Internal Policies and Procedures of the Utah State Board of Education	
Policy #	05-08
Subject:	Data Protection
Date Approved	February 21, 2024
Policy Owner's Title	Chief Information Security Officer
Policy Officer's Title	Deputy Superintendent of Operations
References: NIST Special Publication 800-111	

1) Purpose and Scope

a) The purpose of this policy is to set a baseline for Utah State Board of Education (USBE) data protections.

i) This document should be used in conjunction with any Policies or official guidance from the USBE Privacy Office.

(1) Data Sensitivity shall be defined by the USBE Privacy Office.

b) This document shall apply as a minimum requirement for all data stored by USBE.

2) Policy

a) Data Documentation

i) All Data documentation should be reviewed yearly at a minimum by relevant employee parties.

ii) Data Inventory

(1) A data Inventory based on USBE's data management process should be regularly maintained. This inventory should include an inventory of sensitive data.

iii) Data Flow

(1) Data Flows should be documented. Data flows should include service provider data flows and be based on USBE's data management process.

b) Data Access

i) Employee data access permissions should be based off a user's need to know.

c) Data Encryption

i) Data at Rest

(1) At a minimum, data that has been defined as sensitive must be encrypted at rest on servers, applications, and databases.

ii) Data in Transit

(1) data that has been defined as sensitive must be encrypted while in transit.

(a) Transit encryption solutions include Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

iii) Removable Media

(1) All removable media should be encrypted.

(a) Encryption should be at a minimum standard of Advanced Encryption Standard (AES) 256 bit.

d) Data Retention

i) Data retention shall be defined by the USBE Privacy Office using data sensitivity rules as well as state and federal laws.

e) Data Segmentation

i) The processing and storage of data deemed to be of a high or critical sensitivity should be separated from that of lower sensitivity data.

3) Definitions

a) Data at Rest: all data in storage. Data at Rest includes but is not limited to archived data, data which is not accessed or changed frequently, files stored on hard drives, Universal Serial Bus (USB) thumb drives, files stored on backup tape and disks, files stored off-site, and on a storage area network (SAN).

b) Data in Transit: data that is actively moving from one location to another. This can be across the internet, within a private network, or from one device to another.

c) Removable Media: Portable data storage medium that can be added to or removed from a computing device or network. Examples include but are not limited to: optical discs (CD, DVD, Blu-ray); external/removable hard drives; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive).

4) Change History

Date	Version	Author	Changes Made / Section(s)
April 4, 2023	0.1.0	Patrick Hawkins	Initial Draft
December 15, 2023		Patrick Hawkins	Review and Update