Abstract:
This document defines a common set of expectations of all participant organisations to establish a baseline of trust in identity federations.

Audience:
This document is intended for those responsible for the operation of Identity Providers, Service Providers, Identity Federations and Identity Interfederations.

Table of Contents
1. Introduction 1
2. Baseline Expectations of Identity Provider Operators [IdP] 2
3. Baseline Expectations of Service Provider Operators [SP] 2
4. Baseline Expectations of Federation and Interfederation Operators [FO] 2
5. References 3

1. Introduction
This document lists the required operational behaviours of Identity Provider, Service Provider and Federation Operators to meet Identity Federation Baseline Expectations (IFBE) for a common trust framework.

Identity Federation Baseline Expectations are met by satisfying the below requirements; how those requirements are met is covered in supporting documentation [IFBE] and subject to continual trust improvements. They are not a fixed target but a long-term commitment to an improving technical and policy landscape, the process being an evolutionary journey rather than a final destination.

In these statements, the terms “Identity Provider,” “IdP,” “Service Provider,” and “SP” refer to their usage within the SAML Browser SSO profile [SAML2prof] as operational entities that act in the federation and not to the organizations that operate them.
2. Baseline Expectations of Identity Provider Operators [IdP]

- [IdP1] Your Identity Provider is operated with organizational-level authority
- [IdP2] Your Identity Provider is trusted enough to be used to access your organization’s own systems
- [IdP3] Your Identity Provider must have contact information published allowing timely response to operational issues
- [IdP4] You apply security practices to protect user information, safeguard transaction integrity, and ensure timely incident response
- [IdP5] You ensure the metadata registered in Federation is complete, accurate and up to date
- [IdP6] You support applicable and necessary automated release mechanisms of user information

3. Baseline Expectations of Service Provider Operators [SP]

- [SP1] You ensure that controls are in place to protect user privacy in the service
- [SP2] You do not share information received from Identity Providers with third parties without relevant notification and the information is stored only whilst necessary for operational purposes
- [SP3] Your Service must have contact information published allowing timely response to operational issues
- [SP4] You apply security practices to protect user information, safeguard transaction integrity, and ensure timely incident response
- [SP5] You ensure the metadata registered in Federation is complete, accurate and up to date
- [SP6] You publish requirements for any user information required to access service; ensure these requirements are appropriate and respects user privacy (unless governed by an applicable contract)

4. Baseline Expectations of Federation and Interfederation Operators [FO]

- [FO1] You focus on trustworthiness of Federation as a primary objective and be transparent about such efforts
- [FO2] Your Federation must have contact information published allowing timely response to operational issues
- [FO3] You apply security practices to federation operations and ensure timely incident response
- [FO4] You follow good practices to ensure authentic, accurate and interoperable metadata to enable secure and trustworthy federated transactions
● [FO5] You implement and support frameworks that improve trustworthy and scalable use of Federation and promote their adoption by members and other participants
● [FO6] You collaborate with other organisations to promote realization of baseline expectations nationally and internationally

5. References

● [IFBE] REFEDS Identity Federation Baseline Expectations, {Link TBD}