Federation Participant Information

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name: University of Denver

The information below is accurate as of this date: 08/16/2016

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): http://www.du.edu/uts/policies/confidentiality.html
http://www.du.edu/registrar/privacy/index.html http://www.du.edu/uts/policies/application-access.html

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: Will Bass
Title or role: Director, Computer Operations
Email address: will.bass@du.edu
Phone: 303-871-3722 FAX

2. Identity Provider Information

The most critical responsibility that an IdentityProvider Participant has to the Federation is to provide trustworthy and accurate identity assertions. 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?
Electronic identities are created for admitted students, former students, faculty, staff, vendors, donors, University Advancement friends, corporate sponsors, and special community members via the University’s ERP system (Banner).

2.2 "Member of Community" 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?

Any person identified in the university’s ERP as active staff, faculty, or special community member.

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."

Electronic identities are established as a result of data being entered into the ERP. This data is the result of normal business process in the following departments:

Registrar’s Office for current and former students;
Human Resources for faculty, staff, and special community members;
Admissions Services for admitted students;
Purchasing and Accounts Receivable for vendors;
University Advancement for Donors, Friends, and Corporations that contribute to the University.

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?

UsedID/Password key pairs via either LDAP or Kerberos.

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:

All UsedID/Password key pairs are encrypted before transmission.
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.

Our SSO only supports internal applications at this time. If / when this changes our documentation will be updated accordingly.

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 identifiers in our environment are unique for all time.

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?

User information is acquired and updated in the University’s enterprise business system (Banner). Individuals are only allowed to alter their personal information (home address, phone number) online. Individuals are not allowed to alter University provided credentials (login name, ID Number, e-mail address). Name changes require administrative assistance and cannot be done by individuals.

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

DU has designated certain information as directory information in order to disclose information on a student without violating FERPA. While directory information may be disclosed, DU will only share directory information to perform institutional functions.

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.

Most online applications other than Banner utilize the university’s electronic identity credentials. These applications include library services, parking services, learning management, HR management, web content management, and Office365.

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:

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

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

[X] 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?

We only pass directory information and our expectation is that any information we release would only be used for the stated purpose of the application and not be passed to other parties or used for additional purposes.

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?

We do not release any data to any federation that is covered under HIPAA or FERPA.

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 resource ProviderID that you have registered.

None. We have no plans to be a service provider at this time.

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.?

None

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?

N/A

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?

N/A

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

N/A

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.

Shibboleth 3.1.2

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?

We have no other considerations or information to share.