

# UCLA Policy 404

---

*Draft 11 – April 27, 2009*

## **Major policy changes: allowing for organizational variance**

These two changes give Organizations latitude to comply with Policy 404 in the manner and along a timeline most effective for each environment.

- a. Campuswide Standard: “Personal Information being stored electronically shall be encrypted **or otherwise protected against loss or theft of the data and/or System.**”
- b. 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.

## IV.B Campuswide Standards for Electronically Storing Personal Information

New policy defined by 404

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".

Existing policy

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.

If it is not possible to meet one or more of these campuswide standards, a written request for an exception that describes the circumstances justifying an exception and the proposed compensating controls providing equal or greater security may be made to the appropriate Organization Head. An exception to Policy 401 shall be requested through the procedure documented in that Policy.