InCommon Participant Operational Practices (POP)

Federation Participant Information

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name: Loyola Marymount University

The information below is accurate as of this date: June 1, 2018

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): _____

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: Sylvester Creado

Title or role Manager Identity and Software Solutions

Email address Sylvester.Creado@lmu.edu

Phone 310-338-7895 FAX 310-338-2326

Identity Provider Information

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?

An electronic identity is created for

1. Applicants, admitted applicants, and students with sufficient data entered into the University's Student Information System.
2. Faculty and staff entered into the University's Human Resources Information System
3. Contractors and other accounts entered into University's Identity Management System by Helpdesk

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?

Anyone identified in the university ERPs as current faculty, staff, student, or contractor.

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."

Normal business processes in the following offices result in the ERP data entry that establishes an electronic identity.
HR for faculty, staff;
Admissions Services for admitted applicants;
Registrar's Office for current and former students.
Helpdesk for auxiliary staff

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?

Kerberos, userID/Password-applies to all users.

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:

No. Passwords are not transmitted unencrypted.

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.

We currently support CAS/Shibboleth SSO solution. The session timeouts are enforced by both the Service Provider and Identity Provider.

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?

Yes, they 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?

The information is acquired and updated through automated programming from the University's enterprise systems. Individuals cannot update their information online without approval from the Registrar or HR.

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

The information is considered directory but not public as individuals may suppress selected, or all, items in the information from pure public view. Information will not be passed to just any interested party unless they are an approved member of an approved federation.

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 (purchased and in-house) other than the Student Information System and HR Systems utilize the university's electronic identity credentials. These applications include the learning management system, the web content management system, and the private online directory.

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 but expect that the information would not be 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?

Attribute information that LMU currently releases to other Federation participants is not governed by any policies such as 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.

LMU has no service Providers. Hence 3.1 to 3.5 below are not applicable

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.

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.?

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?

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?

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

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.

IDP version 3.3.x.

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