Technology users are advised to carefully handle University Protected Data in their possession, especially data that is present on a mobile device. The **top 3 items to remember**:

1. **Be safe, Encrypt.** Due to the risk of loss of a mobile device (laptop, tablet, and smart phone such as an iPad, iPhone, Droid, Blackberry), users are instructed to check encryption settings. This practice avoids unintended disclosure of University Protected Data. Remember, when transferring and storing University Protected Data onto/from the mobile device to another system or server, encryption must be used.
2. **Proper erasure required.** When a mobile device is no longer needed, the University Protected Data on the device must be properly erased so there is no possibility of subsequent data recovery. The University IT Rollout can help users properly destroy or erase the Protected Data present on a mobile device.
3. **“Security Breach or Device Theft/Loss = Notification”.** California State law requires notification of a Security Breach, Device Theft, or Device Loss. The law requires prompt investigation and subsequent notification to individuals should their unencrypted personal identity information be involved in a security breach/loss, or if it was "reasonably likely" to have been involved in the breach/loss. **You must notify the campus Information Security Officer and local law enforcement immediately if a mobile device containing CSU Defined Protected Level 1 information/data, for which your campus has responsibility, is stolen, lost, or compromised in any manner.** *This notification needs to occur even if you are not completely sure there was a breach/loss, and even if you think the device may only be temporarily misplaced and will show up soon.* This is necessary for compliance with state law and to provide appropriate stewardship for data entrusted to our care. If you are not sure, call the 657-278-3765 for clarification.

**No encryption requires permission.** An advance written directive from the campus ISO and CIO is required for cases where University Protected Data transmission or storage is not encrypted by the mobile device. Contact the campus ISO office to obtain information on the approval process.

Some examples of Protected Data are:

* Enrollments, grades, academic status (see <http://www.calstate.edu/EO/EO-382.pdf> )
* Electronically health information about employees/students (HIPPA 1996)
* Financial information about employees / students including credit cards, loans, status
* Identity information, especially Driver’s License/State ID and/or Social Security Number combined with the owner’s name, login credentials and passwords
* Student, staff or faculty personnel records including performance, interviews, recruitments, disciplinary proceedings
* Information covered by confidentiality or non-disclosure agreements
* Other information governed by local, state, or federal regulatory control or deemed non-public, classified, or restricted by the University.