AUSTRALIAN ACCESS FEDERATION

NCRIS National Research Infrastructure for Australia An Australian Government Initiative

AAF is enabled by NCRIS

[PDK00]

Instructions on how to use the AAF Policy Development Toolkit

The AAF Policy Development Kit v1.5 is based on and derived from the AARC BPA / PDK v1.

Step 1. Define the Collaboration

a) Describe the collaboration by identifying its purpose, the parties involved, and whether it is time-bound or ongoing. These inputs inform the development of the Top-Level Collaboration Policy (PDK01).

Step 2. Assessing Risk

a) Begin completing the Risk Assessment (PDK09). The risk assessment is a living document - it should be started here and revisited as each subsequent policy is developed, particularly during Step 5 (Security Management). To get started, consider the following questions:
   - What personal information is being collected or processed within the collaboration?
   - Who will access that information, and under what circumstances?
   - What could go wrong — and what measures exist or are planned to address those risks?

   PDK09 provides a risk table to help structure your thinking across risk sources, potential impacts, and mitigation measures. For collaborations processing sensitive personal information, consider whether a full Privacy Impact Assessment (PIA) is warranted.

Step 3. Managing Membership

a) Consider your future users and what level of authentication assurance is appropriate for your collaboration. The Acceptable Authentication Assurance Policy (PDK05) supports this assessment. AAF has adopted the REFEDS Assurance Framework V2 (RAF V2) as the basis for authentication assurance decisions within the NCRIS context.

b) The Acceptable Use Policy (PDK04) defines the rules and conditions that govern user access to and use of the collaboration's resources and services. PDK04 contains 10 standardised base clauses that must not be altered - this ensures consistency across services in the collaboration. Additional clauses specific to your collaboration may be added. The Acceptable Use Policy must address at least the following areas:
   i. The aims, purposes, and basis of membership of the community
   ii. Acceptable use
   iii. Non-acceptable use
   iv. Maintenance of user registration data
   v. Protection and use of credentials
   vi. Data protection and privacy *(this section must address the relationship with the policies on Processing of Personal Information, Security Traceability and Logging, and Service Operations Security)*

Other Sources / Attribution / Acknowledgements: The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Template derived from the GÉANT Data Protection Code of Conduct version 2, used under CC BY-NC-SA 4.0. 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).

When developing your AUP, also consider whether your collaboration requires specific conditions governing the use of artificial intelligence in research applications. PDK04 includes a prompt for this, reflecting the growing relevance of AI use policies across the NCRIS ecosystem.

c) The Membership Management Policy (PDK06) covers the full membership lifecycle, including:
   i. Registration (*Note: The types of information recorded at registration must be listed in the Policy on the Processing of Personal Information (PDK03))*
   ii. Assignment of attributes
   iii. Renewal
   iv. Suspension
   v. Termination

Step 4. Privacy Management

a) Complete the Privacy Policy (PDK02) and the Policy on the Processing of Personal Information (PDK03) together — these two documents are interdependent and should be developed in parallel. PDK02 is formatted as a table with instructions and questions to guide completion. One section asks for "Personal Information processed and the legal basis" - the required and recommended registration data for this section is defined in Schedule 1 of PDK03.
PDK03 defines the obligations of service providers and the principles governing the lawful processing of personal information within the collaboration.

Step 5. Security Management

a) Complete the Service Operations Security Agreement (PDK07). This agreement requires service providers to commit to the secure and compliant operation of their services within the collaboration, including:
   - Compliance with all collaboration policies
   - Nominating a Security Contact to support Sirtfi Framework compliance
   - Processing personal information in accordance with PDK03 and PDK06
   - Responding to security notices within specified timeframes

   This is also a good point to revisit the Risk Assessment (PDK09) in light of the security obligations now defined across the collaboration policies.

b) Complete the Incident Response Procedure (PDK08), which provides a step-by-step process to follow in the event of a suspected or confirmed security incident.

Other Sources / Attribution / Acknowledgements: The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Template derived from the GÉANT Data Protection Code of Conduct version 2, used under CC BY-NC-SA 4.0. 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).