**justice Information sharing federation**

**Participation AGREEMENT Template**

1. **Purpose**

This agreement formally establishes the governance, responsibilities, and obligations of the participants of the [Initiative Name] Federation. The [Initiative Name] Federation is required to identify, manage, and support distributed access control and permissions among participating identity and service providers.

1. **Rationale**

Federated Identity and Privilege Management provides the ability to separate the management of user identities from the management of the systems and applications that use those identities. In a federation, user identities are managed by identity providers (IdPs) and applications and other resources are managed by service providers (SPs). Federated identity management enables reuse of user credentials in order to access information across distributed applications (i.e., single sign-on). The federation supports decentralized privilege management, or access control. This allows federation participants to establish and enforce application or system specific requirements and policies.

1. **Governance of federation**

The Parties hereby create [Initiative Name] Federation Governing Board (“Governing Board”) to create Bylaws for the operation and governance of the Federation, and to suggest changes to this Agreement for Party consideration. Each Party agrees to participate in the governance of the Federation in a meaningful manner which shall include, but not be limited to: the designation of an appropriate representative as a member of the Governing Board, regular participation in Governing Board meeting, and a good faith commitment to seek resolution of any disagreement or grievance arising from participation in the Federation through the prescribed governance process.

1. **Participation as an Identity Provider Organization**

An identity provider (IdP) is responsible for authenticating the credentials of their designated Authorized Users. Each Party must share information (claims) about the authentication of their designated Authorized Users with Service Providers (SPs) when those users attempt to access the SP’s protected resource. Generally, an IdP maintains or leverages a directory of Authorized User accounts to support authentication as well as maintenance of attributes about Authorized Users (such as job title or function, agency or unit, email address, trainings and certifications, etc.) The IdP shares user authentication and attribute information with an SP by forming standards-based “assertions” (messages containing Authorized User authentication and attribute information) and including those assertions electronically with each request for access.

A Federation Member that operates one or more IdP(s) is called an Identity Provider Organization. Any Party may participate in the Federation as an Identity Provider Organization. Such participation is subject to the consent of the Governing Board, in accordance with the provisions of the Federation’s Bylaws or other Federation policies.

When participating as an IdP, each Party agrees as follows:

1. Party will ensure that the Authorized User assertions formed by the IdP conform to the assertion requirements established in the [Integration Initiative Name]Architecture document, and that they accurately reflect the Authorized User’s information at all times. Each Party agrees that Authorized User assertions will reflect changes in Authorized User status within eight hours of the Party being notified of the status change.
2. Party will produce the Authorized User assertions that contain the minimum Authorized User attributes as determined by the Governing Board, and documented in the [Integration Initiative Name]Architecturedocument. Party will ensure that attribute values in Authorized User assertions are set in accordance with the attribute definitions established in the [Integration Initiative Name]Architecture document. The [Integration Initiative Name]Architecture document is hereby incorporated by reference into this Agreement. New versions of the [Integration Initiative Name]Architecture document are likewise incorporated by reference as of the date they are sent by the Governing Board to the Parties.
3. Party will audit IdP operations in conformance with Federation policy at a minimum, and at a frequency determined by the Federation. Scope of audit will be limited to the provisions of this section and any Federation policies related to IdP operation. Party agrees to share the material results of audits with other Federation members upon request.
4. Party, upon learning of unauthorized access, will take reasonable precautions to prevent unauthorized access to systems that maintain Authorized User information and form assertions, and, should such unauthorized access occur, will notify the other members within eight hours of the unauthorized access.
5. Party will take reasonable precautions to prevent compromise of private cryptographic keys, to effect immediate revocation of any certificates for which the private keys have been compromised, and to notify all of the other members within eight hours of learning about any such compromise.
6. Party will ensure that Authorized Users whose identities are asserted through the IdP are informed, through training, notices, policies, and other generally accepted security practices, of the importance of safeguarding authentication credentials and other security practices to include the policies published by the service provider organizations in their service provider policy documents.
7. Party will develop and adopt policies, operational standards, and technical standards established by [Integration Initiative Name]Architecture document, or as otherwise approved as acceptable by, the Federation.
8. Party will cooperate with reasonable and legitimate requests from other Federation members for assistance in Federation operations, including but not limited to investigations of Authorized User misconduct or unauthorized access and troubleshooting technical or operational issues.
9. **Participation as a Service Provider Organization**

A service provider (SP) is a technology mechanism that allows a Federation Member to provide other Federation Members with secure access to a protected resource (such as an application or dataset). The SP receives, with each request for access, information about the authenticity of the end user, which allows the SP to decide whether to grant the requested access.

A Federation Member that operates one or more SP(s) to protect its resources is called a Service Provider Organization.

Any Party may participate in the Federation as a service provider organization. Such participation is subject to the consent of the Governing Board, in accordance with the provisions of this Agreement, the Federation’s Bylaws, or other Federation policies.

When participating as a service provider organization, each Party agrees as follows:

1. Party will trust Authorized User authentication statements provided by identity providers in the Federation and will accept those authentication statements as a valid means of authenticating Authorized Users for accessing services (subject to access control restrictions).
2. Party will publish, in a manner acceptable to the Federation, a Service Provider Policy document for each service provider and protected resource. This document must, at a minimum:
   1. Designate a technical and data quality point of contact to coordinate with Authorized Users on matters involving implementation of Service Provider access and data quality.
   2. Include a description of the resource, sufficient to inform a potential end user of the data, content, or functionality available.
   3. Identify who is authorized to access the resource and under what conditions or circumstances.
   4. Include any obligations that end users must accept as a condition of accessing the information.
   5. Describe how the service provider utilizes and protects personally identifiable information (PII) of end users, including, but not limited to, retention, auditing, and destruction of data.
3. Party will provide written notification to all Federation Members as soon as reasonably possible of any change to a published Service Provider Policy document and will require timely compliance and conformance with these changes.
4. Party will take reasonable precautions to prevent compromise of private cryptographic keys, to effect immediate revocation of any certificates for which the private keys have been compromised, and to notify all members within eight hours of learning of any such compromise.
5. Party will develop and adopt all policies, operational standards, information security safeguards and controls, and technical standards required by law or as otherwise approved as acceptable by, the Federation.
6. Party will cooperate with reasonable and legitimate requests from all Federation Members for assistance in Federation operations, including, but not limited to, investigations of Authorized User or end user misconduct or unauthorized access and troubleshooting technical or operational issues.
7. Party agrees to log all user activity and all user access and share material portions of those logs with any Federation Member upon request, using a standards-based format.

As a Service Provider Organization in the Federation, Party retains full control at all times over which Authorized Users are able to access its data and protected resources. Nothing in this agreement obligates or requires a participant to share any data or resources with any other Party, Authorized User, or individual.

1. **Federation Management Responsibilities**
2. Designation of a Member to Maintain the Federation Registry. The Governing Board will designate one of the Federation Members to maintain the Federation’s Cryptographic Trust Document. That member agrees to maintain accurate, current entries in the Federation’s Cryptographic Trust Document (the formal participant registry) for all members’ IdPs and SPs.
3. Designation of a Member to Maintain a “Where Are You From” (WAYF) Service. The Governing Board will designate one of the Federation Members to stand up and maintain a WAYF service. Such member agrees that the WAYF service will be available with minimal downtime and will provide access to all IdPs in the Federation’s Cryptographic Trust Document.

1. **Assumption of Cost**

The Parties acknowledges that any costs associated with participation in the Federation that is not covered by federal funding or other external resources will be the Party’s responsibility and cost of each participating jurisdiction. Nothing contained in this Agreement shall be construed to obligate any expenditure or reservation of funds in excess or advance of appropriations, or to obligate any expenditure that is not in accordance with applicable state and federal regulations and laws.

1. **No Third Party Beneficiary**

This document shall not and is not intended to benefit or to grant any right or remedy to any person or entity that is not a party to this document.

1. **Notices**

All notices, certificates, acknowledgments, or other written communications shall be sent by the most expeditious means available. The notice shall be in writing and be deemed received and properly delivered, if duly mailed by certified or registered mail to each member at the address provided in Attachment 2, or to such other address, by written notice, designated by a member of the Federation.

1. **responsibilities**

Parties agree to adhere to the following terms and limitations on the use of the shared data:

1. The Parties shall use such information only for the purposes defined in this Agreement and permitted by state and federal law.
2. The Parties shall not further disseminate such information to any third parties, unless such dissemination is done in compliance with applicable federal and state law and for a purpose defined in this Agreement.
3. The Parties shall not disseminate any data to unauthorized users without the express written consent from the Service Provider or Identity Provider.
4. The Parties shall not disseminate any PII or other data about Authorized Users unless otherwise necessary for a purpose permitted by this Agreement without the express written consent from the Identity Provider.
5. The obligations under this Section shall survive the termination of this Agreement.
6. Except as otherwise prescribed by law, no Party has any responsibility or accountability for the use or disclosure of data made available by or to another Party after that data has been accessed or disclosed in accordance with this Agreement.
7. Each Party shall make reasonable efforts to ensure that the data it shares it was accessed and provided and is maintained in compliance with all applicable state and federal laws, regulations, and agency policies and procedures. No other promises are offered as to the quality or accuracy of the data.
8. ALL DATA AND DATA ACCESS IS PROVIDED “AS IS” AND WITHOUT ANY WARRANTY OF ANY KIND TO THE PARTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY. NO PARTY WARRANTS THAT THE DATA WILL BE ERROR-FREE, OR THAT THE ELECTRONIC NETWORK WILL BE ERROR FREE OR UNINTERRUPTED, OR THAT ERRORS WILL BE CORRECTED. ALL PARTIES HEREBY DISCLAIM ALL IMPLIED AND EXPRESS WARRANTIES, CONDITIONS AND OTHER TERMS, WHETHER STATUTORY, ARISING FROM THE COURSE OF DEALING, OR OTHERWISE, INCLUDING WITHOUT LIMITATION TERMS AS TO QUALITY, MERCHANTABILITY, FITNESS FOR PURPOSE AND NONINFRINGEMENT.
9. **POINTS OF CONTACT.**

[Provide contact information here or as attachment. Include primary contacts for IdPs, SPs and Federation Manager Organization]

1. **Dispute Resolution AND GOVERNING LAW**

## The Parties shall attempt in good faith to resolve any dispute arising out of or relating to this Agreement promptly by negotiations between representatives who have authority to settle the controversy. The Parties intend that all disputes arising under this Agreement be resolved expeditiously. Disputes under this Agreement shall be initially submitted to the Governing Board for informal resolution, failing which mediation shall be undertaken, in accordance with the Governing Board policies and procedures. If, at any point during the Dispute Resolution Process, all of the Parties to the dispute accept a proposed resolution to resolve the dispute, the Parties agree to implement the terms of the resolution within the agreed upon timeframe.

Notwithstanding the foregoing, a Party may be relieved of its obligation to participate in the Dispute Resolution Process if such Party (i) believes that the other Party’s acts or omissions create an immediate threat to the confidentiality, privacy or security of data or will cause irreparable harm to the Party or any third party, and (ii) pursues immediate relief against such other Party in a court of competent jurisdiction. The Party pursuing immediate relief must notify the Parties’ governing body of such action within twenty-four hours of filing for the relief and of the result of the action within twenty-four hours of learning of same. If the relief sought is not granted and the Party seeking such relief chooses to pursue the dispute, the Parties must then submit to the Dispute Resolution Process described herein.

1. **PUBLICITY**

Parties agree to provide notice in advance, and to receive the approval of the Governing Board, of any publicity releases in connection with the activities under this Agreement. A publicity release is defined as an act or device designed to attract public interest, specifically information with news value issued as a means of gaining public attention or support.

1. **LIMITATION OF RIGHTS**

The Parties represent and warrant that this Agreement, when duly executed and delivered, will constitute the legal, valid, and binding obligation of each Party, enforceable by each Party against the other, and subject to all provisions of law. Except as specifically stated herein, this document does not, and shall not be construed to create any other rights, substantive or procedural, enforceable at law by any person in any matter, civil or criminal.

1. **Signatures**

This Agreement may be executed in any number of counterparts, and by different parties in separate counterparts. The signed copies will together form a single Agreement. Additional Parties may be added by their full execution of a counterpart to the Agreement. The effective date of this Agreement as to any Party is the date of affixation of the final required signatory for that Party. All then-existing Parties must be notified of the pendency of additional Party counterparts prior to the additional Party’s effective date by virtue of an updated version of Attachment #2 and an executed counterpart of this Agreement. Delivery by electronic transmission of an executed counterpart of this Agreement is as effective as delivery of an original executed counterpart of this Agreement.

Signatures affixed must be sufficient to legally bind the Parties. All parties, and their respective signatories on their behalf, represent that they and their signatories have full authority to enter into this Agreement.

1. **JOINTLY DRAFTED**

This MOU shall be deemed to have been drafted by the Parties and, in the event of a dispute, shall not be construed against any Party.

END OF NUMBERED TERMS

**Signature Page(s)** [include authorized signatures for each IdP, SP and the Federation Management Organization, also include attorney and Federation Governing Board signatures if required]

**IN WITNESS WHEREOF** the parties hereto have executed this MOU, effective as to each party as of the last date affixed by each party:

This agreement has been approved for form and legal sufficiency.

|  |  |  |
| --- | --- | --- |
| [Name]  [Title]  [Department] |  | Date |
| [Name]  [Title]  [Department] |  | Date |
| [Name]  [Title]  [Department] |  | Date |
| [Name]  [Title]  [Department] |  | Date |