

Data Contingency Operations

EHA AJ

The intent of this document is to establish and implement policies and procedures for responding to an emergency or other occurrence (e.g. fire, vandalism, system failure, and natural disaster) which damages Crook County School District #1 data access capabilities. It applies to CCSD#1 in its entirety, including all work force members including, but not limited to, full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to student data and sensitive information by CCSD#1. All work force members are responsible for the security of protected information.

The core objective of this policy is to ensure the expeditious restoration of CCSD#1 critical resources while preserving the confidentiality, integrity and availability of student, teacher, Personally Identifiable Information (PII) and data otherwise deemed sensitive.

The superintendent will be responsible for ensuring the implementation of the requirements of this policy. Failure to comply with this or any other security policy will result in disciplinary actions as per policy. Legal actions also may be taken for violations of applicable regulations and standards such as state and federal rules to include the Family Educational Rights and Privacy Act (FERPA).

References:

- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
- International Standards Organization (ISO 27002).

Adopted: October 17, 2016