

[PDK01]

Top-Level Collaboration Policy

Context

A primary objective of the Collaboration is to provide a unified, coherent policy environment that facilitates the implementation of best practice, limits exceptions to operations and compliance, and streamlines the User experience.[‡] The development of Collaboration policies should be a cooperative exercise, however decisions on oversight and management (which actors or representatives oversee the management of the Collaboration), policy harmonisation (how do local and Collaboration Policies work together), and resourcing (how will delegated functions within Collaboration policies be implemented) should be considered.

Key questions to inform policy development:

- Who are the key actors in the Collaboration (entities bound by agreements, Service Providers, etc)
- What are the desired governance arrangements for the Collaboration?
- Are there sufficient personnel available to take on necessary roles and responsibilities?
- Are the operational security arrangements appropriate to the Collaboration?
- Will local and Collaboration policies work effectively when implemented together?
- What are the legislative requirements of the Collaboration? Are actors from different jurisdictions (e.g. Australia, EU / Queensland, Victoria)?

[‡] See Stevanovic, U. et al (2019) *Accounting and Traceability in Multi-Domain Service Provider Environments* [AARC2-DNA3.2], GÉANT Association, aarc-community.org/wp-content/uploads/2019/04/AARC2-DNA3.3_Accounting-and-Traceability-in-Multi-Domain-Service-Provider-Environments-1.0.pdf, p11.

*Delete this box after completing the policy.

1 Introduction and Purpose

1.1 Objectives

To fulfil its mission, the Collaboration must operate in a shared, consistent policy environment and protect its assets. This Policy describes the principles guiding the management, operation and security of the Collaboration, assigns responsibilities, and gives authority for actions which may be carried out by designated individuals to execute those functions.

This Policy defines key principles toward the management of the Collaboration. Those entities that have agreed to establish or formally agree to join the Collaboration (Service Providers) are listed in Schedule 1.

1.2 Scope

This Policy applies to all entities listed in Schedule 1.

This Policy augments Service Provider's local policies by setting out additional requirements specific to the Collaboration and defines structure for the governance and management of the Collaboration. For the purposes of the management, operation and security of the Collaboration, Collaboration Policies will take precedence where a local policy is in conflict.

AAF NRI Policy Development Kit – Top-Level Collaboration Policy [PDK01]

© Owned by the authors and made available under license: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

Other Sources / Attribution / Acknowledgements: SCIV2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, 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). 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.

1.3 Definitions

The following definitions apply across all Collaboration Policies. Definitions specific to a policy will be listed in that document.

Collaboration: The bounded collection of universities, laboratories, institutions or similar entities, which adhere to the Collaboration Policies.¹ The Collaboration offers research infrastructure to the Community.

Collaboration Policies: The set of policies governing the management, operations and security of the Collaboration as approved by Management.

Community: A group of Users, organised with a common purpose, and jointly granted access to the Collaboration. It may act as the interface between individual Users and the Collaboration.

Community Manager: A nominated individual responsible for the management of the members (Users) of a community and/or the Collaboration.

Infrastructure: The IT hardware, software, networks, data, facilities, processes and any other elements that together are required to develop, test, deliver, monitor, control or support services.

[Management]: The collection of the various boards, committees, groups and/or individuals mandated to oversee and control the Collaboration. *[Implementation note: Where this is a governing body, 'Management' should be customised to the Collaboration. For example, the ABC Steering Committee (ABC-SC).]*

Security Contact: A nominated individual or group responsible for the operational security of the Collaboration. This includes the Collaboration Security Contact, if applicable, and nominated Security Contacts within or operating on behalf of a Service Provider.

Service: A Collaboration element fulfilling a need of Users, such as computing, storage, networking or software systems.

Service Provider: An entity or agency responsible for the management, deployment, operation and security of a Service.

User: An individual authorised to access and use Services.

1.3.1 Requirement Levels (Key Words)

In all Collaboration Policies, the key words 'must', 'must not', 'required', 'shall', 'shall not', 'recommended', 'may', and 'optional' are to be interpreted as described in RFC 2119.²

2 Collaboration Management, Operations and Security

2.1 Collaboration Management

[The Collaboration must define or appoint an overseeing governing body. For the purposes of this policy, this role is currently referred to as Management and should be formalised in the final version. This text is provided as drafting guidance and should be deleted prior to policy finalisation.]

¹ Refer to: <link to Collaboration Policies>

² Refer to datatracker.ietf.org/doc/html/rfc2119

AAF NRI Policy Development Kit – Top-Level Collaboration Policy [PDK01]

© Owned by the authors and made available under license: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

Other Sources / Attribution / Acknowledgements: SCIV2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, 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). 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).

The Collaboration must define an overseeing governing body ([Management]), with an appropriate Terms of Reference and Composition to effectively oversee the management, operation and security of the Collaboration. This will include an appropriate meeting schedule relevant to the aims and size of the Collaboration.

[Management] provides, through the approval of this Policy and through its representations of the Collaboration, the overall authority for the decisions and actions resulting from this Policy.

[Management] oversees the Policies approved for use within the Collaboration and ensures that Service Providers, Collaboration personnel and Users are aware of their roles and responsibilities. Collaboration Policies must meet the requirements of the Snctfi framework.³

2.1.1 Decisions and Actions of [Management]

The decisions and actions of [Management] are limited to the oversight, management and security of the Collaboration, including relevant infrastructure, in accordance with its Terms of Reference and Collaboration Policies.

[Management] may delegate authority to specific <Collaboration and/or Community personnel> to take action (immediate or urgent) on its behalf as may be necessary for the operation and security of the Collaboration from time to time. Such actions should be reviewed by [Management] at an appropriate occasion, which may be at the next scheduled meeting or sooner, for oversight and continuous improvement purposes.

[Management] must ensure that the Collaboration abides by any arrangements, agreements or Memoranda of Understanding in reaching its decisions. Records of decisions and actions (minutes and associated papers) must be maintained securely for the duration of the Collaboration and made available to <Service Providers and Collaboration personnel> upon request, where appropriate.

2.1.2 Resolution of Disputes

Where disputes arise within the Collaboration on the management, operation or security of the Collaboration, all efforts should be made to resolve those disputes informally and in accordance with any agreements, arrangements or Memoranda of Understanding as pertaining to the Collaboration. Where resolution is not provided for in these mechanisms, an agreed external mediator should be engaged at shared cost.

Disputes about the management, operations or security of the Collaboration may be escalated to [Management] for consideration at its discretion. Unless otherwise stated in Collaboration Policies, in such cases the decision of [Management] is final.

2.1.3 Periodic Review of the Collaboration

[Management] should review the Collaboration arrangements for their effectiveness at least every <three> years. These reviews must be informed by an approach of continuous improvement as part of regular oversight activities. Records of improvement and review must be maintained securely for the duration of the Collaboration.

Outcomes of reviews of the Collaboration may include the renegotiation or cessation of arrangements with Service Providers. In such cases, a transition plan and communications plan must be developed in accordance with all Collaboration Policies and approved by [Management] to minimise the impact of these decisions upon Users, where necessary.

³ The *Scalable Negotiator for a Community Trust Framework in Federated Infrastructures*. Refer to www.igtfn.net/snctfi/.

AAF NRI Policy Development Kit – Top-Level Collaboration Policy [PDK01]

© Owned by the authors and made available under license: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

Other Sources / Attribution / Acknowledgements: SCIV2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, 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). 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).

2.2 Service Providers

The responsibilities of Service Providers may vary according to the nature of their engagement with the Collaboration, including the provision of infrastructure and resources. All Service Providers are required to complete a Risk Assessment using the Collaboration template,⁴ and contribute to risk management activities as may be required by [Management] from time to time.

Service Providers may engage in, offer Services, or utilise Services and Service Providers outside of the Collaboration, ensuring in doing so the Service Provider abides by Collaboration Policies at all times. Service Providers must declare all perceived, potential, and actual conflicts of interest to [Management] as soon as they arise.

2.3 Communities and Membership

A Community is a group of Users who have jointly been granted access to the Collaboration through their membership to the Community. Community membership is governed by the Collaboration Membership Management Policy. The Collaboration must establish at least one Community to facilitate the management of its Users in accordance with the Collaboration Membership Management Policy.⁵

2.3.1 Community Managers

The <Collaboration/Community> must define the role and responsibilities of the Community Manager and assign this role to at least two individuals. These roles and responsibilities must not conflict with Collaboration Policies. Community Managers may be appointed from Collaboration personnel.

Community Managers are responsible for the review and maintenance of Collaboration Policies and reporting to Management in accordance with s3.1.3 of this Policy.

Community Managers are responsible for implementing the Collaboration Membership Management Policy in compliance with all relevant Collaboration Policies. Community Managers must also give specific consideration given to the Policy on the Processing of Personal Information, any authentication assurance requirements of Service Providers, and any other matter as instructed by [Management].

Community Managers report to Management <at least twice per year> in a format specified by [Management] on:

- Collaboration Policies
- Matters pertinent to Membership life cycles, including any Sanctions that may have been applied in the reporting period, and
- Other matters as requested by [Management].

2.3.2 Users

Users are individuals registered to use Collaboration Services (when authorised), usually through a Community. Users who are registered to a Community are in general not required to separately negotiate access to Services within the Collaboration unless Users lack the appropriate credentials to authorise access. Users and Service Providers are not precluded from engaging directly or outside the bounds of the Collaboration.

⁴ Refer to [PDK09 hyperlink]

⁵ Refer to [PDK06 hyperlink]

AAF NRI Policy Development Kit – Top-Level Collaboration Policy [PDK01]

© Owned by the authors and made available under license: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

Other Sources / Attribution / Acknowledgements: SCIV2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, 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). 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).

Users who are not registered to a Community are typically Collaboration personnel (such as a Security Contact, or Collaboration-nominated Community Manager, or other individual) responsible for the maintenance, security and operation of a service.

All Users must acknowledge and accept all relevant Acceptable Use Policies before access to Collaboration Services is granted. All Users are deemed to be acting in a professional capacity when interacting with, accessing or using Collaboration Services.

2.3.3 Acceptable Use Policies

A Collaboration Acceptable Use Policy (AUP) must be developed and approved by [Management] using the Collaboration template.⁶ It is a threshold requirement for all Users who access Collaboration Services to acknowledge and accept the Collaboration AUP.

To ensure consistency across the Collaboration, clauses 1 through 10 of the Collaboration Acceptable Use Policy Template must not be altered. Additional clauses may be added by a Service Provider in accordance with their requirements. Any amendments to the base Collaboration AUP Template must be approved by Collaboration Management.

In general, it is preferable that one (aggregated) Acceptable Use Policy is developed for the Collaboration. Service Providers or Communities may require Users to accept a specific Acceptable Use Policy to access Collaboration Services. These AUPs must be based on the Collaboration template and must not conflict with the Collaboration AUP. Where there are multiple AUPs, Users will be required to also accept the Collaboration AUP as a prerequisite for registration to a Community, or access to a Service. [Management] will maintain a register of all current Acceptable Use Policies, in consultation with the Community Manager.

Acceptable Use Policies must be shown to all persons joining the Collaboration and its Communities or otherwise accessing Collaboration Services. Acceptance of the AUP by Users must be an explicit action, must be recorded, and must be a prerequisite for registration in the Community.

The AUP must address at least the following areas:

- The aims and purposes, and the basis of membership of the Collaboration (or Service Provider or Community)
- Acceptable use
- Non-acceptable use
- Maintenance of User registration data
- Protection and use of credentials
- Information protection and privacy

The AUP must align with Collaboration Policies on the Processing of Personal Information and Service Operations Security.

Community procedures must be developed by the <Collaboration delegate/Community Manager> to ensure Users are informed of and explicitly consent to material changes to Collaboration Policies and/or specific Acceptable Use Policies, including those arising from new Service Providers joining the Collaboration, as soon as feasible.

⁶ Refer to [PDK04 hyperlink]

AAF NRI Policy Development Kit – Top-Level Collaboration Policy [PDK01]

© Owned by the authors and made available under license: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

Other Sources / Attribution / Acknowledgements: SCIV2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, 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). 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).

2.3.4 Privacy Management

Service Providers must nominate a Privacy Officer to undertake the responsibilities outlined in the Policy on the Processing of Personal Information⁷ and in accordance with the *Privacy Act 1988* (Cth)⁸. [Management] will identify a central administrative contact point (i.e. an email address) for Users to contact with privacy concerns that will be referred to the relevant Service Provider.

2.4 Operational Security

Operational security capabilities of the Collaboration are coordinated by a Security Contact nominated by the Collaboration as a central contact and support point for security incidents affecting the Collaboration (the Collaboration Security Contact). This includes enabling of the Collaboration's compliance with the Sirtfi framework (v2.0).⁹

[Management] must identify and notify each Service Provider that requires a Security Contact upon joining the Collaboration. That Service Provider must inform the Collaboration of the nominated Security Contact(s), and the Collaboration must maintain this information.

The Collaboration Security Contact works in conjunction with Security Contacts within Service Providers and may nominate a Security Incident Response Coordinator from these personnel in the event of a security incident. The Collaboration Security Contact is responsible for the implementation of the Collaboration Service Operations Security Policy and Incident Response Procedure within their organisation as it pertains to the Collaboration. The Collaboration Security Contact may, in consultation with the [Management] and other appropriate personnel, require actions by Service Providers as deemed necessary to protect the Collaboration from, or contain the spread of, IT security incidents.

2.4.1 Physical Security

All the requirements for the physical security of Services are expected to be adequately covered by each Service Provider's local governance arrangements, security policies and practices and in accordance with relevant legislation. These should, as a minimum, reduce the risks from intruders, fire, flood, power failure, equipment failure and environmental hazards. Stronger physical security may be required for equipment used to provide certain critical services such as Community membership services, the Authentication Proxy, or credential repositories.

2.4.2 Network Security

All the requirements for the networking security of Services are expected to be adequately covered by each Service Provider's local governance arrangements, security policies and practices and in accordance with relevant legislation. To support specific Community workflows, it may be necessary to permit inbound or outbound network traffic. It is the responsibility of the Service Providers to accept or mitigate the risks associated with such traffic.

2.5 Collaboration Policies

2.5.1 Unified Approach

Collaboration Policies augment local policies and procedures to ensure the operation and security of the Collaboration. It is expected that all relevant Collaboration stakeholders will cooperate in the development and

⁷ Refer to [PDK03 hyperlink], cl 3.6.d.

⁸ See the *Privacy Act 1988* (Cth) www.legislation.gov.au/C2004A03712

⁹ The *Security Incident Response Trust Framework for Federated Identity* (v2.0). Refer to refeds.org/sirtfi. Sirtfi v2.0 compliance includes but is not limited to compliance with v1.0.

AAF NRI Policy Development Kit – Top-Level Collaboration Policy [PDK01]

© Owned by the authors and made available under license: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

Other Sources / Attribution / Acknowledgements: SCIV2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, 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). 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).

implementation of Collaboration Policies, which may include assuring [Management] of local policies and operations in place.

2.5.2 Exceptions to Compliance

Where the processes described in Collaboration Policies lead to obvious injustice and hardship due to an implementation of the process being unduly hard, a time-limited and documented exception may be implemented after the explicit, written approval of [Management].

Any such exception must be followed by immediate and concrete steps to address the deficiencies created within a limited time, commensurate with the discrepancy induced. The invocation of this hardship clause must not compromise the integrity or trustworthiness of the Collaboration.

2.5.3 Sanctions

Service Providers, Communities and Users that fail to comply with this policy may lose their rights and benefits until compliance has been satisfactorily demonstrated. Any activities thought to be illegal may be reported to home organisations or law enforcement agencies as appropriate.

2.5.4 Policy Management

Collaboration Policies are managed by delegated Collaboration personnel, in consultation with [Management] and other appropriate personnel within the Collaboration. This delegate is responsible for ensuring Collaboration Policies are maintained and reviewed in accordance with this s2.5.5 of this Policy, and that the most current versions are published and available to the Collaboration and its Users.

2.5.5 Approval and Review

Collaboration Policies and any relevant procedures are approved by [Management] and must be adopted by the entire Collaboration upon establishment, and subsequent review. Policies must be reviewed at least every three years and resubmitted for formal approval by [Management].

Major changes to Collaboration Policies, either through review or as may be required from time to time, must be approved by [Management]. Minor administrative changes to correct typographical, grammatical and formatting errors within Collaboration Policies may be approved by the <[Management] Chairperson>.

Current versions of all Collaboration Policies are available online at <hyperlink>.

3 Associated Documents

3.1 Collaboration Policies

- Privacy Policy [PDK02]
- Policy on the Processing of Personal Information [PDK03]
- Acceptable Use Policy [PDK04]
- Acceptable Authentication Assurance Policy [PDK05]
- Membership Management Policy [PDK06]
- Service Operations Security Agreement [PDK07]
- Incident Response Procedure [PDK08]

3.2 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]

AAF NRI Policy Development Kit – Top-Level Collaboration Policy [PDK01]

© Owned by the authors and made available under license: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

Other Sources / Attribution / Acknowledgements: SCIV2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, 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). 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.

- *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)*

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, legislation; introduction of good governance principles and review of Collaboration, including of Community Membership Management governance requirements (PDK06). Refinement of context statements. Corrected attributions. Updated disclaimer.	March 2025

AAF NRI Policy Development Kit – Top-Level Collaboration Policy [PDK01]

© Owned by the authors and made available under license: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

Other Sources / Attribution / Acknowledgements: SCIV2 from the WISE Community, used under CC BY-NC-SA 4.0. EGI e-Infrastructure Security Policy EGI-SPG-SecurityPolicy-V2, 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). 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.

Schedule 1

The following entities have agreed to be Service Providers of [Name of Collaboration]. Each entity listed has agreed to abide by all Collaboration Policies.

Table 1 [Name of Collaboration] Service Providers

Organisation	Role	Location
Organisation A	IdP	London, UK
Organisation B	Service Provider	Western Australia, AU
Organisation C	Research Group (Data Sharing)	Queensland, AU