CSU The California State University
OFFICE OF THE CHANCELLOR

CSUconnect Federation Standards and Procedures

CSU System-wide Identity and Access Management (IAM) Infrastructure

The California State University
Office of the Chancellor
March 19, 2008

http://its.calstate.edu/iam/

Table of Contents

Appendices

I. PURPOSE AND SCOPE

The purpose of this document is to define the standards, procedures and practices that all participants agree to as members of the California State University *CSUconnect* Federation, hereinafter referred to as the Federation. These standards, procedures and practices are necessary to support a unified identity and access management infrastructure across the CSU System that enables authorized campus individuals to use their local campus digital identity credentials to gain access, as appropriate, to resources and services throughout the System through adherence to a common set of standards, identity attributes, data and data definitions, and identity management practices. Roles, responsibilities and requirements for all participants in the Federation are outlined in this document. Refer to *Appendix A: Definition of Terms* for clarification on terminology in this document.

II. ROLES AND RESPONSIBILITIES

Responsibility for participation in the Federation lies with Identity Providers, Service Providers, and Campus Users across the California State University System. The following outlines the roles and responsibilities of these members.

A. Identity Providers

Access

- *Timeliness* of information in the enterprise directory.
- *Availability* of the network-based services that provide access to information in the enterprise directory.

Security

- *Audit logs* that enable investigation of security incidents and misrepresentation of identity and that comply, at a minimum, to requirements outlined in the *CSU Retention Policy* (Executive Order 1031) and with the *CSU Information Security Policy*.
- *Accuracy of the binding* of campus users to information in the enterprise directory and level of assurance asserted when identity has been properly vetted. Refer to *Appendix B: Levels of Assurance* for full definitions of all levels.

Privacy

- *Privacy* of information in the enterprise directory requires a registration process by which Service Providers are authorized to utilize identity information.

Support

- *Education* about standards and best practices for the campus' Service Provider and campus users in the use and protection of identity information.
- *Help desk function* for campus users to resolve issues.
- *Technical support contact* for Service Providers and Federation Administration.
- *Troubleshoot problems* by sharing log information with Service Providers when issues occur.
- *Publish and maintain* identity management documentation as required by the *CSUconnect* Federation.

Identity Providers must act in conformance with their stated service and assurance levels so that Service Providers may meet their policy, legal, and fiduciary requirements. As part of the membership requirements for the Federation, Identity Providers must provide documentation describing their compliance with these responsibilities. The Federation Administration, Chancellor's Office CSU-IAM Program office, maintains a repository of this information.

Failure to demonstrate ongoing compliance with *CSUconnect's* standards, practices and requirements in all material respects that is not resolved in a timely manner will result in removal of that participant from *CSUconnect.*

Refer to Appendix C*: CSUconnect Federation Member Certification of Compliance* for all required documentation and signatures that must be provided by the Identity Provider.

B. Service Providers - Service Providers are responsible for the secure operation of their application services. With respect to their use of identity information, they are responsible for:

- *Awareness of Identity Providers' service levels* When a sufficient service level is not available from the Identity Provider, the Service Provider may need to implement its own identity management services in order to meet its service's security requirements.
- *Audit logs that enable investigation* into security incidents related to information provided by Identity Providers including any retention requirements that are defined in the *CSU Information Security Policy*.
- *Compliance with Identity Provider's standards and recommended practices* for use and protection of identity information.
- *Technical support contact* for inquiries from Identity Providers and the Federation Administration.
- *Adequate protection of* sensitive identity information received from Identity Providers as well as sensitive information that may be provided to the user to meet policy and legal requirements.

Refer to A*ppendix C: CSUconnect Federation Member Certification of Compliance* for all required documentation and signatures that must be provided by the Service Provider.

C. Campus Users – Campus Users are responsible for protection of the electronic credentials provided to them by the Identity Provider. In particular, they are each individually responsible for:

- *Assurance* that their electronic credentials are not knowingly provided to or obtained by other people.
- *Compliance with Identity Providers' standards and recommended practices* for use and protection of identity information.

III. REQUIREMENTS

A. General

1. Each Identity Provider and Service Provider within the Federation must be capable of exchanging attribute information with other members' Identity Providers and Service Providers through the use of standardized protocols, formats, and software required by the Federation and InCommon. This will typically be accomplished through the implementation of Internet2 *Shibboleth*® software.

2. All CSU campuses must be members of InCommon prior to becoming members of the *CSUconnect* Federation. Requirements for InCommon membership can be found at http://www.incommonfederation.org.

3. The Federation maintains an additional set of common identity attributes that are required for participation in the Federation. These attributes are maintained in the calstateEduPerson specification located at https://connect.calstate.edu/sites/TAG. This list contains accepted attribute assertions of identity information to be used across the Federation, including data format and supporting definitions (and the URN that uniquely names the attribute). Rules for governing release and use of all attributes are also provided within the specification.

4. The Federation implements different levels of assurance as outlined in Appendix B.

B. Identity Providers

1. Authentication practices, attribute release, and application services must be operated according to the requirements in the *CSU Information Security Policy*.

2. If campus identities exist that have not been verified according to current Federation requirements, those identities must be re-verified prior to those individuals' use of Federation services.

3. If secret identity credentials, such as passwords, are transmitted during authentication, encryption that sufficiently meets State of California (*Information Practices Act, California Civil Code §1798, et seq.)* privacy requirements to protect the privacy of that exchange and the information it protects must be used.

4. In order to provide interoperability with Service Providers, specific attributes identified in the calstateEduPerson specification must be implemented and available.

5. There is no identity proofing requirement at assurance level 1. The authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data.

6. Identity providers must verify level 2 assurance and above through well-documented practices.

7. When a campus is prepared to provide electronic credentials for level 2 assurance, the user requesting level 2 assurance shall be approved based on the *Electronic Authentication Guideline* published by the *National Institute of Standards and Technology (NIST)* (see Appendix B)*.*

8. The registration process must include provisions to avoid the use of secret identity credentials that can be easily guessed or reverse engineered.

9. If single sign-on technology is utilized to alleviate the need for a user to provide independent credentials for each application separately, session timeouts as appropriate must be implemented to mitigate the risk presented by unattended workstations and devices being used by unauthorized people.

10. Identity Providers must publish and maintain information in a format accessible to participating Service Providers and include the following:

- Description of each attribute assertion of identity information that is available to the Federation, including data format and the URN that uniquely names the attribute.

- Rules for governing release and use of attributes.

- Description of the identification process that the campus uses to manage the repository of identity information for the campus community, linking an individual with their equivalent electronic identity and electronic credential (e.g., password, etc.).

- Description of the registration process used to issue electronic credentials.

- Description of authentication technologies used to perform actions within the Federation. This includes cases where multi-factor authentication is used.

- Description of the maintenance procedure used to ensure that identity information is current and synchronized with repositories of record, especially as it relates to de-provisioning and revocation of permissions.

- Service level statement covering at the minimum, the expected availability, responsiveness, security, timeliness and accuracy of information, and retention of logging of the identity credentials system.

11. Identity Providers must provide a help desk function and associated contact information for problem resolution related to identity management and authentication.

12. The Federation requirements for identifying *level of assurance* are present and available when requested in any assertion process including a Shibboleth transaction.

C. Service Providers

1. Applications that utilize the Federation must be compliant with all university policies regarding privacy, security, and application development.

2. Service Providers are responsible for the security of their services. They must implement any additional authentication measures required for the criticality or sensitivity of the application or the data accessed by the user.

3. Service Providers must address appropriate accessibility concerns related to Section 508 compliance prior to registration with the Federation Administration.

4. Service Providers must provide a help desk function and associated contact information for problem resolution related to the application services.

It is anticipated that higher levels of assurance will be implemented for the Federation in the future. Those higher levels of assurance will include different sets of requirements for Identity and Service Providers.

IV. FEDERATION ADMINISTRATION

Administration of the Federation will be done by the Chancellor's Office Identity and Access Management program office within Technology Infrastructure Services. Federation Administration will:

- Facilitate participation by assisting campuses in completing all required documentation
- Maintain information on:
  - Member Certifications
  - Service description requirements
  - Descriptions of calstateEduPerson attributes
  - Technical support contact information for all Identity Providers and Service Providers

The Chancellor’s Office will collect and maintain copies of the CSU campus’ InCommon Federation Participation Agreements, Participant Operational Practices and required *CSUconnect* Federation documents. The Participant Operational Practices will be posted on the IAM site. CSU policies and procedures developed by the Chancellor’s Office and campuses for the Federation will be documented and distributed by Identity and Access Management (IAM) staff.

Appendix A: Definition of Terms

Attribute A single piece of information associated with an electronic identity database record (e.g., name, phone number, group affiliation [faculty, staff, and student], etc.)

Audit An independent review and examination of a member's records and activities to determine the adequacy of system controls to ensure compliance with established processes and procedures, and to recommend needed changes.

Audit logs Computer files containing details of amendments including review of system activity, identification of the user ID that performed an action and to allow access to records in the event of system recovery.

CalstateEduPerson An LDAP object class authored and promoted by the CSU Directories Working Group in 2001 and further reviewed and updated by the CSU-IAM TAG Working Group in 2006. It is based on the EDUCAUSE/Internet2 eduPerson object class that is focused on the attributes of individuals.

Campus users Campus users are the individuals who have officially established an affiliation with a campus. They are the individuals who use the Service Providers' services and whose electronic identity is managed by Identity Providers.

CSUconnect Federation Administration The Administration of the CSU Federation is managed by the CSU-IAM Program Office at the Chancellor's Office.

Credentials Service Provider A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers.

Enterprise directory The campus' repository of information about the users in the campus community. It is generally composed of an LDAP directory and a person registry.

Federation A federation is an association of organizations that come together to exchange information as appropriate about their users and resources in order to enable collaborations and transactions.

Federation Administration Federation Administration is managed by the Chancellor's Office CSU-IAM Program office.

Identity credential An electronic identifier and corresponding personal secret associated with an electronic identity (e.g., user ID and password). An identity credential typically is issued to the person who is the subject of the information to enable that person to gain access to applications or other resources that need to control such access.

Identity Providers Identity Providers are the campus organizational units that manage electronic identity information and provide identity information and authentication services for their campuses/sites. Identity Providers are responsible for the identification, registration, and authentication processes that bind specific campus users to the information about those members in the enterprise directory.

InCommon federation InCommon is a formal federation of organizations focused on creating a common framework for trust in support of research and education. The primary purpose of the InCommon federation is to facilitate collaboration through the sharing of protected network-accessible resources by means of an agreed-upon common trust fabric. InCommon participation is separate from membership in Internet2.

Level of Assurance A level of assurance describes the policies and practices that have been applied to a particular identity assertion. This level of assurance can be used by Service Providers to determine their confidence in the identity information they received.

Lightweight Directory Access Protocol (LDAP) An IETF standard for directory services.

Metadata Data about data or information known about an object in order to provide access to the object. Usually includes information about intellectual content, digital representation data, and security or rights management information.

Multi-Factor Authentication An authentication protocol that requires multiple methods of establishing identity such as something you know and something you have or something you are. A common example is a bank card. The debit card is the physical item that one has and the personal identification number is the data that one knows that uniquely goes with the card.

Participant Operational Practices (POP) Required InCommon form in which each participant outlines its Identity Management and/or Service system(s). Service Providers will use the POP to determine their level of trust for assertions from each participant.

Service Providers Service Providers are the organizational units that manage electronic information resources, applications and services that have been registered with *CSUconnect* Federation.

Shibboleth® Open source software developed by Internet2 to enable the sharing of web resources that are subject to access controls such as user IDs and passwords. Shibboleth leverages institutional sign-on and directory systems to work among organizations by locally authenticating users and then passing information about them to the resource site to enable that site to make an informed authorization decision.

Shibboleth Identity Provider (IdP) The originating location (e.g., campus) for a user in the Shibboleth® software implementation. For InCommon, an IdP is a campus or other organization that manages and operates an identity management system and offers information about members of its community to other InCommon participants.

Appendix B: Levels of Assurance

Levels of Assurance for in-person verification are presented as outlined in the *Electronic Authentication Guideline published by the National Institute of Standards and Technology (NIST)*.

Level 1 – Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data. It allows a wide range of available authentication technologies to be employed and allows any of the token methods of Levels 2, 3, or 4. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.

Plaintext passwords or secrets are not transmitted across a network at Level 1. However this level does not require cryptographic methods that block offline attacks by an eavesdropper. For example, simple password challenge-response protocols are allowed. In many cases an eavesdropper, having intercepted such a protocol exchange, will be able to find the password with a straightforward dictionary attack.

At level 1, long-term shared authentication secrets may be revealed to verifiers. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties, or are obtained directly from a trusted party via a secure authentication protocol.

Level 2 – Level 2 provides single factor remote network authentication. At level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2. It allows any of the token methods of Levels 3 or 4, as well as passwords and PINs. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay, and on-line guessing attacks are prevented.

Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated by the Credentials Service Provider (CSP); however, session shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are required. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties, or are obtained directly from a trusted party via a secure authentication protocol.

Level 2	**In-Person**	**Remote**
Basis for issuing credentials	Possession of a valid, current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport)	Possession of a valid Government ID (e.g. a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of either number.
Registration Authority actions	Inspects photo-ID, compare picture to applicant, record ID number, address and DoB. If ID appears valid and photo matches applicant then: a) If ID confirms address of record, authorizes or issue credentials and send notice to address of record, or;	• Inspects both ID number and account number supplied by applicant. Verifies information provided by applicant including ID number or account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address other personal information in records

	b) If ID does not confirm address of record, issue credentials in a manner that confirms address of record.	are on balance consistent with the application and sufficient to identify a unique individual. • Address confirmation and notification: a) Sends notice to an address of record confirmed in the records check or; b) Issues credentials in a manner that confirms the address of record supplied by the applicant; or c) Issues credential in a manner that confirms the ability of the applicant to receive telephone communications or email address associated with the applicant in records.

Level 3 – Level 3 provides multi-factor remote network authentication. At this level, identity proofing procedures require verification of identifying materials and information. Level 3 authentication is based on proof of possession of a key or a one-time password though a cryptographic protocol. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. A minimum of two authentication factors is required. Three kinds of tokens may be used: “soft” cryptographic tokens, “hard” cryptographic tokens and “one-time password” device tokens.

Level 3	**In-Person**	**Remote**
Basis for issuing credentials	Possession of a valid, current primary Government Picture ID that contains applicant’s picture, and either address of record or nationality (e.g. driver’s license or passport)	Possession of a valid Government ID (e.g. a driver’s license or passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of both numbers.
Registration Authority actions	Inspects photo-ID, and verify via the issuing government agency or through credit bureaus or similar databases. Confirms that: name, DoB, address and other personal information in record are consistent with the application. Compare picture to applicant, record ID number, address and DoB. If ID is valid and photo matches applicant then: a) If ID confirms address of record, authorizes or issue credentials and send notice to address of record, or; b) If ID does not confirm address of record, issue credentials in a manner	Verifies information provided by applicant including ID number and account number through record checks either with applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. Address confirmation: a) Issue credentials in a manner that confirms the address of record supplied by the applicant; or b) Issue credentials in a manner that

	that confirms address of record.	confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.

Level 4 – Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to level 3 except that only "hard" cryptographic tokens are allowed, FIPS 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and since FIPS 140-2 requires operator authentication at Level 2 and higher, this level ensures good, two factor remote authentication.

Level 4 requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant prove through secure authentication protocol that he or she controls the token. The protocol threats including eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks are prevented. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credential Service Provider (CSP), however session shared secrets may be provided to independent verifiers by the CSP. Strong approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.

Level 4	**In-Person**	**Remote**
Basis for issuing credentials	In-person appearance and verification of two independent ID documents or accounts, meeting the requirements of Level 3 (in-person and remote), one of which must be current primary Government picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport), and a new recording of a biometric of the applicant at the time of application.	Not Applicable
Registration Authority actions	*Primary Photo ID:* Inspects photo-ID, and verify via the issuing government agency, compare picture to applicant, record ID number, address and DoB.	Not Applicable

	Secondary Government ID or financial account: a) Inspects photo-ID and if apparently valid, compare picture to applicant, record ID number, address and DoB, or; b) Verifies financial account number supplied by the applicant through record checks or though credit bureaus or similar databases, and confirms that: name, DoB, address other personal information in records are on balance consistent with the application and sufficient to identify a unique and sufficient to identify a unique individual. *Record Current Biometric* Record a current biometric (e.g. photograph or fingerprints to ensure that applicant cannot repudiate application. *Confirm Address* Issue credentials in a manner that confirms address of record.	

Appendix C: *CSUconnect* Federation Member Certification

Each of the California State University campuses that have joined InCommon shall become participants in *CSUconnect*. Participants join *CSUconnect* by registering their Identity Providers and Service Providers with the *CSUconnect* Federation Administration managed by the CSU-IAM Program office at the Chancellor's Office.

Certification of compliance requires completion and submission of the *CSUconnect Member Certification of Compliance* form, Attachment C1. The Identity Provider or Service Provider should follow these steps to register a new Identity Provider or Service Provider within *CSUconnect*:

a. The campus' CIO/ITAC representative and the Identity Provider or Service Provider shall jointly certify ongoing compliance with the *CSUconnect* standards, practices and requirements set forth in this document. The Identity Provider or Service Provider further attest continued compliance in all material respects with such standards, practices and requirements, as they may be amended, and the requirements of any other documents governing *CSUconnect* that may be adopted in the future, at all times while a participant is in *CSUconnect*.

b. The campus' CIO/ITAC representative shall submit documentation of compliance with the Minimum Requirements identified in this Service Description to the *CSUconnect* Federation Administration for integration into *CSUconnect* Federation's documentation and technical infrastructure.

Failure to demonstrate ongoing compliance with *CSUconnect's* standards, practices and requirements in all material respects that is not resolved in a timely manner will result in removal of that participant from *CSUconnect.*

It should be noted that it may be appropriate for multiple participants to share an Identity Provider when there is a close affinity among those participants with regard to community and/or identity management. For example, a campus and its auxiliary have many users in common; implementing separate Identity Providers could cause confusion for people who belong to both communities. Also, a campus and its auxiliary may share a common enterprise directory.

Attachment C-1

CSUconnect Federation Member Certification of Compliance

Send all copies to:

To: Carol Kiliany, IAM Program Manager
Technology Infrastructure Services
CSUconnect Federation Administration
California State University, Office of the Chancellor
401 Golden Shore, 3rd Floor
Long Beach, CA 90802-4210
FAX: (562) 951-4925

The undersigned certify that ______________________________________complies with the standards, practices and requirements as described in the *CSUconnect* Federation, Standards and Procedures, System-wide Identity and Access Management (IAM) Infrastructure.

The undersigned acknowledges that compliance with the standards, practices and requirements of *CSUconnect* Federation, as they may be amended, is subject to periodic inspection and audit. Failure to demonstrate ongoing compliance with such standards, practices and requirements in all material respects that is not resolved in a timely manner will result in the revocation of the provider's participation in *CSUconnect* Federation.

The following information is included in this certification:

- Completed copy of the *InCommon Federation: Participant Operational Practices* statement that is needed for joining InCommon
- Completed Compliance with Identity Provider Responsibilities (Attachment C2)
- If registering a Service Provider, a completed Compliance with Service Provider Responsibilities (Attachment C3)

____

Signature and Title, Identity Provider *Date*

____

Signature, Campus Chief Information Officer *Date*

____

Signature, Chancellor's Office, Sr. Director, Technology Infrastructure Services *Date*

Attachment C-2

Compliance with Identity Provider Responsibilities

This form is to be included with the *CSUconnect* Federation Member Certification of Compliance

________New

________Updated

CSU Campus____

InCommon Provider ID ____

Administrative Contact Name & Title____

Administrative Contact Email___________________________________ Telephone Number________________

Technical Contact Name & Title____

Technical Contact Email_______________________________________ Telephone Number________________

Help Desk Number____

Identity Providers are the campus organizational units that manage electronic identity information and provide identity information and authentication services for their campus sites.

Please provide responses to the following questions:

1. Please indicate below what level(s) of assurance you will be certifying for campus users and provide information how it will be achieved on your campus.
2. Describe each attribute assertion of identity information that is available to the federation including data format, the URN that uniquely names the attribute and the rules governing the use and release of attributes.
3. Describe the identification process that is used to manage the repository of identity information that links an individual with the equivalent identity and electronic credential.
4. Outline the registration process used to issue electronic credentials.
5. List the authentication technologies used to perform actions within the Federation and include specific cases wherein multi-factor authentication will be used.

6. Provide a detailed account of the maintenance procedures used to ensure that identity information is current and synchronized with repositories of record and how it relates to de-provisioning and revocation of permissions.

7. Describe the level of service that will be provided to the Federation including availability, responsiveness, security, timeliness, accuracy of information and retention of logging of the identity credentials system.

The undersigned certifies that ***name of Campus Identity Provider*** complies with the standards, practices and requirements as described in the *CSUconnect* Federation, Standards and Procedures, System-wide Identity and Access Management (IAM) Infrastructure.

____

Printed Name and Title of person responsible for above information

____

Signature Date

Attachment C-3

Compliance with Service Provider Responsibilities

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

________New

________Updated

Resource Name____

CSU Campus/Facility____

InCommon Provider ID____

IP Host Name ____

Administrative Contact Name & Title____

Administrative Contact Email___________________________________ Telephone Number________________

Technical Contact Name & Title____

Technical Contact Email_______________________________________ Telephone Number________________

Help Desk Number____

Service Providers are trusted to ask 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 by which access to resources is managed and their practices with respect to attribute information they receive from *CSUconnect* Federation participants.

Please provide responses to the following questions:

1. Please describe the service or resource that will be provided, and to whom it will be made available?
2. What attribute information about an individual is required to manage access to this service or resource?
3. How will attribute information that you receive, in addition to basic access control decisions, be used? 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.?

4. What are the levels of assurance required of an electronic credential to use this service or resource, and what differences are provided based on each level?

5. Will attribute information be stored? If yes, what will be stored, how long will it be retained, and what measures will be taken to protect it?

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

7. If the service or resource is compromised, what actions will be taken to notify potentially affected individuals?

The undersigned certifies that ***name of Campus Service Provider*** complies with the standards, practices and requirements as described in the *CSUconnect* Federation, Standards and Procedures, System-wide Identity and Access Management (IAM) Infrastructure.

Printed Name and Title of person responsible for above information

Signature Date