AUSTRALIAN ACCESS FEDERATION

NCRIS National Research Infrastructure for Australia

AAF is enabled by NCRIS

[PDK07]

Service Operations Security Agreement

Key questions to inform policy development:

- How strongly can connected services rely on resources or software provided by Service Providers?
- For how long is a Service Provider obliged to fulfil its obligations after announcing its retirement?

Note:

- This policy serves as an overlaying multilateral policy that should be considered alongside unilateral contracts, and as such may require legal consultation/review between parties.
- Sirtfi compliance is a key factor in establishing trust with other federated entities and operators, such as eduGAIN and InCommon‡

‡ See eduGAIN *Sirtfi: Supporting Security Incident Response* https://edugain.org/sirtfi-supporting-security-incident-response/

IMPORTANT NOTE: On 29 March 2025, the AARC Policy Working Group released Guidance Note AARC-G084 Security Operational Baseline. AAF is reviewing the impact of this guideline on PDK07 (refer to https://www.nikhef.nl/~davidg/p/PDK-EOSC-Security-Baseline-20210927.pdf for context.)

**Delete this box after completing the policy.*

1 Introduction and Purpose

1.1 Objectives

This document provides the basis for a coordinated operational approach and common trust environment across the Collaboration and its Service Providers.

1.2 Scope

This Agreement applies to all Service Providers within the Collaboration. Service Providers must have their own internal governance and operational processes to ensure the provision of their Services

The Collaboration relies on compliance with the Sirtfi[1] and Scntfi[2] Frameworks to establish its common trust environment. Service Providers must, where relevant, ensure compliance with these frameworks in accordance with Collaboration Policies.[3] In the case of conflict (as it pertains to the management, operation and security of the Collaboration), Collaboration Policies will take precedence.

[1] The *Security Incident Response Trust Framework for Federated Identity* (v2.0). Refer to refeds.org/sirtfi. Entities must be compliant with Sirtfi Framework v1.0 for v2.0 compliance.

[2] The *Scalable Negotiator for a Community Trust Framework in Federated Infrastructures*. Refer to www.igtf.net/snctfi/.

[3] <Link to Collaboration Policies>.

© Owned by the authors and made available under license: https://creativecommons.org/licenses/by-nc-sa/4.0/
Other Sources / Attribution / Acknowledgements: EGI Service Operations Security Policy, used under CC BY-NC 3.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

This document is provided as guidance only. Each organisation or Collaboration must consider its own unique context, legislative obligations, and trust and identity requirements to complete and implement the Trust and Identity Policy Development Kit. AAF and other national research infrastructure members of the Policy Working Group, are not liable for any loss or damage, from any implementation or action taken to implement this Policy.

All Collaboration Service Providers are listed in Schedule 1 of the Top-Level Collaboration Policy.[4] This Agreement must be read in conjunction with all Collaboration Policies.

2 Agreement

Service Providers agree to the conditions laid down in this document and other referenced documents, which may be subject to revision:

1. You (the Service Provider) shall comply with all relevant Collaboration Policies.

2. You shall provide and maintain accurate contact information, including at least one Security Contact who shall support the Collaboration's compliance with the Sirtfi Framework on behalf of the Service.

3. You are held responsible for the safe and secure operation of the Service in accordance with local processes and relevant legislation. Any information you provide regarding the suitability and properties of the Service should be accurate and maintained. The Service shall not be detrimental to the Collaboration.

4. You should follow IT security best practices including proactively applying updates or configuration changes related to security. You shall respond appropriately, and within the specified time, on receipt of security notices from the Collaboration in accordance with Collaboration Policies and the Sirtfi Framework.

5. Personal information must be processed in accordance with the Policy on the Processing of Personal Information and the Community Membership Management Policy.[5]
    a. You shall apply due diligence in maintaining the confidentiality of user credentials and of any data you hold where there is a reasonable expectation of privacy, and otherwise in accordance with Collaboration Policies and relevant legislative requirements.
    b. You shall collect and retain auditing information in compliance with Collaboration Policies and associated procedures, and must assist the Collaboration in security incident response.
    c. You shall use logged information, including personal data, only for administrative, operational, accounting, monitoring and security purposes. You shall apply due diligence in maintaining the confidentiality of logged information.

6. Provisioning of Services is at your own risk. Any software provided by the Collaboration is provided <on an as-is basis> / <in accordance with service-level agreements>, and subject to its own license conditions. There is no guarantee that any procedure applied by the Collaboration is correct or sufficient for any particular purpose. Neither the Collaboration nor its Service Providers are liable for any loss or damage in connection with your participation in the Collaboration or connection to its Infrastructure.

7. You may control access to your Service for administrative, operational and security purposes and shall inform the affected Users and Collaboration Management where appropriate.

8. Your Service's connection to Collaboration Infrastructure may be controlled for administrative, operational and security purposes if you fail to comply with these conditions

[4] <Link to PDK01>
[5] Refer to <Link to PDK03> and <Link to PDK06>

© Owned by the authors and made available under license: https://creativecommons.org/licenses/by-nc-sa/4.0/
Other Sources / Attribution / Acknowledgements: EGI Service Operations Security Policy, used under CC BY-NC 3.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

This document is provided as guidance only. Each organisation or Collaboration must consider its own unique context, legislative obligations, and trust and identity requirements to complete and implement the Trust and Identity Policy Development Kit. AAF and other national research infrastructure members of the Policy Working Group, are not liable for any loss or damage, from any implementation or action taken to implement this Policy.

Upon retirement of a Service, the obligations specified in clauses 1, 2, 5 and 6 shall not lapse for the retention period <of X months> as agreed with the Collaboration.

3 Associated Documents

3.1 Collaboration Policies

- Top-Level Collaboration Policy [PDK01]
- Privacy Policy [PDK02]
- Policy on the Processing of Personal Information [PDK03]
- Acceptable Use Policy [PDK04]
- Acceptable Authentication Assurance Policy [PDK05]
- Community Membership Management Policy [PDK06]
- Security Incident Response Procedure [PDK08]

3.2 Service Provider Policies

- List relevant Service Provider Policies (if applicable)

3.3 Relevant Legislation, Standards & Frameworks

[Include all legislation, standards, and frameworks relevant to the Collaboration, highlighting their alignment with Australian laws as well as applicable international standards and regulations.]

- *Privacy Act (1988)* (Cth) (Australian Privacy Principles)
- *[Example] Data Availability and Transparency Act 2022 (Cth) (DAT Act)*
- *[Example] Defence Trade Controls Act 2012 (Cth)*
- *[Example] Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act)
- *Other relevant international standards and legislation (e.g. General Data Protection Regulation (GDPR), FAIR and CARE Principles)*

© Owned by the authors and made available under license: https://creativecommons.org/licenses/by-nc-sa/4.0/
Other Sources / Attribution / Acknowledgements: EGI Service Operations Security Policy, used under CC BY-NC 3.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

This document is provided as guidance only. Each organisation or Collaboration must consider its own unique context, legislative obligations, and trust and identity requirements to complete and implement the Trust and Identity Policy Development Kit. AAF and other national research infrastructure members of the Policy Working Group, are not liable for any loss or damage, from any implementation or action taken to implement this Policy.

Version Control

Document Control			
Document Approved:		**Date Effective:**	
Last Review Date:		**Next Review Date:**	
Version Control			
Version	**Author**	**Summary of Changes**	**Date**
1.5	AAF	Review and alignment of language; increased clarity of onus of Service Providers to be responsible for ensuring appropriate policies, procedures and governance frameworks are in place. Refinement of context statements. Corrected attributions. Updated disclaimer. Updated references to international legislations/frameworks (if relevant). **NOTE: Refer to context statement re AARC-G084 release.**	March 2026

AAF NRI Policy Development Kit - Service Operations Security Agreement [PDK07]
© Owned by the authors and made available under license: https://creativecommons.org/licenses/by-nc-sa/4.0/
Other Sources / Attribution / Acknowledgements: EGI Service Operations Security Policy, used under CC BY-NC 3.0. The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

This document is provided as guidance only. Each organisation or Collaboration must consider its own unique context, legislative obligations, and trust and identity requirements to complete and implement the Trust and Identity Policy Development Kit. AAF and other national research infrastructure members of the Policy Working Group, are not liable for any loss or damage, from any implementation or action taken to implement this Policy.