Policy Change	☒	Subject Matter Area Review	☒	KEY:
Procedure Change	☒	Constituency Group Review	☒	BOLD= new language
New Policy	☐	District Council	☐	~~strikethrough~~= delete language
New Procedure	☐	Board 1st Reading	☐	
		Board 2nd Reading	☐	

Comments:
Recommended changes from IT
Changes from Board resolution

Referred to:

Edited:
8/17/16

Yosemite Community College District Policies and Administrative Procedures **No. 3310**

Policy

3310 Records Retention and Destruction

The Chancellor shall establish administrative procedures to assure the retention and destruction of all District records – including electronically stored information as defined by the Federal Rules of Civil Procedure – in compliance with Title 5. Such records shall include**,** but not be limited to student **records**, employment **records** and financial records.

References:
Title 5~~,~~ Section**s** 59020 et seq.; Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37 and 45~~.~~

Adopted: April 10, 2013
Last Reviewed:

Administrative Procedure

3310 Records Retention and Destruction

I. "Records" means all records, maps, books, papers, data processing output, and documents of the District~~,~~ required by Title 5 to be retained**,** including but not limited to records created originally by computer and "electronically stored information" ("ESI"), as that term is defined by the Federal Rules of Civil Procedure.

II. The Chancellor**'**s~~'~~ Office shall supervise the classification and destruction of records and ESI. **The Board of Trustees may delegate the authority to the Chancellor or designee to classify and retain or destroy "records" of the District in accordance with applicable code sections and implementing District policy/administrative procedure.** The District must preserve ESI that is relevant to actual or potential litigation pursuant to the Federal Rules of Civil Procedure. The District shall comply with the Federal Rules of Civil Procedure and produce relevant ESI in the form in which it is ordinarily maintained or readily usable. ~~An annual report shall be made to the Board of Trustees regarding the classification and destruction of records.~~

III. Records shall be classified as required by Title 5 and other applicable statutes, federal and state regulations.

IV. Records shall annually be reviewed to determine whether they should be classified as Class 1 – Permanent, Class 2 – Optional, or Class 3 – Disposable (as defined in Title 5).

V. Class 3 – disposable records shall be maintained for the period required by applicable law or regulation, but in any event shall be retained for at least three college years after the year in which they were originally created.

VI. Destruction is by any method that assures the record is permanently destroyed, e.g. shredding, burning**,** and pulping.

VII. Under the direction of the Chancellor, the Assistant Vice Chancellor Information Technology will establish electronic data backup and tape storage for each enterprise system in support of record retention and destruction. Those scheduled backups are established to protect data integrity and are designed for the purpose of restoring the original data in case of accidental deletion, hardware failure, data corruption or disaster recovery. These backups are not to serve as the official means for data retention. The current schedule is as follows:

Authentication servers	**30 days**
CC, MJC and District Main Web servers	**90 days**
Cisco Unified Communication Manager	**90 days**
Cognos and related systems	**365 days**
Computer Lab Servers (CC and MJC)	**365 days**
Colleague Reporting and Operating Analytics (CROA) and related systems	**365 days**
Ellucian Colleague (including all applications servers, web servers and the database server)	**365 days**

Email (YCCD employees, excluding students)	**30 days**
File Shares (YCCD employees, excluding students)	**180 days**
Library Systems	**365 days**
Matrix OnBase System	**180 days**
Network equipment (including firewalls and routers)	**180 days**
Scheduling and Reporting Software (SARS) systems	**365 days**
SharePoint and database server	**180 days**
Video Surveillance System	**90 days**

All backups will take place between the hours of 5:00 p.m. and 7:00 a.m. If operations is aware that the backup schedule in some way interferes with a crucial work process, then a specific alternate schedule will be implemented. Incremental backups (all files changed since the last full backup) will be performed daily, Monday through Thursday and twice over each weekend. These tapes will be stored onsite after the incremental backup cycle. A full backup will be performed once each weekend (Friday, Saturday or Sunday depending upon the system schedule). These tapes will be stored offsite at an appropriate facility. The schedule in the table above refers to the weekly full backup for the retention schedule.

References:
Title 5~~,~~ Sections 59020 et seq.; Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37 and 45~~.~~

Procedure Last Revised: ~~March 13, 2013,~~ April 10, 2013
Last Reviewed: