guidelines/#policy

R11. Logging recommendations from the UK National Cyber Security Centre - https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes

R12. https://refeds.org/sirtfi (Normative Assertions on Traceability - SIRTFI v1.0 Section 2.3)