Policy 404

Responsibility for Personally Identifiable Information

Review of Policy and Implementation Plans

May 2009
UCLA’s Personally Identifiable Information (PII) Risk Landscape

Mobile Devices – Greatest Risk of Physical Loss

It is effectively impossible to guarantee a mobile device’s physical security. Encryption is the only technique available to protect personal information stored on mobile devices.

Desktop Devices – Second Greatest Risk of Physical Loss

Although not considered mobile, these devices may not be stored in physically secure locations and/or many people may have physical access. Theft by electronic means is also a possibility. Encryption enhances the desktop’s overall security.

Servers – Least Risk of Physical Loss but Greatest Risk of Technical Hack

In general, servers are in physically secure locations. There is little risk of physical loss but theft by electronic means is still a possibility. Encryption enhances the server’s overall security.
How UCLA’s Risk is Distributed

Financial Risk to Organizations
“Any financial liability to the University resulting from failure by a unit to comply with Policy 420 shall be assigned to the unit where the Security Breach occurred.”

Risk to Institutional Reputation
Whose identity was breached?
- Celebrity – Britney Spears, Farrah Fawcett, the Governor’s wife

Which organization suffered the Breach?
- Donors – Ohio University suffered alumni repercussions

Can we trust the university with our information?
- Research data, patient data and student data

Risk of Legislative consequences
- Berkeley’s 2005 breach resulted in Civil Code Section 1798.24(t), placing new restrictions on the circumstances under which UC and other researchers are able to gain access to state data involving personally identifiable information for research purposes.

- UCLA’s 2006 breach resulted in California Education Code §66018.55, mandating the creation of the University and College Social Security Number Task Force, whose report on use and recommendations about the use of SSNs in California higher education institutions is due July 2010.

- UCLA’s 2007 breach of celebrity patient records resulted in Health and Safety Code §1280.15 and California Civil Code §56.36, significantly raising penalties, adding a 5-day notification requirement and much more for inappropriate access to patient records.

Mitigating UCLA’s Risk
Policy 404’s purpose is to protect the data that University stores and to protect the University from legal and financial liability due to the loss or theft of personal information. It establishes personal responsibility.
UCLA Policy 404

Summary of Campus wide Standards

1. Personal Information being stored electronically shall be encrypted or otherwise protected against loss or theft of the data and/or System. In the event of a Security Breach as defined by Procedure 404.1, notification is not required under Procedure 404.1 if the data is encrypted; otherwise, notification is required and the cost shall be borne by the Organization. If encryption is used, the provisions of the Policy 403, Institutional Encryption Requirements must be followed.

2. An institutional registry of Personal Information being stored electronically shall be maintained. Each Organization shall maintain a registry of Personal Information under its purview. These registries shall be considered restricted information as defined in UC BFB IS-2 and marked with the header “Confidential: Security Sensitive Information – Not for Public Disclosure”.

3. The requirement for a background check for staff must be fulfilled as per UCLA Human Resources Procedure 21.

4. If a third-party will be working with Personal Information, the agreement must comply with the requirements in Protecting University Data Through Agreements or Contracts with Third-Party Vendors. The language in the UC Model Data Security Appendix may be used as a basis for contract language.

5. If the System connects to the UCLA network, it must comply with Policy 401 on Minimum Security Standards.

Implementing Plan for Each Organization

Each Organization shall develop an implementing plan, approved by the Organization Head, that documents how that Organization will comply with this Policy. Further and/or more restrictive requirements may be imposed at the discretion of the Organization Head based upon this Policy. As a Security Breach can impact the institution as a whole and not just the Organization in which it occurs, each implementing plan shall also be reviewed and approved by the Associate Vice Chancellor, Information Technology for institutional impact and alignment.
UCLA Policy 404 (continued)

Oversight, Management and Enforcement

- The Deans and Vice Chancellors are the primary enforcement authority. The IT Compliance Coordinators are the management and communications points of contact for the campus organizational units.
- The Oversight Committee on Audit and Controls is designated in Policy 404 and is the highest-level enforcement authority for university-wide response and action.
- The Campus Ethics and Compliance Risk Committee (CECRC) is the operational authority on university actions and responses and response to UC requirements and actions.
- The authority for institutional approval of organizational implementation plans will rest with the AVC-IT who will periodically report on campus plans to both the CECRC and Oversight Committee.
Encryption

The risks to the personal information primarily fall into 3 categories:

- physical loss of a device
- electronic theft of information
- inappropriate access to the information

Encryption:

- solves the problem of physical loss
- adds an additional layer of security protection that helps mitigate the electronic theft of information
- significantly enhances the security of information
- adds a complex layer of system administration

There are a variety of encryption methods that encompass a vast array of requirements and possible device configurations.

- Windows?
- MacOS?
- Linux?

- Folder/File Encryption?
- Partition Encryption?
- Whole Disk Encryption?
- Hardware Encryption?

Acceptable cryptographic methods include AES (Advanced Encryption Standard), Twofish, Serpent, MARS, RC6, RC4, Blowfish, RSA, Rabin, DESX, Triple-DES.

Acceptable encryption key length should be a Symmetric key length of no less than 128, a Public key length of no less than 2048, an Elliptic curve key length of no less than 256, a Hash key length of no less than 256, and MAC key length of no less than 256.

An encryption options matrix is being developed in order to advise the campus on the different solutions and options available.

Pilot projects are being created in order to test the different encryption solutions.
Implementation Plan

**Communicating the Risk Message:**

- Communication from Dean/VC encouraging compliance
- Presentations by OIT to various key constituents
- Referrals to OIT compliance resources

**Establishing Roles and Expectations for IT Compliance Coordinators (ITCCs), with direct cooperation of their Dean/VC:**

- Ensure communications regarding risk and compliance with constituents
- Develop implementation plan for full compliance with 404
- Assist in removing or de-identifying data where possible
- Register remaining cases of stored Personally Identifiable data
- Determine appropriate protection method based on risk, storage location, criticality of data
- Encrypt wherever possible and practical
- Work directly with campus ITCC and campus CSO

**Identifying and Registering Storage of 404-related (Personally Identifying) Data:**

- Implement method to register PI data with the unit’s ITCC
- The data owner, ITCC, and Dean/VC will sign off on the registry.
- A copy of the registry will be kept locally and a copy will be forwarded to campus ITCC for retention on behalf of Jim Davis.
- The registry will be kept up locally as data storage changes

**Encrypting and otherwise Protecting Essential 404-related data:**

- See encryption testing and implementation details attached

**Planning Unit Implementations and Compliance Schedules:**

- Each unit will need to draft a plan of exactly how they plan to comply and in what timeframe.
Known elements of policy implementation will begin immediately.

2009 Spring Quarter

- Endorsements to begin formal campus review
- Dean/VC letter to communicate within organizations
- ITCC and OIT to work out encryption solutions
- Data de-identification or registration
- Encryption/protection of high-risk databases

2009 Summer Quarter

- Finalization of policy.

2009 Fall Quarter

- October and November – 60 day review and comments.
- December and January – Final policy

2010 Winter Quarter

- Final review and endorsements if needed.

2010 Spring Quarter

- Formal adoption of policy.
- X months to develop an implementing plan for coming into compliance.