Internal Policies and Procedures of the Utah State Board of Education	
Policy #	05-07
Subject:	Continuous Vulnerability Management
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 800-53 Rev. 5 -Vulnerability Management Process -Vulnerability Remediation Process	

1) Purpose and Scope

a) This policy sets forth a minimum set of requirements to continuously assess and track vulnerabilities on all enterprise assets within the Utah State Board of Education (USBE) infrastructure.

2) Policy

a) Documents should be created and maintained to define processes for:

i) Vulnerability Management

(1) This documentation should be reviewed and updated at least annually, or when significant enterprise changes occur that could impact this Safeguard.

ii) Risk-Based Remediation Process:

(1) This documentation should be reviewed at lease monthly.

b) Automated Patch Management

i) Operating System updates should be performed through automated patch management on at least a monthly basis.

ii) Application updates should be performed through automated patch management on at least a monthly basis.

c) Automated Vulnerability Scanning

i) Automated vulnerability scans should be performed, at least monthly, on all USBE assets by a Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool.

(1) Both authenticated and unauthenticated scans should be performed.

(2) Tools can include: Tenable, CIS-CAT Pro Assessor, Microsoft System Center Configuration Manager, etc.

d) Vulnerability Remediation

i) Based on the Remediation process, detected vulnerabilities should be remediated at least monthly.

3) Change History

Date	Version	Author	Changes Made / Section(s)
May 25, 2023	0.1.0	Patrick Hawkins	Initial Draft
