Sierra College
ADMINISTRATIVE PROCEDURE AP 3721

Data Backup and Recovery Procedures

Date Adopted:	4/13/2012
Date Revised:	10/10/2025
Date Reviewed:	10/10/2025
References:	Government Code Sections 6250 et seq; California Code of Regulations Title 5, Sections 59020 et seq.; Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45; Education Code Section 71091 and 76200 et seq.; Title 5 Sections 54600 et seq., 20 U.S. Code Section 1232g (j); Civil Code Section 1798.85; The Family Educational Rights and Privacy Act; ACCJC Accreditation Standard 2

1. PURPOSE

The purpose of this procedure is to enhance the recoverability of District data and critical applications in a manner to coincide with District business continuity goals. Goals are identified as follows:

Recovery Point Objective (RPO) – The point in time that data must be recovered (hourly, daily, weekly, monthly, etc.).

Recovery Time Objective (RTO) – How long the recovery process must take in order to meet the RPO (4 hours, 24 hours, 2 weeks, etc.).

A Disaster Recover List for District mission critical applications and data will be maintained by the District's Information Technology Services (ITS) Division based on peer reviews performed periodically by the District's Educational Technology Advisory Council (Ed Tech) and the Team Leads (functional Leads and Data Stewards). ITS will assure that backup and recovery capabilities are in place to meet the RPO and RTO established for mission critical applications called for in this procedure pending available funding.

2. RETENTION POLICIES

Backup schedules and rotations must comply with Data Retention requirements as stated in Administrative Procedure 3300 – Public Records, Administrative Procedure 3310 – Records Retention and Destruction, and Administrative Procedure 5040 – Student Records, Directory

Information and Privacy or departmental Data Retention Standards. Data Retention Standards are defined and communicated to ITS by the Data Stewards (position defined in Administrative Procedure 3722 – Electronic Information Security) in the District's divisions/departments. It is the responsibility of the Data Steward in the division/department to assure Data Retention Standards are periodically reviewed and communicated to ITS unless otherwise documented in the District Board Policies and Administrative Procedures.

ITS will assure that data is backed up according to the recovery requirements requested by division/department Data Stewards and submitted to ITS. The system backups do not necessarily have to provide backups for the full duration of the data retention requirements as long as the data elements are accessible for the retention requirement. For example, some division/departments may require 7 years retention for spreadsheets that exist on a network server. As long as the server contains the files going back 7 years, the requirement is met. If the server is destroyed ITS may only need to restore the server from one day prior to the destruction of the server as long as the backup copy contains all files going back 7 years.

3. DOCUMENTED RECOVERY PROCEDURES

It is the responsibility of the ITS Division to assure that document recovery procedures (a Disaster Recovery Plan) are up to date and available in the event of a catastrophic event for all defined systems in the Disaster Recovery List from Section 1 above. The recovery procedures must be invoked by the District's Chief Technology Officer or member of the Executive Team whenever the invocation is necessary due to a declared emergency. In the event ITS is recovering a single failed server in the course of day-to-day operations the ITS Division will follow its standard server recovery procedures.

4. BACKUP AND DATA RETENTION

The District will maintain backup copies of critical system data on redundant disk, tape, or other available media in geographically diverse locations for a minimum of seven days. Additionally, ITS shall maintain at least one set of off-line or immutable backups. Backups are designed to recover from a complete server failure or catastrophic event and are not designed for file restoration and archiving. Services for file recovery and archiving will be documented and communicated by ITS.

It is also necessary for the District to have a formal Policy and Procedure addressing data retention to establish what may or may not be accessible as evidence through e-Discovery and to preserve electronic and non-electronic records and other data which may be relevant evidence for or against any existing or reasonably likely claim or suit. Subject to that obligation, the District will treat electronic records and electronic mail messages as either public records or records that can be discarded the same as it would treat paper records. It is the responsibility of the Data Stewards to define records retention standards for both electronic and paper-based documents for all users who they authorize to have access to relevant data and communications.

See Board Policy 3720 and Administrative Procedure 3310