Attachment C-3

Service Provider Registration

This form is to be completed for each Service Provider and will be included with the CSUconnect Federation Member Certification of Compliance on file

Date 4/8/2019

Service Provider Name ScholarWorks

Service URLs https://ds.calstate.edu/?svc=scholarworks

InCommon Entity ID* https://scholarworks.calstate.edu/shibboleth

SAML Version Supported (SAML 1.1) (SAML2 X)

Hosting Campus & Facility California State University, Office of the Chancellor

Administrative Contact Name & Title David Walker, Director of Systemwide Digital Library Services

Administrative Contact Email dwalker@calstate.edu Telephone Number 562-355-4845

Technical Contact Name & Title Kevin Cloud, Digital Repository Services Manager

Technical Contact Email kcloud@calstate.edu Telephone Number

Help Desk Number and/or Email library@calstate.edu

Service Providers are trusted to request only the information necessary to make an appropriate access control decision and use it in accordance with what is described within this document. Service Providers must describe how resource access and attribute information from CSUconnect Federation participants will be managed, and are responsible for updating and resubmitting this document if any responses change.

Please provide responses to the following questions:

1. Describe the services or resources that will be provided, and to whom they will be made available?

   ScholarWorks is the system-wide institutional repository service for the CSU libraries. Participating campuses deposit electronic theses, dissertations, faculty publications, data sets, and other approved research materials into ScholarWorks to both preserve that scholarly output and to make it available to interested researchers from around the world. CSU faculty, students, and staff will authenticate in order to upload materials to ScholarWorks.

2. Describe the process that a prospective organization must follow to gain access to the services or resources for their users.

User must have a valid, active account at a CSU campus. New accounts are automatically provisioned at login time using attributes asserted to the SP. Authorization to upload is granted by respective campus institutional repository administrator.

3. What attribute information is required to manage access to the services or resources? Please provide the response in the table below. **

Attribute Name	SAML Name	Acceptable Values	# of Values	Use	Stored
calstateEduPersonOrg	urn:oid:1.3.6.1.4.1.10396.2.1.1.15	See CSU Attributes Standards in CSYOU	Single	User Profile	Y
eduPersonPrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	See the eduPerson object class definition	Single	User Profile	Y
eduPersonAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.1	See the eduPerson object class definition	Multi	User Profile; Authorization	Y
mail	urn:oid:0.9.2342.19200300.100.1.3	See CSU Attributes Standards in CSYOU	Single	User Profile; user notifications	Y
givenName	urn:oid:2.5.4.42	See CSU Attributes Standards in CSYOU	Single	User Profile	Y
sn	urn:oid:2.5.4.4	See CSU Attributes Standards in CSYOU	Single	User Profile	Y

4. What optional attribute information is accepted by the service provider? Please list the response in the table below. **

Attribute Name	SAML Name	Acceptable Values	# of Values	Use	Stored
(none)					

5. How will attribute information you receive be used beyond basic access control decisions?

Identifiers and attributes are relayed to ScholarWorks by campus IdP release policy. The attribute information, once securely received, is used by ScholarWorks for authentication and authorization. Email address will be used as the principle way the system alerts users who upload materials to status changes with their submission as it is approved or handled by repository administrators.

6. If attribute information will be stored, how long will it be retained, and what measures will be taken to protect it? If the approach varies based on some factor (e.g. level of assurance or affiliation), please explain for each.

   ScholarWorks will store attribute information indefinitely to maintain author profiles.

7. What levels of assurance are required of an electronic credential to use the services or resources? Please explain the differences between what is provided to each level. ***

   Existing processes used by CSU campuses to assign identities to employees and students are acceptable.

8. What security measures are in place to protect privileged accounts? ****

   Privileged accounts are limited to those used by Chancellor's Office Systemwide Digital Library Services staff.

9. Do any of the services or resources contain security level 1 or level 2 data? If so, will the service log and retain access information in compliance with the CSU System-wide Information Security Policy?

   No.

10. If any of the services or resources are compromised, what actions will be taken to notify potentially affected individuals? Please clarify any differences that may exist if more than one service or resource is protected.

    Any exposure or breach of data associated with this service shall be handled in accordance with existing CSU Information Security Policies in the 8000 section of the Integrated California State University Administrative Manual (ICSUAM).

11. What steps have been taken to ensure Section 508 compliance? If there are any known limitations, are there alternative approaches that are recommended to use those services or resources?

    ScholarWorks is an implementation of the open source Samvera Hyrax system. That application has undergone extensive accessibility review and work. Additionally, the Chancellor's Office and the CSU Libraries have a task force currently undertaking a formal accessibility review, creation of a VPAT, and roadmap for improvements, if necessary.

Notes:

* The InCommon EntityID is equivalent to the Shibboleth SP ProviderID.

** If you are the service owner, please work with the campus identity management team or the Chancellor's Office (iamadmin@calstate.edu) to identify the appropriate attributes and values. For each attribute, you will need to explain how it will be used and why it is needed, as well as if you will be storing the values passed from an identity provider.

*** See NIST standards documentation for an explanation of different levels of assurance: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

******** A **Privileged Account** is an account with rights or permissions that enable a user to access sensitive data, control system or network infrastructure configurations, manage users or other system and network resources, or manage applications, file systems, and other IT systems. Examples of privileged accounts include root, administrator, or “super user”; administrator-level or system-level access.