Data Security Guidelines

Policy 420 is intended to enhance the management of Personal Information that could be used, possibly in conjunction with other information, to impersonate an individual in ways that might cause loss of privacy and/or financial damage. Departments are urged to establish best practices to minimize the collection, distribution, and retention of personally identifying electronic data if this data is not critical to their business needs. Such practices should comply with the following principles:

- collect and retain only that data which is essential to the performance of assigned tasks;
- delete personal information when there is no longer a business need for its retention on computing systems;
- provide staff access to sensitive data only as needed to perform assigned duties;
- design database systems so that personal information can be identified;
- when personally identifying information is included in the distribution of data to any downstream users, include notification of that fact, including reference to this Policy;
- redact personal information not critical to the task when distributing full data sets to downstream users;
- whenever possible, configure electronic applications that check authorizing or authenticating databases to return confirming responses rather than personal information;
- review and update agreements with external service providers to ensure vendor compliance with these requirements;
- be prepared in advance in the event of the need for any immediate notification to individuals whose personal data is retained on computing systems;
- never leave sensitive data exposed on computer screens when not in use or leave computer screens unattended without appropriate screen access controls;
- don’t store sensitive data on devices that may be prone to loss or theft such as laptop computers, personal digital assistants (PDAs), cell phones, iPods™, universal serial ports (USPs), or that require managerial approval to do so.

Further information can be found in the Administrative Responsibilities Handbook
www.fmp.ucla.edu/Administrative%20Responsibilities%20Handbook.pdf