Internal Policies and Procedures of the Utah State Board of Education	
Policy #	05-13
Subject:	Service Provider Management Policy
Date Approved	February 21, 2024
Policy Owner's Title	Chief Information Security Officer
Policy Officer's Title	Deputy Superintendent of Operations
References: -Center for Internet Security (CIS) Critical Security Controls – Control 15	

1) Purpose and Scope

a) The purpose of this policy is to set a baseline for the process to evaluate service providers who hold sensitive data or are responsible for a Utah State Board of Education's (USBE) critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.
   i) This document should be expanded upon with additional policies and USBE operating procedures created in tandem with relevant USBE parties.

2) Policy

a) An inventory of service providers should be established and maintained.
   i) The inventory is to list all known service providers, include classifications, and designate an enterprise contact for each service provider.
   ii) The inventory should be reviewed and updated at least annually, or when significant enterprise changes occur.
b) A service provider management policy should be established and maintained.
   i) The policy should address the classification, inventory, assessment, monitoring, and decommissioning of service providers.
   ii) The policy should be reviewed and updated at least annually, or when significant enterprise changes occur.
c) A Classification system for service providers should be established and maintained.
   i) Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk.
   ii) Classifications should be reviewed and updated at least annually, or when significant enterprise changes occur.
d) Service provider contracts should include security requirements.
   i) Requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments.
   ii) These security requirements must be consistent with the enterprise's service provider management policy.

iii) Service provider contracts should be reviewed annually, or when significant enterprise changes occur.

3) Change History

Date	Version	Author	Changes Made / Section(s)
August 22, 2023	0.1.0	Patrick Hawkins	Initial Draft