Administrative Procedure

Number:	708
Effective	7/12/83
Supercedes:	
Page:	1 of

Subject: DESTRUCTION OF CONFIDENTIAL RECORDS

1.0. PURPOSE:

To establish the policies and procedures for the destruction of confidential records maintained by the University.

2.0. ORGANIZATIONS AFFECTED:

2.1. All units of the University.

2.2. Auxiliary organizations.

3.0. REFERENCES:

3.1. California Civil Code, Section 1698 ff (Information Practices Act of 1977).

3.2. State Administrative Manual (SAM), Sections 1639 and 1693.

3.3. Office of the Chancellor Memoranda, FSA 78-38 and TL/WC 80-01.

3.4. Cal State L.A. Administrative Procedure, "Record Retention and Disposition".

4.0. POLICY:

Reports containing personal or confidential information will be safeguarded when in use and promptly destroyed when no longer required or timely.

Department managers will insure that all documents, reports, files and systems which do not meet current "relevant and necessary" criteria are destroyed.

Department managers will, through Computer Center support, promptly degauss and/or destroy automated records that do not meet the "relevant and necessary" criteria or are no longer timely.

Approved: **Date:**

5.0. DEFINITIONS:

5.1. Automated--Records, files, and systems that are maintained through the use of a computer.

5.2. Confidential Information--Any record or paper that allows identification of a person by name, social security number, address, physical description, salary or money received. This definition also includes medical or criminal records, and records subject to the Information Practices Act of 1977.

5.3. Degauss--To demagnetize electronically maintained records.

5.4. File--A collection of records.

5.5. Destruction of Documents--Shredding paper forms so that they are unreadable and may not be reconstructed to be readable.

5.6. Information Practices Officer--Individual appointed by the President to implement the Information Practices Act of 1977 and to file the required annual notices with the Office of Information Practices. The Campus Information Practices Officer is the Director of Information Services and Data Processing.

5.7. Information Security Designee--The individual in a department with the day-to-day responsibility for ensuring that confidential or sensitive information is safeguarded from inappropriate disclosure. The designee should typically be at the management or supervisory level. The designee may receive guidance and instruction from the University Information Practices Officer.

5.8. Personal Information--Any information about an individual, includi9ng but not limited to, his or her education, employment history, financial transactions, medical or behavioral history that contains his or her name, identification number, or other identifying particular.

5.9. Relevant and Necessary--Personal or confidential information which is relevant and necessary to accomplish a purpose of the department required or authorized by the University, State, Federal government or other legal authority.

5.10. Record--Any grouping of information about an individual.

5.11. System--A collection of files.

5.12. State Record Center--Repository for records that are considered to be "critical state documents" - i.e., the information is unavailable elsewhere.

On a quarterly basis, Support Services distributes a list of all records stored in the Lawndale Facility that have reached their scheduled destruction date as outlined in the Administrative Procedure on "Record Retention and Disposition".

6.0. RESPONSIBILITIES:

6.1. School Deans and Senior Administrators will ensure that departments have a destruction procedure 1n place and that the task of destroying confidential documents is carried out promptly.

6.2. Department Heads will:

6.2.1. Appoint an Information Security Designee to ensure the destruction of confidential documents.

6.2.2. Be finally responsible for all records and documents until informed that destruction of records and documents has, in fact, taken place.

6.3. Department Information Security Designees will:

6.3.1. Be responsible on a day-to-day basis for ensuring that personal or confidential information is protected from unauthorized disclosure. This may be accomplished by:

a. Training of employees

b. Supervision of work involving sensitive information

c. Development of written operating instructions to address information security.

6.3.2. Shred documents using the school/department shredding equipment or request the Property Office to pick up materials to be shredded.

6.3.3. Request to witness destruction if it is departmental policy to do so.

6.3.4. Require notification of actual destruction of documents.

6.3.5. Authorize destruction of records stored at the State Records Center.

6.4. The Property Officer will:

6.4.1. Provide forms and instructions for preparing documents for destruction as necessary.

6.4.2. Establish and maintain a destruction schedule.

6.4.3. Notify the requesting department of actual destruction as requested by the department.

6.4.4. Safeguard materials scheduled for destruction until destroyed, including:

a. Expedient pickup of material and direct transit to the destruction area.

b. Controlled access to the destruction area. Access is to be restricted to only those individuals charged with destruction or an authorized departmental representative with a legitimate need to witness destruction.

7.0. PROCEDURES:

7.1. The Information Security Designee will make use of departmental shredding equipment, if available, or will complete a Request For Document Destruction. Request Forms are available from the Property Office.

7.2. The Information Security Designee will obtain the approval of the department head and forward the request to the Property Office.

7.3. Departments will remove all binding rods, paper clips, and metal fasteners, and place materials to be destroyed in boxes. Items which are loose and not properly boxed will not be picked up.

7.4. The Property Office will pick up the material to be destroyed and notify the department, as requested. If the department requests to witness destruction, arrangements must be made in advance.

8.0. APPENDICES:

8.1. Request for Document Destruction.