Administrative Policy

Number:	P-008
Effective:	6/13/2013
Supersedes:	N/A
Page:	1 of 5

Subject: POLICY FOR TECHNOLOGY AND INFORMATION SECURITY COMPLIANCE

1.0. PURPOSE:

To establish the policy for the implementation, access, use, disposal and legal compliance of technology resources and information assets.

2.0. ORGANIZATIONS AFFECTED:

All organizational units of the University, including auxiliaries and third-party service providers.

3.0. REFERENCES:

3.1. Fair and Accurate Credit Transactions Act of 2003 (FACTA), the Red Flag Rules.

3.2. Fair Credit Reporting Act (FCRA), U.S. Code, Title 15, Section 1681 et seq.

3.3. Family Educational Rights and Privacy Act (FERPA), Title 34, Part 99.

3.4. Federal Privacy Act of 1974, 5 U.S.C., Section 552a.

3.5. Gramm-Leach-Bliley Act (GLB), 15 USC, Subchapter 1, Sections 6801-6809.

3.6. Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R., parts 160 and 164.

3.7. Higher Education Opportunity Act (HEOA), (Public Law 110-315), U.S. Department of Education.

3.8. The Donor Bill of Rights, Association of Fundraising Professionals.

3.9. United States Digital Millennium Copyright Act, U.S. Copyright Office, Public Law 105-304.

3.10. California Public Records Act, Government Code Sections 6250-6270.

3.11. California State Records Management Act, Government Code Sections 14740-14769.

3.12. California Government Code, Section 8314.

Approved: _____ **Date:** _____

3.13. California Penal Code, Sections 502, 502.1 and 653m.

3.14. California Civil Code, Sections 1747.08 and 1747.09.

3.15. California Civil Code, Sections 1798.29, 1798.80, 1798.81, 1798.82, 1798.84, and 1798.85.

3.16. CSU Executive Order 796, Privacy and Personal Information Management Student Records Administration.

3.17. CSU Executive Order 999, Illegal Electronic File Sharing and Protection of Electronic Copyrighted Material.

3.18. CSU Executive Order 1014, California State University Business Continuity Program.

3.19. CSU Executive Order 1031, Systemwide Records/Information Retention and Disposition Schedules Implementation.

3.20. Integrated CSU Administrative Manual (ICSUAM), Information Security Policy, Sections 8000-8095.

4.0. POLICY:

California State University, Los Angeles (Cal State L.A.) is committed to complying with all current and future state and federal laws and regulations, California State University (CSU) Executive Orders and the CSU Information Security Policy pertaining to all security aspects of University technology resources and information assets.

5.0. DEFINITIONS:

5.1. 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 Information Technology Services (ITS).

5.2. Information Assets – Information systems, data and network resources, including automated files and databases that contain Level 1 and Level 2 confidential data.

5.3. Information Security Officer (ISO) – The Cal State L.A. information security officer is the director for IT Security and Compliance.

5.4. Information Security Program – A Cal State L.A. program that includes, but is not limited to, security policies, standards, procedures and guidelines plus administrative, technical and physical controls designed to protect campus information assets.

5.5. 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.

5.6. 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.

5.7. Technology Resources – The cable and wiring infrastructure, networks, systems, applications, auxiliary equipment, data centers, network hubs, server rooms and other locations that transport or house information assets.

6.0. RESPONSIBILITIES:

6.1. The President will:

6.1.1. Appoint an information security officer to oversee the campus information security program.

6.1.2. Report information security incidents to the Chancellor.

6.2. The Vice President for Information Technology Services/Chief Technology Officer or designee will:

6.2.1. Establish and implement the campus information security program.

6.2.2. Establish and implement a campus information security awareness and training program.

6.2.3. Develop and implement appropriate technical controls to minimize risk to the information technology infrastructure.

6.2.4. 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.

6.2.5. Establish and document a process to manage changes to campus information assets containing Level 1 and Level 2 confidential data to minimize the risk of introducing unexpected vulnerabilities and ensure that existing security protections are not adversely impacted.

6.2.6. Develop and maintain the campus data classification standard.

6.2.7. Create and support the Campus Information Security Response Team (CISRT) to investigate, respond to, report and recover from incidents involving loss, damage, misuse of information assets, or improper dissemination of critical or protected data.

6.2.8. Report security incidents involving information assets to the President.

6.2.9. Develop and publish information security guidelines and standards that comply with applicable laws and regulations and the CSU policies that apply to information assets.

6.3. Vice Presidents will:

6.3.1. Identify and assess risks, and then mitigate, transfer or accept the risk for all technology and information assets within the respective division.

6.3.2. Submit an annual risk assessment report to the University internal auditor.

6.3.3. Ensure that an appropriate separation of duties is maintained for all systems containing Level 1 and Level 2 confidential data to avoid issuing credentials that allow a user greater access or more authority over information assets than is required by the employee's job duties.

6.3.4. Identify areas that must be protected from unauthorized physical access, such as data centers, server rooms, offices and other locations where electronic and printed information assets are stored.

6.3.5. Prepare and review annually a disaster recovery plan for centralized and decentralized systems in the respective division.

6.3.6. Prepare and review annually a business continuity plan for the continuity of essential functions and operations following a catastrophic event.

6.4. Administrators will:

6.4.1. Review and approve all employee requests for access to systems containing Level 1 and Level 2 confidential data. Approval for system access must be based on the employee's duties and responsibilities as outlined in a current, approved position description, and access rights must be strictly limited to need-to-know data only.

6.4.2. Notify ITS when an employee with system access moves from a department, or takes another position as a result of a promotion or other type of transfer.

6.4.3. Manage third-party vendors requiring access to, or who may come in contact with, University information assets. This includes, but is not limited to, adding appropriate contract language to purchase documents, obtaining a signed confidentiality agreement, requiring third-party account access forms for review and approval, responding to any potential security incidents, and any other forms or actions requested by the campus information security officer.

6.4.4. Ensure data sanitization is performed on all computers and electronic storage media prior to transfer, relocation, donation or disposal.

6.5. Employees will:

6.5.1. Submit an account access request for approval to access or use Level 1 and Level 2 confidential data on centrally-managed or decentralized systems.

6.5.2. Encrypt all documents on computers and electronic storage media [at rest] and in e-mail messages [in transit] to prevent unauthorized access.

6.5.3. Create and utilize passwords in a manner that meets the University's published password standards.

6.5.4. Maintain a secure work area and abide by all CSU policies and Cal State L.A. guidelines and standards related to information security.

6.6. Third-party Service Providers will:

6.6.1. Comply with all state and federal regulations, CSU policies and Cal State L.A. guidelines and standards related to information security.

6.6.2. Comply with all Cal State L.A. information security requirements appended in the initial procurement contract or service order.

6.6.3. Submit an account access request form and obtain appropriate approvals whenever direct access to Cal State L.A. information assets is required to perform contracted work.

6.6.4. Complete an Information Confidentiality/Non-disclosure Agreement before being granted direct access to any Cal State L.A. information assets.

7.0. GUIDELINES AND STANDARDS:

Information Technology Services maintains a library of information security standards and user guidelines on its website. Standards describe the state and federal laws, regulatory rulings, audit requirements and industry standards to which Cal State L.A. must comply. User guidelines provide the tools, actions and reporting requirements that departments and employees must follow to comply with the standards. Documents are created and updated as legal requirements and technology changes occur.