1. Federation Participant Information

1.1 – The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name – **University of Northern Colorado**
The information below is accurate as of this date – **1/17/13**
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 online at:

http://www.unco.edu/generalcounsel/privacy.htm

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: **UNC Technical Support Center**
Title: **Technical Support Center**
Email address: **Technical.Support@unco.edu**
Phone: **970.351.4357**
FAX: **970.351.1650**

2. Identity Provider Information

The most critical responsibility that an Identity Provider Participant has to the Federation is to provide trustworthy and accurate identity assertions. It is important for a Resource 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?
Our account creation information is available at http://help.unco.edu select the group in question on the left and navigate to Account Access.

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?
In addition to students, faculty, emeritus and employees, we may issue credentials to individuals whose affiliation to the College is contractual rather than as an employee or student. However, these individuals will not be granted access to federated services.

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."

Students receive their employee ID and account once they confirm admission. Employees receive tehri Employee ID and Account once they entered into the ERP system by the HR Department. Registrar's Office for students, HR Office for Employees.

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?

UserID/Password in LDAP

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:

Contact the Technical Support Center, and they will contact an Information Security Analyst to assist.

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.

ADFS will be used for campus SSO to federated services.

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?

All IDs are unique to each individual and are not reused.

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 online?

Only individuals from our IT staff (and in our systems group) can modify the electronic identity database, or automated processes they code. Individuals can request updates and modify a very small set of attributes (phone, address).

2.9 – What information in this database is considered "public information" and would be provided to any interested party?
We intend only to release attributes that are required by specific Service Providers

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.
Web applications
Network File Storage
Network Access (wired and wireless)

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:

control access to on-line information databases licensed to your organization? – **YES**
be used to purchase goods or services for your organization? – **YES**
enable access to personal information such as student loan status? – **YES**

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 don't plan on placing restrictions on the use of these attributes by federated partners. We do not intend to provide attributes if they require restrictions.

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 have a privacy statement available at: http://www.unco.edu/generalcounsel/privacy.htm.
This policy would also apply to the data in our Identity Management Database. We also do store some information that would be subject to FERPA regulations, but no data in our IdM database would relate to HIPPA.

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.
We currently do not have services that we will be presenting to Federation Participants.

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 currently do not have services that we will be presenting to Federation Participants.

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?
We currently do not have services that we will be presenting to Federation Participants.

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?
We currently do not have services that we will be presenting to Federation Participants.

3.5 – If personally identifiable information is compromised, what actions do you take to notify potentially affected individuals?
We will contact the individual(s).

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.
Both SAML 1.1 and 2.0.

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?
N/A