User Access Controls and Risk Management for Decentralized Systems	Standard No ITS-2011-S	Rev A
	Owner IT Security and Compliance	
	Approved by Sheryl Okuno, Director IT Security and Compliance	
	Issued 3-10-11	Revised 2-9-17 (Interim)
		Page 1 of 11

Table of Contents

1 Purpose

Cal State LA is required by CSU information security policy, standards and audit requirements to have proper security access controls in place for decentralized campus systems and to ensure that access controls are consistently implemented and enforced. This standard was created to ensure that constituents are aware of information security audit requirements, responsibilities and reporting necessary to maintain proper security access controls.

2 Related California State University Policies and Standards

The following documents of the latest issue in effect represent the criteria against which University information security audits shall be based and shall apply to the extent specified herein. Standards provide detailed supporting and compliance information for policies.

ID/Control #	Description	Title
8015.0	**Policy**	**Organizing Information Security**
8015.S000	Standard	Information Security Roles and Responsibilities
8020.0	**Policy**	**Information Security Risk Management**
8020.S000	Standard	Information Security Risk Management – Exception Standard
8020.S001	Standard	Information Security Risk Management – Risk Assessment Standard
8045.0	**Policy**	**Information Technology Security**
8045.S200	Standard	Malicious Software Protection
8050.0	**Policy**	**Configuration Management**
8050.S100	Standard	Configuration Management – Common Workstation Standard
8050.S200	Standard	Configuration Management – High-Risk/Critical Workstation Standard
8060.0	**Policy**	**Access Control**
8060.S000	Standard	Access Control

In support of the CSU policies and standards, the University publishes **standards** (define the minimum requirements necessary to meet CSU policy) and **user guidelines** (provide general recommendations and instructions for users to comply with the policy). These supporting documents are available on the IT Security website under the policy title noted above.

3 Entities Affected by this Standard

This standard applies to all system administrators, data owners and data stewards at Cal State LA and University Auxiliary Services who: a) install, manage, secure, maintain or permit shared access to any equipment defined as a departmental or divisional decentralized system; and b) review, approve, establish and terminate user access to departmental or divisional decentralized systems. This standard also applies to all individuals responsible for the ongoing risk assessment, review and reporting of periodic access control audits.

4 Definitions

a) Access Controls: The ability to permit or deny the use of a particular resource by a particular entity, generally by administering permissions or access rights to specific users or groups of users. These permission or access rights control the user's ability to view or make changes to the contents of the system.

b) Data Owner: Person identified by law, contract or policy with responsibility for granting access to and ensuring appropriate controls are in place to protect information assets. The duties include, but are not limited to, classifying, defining controls, authorizing access, monitoring compliance with CSU security policies and campus standards and guidelines, and identifying the level of acceptable risk for the information asset. A data owner is usually a member of management, in charge of a specific business unit and is ultimately responsible for the protection and use of information within that unit.

c) Data Steward: An individual who is responsible for the maintenance and protection of the data. The duties include, but are not limited to, performing regular backups of the data, implementing security mechanisms, periodically validating the integrity of the data, restoring data from backup media and fulfilling the requirements specified in CSU security policies and University standards and guidelines.

d) Decentralized System: Any data system or equipment containing data deemed private or confidential, or which contains mission-critical data, including departmental, divisional and other ancillary system or equipment that is not managed by central ITS.

e) Department Administrator: Management Personnel Plan (MPP) employee who serves in a leadership role within a unit, department or division. Department administrators generally have a combination of decision making roles including, but not limited to, financial or budgetary, procurement, personnel, project management, user account approval and signatory authority.

f) Information Assets: Information systems, data and network resources, including automated files and databases that contain Levels 1 and 2 Confidential Data.

g) Level 1 Confidential Data: Confidential data is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Its unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in severe damage to the CSU, its students, employees or customers. Financial loss, damage to the CSU's reputation and legal action could occur if data is lost, stolen, unlawfully shared or otherwise compromised. Level 1 data is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information.

Disclosure of Level 1 data to persons outside of the University is governed by specific standards and controls designed to protect the information. Confidential information must be interpreted in combination with all information contained on the computer or electronic storage device to determine whether a violation has occurred.

h) Level 2 Internal Use Data: Internal use data is information that must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights or make legal action necessary. Non-directory educational information may not be released except under certain prescribed conditions.

i) Protected Data: An all-encompassing term that includes any information defined herein as confidential, personal, proprietary, health insurance or medical information. See Level 1 Confidential Data and Level 2 Internal Use Data.

j) Risk Assessment: A process by which quantitatively or qualitatively, risks are identified and the impacts of those risks are determined. The initial step of risk management.

k) Risk Management: A structured process that identifies risks, prioritizes them and then manages them to appropriate and reasonable levels.

l) Separated Employee: Any faculty or staff who severs employment with the University by choice, mutual agreement, end of temporary appointment or non-renewed, automatic resignation (i.e., AWOL), is non-retained or is dismissed for reasons under Education Code 89535.

m) System Administrator: Individual(s) who manage, operate, support campus information systems or manage networks. Duties generally include installation, support of operating system and application software, security, troubleshooting and training.

n) System Data Steward: The highest level of custodial review and data oversight from all functional areas within the respective steward's sphere of responsibility. This person approves or denies access to their respective systems through account privileges. An individual who has management responsibilities (e.g., planning, policy, etc.) for defined segments of the University data as it relates to their functional operations.

o) Vulnerability Assessment: The process of identifying and quantifying vulnerabilities in a system.

5 Standards

Cal State LA must maintain approved security controls and procedures that meet the CSU Information Security Policy and Chancellor's Office audit requirements.

5.1 Access Control

As outlined in CSU Information Security Policy, Section 8060.0, access to University information assets containing Levels 1 and 2 Confidential Data must include a process for documenting appropriate approvals before access or privileges are granted.

5.1.1 Department Access Control Standards

Key department access control requirements include, but are not limited to:

- The department administrator or system data owner must have a formal business process that defines user access requirements.
- Departments must retain documented user access forms and be prepared to provide the forms to CSU auditors during routine information security audits if requested to do so.
- The access procedure must include both physical (e.g., secured location, environmental conditions, etc.) and logical (e.g., system security, transmissions standards, communications ports, roles, etc.) access controls.
- The roles for user access must be defined and documented (e.g., in a position description).
- Requests for access must be reviewed and approved by the department administrator who is knowledgeable of the applicant's job duties.
- Users should be granted the lowest level of access necessary to perform job duties.
- Access for employees whose job requirements no longer require access to the decentralized system must be removed immediately. The access modification or removal date must be recorded on the user's access request form.

5.1.2 System Administrator Access Control Standards

Key system administrator access control requirements include, but are not limited to:

- The system administrator establishing the user access to the decentralized system cannot be the access form reviewer or approver.
- Each system administrator must have a unique user id that identifies the administrator, (i.e., sysadmin1, sysadmin2 are unacceptable user ids; tjones, robertm are acceptable user ids).
- Each user must have a unique user id. It is recommended that user ids match the *myCSULA Identity* user id, if the decentralized system support this.
- System administrators may not share system administrator rights or log any individuals onto the decentralized system who are not approved by their department administrator to have those rights or access.
- Passwords stored on the decentralized system must be protected and not stored in clear text.
- Remote diagnostic ports, if used, must be secured and restricted.
- If the decentralized system operates on an internal subnet, ITS assigns the subnet to the appropriate VLAN and ensures there is proper firewall protection from the internet.
- The decentralized system must be physically secured with physical access limited to only authorized system administrators and department administrators.
- System backups of the protected data must be physically secured (e.g., in a locked cabinet or stored at a reputable off-site backup storage facility).
- System data and files containing protected data must be encrypted.

5.1.3 User Access Control Standards

Key user access control requirements include, but are not limited to:

- For documentation purposes, users must complete a user access request form to request access to the decentralized system.
- Users may not request access privileges beyond those required to perform the duties of their position description.
- Users must have a signed Confidentiality Agreement and an Access and Compliance form on file with Human Resources Management.
- Users must meet all University standards for password security as outlined in *ITS-2008-S Password Standards* available at http://www.calstatela.edu/its/policies.
- Users must not share passwords or log any individuals onto the decentralized system who are not authorized to access the system.

5.2 Configuration Management

As outlined in CSU Information Security Policy, Section 8050.0, the University must develop, implement and document configuration standards to ensure that information technology systems, network resources and applications are appropriately secured to protect confidentiality, integrity and availability.

5.3 Information Technology Security

As outlined in CSU Information Security Policy, Section 8045.0, the University must take reasonable steps to manage and monitor information technology security, including protecting information assets from malicious software, and managing network security, remote access and mobile devices. Decentralized systems managed by Information Technology Services meet the requirements of this section. For non-Baseline decentralized systems, ITS works with department Information Technology Consultants (ITCs) to ensure adequate and appropriate controls are in place.

5.3.1 Malicious Software Protection

- All decentralized systems must be secured with current versions of University approved anti-malware software unless an exception is authorized by the director for IT Security and Compliance.
- Anti-malware software must:
  - Be capable of detecting, removing and protecting against malicious software, including viruses, spyware and adware.
  - Scan all data in “real time,” including both stored and incoming system data before data files ae opened and before software is executed.
  - Be capable of tracking and reporting significant actions taken by the software (e.g., deleted or quarantined malware).
  - Check for and install updates and signatures at least daily.
- Users must not bypass or turn-off malware software installed on any University decentralized system.

5.3.2 Network Management

The University network is designed and managed to ensure the confidentiality, integrity and availability of all information assets. One important step involves identifying all critical decentralized systems connected to the University network that house protected data. The IT Security and Compliance and IT Infrastructure Services units routinely perform vulnerability scans of critical servers to identify and remediate any risks that threaten the integrity of the system data. See Section 6 for more information on vulnerability assessments.

In some circumstances, the critical nature of system information assets may require network protections beyond that normally implemented. These systems may contain content such as public safety or public health data. Departments needing additional network or firewall security configurations should contact IT Infrastructure Services to request assistance.

5.3.3 Remote Access

Decentralized systems containing Levels 1 and 2 Confidential Data that are accessed remotely must require authentication or another special access process.

- All remote access to these decentralized information assets must:
  - Be authorized and authenticated by use of a unique user ID.
  - Pass through a campus-approved access control device, such as a firewall or proxy server.
  - Be made using an approved secured access tool, such as VPN tunnel.
  - Use a secure encrypted protocol for the entire session.
  - Be logged and tracked consistent with campus logging procedures.

5.3.4 Use of Mobile Devices

Departments should carefully consider the risks when permitting users to access systems containing Levels 1 and 2 Confidential Data from a University-issued mobile device. The use of personal mobile devices for such activity is discouraged. When allowing the use of mobile devices, the device should be protected with appropriate security controls, which can include, but are not limited to:

- Access control
- Screen security (e.g., password/PIN lock or pattern screen authentication)
- Encrypted wireless transmission
- File encryption is enabled
- Use of anti-malware
- Security updates are automatically installed
- Secured wireless connections
- Strong system passwords
- Two-factor authentication
- Remote disabling feature in the event the device is lost or stolen
- Personal firewall

The following conditions apply to accessing Level 1 data on a mobile device.

- Level 1 data may not be stored on a mobile device unless authorized by the appropriate University administrator and encrypted via an IT Security and Compliance-approved method.
- An inventory of University mobile devices that contain Level 1 data must be included on form I*TS-2824 Decentralized Systems Annual Review* for the annual report.
- The user, department administrator or designee must immediately report the actual or suspected loss, theft or compromise of any mobile device (including personal devices) to the director for IT Security and Compliance.

6 Information Security Risk Management

As outlined in CSU Information Security Policy, Section 8020.0, the University must develop of risk management business process that identifies, assesses and monitors risks to information assets containing Levels 1 and 2 Confidential Data.

Procedure *ITS-2016 Vulnerability Management for Servers* describes in detail the effective procedures and controls needed to maintain a high level of system and application security of servers and decentralized systems. All decentralized systems containing Levels 1 and 2 Confidential Data are required to follow these procedures.

6.1 Inventory Management

Changes in equipment inventory must be reported to Property Management. If theft or loss occurs, report it immediately to Public Safety, and complete form *ITS-2804 Lost or Stolen Computer or Electronic Storage Device Report* and submit the form to IT Security and Compliance.

6.1.1 Academic and Administrative Departments

Each University department with decentralized systems is responsible for maintaining their respective department equipment and data inventory, and reporting server or system information to the director for IT Security and Compliance as new implementations or changes to existing systems occur. All departments must be knowledgeable regarding the data contained in the decentralized system.

6.1.2 IT Security and Compliance

The director for IT Security and Compliance or authorized designee is responsible for maintaining a cumulative up-to-date inventory of all University servers and systems containing Levels 1 and 2 Confidential Data. The inventory contains information on the equipment, who manages or is responsible for the system, the information assets on the system and how the assets are protected. This inventory is validated annually through the *ITS-2824 Decentralized Systems Annual Review* process. The inventory and supporting documents may be required for submission to, or onsite review by, Board of Trustee auditors during scheduled information security audits.

6.2 Vulnerability Assessment

Based on the inventory, IT Security and Compliance is responsible for assessing risks to the University's information assets. These assessments must be based on established **severity** and **likelihood** criteria, and managed through ongoing evaluation and review activities. Every server must undergo an individual vulnerability assessment and the results of the assessment must be identified.

There are four steps involved in assessing vulnerability risk:

1. Determining the severity of a potential incident.
2. Determining the likelihood of an incident occurring.
3. Mapping the vulnerability risk.
4. Remediating the vulnerability in a timely manner reflective of the risk.

6.3 Vulnerability Scan Frequency

IT Security and Compliance is responsible for conducting ongoing vulnerability scans of all ITS-managed and decentralized servers containing Levels 1 and 2 Confidential Data.

In addition to regularly scheduled scans, by-request or as-needed requests may be issued by the director for IT Security and Compliance when circumstances are warranted (e.g., identified, reported or suspected intrusion; audit request for documentation).

- Systems are scanned weekly.
- Scans are scheduled sequentially to ensure the least amount of impact to the infrastructure.

6.4 Risk Remediation

Vulnerability reports provide ITS and department server data owners and administrators with the tools to identify and evaluate the potential risk to University information assets that may be exposed by system vulnerabilities. Proactive steps can then be taken to address the identified vulnerabilities.

Remediation management is a shared responsibility encompassing IT Security and Compliance, IT Infrastructure Services, System Administration, Network Operations, and departments and their ITCs as required. Dissemination of actionable weekly system reports and prioritization discussions are conducted at weekly vulnerability management meetings. When remediation affects departments external to ITS, ITS will communicate to the appropriate ITC(s) so they can develop a remediation plan. If necessary, the ITC(s) will be invited to attend the weekly meeting.

A complete list of current remediation responsibilities is available online in *ITS-2019-P Vulnerability Management for Servers*, Section 9, Remediation Management.

6.5 Requesting an Exception

Vulnerabilities may exist that cannot be remediated for several reasons. For example, some vendor appliances may not be patchable, along with services that may be exposed for proper application operation, or end-of-life systems may remain in operation but are no longer supported by the vendor. Exceptions must be requested through IT Security and Compliance and must include reasons for the exceptions and mitigating controls will be established in collaboration with the department.

6.5.1 Exception Request Types

Reasons for exceptions can fall under any of the following categories:

1. Compensating Controls – There is a means for mitigating the risks around the vulnerability.
2. Acceptable Use – Some use for applications might be interpreted as a vulnerability but its use may be acceptable under certain practices.
3. Acceptable Risk – Some situations pose low risk, but actions to remediate are too costly or an applications will fail if the vulnerability is remediated.
4. False Positives – If a report shows a vulnerability is a false positive, there must be some form of documentation to show that the report has been tested and verified. The exception report for a false positive must include names of individuals involved in testing, requesting and approving the exception, relevant dates and information about the testing.

6.5.2 Submitting Exception Requests

To allow for these conditions, exception requests can be submitted in writing to the director for IT Security and Compliance by the department manager responsible for the decentralized system. Exception requests are never permanent and must be reviewed periodically by the IT Security and Compliance office to prevent an approved exception being permanently ignored. All exception requests must include the following:

- The exception type *(See Section 6.5.1)*
- Justification for the request
- The expiration date

7 Contacts

a) Questions regarding this document should be directed to: ITSecurity@calstatela.edu.

b) Questions regarding compliance, audits and auditing procedures should be directed to the University internal auditor at 323-343-5105.

8 Applicable Federal and State Laws and Regulations

Federal	Title
Family Educational Rights and Privacy Act (FERPA)	**Family Educational Rights and Privacy Act (FERPA)** http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html This is a federal law that protects the privacy of student education records.
Gramm-Leach-Bliley Act 15 USC, Subchapter I, Sec. 6801-6809	**Gramm-Leach-Bliley Act** http://www.ftc.gov/privacy/glbact/glbsub1.htm This is a federal law on the disclosure of nonpublic personal information.
Health Insurance Portability & Accountability Act (HIPAA), 45 C.F.R. parts 160 & 164	**Standards for Privacy of Individually Identifiable Health Information** http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html This is a federal law that protects the privacy of health records.
State	**Title**
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	**California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that, as amended by SB 1386 (2003), AB 1298 (2007) and SB 24 (2011), provides information on safeguarding personal information, requires notification to California residents whose personal information was or is reasonably believed to have been acquired by unauthorized individuals and requires notification to the Attorney General if more than 500 California residents are involved..