

1. Federation Participant Information

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name *InfoEd International, Inc.*

The information below is accurate as of this date *10 November 2015*

1.2 Identity Management and/or Privacy information

Additional information about the Participant's identity management practices and/or privacy policy regarding personal information can be found on-line at the following location(s).

URL(s)

https://www.infoedglobal.com/application/files/2416/0691/6646/incommonpop_InfoEdGlobal.pdf

1.3 Contact information

The following person or office can answer questions about the Participant's identity management system or resource access management policy or practice.

Name *Roger Wood*

Title or role *Associate Vice President, Product Management*

Email address *rwood@infoedglobal.com*

Phone *518-713-4200* FAX *518-713-4201*

2. Identity Provider Information

The most critical responsibility that an IdentityProvider Participant has to the Federation is to provide trustworthy and accurate identity assertions.¹ It is important for a Service Provider to know how your *electronic identity credentials* are issued and how reliable the information associated with a given credential (or person) is.

Community

2.1 If you are an Identity Provider, how do you define the set of people who are eligible to receive an *electronic identity*? If exceptions to this definition are allowed, who must approve such an exception?

InfoEd International is a service provider only. We do not provide identity services at this time.

¹ A general note regarding attributes and recommendations within the Federation is available here: <http://www.incommonfederation.org/attributes.html>

2.2 "Member of Community"² is an assertion that might be offered to enable access to resources made available to individuals who participate in the primary mission of the university or organization. For example, this assertion might apply to anyone whose affiliation is "current student, faculty, or staff."

What subset of persons registered in your identity management system would you identify as a "Member of Community" in Shibboleth identity assertions to other InCommon Participants?

NA

Electronic Identity Credentials

2.3 Please describe in general terms the administrative process used to establish an electronic identity that results in a record for that person being created in your *electronic identity database*? Please identify the office(s) of record for this purpose. For example, "Registrar's Office for students; HR for faculty and staff."

NA

2.4 What technologies are used for your electronic identity credentials (e.g., Kerberos, userID/password, PKI, ...) that are relevant to Federation activities? If more than one type of electronic credential is issued, how is it determined who receives which type? If multiple credentials are linked, how is this managed (e.g., anyone with a Kerberos credential also can acquire a PKI credential) and recorded?

NA

2.5 If your electronic identity credentials require the use of a secret password or PIN, and there are circumstances in which that secret would be transmitted across a network without being protected by encryption (i.e., "clear text passwords" are used when accessing campus services), please identify who in your organization can discuss with any other Participant concerns that this might raise for them:

NA

2.6 If you support a "single sign-on" (SSO) or similar campus-wide system to allow a single user authentication action to serve multiple applications, and you will make use of this to authenticate people for InCommon Service Providers, please describe the key security aspects of your SSO system including whether session timeouts are enforced by the system, whether user-initiated session termination is supported, and how use with "public access sites" is protected.

NA

² "Member" is one possible value for eduPersonAffiliation as defined in the eduPerson schema. It is intended to include faculty, staff, student, and other persons with a basic set of privileges that go with membership in the university community (e.g., library privileges). "Member of Community" could be derived from other values in eduPersonAffiliation or assigned explicitly as "Member" in the electronic identity database. See <http://www.educause.edu/eduperson/>

2.7 Are your primary *electronic identifiers* for people, such as “net ID,” eduPersonPrincipalName, or eduPersonTargetedID considered to be unique for all time to the individual to whom they are assigned? If not, what is your policy for re-assignment and is there a hiatus between such reuse?

Electronic Identity Database

2.8 How is information in your electronic identity database acquired and updated? Are specific offices designated by your administration to perform this function? Are individuals allowed to update their own information on-line?

NA

2.9 What information in this database is considered “public information” and would be provided to any interested party?

NA

Uses of Your Electronic Identity Credential System

2.10 Please identify typical classes of applications for which your electronic identity credentials are used within your own organization.

NA

Attribute Assertions

Attributes are the information data elements in an attribute assertion you might make to another Federation participant concerning the identity of a person in your identity management system.

2.11 Would you consider your attribute assertions to be reliable enough to:

[NA] control access to on-line information databases licensed to your organization?

[NA] be used to purchase goods or services for your organization?

[NA] enable access to personal information such as student loan status?

Privacy Policy

Federation Participants must respect the legal and organizational privacy constraints on attribute information provided by other Participants and use it only for its intended purposes.

2.12 What restrictions do you place on the use of attribute information that you might provide to other Federation participants?

NA – We do not provide information to other Federation participants

2.13 What policies govern the use of attribute information that you might release to other Federation participants? For example, is some information subject to FERPA or HIPAA restrictions?

NA – We do not share information with other Federation participants.

3. Service Provider Information

Service Providers are trusted to ask for only the information necessary to make an appropriate access control decision, and to not misuse information provided to them by Identity Providers. Service Providers must describe the basis on which access to resources is managed and their practices with respect to attribute information they receive from other Participants.

3.1 What attribute information about an individual do you require in order to manage access to resources you make available to other Participants? Describe separately for each service ProviderID that you have registered.

InfoEd requires the user's unique institutional identifier and as well as their given name, surname, and email address.

3.2 What use do you make of attribute information that you receive in addition to basic access control decisions? For example, do you aggregate session access records or records of specific information accessed based on attribute information, or make attribute information available to partner organizations, etc.?

We use attribute information solely to authenticate users and provide access to subscribed services. Limited session data are tracked for diagnostic and support purposes. We do not aggregate session data, share attribute information with other organizations, nor use attribute data for marketing or other purposes. A separate unique ID is created for each user and that local unique ID is used for all data tracking within InfoEd systems.

3.3 What human and technical controls are in place on access to and use of attribute information that might refer to only one specific person (i.e., personally identifiable information)? For example, is this information encrypted?

All data are SSL encrypted during transmission. Data are stored on servers with 24-hour access control and video surveillance among other protections. User account information can be accessed by the user and his/her institutionally authorized administrators as well as authorized InfoEd staff as necessary to provide support. Users control all other personal data stored and determine which of their data is publicly searchable and which is not. Non-public data can only be accessed by the user him/herself or by authorized InfoEd staff providing support.

3.4 Describe the human and technical controls that are in place on the management of super-user and other privileged accounts that might have the authority to grant access to personally identifiable information?

Only select, authorized InfoEd staff are granted permission to access user data on an as needed basis to perform maintenance and provide support. Access is limited to authenticated users. InfoEd follows defined SOPs for creating, managing, and terminating user access based on employment, training and assigned duties.

3.5 If personally identifiable information is compromised, what actions do you take to notify potentially affected individuals?

In the event of a security breach, notice would be provided to administrators and key contacts at all affected parties in accordance with relevant state security breach notification laws (<http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>).

4. Other Information

4.1 Technical Standards, Versions and Interoperability

Identify the version of Internet2 Shibboleth code release that you are using or, if not using the standard Shibboleth code, what version(s) of the SAML and SOAP and any other relevant standards you have implemented for this purpose.

InfoEd is uses Shibboleth 2.6.x for InCommon authentication.

4.2 Other Considerations

Are there any other considerations or information that you wish to make known to other Federation participants with whom you might interoperate? For example, are there concerns about the use of clear text passwords or responsibilities in case of a security breach involving identity information you may have provided?

None.

