Best Practices for Storing University Records

Q: When does a document become a University record?

A: A "University record" is any item of information that is collected, maintained, and used by the University for the purpose of carrying out the business of the University, especially when it is related to the creation or enforcement of policies or procedures, documents a decision making process, or is needed for audit purposes. Examples of things that are *not* University records include meeting notices, routine requests for information, acknowledgements, superseded drafts, research data, and scholarly work.

The University record designation applies regardless of the media on which it is stored. This includes, but is not limited to:

- Electronic communication such as e-mail content and attachments, voicemail, and instant messages;
- Content on web sites, PDAs, mobile devices, desktops, and servers;
- Information/data captured in various databases;
- Physical paper files, such as memos, contracts, reports, photographs and architectural drawings;
- Licenses, certificates, registration, and identification cards;
- Handwriting, typewriting, printing, photographing, photocopying, transmitting by electronic mail or facsimile; and
- Backups of electronic information.

University records must be available to the University and other individuals as required under University policies and state and federal laws, and are subject to CSU Records Retention and Disposition Schedules, CSU Information Security Policies, CSU Data Classification Standards and other appropriate controls depending on the sensitivity of the data.

Q: Where should I store University records?

A: University records should be stored in a secure, environmentally stable location at all times. Paper or other physical records can be stored by an individual in file cabinets or other office furniture, or transferred to a more central storage area (e.g., department offices). Any University record containing Level 1 or Level 2 data must be in a locked, secure location whenever they are not actively in use. **This means, at minimum, behind a locked closet door or in a locked cabinet or drawer.** University records containing Level 1 or Level 2 data should never be left unattended on desks or other open office surfaces at any time, even if the office door is locked.

Digital records are best stored on the University network where they are appropriately protected by University information security mechanisms. The campus currently provides departmental shares for most departments, as well as individual space on Network Folders (see Document Storage Recommendations for options). It is not recommended that University records be stored on local computers where information security mechanisms may be lacking. **In particular, storing Level 1 data on a local computer or mobile storage device (external hard drives, USB drives, cds or dvds) is a high risk practice that always requires permission from the President, and must always be protected by strong encryption.** Any University records downloaded to mobile storage devices must be stored in a

physically secure location at all times and should not be removed from University premises, even temporarily.

Q: Can I store University records in my email account?

A: If an email or email exchange is the only documentation of a decision making process or a policy decision or action, it should be retained as a University record. However, email systems are not designed to be file storage systems, and do not meet the requirements for being a suitably secure location for archiving University records. If a University record exists solely as email, it should be copied out of the mail system as either a paper or PDF document and stored in a secure location. If email is used to send a final product, such as a contract, memo, or report, which is already stored with departmental files, the specific email would not need to be saved as well

Q: Is it safe to store Level 1 or Level 2 University data in the cloud?

A: Google Drive is an acceptable place to store Level 2 FERPA data based on specific contract language between Google and the CSU, **but is not an appropriately secure location to store Level 1 data**! Other currently available cloud storage solutions (e.g., Dropbox, Box.net, SkyDrive, Adobe Document Cloud) **do not provide the level of protection required for either Level 1 or Level 2 data**. Departmental shares are provided for most departments as well as individual space on Network Folders for storage of HSU data and are the best places to store University records in digital format.

Q: Is Google Drive appropriate for class work as well as personal files?

A: Yes, Google Drive is appropriate for storing class work and personal files, and very convenient because you can access the files from wherever you are as long as you have an Internet connection. The CSU has a contract with Google that protects the ownership and privacy of files you store in their system. No similar arrangements exist with Dropbox or any other provider of cloud storage solutions, so files stored with these other providers are more vulnerable.