

University of Southern California Information Security Policy

Date Issued: April 7, 2004

Authority: Lloyd Armstrong, Jr.,
Provost and Senior Vice President for Academic Affairs

Dennis F. Dougherty
Senior Vice President for Administration

1.0 **Purpose**

The University of Southern California (USC) is committed to respecting and protecting the security and privacy of information it creates, uses, transmits, stores and destroys in accordance with applicable laws and regulations as well as reasonable business judgment, discretion and common sense.

The university community shall use information that supports the university's mission and core business operations in a responsible and appropriate manner. However, certain types of information require additional protections under federal and state law.

This policy:

- Identifies information that requires enhanced protection and security under federal and state law
- Describes methods to provide physical and technical security of such information
- Explains the responsibilities of stewards, managers and users of university information
- Describes the obligation for reporting security breaches that violate this policy
- Provides additional university and external resources regarding information security

This policy is intended to establish an organizational framework for the university's policies related to information security. **Appendix B** will incorporate the university's procedures for implementing this information security policy.

Future policies, procedures and guidance in this area shall adhere to the structure set forth in this policy and shall be located at: www.usc.edu/policies and www.usc.edu/compliance.

Questions regarding implementation of this policy should be directed to the USC Office of Information Security at (213) 743-4900 or infosec@usc.edu.

2.0 Scope

This policy applies to all university faculty members (including part-time and visiting faculty), staff and other employees, (such as postdoctoral scholars) and students (including postdoctoral fellows and graduate students).

In addition, all third parties, including vendors, who have access to or control of USC information described in this policy, must agree in writing to maintain such information confidentially and in accordance with federal and state laws, as described in further detail in Section 3.2.6 of this policy.

3.0 Policy

All university information security policies, standards, guidelines and practices shall be coordinated through the Office of Information Security and shall be consistent with a university-wide approach in developing, implementing and managing information systems security.

University faculty, staff, students, volunteers, vendors or any third party under USC control who have access to USC information described in this policy are expected to exercise discretion, common sense and reasonable judgment in connection with their use of information created, stored, transmitted or disposed in the course of their job duties, regardless of the medium in which that information is maintained. This includes:

- Personal information collected from and about students, faculty, staff, donors, business partners and others affiliated with the university
- Information relating to the core business practices of the university, including certain financial, legal and operational information
- Other information relating to university operations that may be of a sensitive nature

Notwithstanding the above, Section 3.1 of this policy identifies certain information that requires enhanced protections under the law. Stewards, Managers and Users of such information all have obligations to identify such information and take reasonable precautions to ensure that such information is kept confidential. Section 3.2 describes the roles and responsibilities of Stewards, Managers and Users in further detail.

3.1 Information Requiring Enhanced Protection

The following describes information that requires particular protections by law. University faculty, staff and students who create, use, transmit or dispose of information in any of the following categories are expected to appropriately maintain

Issued by: Lloyd Armstrong, Jr.
Provost and Senior Vice President, Academic Affairs
Dennis F. Dougherty
Senior Vice President for Administration

Date issued: April 7, 2004

the confidentiality of such information in accordance with this policy and procedure as well as federal and state law.

- “*Education Records*,” including files documents or other materials (regardless of the medium maintained), which contain information directly related to a student and maintained by USC. “Education Records,” as defined by federal law, are protected under the Family Educational Rights and Privacy Act of 1974 (FERPA). USC’s FERPA policy is referenced in Section 7.0 of this policy.
- “*Protected Health Information*,” created or received by a health care provider that: (1) identifies an individual; and (2) relates to that individual's past, present or future physical or mental health condition or to payment for health care. Protected Health Information is covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). USC’s HIPAA policies are referenced in Section 7.0 of this policy.
- “*Customer Information*” as defined under the Gramm-Leach-Bliley Act, includes personal identifiable financial information that USC collects about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available. Financial products or services offered by USC include: (1) Student financial aid packages, and (2) Faculty housing loans. USC’s Gramm-Leach-Bliley policy is referenced in Section 7.0 of this policy.
- “*Personnel Records*,” protected under state law, which include letters of offer, employment records, salaries, fringe benefits, and other personnel information.
- “*Social Security Numbers*,” particularly when combined with an individual’s name or birth date. USC’s Personal Information Policy is referenced in Section 7.0 of this policy.
- “*Personal Information*,” protected under state law (formerly known as SB 1386), applies to California residents and protects an individual’s first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
 - Social Security number
 - Driver’s license number or California Identification Card

Issued by: Lloyd Armstrong, Jr.
Provost and Senior Vice President, Academic Affairs
Dennis F. Dougherty
Senior Vice President for Administration

Date issued: April 7, 2004

- Account number, credit or debit card number, in combination with any required password, security or access code that permits access to the individual's financial account.
- "Research Records" that are protected by copyright, trademark, trade secret, patent or other intellectual property right. USC's Intellectual Property Policy is referenced in Section 7.0 of this policy.

3.2 Roles and Responsibilities

All members of the university community share in the responsibility for protecting information. This section of the policy defines and describes those groups that have particular responsibility in this regard: (1) Stewards; (2) Managers; and (3) Users.

3.2.1 Stewards

Stewards are those members of the university community who have responsibility for particular USC-generated or maintained information. Stewards oversee and manage the official repository of such information and, therefore, are responsible for the integrity of that data (e.g., Registrar's office for student transcripts). Stewards have a responsibility to use reasonable efforts to ensure that other individuals and third parties who receive such information understand their respective rights and responsibilities in using and transmitting the information to others. Joint stewards are mutually responsible for such information.

3.2.2 Users

All members of the university community are "Users" even if they do not have responsibility for managing the resources. Users include, for example, students, faculty, staff, contractors and volunteers. Users are responsible for protecting information resources to which they have access. Their responsibilities cover both computerized and non-computerized information and information technology devices (paper, reports, books, film, microfiche, microfilm, computers, PDAs, disks, printers, phones, fax machines, etc.) that are in their care or possession. They shall follow the information security policies and procedures as well as any departmental or other specific applicable information security practices.

Users are responsible for completing education regarding information

Issued by: Lloyd Armstrong, Jr.
Provost and Senior Vice President, Academic Affairs
Dennis F. Dougherty
Senior Vice President for Administration

Date issued: April 7, 2004

security, adhering to the university's policies and procedures regarding information security and reporting breaches of the policies to their respective managers or stewards, as appropriate.

“Users” of personal or sensitive information or information protected under federal and state law are expected to comply with the procedures to implement this policy, as appropriate, to protect the privacy and security of such information.

3.2.3 Managers

Managers are members of the university community who have management or supervisory responsibility, including deans, department chairs, directors, department heads, group leaders, supervisors, etc. Faculty who supervise teaching and research assistants are included.

Manager responsibilities include: Ensuring that their unit has completed education regarding information security, overseeing compliance with university policies and procedures in this regard, and immediately reporting breaches of this policy to the university's Information Security Officer.

“Managers” and “Stewards” are expected to oversee User compliance with this and other information security policies.

3.2.4 Information Security Officer

The university's Information Security Officer has primary responsibility for oversight of information security, security policy and procedure development, revision and oversight, implementation of the university's information security plan and educating the University community about security responsibilities.

All incidents of actual or suspected security breaches must be reported immediately to the Information Security Officer of the Office of Compliance at (213) 743-4900 or infosec@usc.edu. The Information Security Officer will investigate the incident and coordinate with necessary members of the university community and will comply with federal and state law requirements regarding incident reporting and notice as set forth in this policy.

The USC Office of Information Security shall issue policies, procedures

Issued by: Lloyd Armstrong, Jr.
Provost and Senior Vice President, Academic Affairs
Dennis F. Dougherty
Senior Vice President for Administration

Date issued: April 7, 2004

Page 5 of 11

and additional guidance to assist the university community in implementing this and other information security-related policies. This policy is the umbrella policy for future policies and procedures related to information security.

3.2.5 Information Security Liaisons

Information Security Liaisons are designated by the Deans or Vice Presidents of their respective units to serve as the liaison between that school or unit and the Office of Information Security for all matters relating to information security. This individual coordinates with the Office of Information Security to implement the university's policies, procedures and education at the relevant school or unit and is the information security office's contact for information security issues relating to that school of unit. Specifically, this individual's responsibilities include:

- Assisting the Information Security Office in conducting an inventory of information covered by this policy that is maintained by his/her department or unit
- Assisting the Information Security Office in determining categories of individuals who have access to such information and under what circumstances
- Disseminating educational information to his or her department or unit to raise awareness about information security related issues
- Acting as the Information Security Office's primary contact for monitoring and auditing of implementation of USC's information security plan
- Assisting the Information Security Office in implementing corrective action resulting from an investigation of an incident report under this policy

3.2.6 Vendors and Other Third Parties

Vendors and other third parties that access USC information covered under this policy are required to comply with the applicable privacy and security regulations and requirements set forth in this policy. University faculty and staff members shall take reasonable and appropriate steps to ensure vendor compliance, including any of the following as applicable:

- Utilizing the university's standard Purchase Order, which contains confidentiality provisions,

Issued by: Lloyd Armstrong, Jr.
Provost and Senior Vice President, Academic Affairs
Dennis F. Dougherty
Senior Vice President for Administration

Date issued: April 7, 2004

- Executing the university’s standard independent contractor agreement with the vendor or third party,
- Executing a template confidentiality agreement, attached as **Appendix A.**¹

Vendor’s non-compliance with this policy should be reported to the appropriate supervisor or individual responsible for overseeing the vendor as well as the Information Security Officer.

4.0 Education and Awareness

The USC Information Security Office, in conjunction with other appropriate units, shall disseminate educational information to the university community regarding information security issues. Information also can be found at: www.usc.edu/compliance.

5.0 Incident Reporting

5.1 General Security Breaches

It is the responsibility of all university employees aware of an actual or suspected information security breach, as defined below, to report it immediately to their respective supervisor and the USC Information Security Officer for review. A “security breach” means an unauthorized acquisition of data that compromises the security, confidentiality, or integrity of information maintained by USC and covered under this policy. This includes breaches that involve physical security as well as computer or information systems security.

It also may be necessary to report such a breach to other USC departments or units, such as the Department of Public Safety, Audit Services or Personnel Services, depending upon the nature of the actual or suspected breach. Contact the Information Security Officer or your supervisor if you are uncertain if other departments should be notified.

At the direction of General Counsel, the USC Information Security Officer will conduct an investigation of the actual or suspected breach as well as review internal procedures and controls. The Information Security Officer will notify and coordinate with the Information Security Liaison of the

¹ The Office of General Counsel should review any modifications to the template confidentiality agreement.

Issued by: Lloyd Armstrong, Jr.
Provost and Senior Vice President, Academic Affairs
Dennis F. Dougherty
Senior Vice President for Administration

Date issued: April 7, 2004

impacted department or unit, as necessary and appropriate, to conduct the investigation.

Departments or units should not conduct their own investigation without first consulting with the USC Information Security Officer.

A final report of the findings will be forwarded to the Office of General Counsel. The Information Security Officer, in consultation with the Office of General Counsel, shall make recommendations to the appropriate senior administrator for review and implementation and assist in implementation of such recommendations, as appropriate. Impacted departments or units are required to implement the corrective action agreed to by the senior administrator to improve departmental controls over information security.

5.2 Computer Security Breaches

State law requires USC to notify any California resident for whom USC maintains "Personal Information" as defined in Section 3 of this policy, of any computer security breach that allowed an unauthorized person to acquire such resident's information. The notice requirement is triggered if: (1) there is a breach of the security of USC computer system containing such personal information; (2) USC becomes aware of such breach; and (3) USC believes that an unauthorized person has acquired the personal information.

In the case of a computer security breach, the USC Information Security Officer must be notified immediately.

This state law notification requirement only applies to computer or electronic security breaches and not to other breaches, such as incidents involving physical security.

The USC Information Security Officer will coordinate with the Senior Associate Vice President for the Office of Compliance, the Office of General Counsel and any other relevant units (e.g., Audit Services, Department of Public Safety, the unit where the actual or suspected breach occurred), to provide the notification required under state law.

Notification to affected individuals may not occur without prior consultation and approval from the USC Information Security Officer.

Issued by: Lloyd Armstrong, Jr.
Provost and Senior Vice President, Academic Affairs
Dennis F. Dougherty
Senior Vice President for Administration

Date issued: April 7, 2004

Page 8 of 11

6.0 Enforcement

All university faculty, staff and other employees must comply with this policy, including all future information security policies and implementing procedures.

Compliance with the university's information security policies and procedures shall be monitored regularly in conjunction with the university's monitoring of its information security program. Audit Services will conduct periodic internal audits to ensure compliance with federal and state laws and regulations as well as university policy.

Individuals who do not comply with these policies shall be subject to remedial action in accordance with the Faculty Handbook, the Staff Employment Policies and Procedures and SCampus, as appropriate. Any disciplinary action under this policy shall take into account the severity of the offense and the individual's intent.

The Office of Audit Services and/or the Office of Compliance will conduct a follow-up review to ensure the prescribed action has been taken.

7.0 USC Resources

Family Educational Rights and Privacy Act (FERPA) policy
Health Insurance Portability and Accountability Act (HIPAA) privacy policies
Gramm-Leach-Bliley Act Policy
Personal Information Policy
Intellectual Property Policy
Policy Regarding Misappropriation of Assets
Faculty Handbook
Staff Employment Policies and Procedures
Scampus
Information Security Division procedures

All above USC policies are located at: www.usc.edu/policies.

Appendix A

**UNIVERSITY OF SOUTHERN CALIFORNIA
CONFIDENTIALITY AGREEMENT**

_____ (“Vendor”) has entered into an arrangement (the “Arrangement”) with the University of Southern California (“USC”) to engage in or provide services related to the following: _____.
In consideration for USC entering into an Arrangement with Vendor, Vendor agrees to the following:

1. In the course of its Arrangement with USC, Vendor may have access to USC's internal records, systems and methods of operating its business, trade secrets, customer lists, price lists, contract information and other confidential or proprietary information (“USC Information”).
2. Vendor agrees that all such USC Information is the exclusive property of USC, irrespective of whether such USC Information was created or prepared by Vendor or others. Vendor further agrees that Vendor will not, at any time, in any manner, directly or indirectly, disclose such USC Information to any person or entity, or use such USC Information other than in furtherance of the purposes of USC during the time the Arrangement is in effect and for five (5) years after the conclusion of the Arrangement.
3. Vendor agrees that it shall comply with all applicable laws in connection with its possession and use of the USC Information.
4. Upon the conclusion of the Arrangement with USC, Vendor, if requested by USC, will deliver to USC all property of USC, including any written memorial of, or documents relating to, the USC Information described above, in whatever manner maintained or stored.

Agreed to by:

Vendor:

(Print Name of Vendor)

By: _____
(Signature)

(Print Name)

Title: _____

Appendix B

Information Security Implementing Procedures