

# UCLA Policy 404

## Protection of Electronically Stored Personal Information

---

### Policy process and timeline

Policy 404 is an institutional policy intended to apply to all units of UCLA.

Implementation of this policy must be considered in phases, giving first priority to those issues with highest risk, recognizing that not all issues can be addressed simultaneously. Further, different campus units will be affected differently, depending on size and how much Personal Information is in use; and thus different implementation strategies will be needed. Finally, the development of implementation plans to bring *existing* data into conformance with this policy will also be a significant step. The intent is to create sufficient flexibility for realistic implementation while adhering to the intent and goals of the policy.

<p>2008 Winter quarter Spring quarter</p>	<ul style="list-style-type: none"> <li>Principles developed and articulated by the IT Planning Board, including direct input from the Academic Senate</li> </ul>
<p>Summer quarter</p>	<ul style="list-style-type: none"> <li>Principles are implemented as draft Policy 404</li> </ul>
<p>Fall quarter</p>	<ul style="list-style-type: none"> <li>Discussion with ITPB to begin formal vetting process</li> <li>Discussion with Oversight Committee (9/29), Academic Senate Executive Committee (10/16), Deans, IT Compliance Coordinators (9/22), faculty, campus officials</li> <li>Draft a plan for implementation in phases</li> </ul>
<p>2009 Winter quarter</p>	<ul style="list-style-type: none"> <li>Draft policy and implementation plan amended based on discussions</li> <li>Amended draft circulated for final review</li> <li>Final revisions made</li> </ul>
<p>Spring quarter</p>	<ul style="list-style-type: none"> <li>Policy adopted and promulgated</li> <li>Phase I implementation begins</li> </ul>

## Policy 404 summary

### Statement

Personal Information over which UCLA has stewardship **may only be electronically stored when there is a compelling academic or business purpose and with explicit approval by the appropriate Unit Head\***. Personal Information is an individual's name together with SSN, driver's license, financial account information, medical information or health insurance information.

- The Unit Head **shall consider each such request on a case-by-case basis.**
- The **authority to approve such requests may not be delegated.**
- Any **financial liability resulting from failure by a unit to comply with this Policy shall be assigned to that unit.**
- Unit Heads may impose further and/or more restrictive requirements.
- A security breach may require the University **to identify any individual employees responsible to local, state or federal authorities.**

The UCLA Oversight Committee on Internal Audit and Internal Controls has final authority for enforcement of this Policy.

### Procedure to request approval to store Personal Information

- An employee wishing to store Personal Information electronically must **first consult with the unit's IT Compliance Coordinator to determine if there is an alternative to having to store the data.**
- If there is no alternative, approval by the Unit Head must be sought.
- If approval is granted, the employee is responsible for ensuring that campuswide and any local standards are met.

### Campuswide standards

1. The **Personal Information being stored must be encrypted. Alternatively, an audit trail capable of tracing exposure must be available.**
2. Credentials, when used, must be encrypted. Alternatively, an audit trail capable of tracing exposure must be available.
3. Minimum Security Standards defined in UCLA Policy 401 must be met.
4. **A background check must be successfully completed by all individuals who will have access to the Personal Information and/or to the System that stores it.**
5. If a third-party will be storing the Personal Information, the agreement must comply with the requirements in Protecting University Data Through Agreements or Contracts with Third-Party Vendors.

If it is not possible to meet one or more of these campuswide standards, approval may still be granted if compensating controls providing equal or greater security are proposed in writing and approved by the IT Compliance Coordinator.

---

\* Dean; Vice Provost; Vice Chancellor; University Librarian; Associate Vice Chancellor, Community Partnerships; Associate Vice Chancellor, Information Technology; Assistant Provost, Academic Program Development; or Executive Director, ASUCLA.