Instructions on how to use the AAF NRI Policy Development Toolkit

NOTE: In this set of instructions, the updated policy/document titles are red in colour and linked to the AARC original policies using their original titles.

Step 1. Define the Collaboration

a. What is the purpose of the Collaboration? Who is involved? Is there a time limit or is this ongoing? These will feed into the Top Level Collaboration Policy (previously Top Level Infrastructure Policy)

Step 2. Assessing Risk

a. Start the Risk Assessment - this is something that will need to be added to as the policies are developed. What data is being used within the collaboration? Who will be using the data? What could go wrong?

Step 3. Managing Membership

a. Consider your future users. You can use the decision tree in the Acceptable Authentication Assurance Policy [*NOTE: The REFEDS Assurance Framework (RAF) has been updated. AAF is adopting the RAF V2, so it would be sensible to remove this graphic and replace it with one for RAF V2 when it is developed to put into the Acceptable Authentication Assurance Guidelines*]

b. The Acceptable Use Policy defines the expectations of the user by the Collaboration. In the Acceptable Use Policy Template there is a set of 10 standardised clauses to which you can add anything that is specific to your collaboration. These base clauses are not to be altered to ensure there is some consistency across Services in the Collaboration. The Acceptable Use Policy must address at least the following areas:

    a. The aims and purposes, and the basis of membership of the Community
    b. Acceptable use
    c. Non-acceptable use
    d. Maintenance of user registration data
    e. Protection and use of credentials
    f. Data protection and privacy – (The data protection and privacy section of the AUP must address the relationship with the Infrastructure policies on the Processing of Personal Data, Security Traceability and Logging, and Service Operations Security.)

c. Membership Management Policy – Includes information about the Membership Life Cycle:
  a. Registration (note: The types of information recorded must be listed in the Policy on the Processing of Personal Data of the Community.)
  b. Assignment of Attributes
  c. Renewal
  d. Suspension
  e. Termination

Step 4. Privacy Management

a. Privacy Policy –
  a. This policy is formatted as a table to be completed using SAML V2.0 Metadata Extensions for Login and Discovery specification. Each section consists of instruction and questions to consider
  b. One of the sections of the table asks for “Personal Information processed and the legal basis”. According to the Membership Management Policy there must be a Registry of Information which must store at least*:
    i. Registration information, including personal information of the User
    ii. attributes assigned to members
    iii. <Add or delete lines as required>
  c. The Registration information for a User comprises verified information on at least:
    i. family name(s)
    ii. given name(s)
    iii. the employing organisation name and address
    iv. any applicable Sponsor identity
    v. a professional email address
    vi. unique and non-reassigned identifier(s) of the User and the source of authority of each identifier
    vii. <Add or delete lines as required>
  d. and is recommended to contain:
    i. professional contact telephone number so as to inform the User promptly during the investigation of security incidents and of lifecycle events
    ii. other contact information, as voluntarily provided and maintained by the User.
  e. The types of information recorded must be listed in the Policy on the processing of Personal Data of the Community.

* This list of information collected should be in the Privacy Policy and references in the Processing of Personal Information policy

b. Policy on the Processing of Personal Information (currently named the Policy on the Processing of Personal Data). Contains definition and scope plus the principles for the processing of personal information

Step 5. Security Management

a. Service Operations Security Agreement (currently named Service Operations Security Policy).
   i. This requires agreement of the service providers to comply with the security and IT requirements of the Collaboration.
   ii. It asks for a person to be identified as the Security Contact
   iii. It reminds members of obligations under the Privacy Policy
   iv. This is likely a good time to revisit the Risk Assessment

b. The Incident Response Procedure provides a step-by-step list of actions to follow if a security incident occurs.