RE: College Business Practice for Handling and Storing Confidential Information

Background

In accordance with University policy 5.10 “Security of Electronic Information”, the college must implement a local security and management practice for the control of confidential information in its possession. Confidential information includes credit card, social security, driver’s license and bank account information.

Procedures

1) Identifying confidential information
   a) The college will use Identity Finder to scan it’s assets for confidential information yearly
   b) It is the responsibility of the computer user to review these scans and take action on any confidential information that is found

2) Validating the need to retain confidential information
   a) Confidential information will only be retained when there is a valid business purpose
   b) For academic units, the chair validates the need
   c) For administrative units, the Assistant Dean of Administration and Finance validates the need

3) Storing confidential information
   a) Confidential information, when retained, will only be stored on a college fileserver or on a mobile device in an encrypted file system
   b) Confidential information will not be copied or moved from identified storage locations, emailed or otherwise propagated

4) Logging and ongoing management of confidential information
   a) The college will maintain a log of the location of all stored confidential information
   b) The owner of the confidential information will review the need for this information yearly
   c) The chair or Assistant Dean of administration will review and approve ongoing storage of confidential information yearly

-Signed-
Randi Rainbow
Director, Information Technology