SUBJECT: INFORMATION TECHNOLOGY DISASTER RECOVERY PLAN AND SERVER BACKUP

This Information Technology Disaster Recovery and Data Backup Policy provides for the continuity, restoration and recovery of critical data systems and continuous Information Technology Services (ITS). The Information Technology Department and individual staff members work together to ensure critical data are backed up on a rotational periodic plan and copies maintained at an off-site location. District departments must develop and maintain a written business continuity plan for critical services performed to mitigate the risk of long-term Information Technology (IT) system and data unavailability.

Information Technology Services (ITS) is responsible for the backup of data held in central systems and related databases. The Information Technology staff will consult with related district departments to ensure backup procedures meet their contingency arrangements.

The responsibility for backing up data held on the workstations of individuals, regardless of whether they are owned privately or by the district, falls entirely to the user (Policy 5831.4). Users should consult with IT support services about effective local back-up procedures.

The disaster recovery section of this policy applies to ITS who are responsible for critical systems and data collections managed centrally.

Note: critical is defined as those essential information systems, data, or communication systems that enable continuity or resumption of business processes in the event of a disaster.

Critical Data Backup

All server backups must conform to the following best practice procedures:

- All data, operating systems and utility files must be adequately and systematically backed up. (Ensure this includes all patches, fixes and updates)
- Records of what is backed up and location must be maintained
- Records of software licensing should be backed up
- The backup media must be precisely labeled and accurate records maintained
- Copies of the back-up media, together with the back-up record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site.
- Regular tests of restoring data/software from the backup copies should be undertaken, to ensure that they could be relied upon for use in an emergency.

Critical IT systems and for most important and time-critical data, mirror systems, or at least a mirror disk should be maintained for a quick recovering.

(Continued)

SUBJECT: INFORMATION TECHNOLOGY DISASTER RECOVERY PLAN AND SERVER BACKUP (CONT'D.)

Disaster Recovery
A disaster recovery plan can be defined as the ongoing process of planning, developing and implementing disaster recovery management procedures and processes to ensure the efficient and effective resumption of critical functions in the event of an unscheduled interruption.

Each district department will develop IT contingency plans as a critical step in the process of implementing a comprehensive contingency planning program. The plan should contain:

- detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption
- document technical capabilities designed to support contingency operations
- tailored to the organization and its requirements
- balance detail with flexibility

The disaster recovery plan will include Notification/Activation, Recovery, and Reconstitution Phases which address a specific action that the organization should take following a system disruption or emergency.

Review and Update
The disaster recovery plan shall be reviewed and updated on an annual basis, or as special events or circumstances dictate.

Related State, Local and District References
District faculty, staff, students, and employees are bound by all applicable laws, rule, policies, and procedures. This policy is not intended to limit the applicability of any law or policy and does not preclude District departments and related affiliate organizations from implementing supplemental or more stringent safeguards.

District Policy references:
3320 Confidentiality of Computerized Information
5565 Financial Accountability
5610 Insurance
5670 Records Management
5676 Privacy and Security for Student Data and Teacher and Principal Data
5681 School Safety Plan
5833 End User Backup
6420 Employee Personnel Records and Release of Information

Adopted: 9/9/2014
Reviewed by Superintendent and Director of Information Technology on 10/30/2023 with no recommended changes; approved by BOE 11/7/2023.