Vendor Management Standard

Effective Date: July 28, 2015

1.0 INTRODUCTION

Third party vendors or contractors that provide support for campus information systems are in some cases provided access to university assets including sensitive or confidential data. Vendors and contractors may represent a critical risk to the confidentiality, integrity, and availability of university systems and data. CSU Policy requires that vendors comply with university information security policies and standards, and that appropriate contract language exists to enforce compliance. This standard is intended to provide requirements for the management of third party vendor access to university resources and data.

2.0 POLICY AND STANDARDS REFERENCES

Implements: CSU Access Control Policy ICSUAM 8060
Policy Reference: http://www.calstate.edu/icsuam/sections/8000/8060.0.shtml

Implements: CSU Access Control Standard ICSUAM 8060.S000
Policy Reference: http://www.calstate.edu/icsuam/sections/8000/8060.0.shtml

Implements: CSU Remote Access to CSU Resources Standard ICSUAM 8045.S302
Policy Reference: http://www.calstate.edu/icsuam/sections/8045/8045.0.shtml

Implements: CSUC Account Management Standard
Standard Reference: http://www.csuchico.edu/isec/documents/account-management-standard.pdf

Implements: CSU Managing Third Parties Policy ICSUAM 8040
Policy Reference: http://www.calstate.edu/icsuam/sections/8000/8040.0.shtml

Implements: CSU Identity Management Policy ICSUAM 7000
Policy Reference: http://www.calstate.edu/icsuam/sections/8000/8060.0.shtml

3.0 SCOPE

This standard applies to all university, university auxiliary, or centers that enter into contracts or agreements with vendors and consultants for purposes of providing access to university data, university systems, or any university asset connected to the university network.

4.0 ROLES AND RESPONSIBILITIES

Role	Responsibility
Campus Sponsor	The campus sponsor is responsible for completion of the Vendor Access Form. The campus sponsor is responsible for ensuring that a current contract with the campus and vendor is on file with Procurement. A copy of the current contract should be provided with the confidentiality form.
IT Support Services (ITSS)	ITSS is responsible for AD and LDAP account creation, and for the issuance of one time passwords to vendors using approved contact information.
Vendor Point of Contact	The vendor point of contact is responsible for communication between the campus and any vendor employees or subcontractors to ensure that required identity validation has occurred, and that employment or responsibility changes are conveyed to the university in a timely manner.
Information Security (ISEC)	ISEC is responsible for reviewing all new vendor accounts to verify that account requirements have been met prior to access. ISEC also performs periodic reviews of vendor accounts.
Network Operations (NOPS)	Network Operations is responsible for creating Special VPN roles that limit access by vendors to only those services that they are authorized to access.
Vendor/Consultant	Vendors/Consultants are responsible for compliance with CSU and campus information security policies, standards, and requirements.
Procurement and Contract Services	CSU, Chico Procurement and Contracts Services is responsible for contractual negotiations and renewals which are conducted through the IT Procurement Review (ITPR) process to identify required contract language. Signed and completed contracts that have completed the ITPR process should be provided to IRES to complete the ITPR process.

5.0 DEFINITIONS

Term	Definition
Account	A combination of a unique username and password or other authentication combination, which allows access to a system or service.
Administrative Account	An account that has a purpose related to administration of a specific system. Typically has privileged access.
Credentials	A combination of a unique username and password or other authentication combination, which allows access to a system or service.
ITPR	Information Technology Procurement Review
NIST Level of Assurance (LOA)	NIST Special Publication 800-63-2 "Electronic Authentication Guideline" is a technical document that provides guidance regarding requirements for Level of Assurance (LOA).
Level 2 Assurance	Identity proofing requirements for Level 2 assurance are listed in Table 3 on Page 33 of NIST 800-63-2. This table can also be found in the appendix of this document.
NAC	Network Access Control
Supplemental Provisions	Supplemental Provisions to General Provisions for IT Procurement
Vendor Contact	An individual identified in the contract as responsible for identifying and certifying the identity of local or remote vendors (individuals).
VPN Special Role	A network restriction configured in the campus VPN to limit access to a specific system or list of systems that a vendor is authorized to access.
VPN	Virtual Private Network

6.0 VENDOR REMOTE ACCESS REQUIREMENTS

Access to campus information systems and protected information must include a process for documenting appropriate authorization by the appropriate Data Owner and departmental appropriate administrator.

- Accounts may only be issued to individual vendors and credentials must not be shared without a written exception by the Information Security Office.
- Access must be reauthorized at least annually
- A valid contract which includes appropriate contract language must be provided prior to vendor access
- A signed confidentiality form must be submitted (and entire form must be returned) to the Information Security Office (ISEC) prior to access being granted.
- All vendor access must be limited to specific systems through the use of VPN Special Roles.
- It is the responsibility of the vendor contact and the campus sponsor to notify the campus when a change to the employment status or responsibilities of a vendor occurs which should result in the termination of access by a vendor.

Requirements for remote access to university systems and networks can be found in 8045.S302 Remote Access to CSU Resources.

7.0 REMOTE COMPUTER SECURITY REQUIREMENTS

Remote computers connecting to campus information assets must meet campus security requirements:

1. **Network Access Control (NAC):** The campus VPN system requires the installation of VPN client and NAC client software. Information on using the Chico VPN can be found at http://www.csuchico.edu/vpn. Chico NAC information is available at http://www.csuchico.edu/nac.

2. **NAC requirements:** The campus NAC enforces the following requirements:
    a. Anti-virus software must be installed, must be configured for updates, and must be configured to perform on-access scanning.
    b. Only vendor supported Operating Systems may connect remotely to the campus network. Operating Systems that are no longer vendor supported for security patches may not access the campus network.

8.0 PROCEDURE DOCUMENTATION

All groups supporting accounts must develop and document account management practices based on the principles set forth in these standards. Documented procedures must exist for account issuance, password changes, suspension and removal, and annual review.

9.0 Remote Vendor/3rd Party Identity Validation

Vendors or 3td parties with access to CSU Level 1 protected data must have identity validation performed in accordance with NIST Identity Proofing for Level of Assurance (LOA) 2.

It is the responsibility of the vendor contact to perform identity validation in compliance with NIST 800-63-2 Level of Assurance 2 as detailed below.

Vendor contacts will provide individual vendor/3rd party contact information to the Information Security Office for those individuals that have been verified to NIST LOA 2.

Appendix

Identity Proofing Requirements by Assurance Level (Level 2)

Taken from NIST 800-63-2

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 of record (e.g., driver's license or Passport).	Possession of a valid current government ID14 (e.g., a driver's license or Passport) number and a financial or utility account number (e.g. checking account, savings account, utility account, loan or credit card, or tax ID) confirmed via records of either the government ID or account number. Note that confirmation of the financial or utility account may require supplemental information from the applicant.

10.0 Documentation Review & Approval

Date	Audience	Action	Version
4/24/2009	Information Security Officer	Approved	V1.0
4/24/2009	Chief Information Officer	Approved	V1.0
5/11/2015	Policies and Standards Group	Reviewed / Recommended	V2.0
7/21/2015	Information Technology Executive Committee (ITEC)	Approved	V2.0