http://www.colorado.edu/avcit/incommon

InCommon Federation

Participation in the InCommon Federation ("Federation") enables a federation participating organization ("Participant") to use Shibboleth *identity attribute* sharing technologies to manage access to on-line resources that can be made available to the InCommon community. One goal of the Federation is to develop, over time, community standards for such cooperating organizations to ensure that shared *attribute assertions* are sufficiently robust and trustworthy to manage access to important protected resources. As the community of trust evolves, the Federation expects that participants eventually should be able to trust each other's *identity management systems* and resource *access management systems* as they trust their own.

A fundamental expectation of Participants is that they provide authoritative and accurate attribute assertions to other Participants and that Participants receiving an attribute assertion protect it and respect privacy constraints placed on it by the Federation or the source of that information. In furtherance of this goal, InCommon requires that each Participant make available to other Participants certain basic information about any identity management system, including the identity attributes that are supported, or resource access management system registered for use within the Federation.

Two criteria for trustworthy attribute assertions by *Identity Providers* are: (1) that the identity management system fall under the purview of the organization's executive or business management, and (2) the system for issuing end-user credentials (e.g., PKI certificates, userids/passwords, Kerberos principals, etc.) specifically have in place appropriate risk management measures (e.g., *authentication* and *authorization* standards, security practices, risk assessment, change management controls, audit trails, etc.).

InCommon expects that *Service Providers*, who receive attribute assertions from another Participant, respect the other Participant's policies, rules, and standards regarding the protection and use of that data. Furthermore, such information should be used only for the purposes for which it was provided. InCommon strongly discourages the sharing of that data with third parties, or aggregation of it for marketing purposes without the explicit permission[1] of the identity information providing Participant.

InCommon requires Participants to make available to all other Participants answers to the questions below.[2] Additional information to help answer each question is available in the next section of this document. There is also a glossary at the end of this document that defines terms shown in italics.

1. Federation Participant Information

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name: University of Colorado Boulder

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):

· Links to University of Colorado administrative policies, University of Colorado Boulder (UCB) policies, guidelines, and campus-wide IT policies http://oit.colorado.edu/policies

· The UCB campus privacy policy http://www.colorado.edu/privacy

· Acceptable use policyhttp://www.colorado.edu/policies/cnr/index.html

· FERPA related policies managed by the UCB campus Registrar http://registrar.colorado.edu/regulations/regulations.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: Kerry Havens

Title or role Program Manager for Identity and Access Management

Email address Kerry.Havens@colorado.edu

Phone 303-735-5682 FAX 303-492-7939

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.[3] 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?

The documenthttp://avcit.colorado.edu/sites/avcit.colorado.edu/files/page_uploads/accessauthor.pdf describes the Access and Authorization policies established by the campus for the Identity

Provider, the Office of Information Technology (OIT). Campus password policy as identified in this policy is weaker than the policy actually imposed for the campus login that is relevant to the Identity Provider. The campus login account (Identikey) password follows the requirements described at http://oit.colorado.edu/node/2006. Regular faculty, staff and students are granted access based on their inclusion in the enterprise student information system or HRMS system. Campus exceptions are typically granted "affiliate" roles based on authorized requests from campus payroll and faculty liaisons, organizational administrative offices, or officers of the university.

2.2 "Member of Community"[4]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 through an Enterprise Source System (Our Human Resources and Student Information Systems) that has a long term service or customer expectation (Faculty, Staff, Student) is a "Member of Community." Additionally, any person with a long term relationship identified as a "Member" (pre-employment appointees, confirmed students not yet enrolled, long term volunteers and contractors) are also treated as members and are eligible for many campus online 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 theoffice(s) of record for this purpose. For example, "Registrar's Office for students; HR for faculty and staff."

Accounts are created and updated at least daily, downstream of the enterprise source system(s) records and are dependent on the creation controls in those source systems. Student identities are granted to persons identified in the Integrated Student Information System (ISIS) and control decisions for that system are relegated to the university Registrars. Employee identities are downstream from records in the university human resource system (HRMS) and are subject to the controls instituted by university Human Resources officials. See campus policy athttp://avcit.colorado.edu/sites/avcit.colorado.edu/files/page_uploads/accessauthor.pdfand university administrative policies and IT policies at https://www.cu.edu/policies/index.html. Some historical policies reference a Self-Account Creation service for students that is no longer supported. Campus specific administrative policies can be found here:http://www.colorado.edu/policies/.

Campus exceptions are occasionally made by direct sponsorship to the campus identity "registry" for cases where there is no identified source system, there is an issue of access timeliness, or there is a new or underdeveloped process. These sponsorships may be to any

affiliation but require authorization from a party otherwise authorized to create source system records such as a human resources liaison, or officer. Typical rationale for exceptions includes faculty appointments that are not yet on payroll systems or access for instructor grading processes that may extend past payroll calendars. Sponsorships are typically to “affiliate” and occasionally “member” affiliations.

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 and Passwords are managed by our campus Identity Manager (IdM) application. Passwords are replicated in Kerberos, LDAP, and Active Directory environments.

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:

Campus IT policy requires encrypted authentication. See section 2.5 of the following policy document: http://www.colorado.edu/its/docs/policies/Minimum_System%20Requirements-2007.pdf

Questions pertaining to campus security policy can be directed to the IT Security Office at security@colorado.edu

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.

Shibboleth is used for campus SSO in a limited capacity. Shibboleth is the only SSO system provided by the campus that will be used to support InCommon Service Providers. Session timeouts are enforced at the Shibboleth IDP level. User logouts are handled only at the Service Provider level and client level and are not propagated back to the IDP.

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?

We utilize a unique user ID (UUID) construct. It is never subject to 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?

Campus identity updates are daily feeds from the enterprise administrative source systems. Employees and Students are able to utilize self-service to modify personal information such as addresses, email selections, and other aspects of their record that may be upstream of the campus identity system and may in turn create changes to their records. They may claim accounts or change passwords through self-service mechanisms that match to security questions or enterprise source private data. IT support staff are required to fix problems or change records downstream from university source systems.

Apart from OIT escalated support and service center, two campus offices (the campus Identity Card function and the Continuing Education Registrar) are typically allowed to create "sponsored" entries for staff and students in order to support housing selection, assignment to certain campus identity card based services, or non-credit and out-of-term course enrollment. The account creation options are limited, restricted to affiliate and member types, and have expiration of either three weeks or one year.

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

We comply with all university and campus privacy regulations and restrictions. Additionally, students can elect privacy or semi-privacy that restricts the publication of additional FERPA directory information. See the FERPA and Private Data Security policies athttp://registrar.colorado.edu/regulations/ferpa_guide.htmlandhttp://www.colorado.edu/its/docs/policies/Requirements_for_Private_Data_Systems_2007.pdf.

Otherwise we will release the common attributes identified athttp://www.incommonfederation.org/attributesummary.htmlto InCommon members or participating SPs. Release of any additional "public information" attributes will be handled on a per service provider basis.

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.

Campus and University Student and Employee Portals

Network Access (Wired, Wireless, and VPN, Secure Web Access, DHCP Registration)

Email and Web Applications

Software Downloads

Student Web File Access and Online Storage

Learning Management System Access

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:

[Yes] 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?

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 require both federation and non-federation partners to agree to abide by the policies of the InCommon federation. We do not require all service providers to be InCommon members, but they must agree to treat any attributes according to the policies and guidelines published by InCommon.

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 information counter to campus FERPA policies athttp://registrar.colorado.edu/regulations/ferpa_guide.html.

· We will release data attributes only as appropriate per university data privacy and security policies such ashttps://www.cu.edu/policies/aps/it/6005.html.

· Applicable university policies can be accessed at https://www.cu.edu/policies/aps-it.html.

· Campus policies can be viewed at http://www.colorado.edu/policies/.

· The campus privacy statement is here http://www.colorado.edu/privacy/.

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.

Presently (when published) the University of Colorado at Boulder has no registered service providers. Typically we will require no more (or some subset of) the attributes posted at http://www.incommonfederation.org/attributesummary.html. We will provide pertinent details when we register a service provider that does not conform to this expectation. We expect to have varying requirements depending on organizational affiliation of the service provider. We expect to classify service providers as campus, university, and InCommon providers initially.

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.?

Attributes received from federated partners are only stored and used by the service application that requests the attributes. They are used to provide access by authenticated users and to keep settings and preferences for returning users, depending on the application. We never release any received attribute information to any third parties. Any future campus service provider will be required to abide by this attribute policy.

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?

Resources where user attributes are stored are accessible to only a small number of operational personnel and are monitored for both access and changes. Access to the attributes themselves is restricted to authenticated queries from known systems, and any transmission of attributes occurs via secure channels.

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?

Organizational standards for privileged access ("Information Security Standard for Trusted Campus Authentication") are published

athttps://www.cu.edu/articles/upload/Information%20Security%20Standard%20for%20Trusted%20Campus%20Authenitcation.pdf. The standard addresses expected procedures for privileged users (e.g. system and network administrators, security administrators, maintainers, and system programmers) including such things as account management, access enforcement, user identification and authentication, identifier management, and authenticator management, amongst others. Reference this and additional user responsibility and security standards at the reference above for current policy details.

The university is continuously updating security standards and is developing further clarification specifically addressing individuals with privileged access. Current draft standards include considerations for such things as minimization and control of "root" or "admin" accounts, training for individuals with privileged access, password controls, logging standards, confidentiality precautions, expected personnel procedures, and oversight authority. Links to relevant policies will appear as they are approved at the OIT policies page and its sub-pages at http://oit.colorado.edu/policies.

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

The campus data breach process states that in the event that PII is compromised a data breach team will be formed by the CIO. The team will include the CIO, IT Security, Legal, Chancellor Chief of Staff, CUPD, and University Communications. Depending on the type of data compromised Registrar, HR or Treasury may be included. Potentially affected individuals will be contacted generally via US Postal Service mail. In the event that an incident is very small a department may choose to contact individuals via phone. In all cases individuals are also provided a phone number to reach the department responsible for the incident.

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.

The University of Colorado Boulder operates the current version of Shibboleth.

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?

Campus service providers are required to adhere to the same policies addressed in this document. Other service providers that are not part of the University of Colorado will not be

provided with attributes that would constitute a security breach concern and are reminded of their responsibility to adhere to applicable privacy and security regulations as part of their service agreement. Any exceptions to this standard will be accompanied by signed agreements and/or non-disclosure agreements appropriate to the attribute release.

IT Security

The Office of Information Technology

Office of the Associate Vice Chancellor for IT and Chief Information Officer

IT Service Center: 303-735-4357 (5-HELP) or help@colorado.edu
Monday - Thursday 7:00 a.m. - 10:00 p.m.
Friday 7:00 a.m. - 7:00 p.m.
Saturday & Sunday 12:00 noon - 6:00 p.m.
*Closed during University Holidays.