



2024 AAF Compliance – Cheat sheet for Rapid IdP Subscribers

AAF Federation Rules

As a Rapid IdP subscriber, management of your Federation IdP is being performed by the AAF. This will affect how you perform your yearly compliance check. This document highlights the Federation Rules where compliance is met automatically due to AAF Rapid IdP subscription.

Your organisation is still responsible for compliance to the AAF Federation Rules and as such you still need to be aware of the rules and the responsibilities that apply to your organisation.

The AAF has identified the Federation Rules that each Rapid IdP organisation needs to comply with to complete your annual Compliance Statement.

Federation Rules

6. SUBSCRIBER RESPONSIBILITIES

Your federation IdP is **compliant** with the following AAF Federation Rules within section 6. The Status items **highlighted in blue** are still the responsibility of the organisation.

Rule	Status
6.1.1 All and any Data, when provided to AAF Ltd or another Subscriber (as the case may be), are accurate and up-to-date and any changes to Metadata are provided promptly to the AAF Operator;	Compliant
6.1.2 It will observe Good Practice in relation to the configuration, operation and security of the System;	Compliant
6.1.5 It will observe Good Practice in relation to the exchange and processing of any Data and in obtaining and managing the domain name service (DNS) names, digital certificates and private keys used by the System;	Compliant
6.1.6 It holds and will continue to hold all necessary licences, authorisations and permissions required to meet its obligations under these Rules;	Compliant
6.1.7 It will not act in any manner which damages or is likely to damage or otherwise adversely affect the reputation of the Federation;	Compliant with the operation of the IdP on behalf of the organisation. The Organisation needs to also assert compliance.
6.1.8 It will give reasonable assistance to any other Subscriber (including to the Subscriber's identity provider) investigating misuse by an End User; and	Compliant with the operation of the IdP on behalf of the organisation. The Organisation needs to also assert compliance.

<p>6.1.9 It will keep contact information required by the Federation Operator up to date, with any changes being updated within five [5] Business Days;</p>	<p>The AAF will assist the organisation with maintaining contact information.</p>
	<p>The organisation is responsible for providing contact information within the given timeframe.</p>

The organisation **must** assert compliance for the following rules in section 6 of the AAF Federation rules.

Rule	Status
<p>6.1.3 it will promptly respond to any Operational Issue that may impact the Federation, any Subscriber or End User, Connected Systems or Data, and must notify the Federation Operator of the Operational Issue in writing within two [2] Business Days of first becoming aware of the Operational Issue, and provide regular updates in its management of the Operational Issue;</p>	<p>Organisation responsibility</p>
<p>6.1.4 it will promptly respond to any Incident that may impact the Federation, any Subscriber, End User, Connected Systems or Data, and it must notify the Federation Operator within two [2] Business Days of first becoming aware of the Incident, and provide regular updates in its management and rectification of the Incident;</p>	<p>Organisation responsibility</p>
<p>6.1.10 when acting in its capacity as a Subscriber of the Federation, it will comply with all applicable laws.</p>	<p>Organisation responsibility</p>
<p>6.2 Subscribers acknowledge that participation in the Federation does not itself grant them or any of their End Users automatic access to the Federation (which includes the Services of Service Providers), and that such access may be conditional upon each Subscriber or End User agreeing to appropriate terms with the relevant Service Provider governing that access. AAF Ltd will not be responsible for, nor have any liability in respect of, the performance or otherwise of those terms and will not be required to resolve any disputes in relation to those terms.</p>	<p>Organisation responsibility</p>
<p>6.3 The Subscriber acknowledges that AAF Ltd may, without incurring any liability to the Subscriber and without prejudice to any other rights or remedies of AAF Ltd, take such action or may require the Subscriber to take such action, as is necessary in the opinion of AAF Ltd to protect the legitimate interests of other Subscribers, the reputation of the Federation or AAF Ltd, or to ensure the efficient operation of the Federation.</p>	<p>Organisation responsibility</p>
<p>6.4 The Subscriber may use the Federation logo in accordance with the Federation logo usage rules (located on the Policies and Resources page at https://www.aaf.edu.au) as determined and updated from time to time by the AAF Ltd.</p>	<p>Organisation responsibility</p>
<p>6.5 The Subscriber grants AAF Ltd the right to:</p>	<p>Organisation responsibility</p>

6.5.1 publish the Subscriber's name and information about Services provided for the purpose of promoting the Federation; and	Organisation responsibility
6.5 The Subscriber grants AAF Ltd the right to: 6.5.2 publish and otherwise use and hold the Subscriber's Metadata for the purpose of administering the operation of the Federation.	

8. ADDITIONAL RULES FOR IDENTITY PROVIDERS

Your federation IdP is **compliant** with respect to the following AAF Federation Rules that are specific to operation of a federation IdP as listed within section 8 of the rules. The Status items **highlighted in blue** are still the responsibility of the organisation.

Rule	Status
8.1 An Identity Provider must comply with the additional rules in this clause 8.	
8.2 The Identity Provider may appoint a contractor to undertake some or all of the identity management functions of the Identity Provider. In the event that an Identity Provider appoints a contractor, the Identity Provider must ensure that the contractor complies with these Rules as if it were itself an Identity Provider. Each Identity Provider nonetheless will continue to be responsible for the performance of its functions notwithstanding that those functions may have been assigned, sub-contracted or otherwise dealt with.	Compliant The AAF is the contractor and is compliant with the AAF rules.
8.3 The Identity Providers must collect or generate the Core Attributes.	Compliant Exceptions for 2024 compliance exist for new the added core attributes samlSubjectID, samlPairwiseID and for the new values provided in eduPersonAssurance.
8.5 The Identity Provider must ensure that it complies with all Privacy Laws and clause 12 of these Rules.	
8.6 Identity Providers may only release Attributes to a Service Provider, or another Identity Provider, with the permission of the End User.	Compliant All Rapid IdP instances have user consent enabled.
8.8 Identity Providers must ensure the accuracy of information provided about End Users, and must ensure that End Users meet the requirements in accessing the Federation, and must comply with the following:	

<p>8.8.2 Where Unique Identifiers are associated with an End User, the Identity Provider must ensure that these Attribute values are not re-issued to another End User; and</p>	<p>Compliant with unique persistent identifiers generated by the Rapid IdP. This includes the auEduPersonSharedToken, eduPersonTargetedId, samlSubjectID, samlPairwiseID and the Persistent Name</p> <p>The organisation is responsible for assuring compliance with all other unique persistent identifiers. This include eduPersonPrincipalName and eduPersonOrcid.</p>
<p>8.10 The Identity Provider must ensure that sufficient logging information is retained for the period specified by the Federation Operator to be able to associate a particular End User with a given session that it has authenticated.</p>	<p>Compliant with the operation of the IdP on behalf of the organisation.</p> <p>The Organisation needs to also assert compliance.</p>
<p>8.11 The Identity Provider must make anonymised usage and log information available to the Federation Operator for the purposes of assisting the Federation Operator to troubleshoot access issues and develop aggregated/anonymised usage statistics.</p>	<p>Compliant</p>
<p>8.13 An Identity Provider must provide a mechanism for transfer of the 'auEduPersonSharedToken' Core Attribute value when an End User transfers to another Identity Provider.</p>	<p>Compliant</p>

The organisation **must** assert compliance for the following rules in section 8 of the AAF Federation rules.

Rule	Status
<p>8.4 The Identity Providers must collect or generate the Conditional Attributes.</p>	<p>Organisation responsibility</p>
<p>8.7 Each Identity Provider must have a documented process for issuing credentials that may give access to Services. This documentation must be made available to the Federation Operator upon request and the Federation Operator will encourage Identity Providers to make these procedures publicly available.</p>	<p>Organisation responsibility</p>
<p>8.8.1 Credentials of End Users who are no longer permitted by the Subscriber to access the Federation must be revoked promptly;</p>	<p>Organisation responsibility</p>
<p>8.8.3 Where an End User's status, or any other information described by the Attributes, changes, the relevant Attributes must be also changed as soon as possible.</p>	<p>Organisation responsibility</p>
<p>8.9 The Identity Provider must use reasonable endeavours to provide those End Users in respect of whom the Identity Provider</p>	<p>Organisation responsibility</p>

provides Attributes with appropriate information on how to use their credentials safely and securely.

8.12 The End User will be responsible for their acts or omissions, including abiding by any licences or other agreements, and complying with the policies set by the Identity Provider and/or the Service Provider. If an End User is subject to conflicting policies, then the more restrictive policy will apply.

Organisation responsibility

All other AAF Federation Rules

The organisation must assert compliance to all other rules not listed above. Please review all sections of the [AAF Federations Rules](#) before submitting the compliance statement for your organisation.

Services operated by the organisation

The organisation must assert compliance with all the Federation Rules for each service it operates in the AAF.

Organisation Contact Information

All **organisation contacts** are listed in the AAF CRM and will be updated before sending the DocuSign Compliance Statement. **Technical contacts** are registered for your organisation in the [Federation Registry](#). These details need to be checked and all changes and updates made in the AAF [Federation Registry](#) or reported to AAF support (support@aaf.edu.au).