Student Affairs Policy for Document and Data Retention and Destruction

The Division of Student Affairs abides by the UCOP document and data retention policy (http://recordsretention.ucop.edu/) and all applicable legal document retention requirements. All appropriate student records, related documents, personnel files, financial records, medical and mental health records, etc. will be kept in accordance with such requirements. New employees should be made aware, during the onboarding process, of retention and destruction policies and guidelines. All records, data, and documents that have expired shall be destroyed by the mechanisms described in these Student Affairs Procedure and Guidelines for Data and Document Retention and Destruction.

Student Affairs Procedure and Guidelines for Data and Document Retention and Destruction

Departmental managers shall keep an up-to-date plan for scheduled data and document destruction maintenance, both electronic and hard copy. This plan shall include details of what is to be kept, for how long, and the date it will be eligible for destruction. Destruction shall commence as soon as reasonably possible once a document or data has expired. Managers are responsible for executing their document and data destruction plans on an annual basis.

ELECTRONIC RECORDS

When electronic records and documents are to be destroyed, departments should follow the procedures below. Assistance is available for deleting documents and files that are not easily deleted. Send requests and questions to support@sa.ucsb.edu.

Email: Delete appropriate messages from folders and then empty the Deleted Items folder in Outlook. Once the Deleted Items folder is purged in Outlook, open the same folder using any and all mobile devices on which email is synced to purge the messages from mobile devices as well.

Network File Shares: Files on network file shares (such as the J: and K: drives) that are past their retention periods should be deleted from the file server. Once files are deleted from network file shares, they will be purged from the system and not included in future backups.

Home Directories: Business data should generally not be kept in users' home directories (H: drive and My Documents). Business data that is stored in home directories is subject to the same retention and purge policies and files past their retention periods should be deleted in the same manner as those on other network file shares.

Local Hard Drives: Business data should not be kept on users' local hard drives (such as the C: or D: drives). If business data exists on these drives, it should be moved to the appropriate location on a network file share or deleted.

Databases: Contact SIS&T (support@sa.ucsb.edu) for help identifying data in databases and assistance in purging all records that are past retention. SIS&T staff may be able to help set up automated mechanisms for review and/or purging of records when retention periods are reached.

Acceptable Incidental Personal Use: Personal files stored locally on a divisional computer hard drive (e.g. on C: or D: drives) as part of acceptable incidental personal use of campus electronic resources should

be stored on a short-term basis. Long-term storage should be on a personally owned flash drive. Files stored on a personally owned flash drive offer a greater level of privacy than storage on C: or D: drives. Files stored on university owned equipment (such as on D:. C:. or H: drives) may be subject to search in the case of legal action and may also be accessible to other people using the computer. Personal non-business related files (e.g. photos, videos, music, etc.) should never be stored on the H: drive, as the division incurs the cost of backing up these files.

HARD COPY RECORDS

When hard copy records and documents are to be destroyed, departments should follow the procedures below:

1) All files with confidential information must be shredded, either manually in the office or through a department-paid document destruction service.
2) Confidential documents and records requiring shredding may not be taken off campus for personal destruction (e.g., an employee owns a paper shredder and offers to shred the documents at home--this is not allowed).
3) Non-confidential documents or records may be destroyed through disposal in departmental or University-controlled recycling bins.

GUIDELINES FOR RETENTION AND DESTRUCTION OF DOCUMENTS/FILES WITH NO LEGAL or UCOP SET REQUIREMENTS

Departments are highly encouraged to establish guidelines for the purging of old files that have no legal or UC policy regarding their retention and for the purging of old files that have expired. A list of suggested guidelines is provided below:

- Documents pertaining to a particular event or program should be retained for 3-5 year, longer only if files are continually utilized.
- Projects that have numerous collaborators should be saved in a shared location. Final versions should be stored in the smallest version possible, once completed (revisions deleted), in a shared location.
- "History" files may be created on the departmental J drive for various projects and programs to hold versions of old event agendas or to-do lists that may be helpful in the future. Only the most relevant or useful documents should be retained in a "History" file.
- Annual memos and notifications that are updated regularly should be written over the previous year's drafts and only the most current version should remain (except in cases where all historical versions need to be retained for audit purposes; some cases require copies of exact versions published).
- Departmental publications should be reviewed by the management to keep a minimum number of versions. Consider saving large publication files to a flash drive or disc instead, and designate a storage space within the office for such drives/discs.
- Departments should hold a "purge day" each year to clear out old files and expired documents. On occasion there are UCSB-wide purge days; consider coordinating as appropriate.

- Departments should establish a designated location to store event photos, logos of historical significance to the department, etc. Duplicate copies should be discarded.
- Departmental managers should designate a staff subject matter expert to analyze and have decision-making authority for deleting expired or duplicate files, or retaining files on the departmental drive.
- Recommendation letters, letters of support, or other one-time requests should only be kept until the request is fulfilled, unless there is good reason to retain them. Keeping a template rather than individual letters may be helpful.
- Paper files that are retained should be limited to only the most relevant and required information.