InCommon Federation
Operating Practices and Procedures

Effective Date: August 7, 2023

This document describes at a high level how the InCommon organization is structured and how it operates in accordance with the Limited Liability Company Agreement of InCommon ("Company Agreement") and Bylaws of the InCommon LLC ("Bylaws") to support the entire InCommon Federation ("Federation"). Specific details and logistics are left to the discretion of the InCommon Executive Director ("ED").

InCommon Federation Participants ("participants") should review this document to guide the assessment of potential risks, if any, which might be incurred by their participation in the Federation. By reviewing the policies and practices of the Federation, participants and potential participants can evaluate the level of assurance of the Federation's services to ensure trustworthy operations and determine whether they meet a participant's minimum requirements.

Please contact the InCommon office for clarification or additional information regarding this document or other Federation matters. Further information about InCommon's services may be found at http://www.incommon.org.

1. Role of the InCommon organization

The InCommon Company Agreement and Bylaws define the mission of InCommon and its Federation and the principles and governance structure under which InCommon and the Federation operates. This Federation Operating Practices and Procedures document ("FOPP") outlines the activities undertaken by InCommon on behalf of its Federation participants.

The administrative and operational functions of InCommon are carried out under the direction of the ED in accordance with the company agreement. These responsibilities include development of the Federation Participant community (including through expanding such community through peering with other federations that share the same mission as InCommon such as research and education federations in other countries (each a "Co-Federation")), processing applications, identifying and authenticating eligible organizations and their trusted officers, processing participant metadata, facilitating the exchange of metadata between participants in InCommon and participants in co-federations ("Co- Federation Participants"), overseeing the operation of InCommon service platforms, dispute resolution, termination processes, accounting and billing, and other duties as assigned by the InCommon Steering Committee or the officers of InCommon.

2. Organizational structure

2.1 Management

Responsibility for management of the business and affairs of the InCommon LLC is vested with the InCommon Steering Committee (“Steering Committee”) as described in the company agreement. Specific authority may be delegated by the Steering Committee to appointed subcommittees of the Steering Committee or the ED.

The Steering Committee approves this FOPP as an accurate reflection of InCommon Federation operations. Any change to this FOPP will be communicated to each participant administrator via email within 15 business days of the change being approved by the Steering Committee.

2.2 Committees

The Steering Committee may designate subordinate or advisory committees to make decisions, develop position papers, and/or provide advice on particular matters of importance to the Federation as outlined in the Bylaws. At least one member of the Steering Committee will participate in each advisory committee to ensure good communication between the committee and the Steering Committee. Additional membership in such committees will be defined by the Steering Committee and typically will be drawn from the Participant community. Other individuals may be asked to participate based on their particular knowledge of the subject matter. Other committees may be formed as detailed in the Bylaws. Current committees are listed on the InCommon website.

2.3 Meetings

The Steering Committee meets no less frequently than once per year, typically by conference call. Minutes are kept of the Steering Committee meetings and, except for confidential personnel or financial matters, are available to Federation participants upon request.

Advisory and other committees meet as needed, typically by conference call. Minutes need not be kept.

2.4 Offices and records

The InCommon Federation office's contact information is:

InCommon
c/o Internet2
3520 Green Court, Suite 200
Ann Arbor MI 48105

Email address: help@incommon.org
Telephone: 734-913-4259
Website: https://www.incommon.org

All records of InCommon are managed by this office.

2.5 Personnel

The InCommon company agreement minimally requires at least two officers: the ED and the secretary. Other officers may be appointed by the Steering Committee. The ED will provide guidelines and direction for the operational aspects of the Federation's support organization. Operational functions are staffed and performed by Internet2.

Internet2 hires and manages personnel who provide legal, administrative, communications, operational, and other support to the ED.

3. Policies, requirements, and standards

The Steering Committee approves all policies, requirements, and standards that apply to the InCommon support organization and its Federation participants. Current governing documents, available from the InCommon office above and on the website, include:

- Limited Liability Company Agreement of InCommon
- Bylaws of the InCommon LLC
- InCommon Federation: Federation Operating Practices and Procedures (this document)
- InCommon Federation: Participation Agreement
- InCommon Federation: Common Identity Attributes
- InCommon Metadata Registration Practices Statement
- eduGAIN Policy Framework Constitution
- InCommon Baseline Expectations for Trust in Federations
- InCommon Community Dispute Resolution Process

Additional documents, guidelines, and other papers are also available on the InCommon website.

4. Application for participation in InCommon

Organizations that wish to participate in InCommon must be eligible under the requirements defined in section 4.1. Applications must be submitted and will be processed as described in section 4.2.

4.1 Eligibility criteria

InCommon currently has three classes of Participants:

(1) Higher Education (accredited post-secondary institutions and their central offices). To qualify as a Higher Education participant, an organization must be:

- A postsecondary institution or program accredited by an institutional accreditor recognized by the U.S. Department of Education; or
- A state higher education system office or another central coordinating office which either governs or manages a collection of accredited institutions. The entity must be commissioned, established, or recognized by a local, state, or national government or must be a cooperative venture organized by and for the benefit of higher education institutions for the above purposes. Documentation substantiating these criteria may be required, and determinations will be made on a case-by-case basis.

(2) Research organizations. InCommon acknowledges that research organizations are critical partners in the research and education efforts supported by InCommon. A Research organization is defined as a lab, facility, or center related to a particular federal research agency and listed on an official publicly available government listing to InCommon's satisfaction. A Research organization may sponsor into the Federation any sponsored partner organization by a formal letter of sponsorship from the active InCommon executive contact at the research organization.

(3) Sponsored partners of any participant in the first two classes. A sponsored partner is any entity that is sponsored for participation in the Federation by a participating category 1 or category 2 organization. A sponsored partner typically provides online resources, research data, informational, or other services to the sponsoring higher education organization. A sponsorship letter must be received by InCommon from the sponsoring category 1 or category 2 participant's designated executive contact, either by email or postal mail. For details see the InCommon website.

The InCommon steering committee may choose to set eligibility criteria for additional types of organizations or may vote on the approval of any applying organization under special circumstances (see section 2.1).

Distributed university or corporate systems are expected to require independent universities or businesses to become separate participants in the InCommon Federation. Examples of such

distributed systems include statewide university systems and large conglomerate corporations where each university or business unit is authorized to commit to and enter into legal agreements on behalf of its own organizational entity. Federations and other complex membership systems will be eligible for InCommon Federation participation on a case-by-case basis.

4.2 Submitting and processing an application

Interested organizations may apply for participation by submitting an online application or by submitting a signed participation agreement for review. InCommon may request additional information concerning the nature or qualifications of the applying organization.

Eligible applicants will be accepted for participation when a signed copy of the participation agreement has been received by the InCommon office and has been countersigned by InCommon.

5. Fees

InCommon fees are established by the Steering Committee. Annual fees are invoiced, based on a calendar year from January 1 to December 31. Current fee schedules are available on the InCommon website.

6. Registration, identification, and authentication of participant's trusted officers

InCommon verifies the identity of all individuals who fill the participant's trusted roles of executive and administrator (see the InCommon website for definitions). By constructing an independently verifiable, out-of-band communication path with these officers, the registration authority establishes a sufficiently strong level of assurance that the person is who he or she declares. Details on the registration process are available on the InCommon website.

7. Registration and management of participant policies, systems, and technical components

The participant's trusted administrator will be given credentials to manage Federation participant data and requests in a secure manner.

7.1 Types of registered systems: identity providers and service providers

Within the Federation, participants may offer services as an identity provider for their respective user community, as a service provider to any participant organization's user community, or both. For instance, a higher education institution serving primarily as an identity provider might also make online information or services available to other InCommon participants or co-federations. Similarly, a sponsored partner that is primarily a provider of online services might also act as an identity provider.

Participants register identity management systems and/or service provider systems using the InCommon participant administrative interface. Higher education institutions and sponsored partners receive an initial quota for each system type and can purchase more as needed, subject to certain restrictions, as outlined in the participation agreement and fee schedule available on the InCommon website.

7.2 Relationship of systems to participant

Any identity management system or service provider system registered by a participant must be under the management hierarchy of the participant organization. The participant is responsible for the actions of any system registered with the Federation. Participants may only register third-party systems that operate services under contract to the participant and for which participant will be responsible, in accordance with the provisions of the Participation agreement. Such third party systems might, for example, include outsourced identity management services.

7.3 Required information components

7.3.1 Baseline Expectations

When participants rely on federations, they are partnering with other organizations to do something that they would otherwise do for themselves or forgo altogether, and because of this interdependency, rely on each other to mutually support a level of practice. For example, a fundamental expectation is that participants in a federation provide authoritative and accurate attribute assertions to other participants and that participants receiving an attribute assertion must protect it and respect any privacy constraints placed on it by the federation or the source of that information.

To enable some level of trust to support this interdependency, the InCommon community has identified Baseline Expectations, including separate requirements for identity providers, service providers, and the Federation. Each participant must at minimum adhere to these Baseline Expectations for the systems they support. Over time, the InCommon community will increase the requirements of Baseline Expectations to reflect strategic value to the Participants. Each stakeholder (identity provider, service provider and the Federation) is expected to support the

increased requirements within the specified period of time. The changed requirements and implementation timeframes will be made available to and vetted by the participants. Information on Baseline Expectations can be found on the InCommon website.

7.3.2 Metadata

A Participant administrator registers its Identity Provider and Service Provider systems through the participant administrative interface by describing components of its systems. The data are collected and digitally signed by InCommon. Secure, up-to-date, trusted information about all participants and their systems is a core service of the Federation. InCommon will make reasonable efforts to verify submitted data and will act in accordance with the practices outlined in the InCommon Registration Practices statement, available on the InCommon website.

InCommon collects this metadata (the technical and administrative data that describe the participating system entities and their properties, support and facilitate the Federation's policy and operational goals). It may be removed or modified by Participant Administrators through the participant administrative interface. Changes to metadata are evaluated within one Internet2 business day following the submission. Under special circumstances, participant executives or administrators may make removal requests via e-mail or telephone as listed on the InCommon website. InCommon will verify these requests using trusted communication channels before processing any removal requests.

InCommon may also collect metadata from metadata registrars of other co- Federations and make it available to participants for the purposes of furthering the mission of the Federation. Metadata may also be exchanged with other co-federations. By participating in the Federation, the participant consents to transfers of its metadata as described in this Section 7.3.2 and its Participation Agreement. Transmission of Federation metadata to participants is not initiated by InCommon. Instead, participants are expected to retrieve metadata compiled by the Federation on a regular basis.

For additional information about how InCommon uses metadata, please see the InCommon website.

7.3.2.1 X.509 Certificates in metadata

X.509 Certificates in metadata are provided by participant and are used to verify participant's message-level signature and encrypt sensitive messages intended for participant. Such certificates may be self-signed since certificate verification is provided by the secure handling and digital signing of all metadata by InCommon.

7.3.2.2 Entity attributes and categories

InCommon adds entity attributes to the Metadata of Participants that adhere to defined entity category requirements. Adherence to these may be self-asserted by the Participant or may be determined by the InCommon Registration Authority, depending on the requirements.

8. Dispute resolution procedures

In the event of any dispute or disagreement among Participants or between a Participant and InCommon arising out of or pertaining to participation in the Federation, Participants should follow the procedures below. Additional information, about the Community Dispute Resolution process below, is available on the InCommon website.

8.1 Disputes among participants in InCommon and/or other co-federations

Participants are expected to make every reasonable effort to settle disputes among themselves, especially if contractual issues among the participants are involved. If circumstances warrant, (for example, if the dispute centers on the interpretation of attribute values or the implementation of standards) InCommon may be asked to act as referee in helping the participants come to a resolution. In the case that such a dispute cannot be so resolved, the disputing participants may use InCommon's Community Dispute Resolution process, which is documented on the InCommon website. The Community Dispute Resolution process is intended to affect a resolution to disagreements among Participants regarding Federation services or the use of those services, including disputes about an entity's operation with respect to Baseline Expectations.

If an InCommon participant has a dispute with an organization in a co-federation relating to services described in this document that cannot be resolved amongst themselves, participants should follow the Community Dispute Resolution process documented on the InCommon website. InCommon will use best efforts to work with the participant, any relevant inter-federation service provider and co- federation operator on a mutually agreed-on solution.

8.2 Disputes between participant(s) and the Federation

Any participant may submit a written Notice of Dispute to the ED regarding any aspect of the operation or services supported by the Federation. The ED will make certain that sufficient information exists to define the dispute and then shall inform the chair of the steering committee. The chair will appoint a steering committee member to serve as a negotiator with the disputing participant(s).

The negotiator will gather all the facts and rationales for the dispute and, as necessary, seek advice from any Federation advisors or other relevant parties. The negotiator will prepare a written report, which shall include a recommended resolution of the dispute. The report shall

be submitted to the chair of the Steering Committee within 30 days of the appointment of the negotiator unless delayed by the required fact-finding.

The chair shall bring the report to a quorum of the Steering Committee. The Steering Committee, after reviewing the report, may ask for additional information or request the Negotiator to take into account further considerations and prepare a modified recommendation. Resolution of the dispute must be approved by the affirmative vote of a quorum of the Steering Committee as defined in the bylaws. If the Steering Committee is unable to affirm a resolution, the status quo is maintained. The ED shall report the Steering Committee's final action to the disputing participant(s) in writing as soon thereafter as is practical. If any disputing party believes it cannot accept the outcome of this process, its only recourse is to discontinue participation in the Federation as stated in the participation agreement.

9. Operations

9.1 Operational assurance level

The operation and performance of the Federation infrastructure are paramount to maintaining its trust fabric. InCommon supports certain operational services, including the secure collection and distribution of Metadata, a registration authority to identity-proof and credential Participant organizations and officers, communications and outreach, and a Help Desk. As the Federation gains more experience with federated identity and access management and as requirements for other federation services emerge, the InCommon Federation's operations will evolve to meet new functional criteria.

9.1.1 Central operations

Complete procedures were developed detailing InCommon's central operations. Information security industry standards and practices [11 Reference] were used to establish the necessary level of assurance. These operations and procedures were approved by a technical advisory group of Internet2 middleware architects. A public listing of these procedures can be found on the InCommon website.

9.1.2 Operations staff credentials and authorization

Operations staff that perform actions critical to security or trustworthiness of Federation operations or services are issued strong identity credentials, commensurate with the risk incurred by unauthorized access to such actions.

9.2 Communications and support

9.2.1 Posting material on the InCommon website

All InCommon operating documents are made accessible via the InCommon website.

9.2.2 Help desk

InCommon provides a help desk for Participant administrative and technical support. The help desk is staffed during normal Internet2 business hours as described on the InCommon website. InCommon also supports a community electronic mailing list for building community involvement and partnerships. Any end users who inadvertently contact the Federation help desk will be referred to their home organization for support in online access to other Participants.

9.2.3 Other information

Software guidelines are provided or referenced on the website, along with deployment guides, attribute policies, testing facilities, and other federation- specific information for the operation of identity providers and service providers in the Federation.

9.3 Federation Technical Infrastructure

InCommon is responsible for the secure operation of a number of technology platforms including a Shibboleth “Discovery Service” (DS) server; a metadata distribution service; a participant administrative interface; and other necessary infrastructure. Operation of the technical infrastructure is described in greater detail in the technical documents available on the InCommon website.

9.3.1 Baseline Expectations

The InCommon community has identified Baseline Expectations for the Federation Operator, which can be found on the InCommon website. InCommon Federation meets these requirements.

9.3.2 Discovery Service (DS)

The Discovery Service, an optional user interface component, is responsible for allowing users to specify their appropriate identity provider for the services they intend to use online. Upon selecting an identity provider, the user is redirected to the identity provider’s login service to authenticate. InCommon operates a redundant DS service and web page on which all identity providers are listed.

9.3.3 Metadata distribution

InCommon digitally signs and publishes metadata submitted by all Participants for the interoperation of identity provider and service provider systems. InCommon may also make a

subset of the Metadata available to peering co-federations. The metadata is maintained on redundant servers.

9.3.4 Participant Administrative Interface

Federation participant administrators use the Participant Administrative Interface to securely manage the data relevant to their organization's participation in the Federation. The particular tasks include submitting certificate signing requests, participant operating practices, and submitting or modifying participant metadata.

9.3.5 Suspension of Federation services

If InCommon suspects compromise of any of its service components, it may take immediate action to remedy the situation or verify non-compromise, including taking components out of service for a limited time for diagnosis and repair. The ED always will endeavor to minimize interruption or inconvenience to participants. Any critical compromise will be communicated to Participants in a timely manner.

9.4 Disaster recovery

InCommon disaster recovery practices ensure the minimum interruption of availability of Federation services in the event of a disaster. This includes providing redundant hardware and secure data backups. Public versions of disaster recovery practices are available on the InCommon website.

10. Participation status: renewal, withdrawal, termination, and suspension

10.1 Renewal

Renewal of participation is automatic as long as the participant remains in good standing and pays its fees in a timely manner.

10.2 Withdrawal or termination

Participant may withdraw from the Federation at any time upon written notice to the InCommon office in accordance with the Participation Agreement.

Termination by InCommon or participant is governed by the terms and conditions of the Participation Agreement.

In all cases of withdrawal or termination, the participant will be removed from the metadata.

10.3 Suspension of participants' services

10.3.1 Suspension for reasons of security

A participant may request the suspension of any Federation services in the case of administrator credential compromise, participant key compromise, or another security compromise within the participant's systems. This request may be made via e-mail or telephone from the executive or administrator and will be verified by InCommon using trusted communication channels. Suspension may include processes such as revoking credentials or removing or modifying metadata.

If InCommon suspects any compromise or negligence on the part of a participant, it will make reasonable efforts to contact participant resolve the issue. In the case of a significant security incident that poses an unacceptable risk to InCommon or other Federation participants, InCommon may take immediate remediation actions commensurate with the impact of the incident.

10.3.2 Suspension for failure to meet Baseline Expectations

If InCommon finds that a participant's entity (e.g., IdP or SP) fails to support the Baseline Expectations, InCommon will alter or remove such entity's information from the metadata to protect the trust level across the InCommon community.

11 References

[RFC 2527] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework; https://www.ietf.org/rfc/rfc2527.txt

[RFC 3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework; https://www.ietf.org/rfc/rfc3647.txt

The American Bar Association PKI Assessment Guidelines,

The Computer Security Handbook 4th edition,

Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure by Housley and Polk,

The Federal Bridge Certification Authority Certification Policy, and others.