Table of Contents

1 Purpose ........................................................................................................................................... 2
2 Entities Affected by this Standard ....................................................................................................... 2
3 Definitions ......................................................................................................................................... 2
4 Standards .......................................................................................................................................... 3
  4.1 Department Access Control Standards ......................................................................................... 3
  4.2 System Administrator Access Control Standards ......................................................................... 3
  4.3 User Access Control Standards .................................................................................................. 4
  4.4 Oversight Requirements ............................................................................................................... 4
    4.4.1 Quarterly Report Requirements ............................................................................................ 4
    4.4.2 Designated Responsibilities .................................................................................................. 5
  4.5 Exception Monitoring and Notification ...................................................................................... 6
    4.5.1 Non-compliance Reporting .................................................................................................. 6
    4.5.2 Requesting an Exception ..................................................................................................... 6
  4.6 Mitigation Procedures .................................................................................................................. 6
  4.7 Documentation Requirements .................................................................................................... 6
  4.8 Documentation Retention Period ................................................................................................ 6
    4.8.1 Summary of Exceptions ...................................................................................................... 6
    4.8.2 Review of Decentralized Systems Access Controls Report .................................................. 7
5 Contacts ........................................................................................................................................... 7
6 Applicable Federal and State Laws and Regulations ....................................................................... 7
7 Related Documents ......................................................................................................................... 8
1 Purpose
California State University, Los Angeles (CSULA) is required by CSU information security policy 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 the information security audit requirements, responsibilities and reporting necessary to maintain proper security access controls.

2 Entities Affected by this Standard
This standard applies to all individuals at CSULA and University Auxiliary Services who review, approve, establish and terminate user access to departmental or divisional decentralized systems. This standard also applies to all individuals responsible for the supervision, review and reporting of periodic access control audits.

3 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) 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.

c) 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.

d) 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.” Disclosure of Level 1 data to persons outside of the University is governed by specific standards and controls designed to protect the information.

e) 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.
f) **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.

g) **Separated Employee**: Any faculty or staff who severs employment with the University by choice, mutual agreement, end of temporary appointment, is non-retained or is dismissed for reasons under Education Code 89535.

h) **System Administrator**: Any employee or third-party vendor employed to maintain and operate a computer system or network. Duties generally include installation, support of operating system and application software, security, troubleshooting and training.

i) **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.

### 4 Standards

CSULA must maintain approved security controls and procedures that meet the Chancellor’s Office audit requirement to identify and correct inappropriate user access.

#### 4.1 Department Access Control Standards

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

- The department administrator or system data steward must have a formal user access request procedure.
- 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.
- 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.
- Access for separated employees must be removed immediately upon separation.

#### 4.2 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. User ids should match the user’s domain user id.
  - If the decentralized system is connected to the campus domain, the decentralized system user id would be the user’s campus domain and domain user id (e.g., nis\jdoe2).
  - If the decentralized system requires a local account, the local user id would be the local domain name and the campus domain’s user id (e.g., local\jdoe2).
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 the default setting includes a firewall 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 document storage facility).

System data and files containing protected data must be encrypted.

### 4.3 User Access Control Standards

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

- Users must apply for access to the decentralized system.
- Users must have a signed Computer Access and Compliance form on file with Human Resources Management. System users who have previously applied for a campus administrative system already have an access and compliance form on file and do not need to submit another form. Users who have not previously signed an access and compliance form can submit ITS-2823 Access and Compliance Form, available at [http://www.calstatela.edu/its/forms](http://www.calstatela.edu/its/forms).
- Users must meet all campus standards for password security as outlined in ITS-2008-S Password Standards available at [http://www.calstatela.edu/its/policies](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.

### 4.4 Oversight Requirements

Department administrators must maintain ongoing oversight of access controls to ensure that employees granted these access controls remain compliant with appropriate access.

#### 4.4.1 Quarterly Report Requirements

System data stewards or system administrators are responsible for preparing a quarterly report of system user access. Department administrators are responsible for reviewing, approving and submitting the final report to the University Internal auditor by the third week of each calendar quarter. The department must immediately remediate any user access discrepancies or errors.

The quarterly report must contain the following:

- An attached system printout of all system administrator (sys admin) ids and user ids.
- Approval by the decentralized system data steward.
- Approval by the department administrator.
### 4.4.2 Designated Responsibilities

The following identifies oversight responsibilities by role:

<table>
<thead>
<tr>
<th>Role/Title</th>
<th>Responsibility</th>
</tr>
</thead>
</table>
| Decentralized System Data Stewards  | a) Reviews account access forms in accordance with the user’s job duties when granting system access.  
                                        | b) Works with the University internal auditor to resolve non-compliant access controls or to seek an exception.  
                                        | c) Notifies employees and the department administrator when non-compliant access controls or lack of segregation of duties requires modification to or termination of access. |
| Decentralized System Administrator  | a) Establishes user access to the decentralized system and removes separated employee user access.  
                                        | b) Oversees physical and operational decentralized system security.  
                                        | c) Prepares system printout of sys admin ids and user ids for quarterly audit reports. |
| Department Administrator            | a) Retains copies of all user access applications.  
                                        | b) Conducts a quarterly review of decentralized system users to ensure that:  
                                        |   ● All decentralized system users have an approved application on file.  
                                        |   ● Unauthorized privileges have not been attained.  
                                        |   ● Separated/transferred employees have been immediately removed from system access.  
                                        | c) Submits *ITS-2824 Review of Decentralized Systems Access Controls* report quarterly to the University Internal auditor.  
                                        | d) Submits copies of corrective action plans and status reports, if requested, to the University internal auditor. |
                                        | b) Reports non-compliant findings to the vice presidents for ITS/CTO and Administration/CFO, and the appropriate divisional vice president, if applicable.  
                                        | c) Reports non-compliant findings to the appropriate system data steward.  
                                        | d) Opens corrective action cases with the department administrator when necessary. |
Role/Title | Responsibility
--- | ---
e) Works with system data stewards to develop exception requests when a non-compliance issue cannot be resolved.
f) Retains the Summary of Exceptions for a minimum of twelve months.
g) Retains the quarterly ITS-2824 Review of Decentralized Systems Access Controls reports for a minimum of five years.

### 4.5 Exception Monitoring and Notification

#### 4.5.1 Non-compliance Reporting

In the event the quarterly review or scheduled external audit report shows that the access controls are non-compliant, the University internal auditor will promptly report the issue in writing to the appropriatevice president or his/her designee and the system data steward. The non-compliance report must minimally contain the following information:

- Exact nature of the non-compliance;
- Date discovered;
- Estimate on the duration of time that the condition may have existed;
- System data steward’s explanation for why that access was provided, if known; and
- Remediation actions and estimated time required to remediate.

#### 4.5.2 Requesting an Exception

In situations where a non-compliant issue cannot be resolved, the University internal auditor will contact the decentralized system data steward to determine appropriate mitigation procedures.

### 4.6 Mitigation Procedures

In the event corrective measures are required, the University internal auditor will open a case with the department administrator to track and record the remediation.

### 4.7 Documentation Requirements

All corrective measures and the procedures taken to remediate the identified problem must be documented on the Summary of Exceptions template provided by the Chancellor’s Office. The department administrator must submit this document to the University internal auditor.

### 4.8 Documentation Retention Period

#### 4.8.1 Summary of Exceptions

Corrective measures documented in the Summary of Exceptions template and evidence of the exception and resolution process will be maintained for a minimum of twelve months by the University internal auditor.
4.8.2 Review of Decentralized Systems Access Controls Report

The quarterly review and remediation summary report will be maintained for a minimum of five years by the University internal auditor.

5 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.

6 Applicable Federal and State Laws and Regulations

<table>
<thead>
<tr>
<th>Federal</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gramm-Leach-Bliley Act</td>
<td>Gramm-Leach-Bliley Act</td>
</tr>
<tr>
<td>15 USC, Subchapter I, Sec. 6801-6809</td>
<td><a href="http://www.ftc.gov/privacy/glbact/glbsub1.htm">http://www.ftc.gov/privacy/glbact/glbsub1.htm</a></td>
</tr>
<tr>
<td></td>
<td>This is a federal law on the disclosure of nonpublic personal information.</td>
</tr>
<tr>
<td>Health Insurance Portability &amp; Accountability Act (HIPAA), 45 C.F.R. parts 160 &amp; 164</td>
<td>Standards for Privacy of Individually Identifiable Health Information</td>
</tr>
<tr>
<td></td>
<td>This is a federal law that protects the privacy of health records.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85</td>
<td>California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85</td>
</tr>
<tr>
<td></td>
<td>This is a state law that provides information on safeguarding personal information.</td>
</tr>
<tr>
<td>SB 1386</td>
<td>California Personal Information Privacy Act, SB 1386</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb1386_bill_20020926_chaptered.html">http://www.info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb1386_bill_20020926_chaptered.html</a></td>
</tr>
<tr>
<td></td>
<td>This bill modified Civil Code Section 1798.29 to require notification to individuals whose personal information is or is assumed to have been acquired by unauthorized individuals.</td>
</tr>
</tbody>
</table>
7 Related Documents

The following documents, forms and logs of the latest issue in effect shall apply to the extent specified herein.

<table>
<thead>
<tr>
<th>ID/Control #</th>
<th>Title</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITS-1014-G</td>
<td>User Guidelines for Student Administration Access</td>
<td><a href="http://www.calstatela.edu/its/policies">http://www.calstatela.edu/its/policies</a></td>
</tr>
<tr>
<td>ITS-2008-S</td>
<td>ITS Password Standards for Personal Systems</td>
<td><a href="http://www.calstatela.edu/its/policies">http://www.calstatela.edu/its/policies</a></td>
</tr>
<tr>
<td>ITS-2010-S</td>
<td>Encryption Security Standards</td>
<td><a href="http://www.calstatela.edu/its/policies">http://www.calstatela.edu/its/policies</a></td>
</tr>
<tr>
<td>ITS-2824</td>
<td>Decentralized Systems Quarterly Review</td>
<td><a href="http://www.calstatela.edu/its/forms">http://www.calstatela.edu/its/forms</a></td>
</tr>
<tr>
<td>ITS-2823</td>
<td>Access and Compliance Form</td>
<td><a href="http://www.calstatela.edu/its/forms">http://www.calstatela.edu/its/forms</a></td>
</tr>
<tr>
<td>CSU</td>
<td>The California State University Information Security Policy</td>
<td><a href="http://www.calstate.edu/icsuam/sections/8000/8000.0.shtml">http://www.calstate.edu/icsuam/sections/8000/8000.0.shtml</a></td>
</tr>
</tbody>
</table>

These guidelines define the criteria for authorized SA access and outline the required steps to obtain and maintain an SA account.

These guidelines provide information on approved encryption algorithms, recommended encryption products and specific encryption tools and practices.

This standard provides guidance for all users regarding the security and management of passwords.

This standard provides the practices that must be followed when using encryption technology.

This quarterly report assesses appropriate user access to decentralized systems and confirms compliance with audit requirements.

This is the approved CSU access and compliance certification.

The document provides policies governing CSU information assets.
<table>
<thead>
<tr>
<th>ID/Control #</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
<td>Chancellor's Office Annual Review of PS Access Controls/Segregation of Duties Summary of Exceptions Template Available from the vice president for ITS office, LIB PW 1070, 323-343-2600 This form identifies approved exceptions to standard audit requirements for user access controls or segregation of duties to any centralized or decentralized system containing University protected data.</td>
</tr>
</tbody>
</table>