Data Backup and Recovery Procedures

Date Adopted: 4/13/2012
Date Revised: 11/2/2018
Date Reviewed: 11/2/2018

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 II.C.8

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 and Instructional Technology (IIT) Department 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). IIT 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 AP 3300 – Public Records, AP 3310 – Records Retention and Destruction, and AP 5040 – Student Records, Directory Information and Privacy or departmental Data Retention
Standards. Data Retention Standards are defined and communicated to IIT by the Data Stewards (position defined in AP 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 IIT unless otherwise documented in the District BP/AP’s.

IIT will assure that data is backed up according to the recovery requirements requested by division/department Data Stewards and submitted to IIT. 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 IIT 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 IIT Department 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 IIT is recovering a single failed server in the course of day-to-day operations the IIT Department 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 or tape media in geographically diverse locations for a minimum of seven days. 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 IIT.

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. The District will treat electronic documents and electronic mail messages as either public information or information that can be discarded the same as it would treat paper documents. 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.