Minneota Public School District
District Procedures

Adopted: August 2023

Updated: October 2024

DISTRICT PROCEDURES: BACKUP AND RETENTION

1. PURPOSE

The purpose of these backup procedures is to ensure that critical data is securely backed up, and can be easily recovered in the event of a disaster, system failure or data loss. These procedures apply to all data and systems owned by Minneota Public Schools – ISD 414 and defines the backup requirements, procedures, and responsibilities for the Technology Director.

2. DEFINITION

Backup is the process of creating a copy of the data on our system that we would use for recovery in case your original data was lost or corrupted. We could also use backup to recover copies of older files if we have previously deleted them from our system(s).

3. PROCEDURES AND SCHEDULE

Backup Frequency:

3.1 All critical data must be backed up daily.

3.2 All non-critical data should be backed up at least once a week.

Backup Retention:

3.3 Daily backups must be retained for a minimum of 7 days.

3.4 Weekly backups must be retained for a minimum of 4 weeks.

3.5 Monthly backups must be retained for a minimum of 6 months.

3.6 Annual backups must be retained for a minimum of 7 years.

Backup Storage:

3.7 Backup data must be stored securely, in multiple locations.

3.8 Any backup media must be rotated on a regular basis to ensure that the most recent data is always available.

Backup Verification:

3.9 The Technology Director must verify the integrity of all backups by conducting test restores every 6 months.

3.10 Failed backups must be immediately investigated and remediated.

4. RESPONSIBILITIES

4.1 The Technology Director is responsible for implementing and maintaining the backup procedures.

4.2 Department managers, with assistance from the Technology Director, are responsible for ensuring that all critical data is identified and backed up as per these procedures.

4.3 All employees are responsible for ensuring that data is saved to the designated network locations to ensure proper backups.

5. DISASTER RECOVERY

5.1 In the event of a disaster or system failure, the Technology Director will restore data from the most recent backup.

5.2 The Technology Director will prioritize data recovery according to the needs of the district, as defined in the disaster recovery plan.

6. PROCEDURES REVIEW

6.1 These backup procedures will be reviewed annually to ensure that they remain relevant and effective.

6.2 Any changes to theses backup procedures must be reviewed by the Technology Director and Superintendent prior to being communicated to relevant staff.

7. COMPLIANCE

Employees who violate these procedures may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

8. EXCEPTIONS TO THESE PROCEDURES

Requests for exceptions to these procedures shall be reviewed by the Technology Director. Departments requesting exceptions shall provide such requests to the Technology Director. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the Technology Director, initiatives, actions, and a timeframe for achieving the minimum compliance level with the procedures set forth herein. The Technology Director shall review such requests, confer with the Superintendent, and communicate back with/to the requesting department.

9. RESPONSIBLE DEPARTMENT

The Technology Director and Superintendent are responsible for updating and maintaining these procedures, along with compliance with the procedures.