Internal Policies and Procedures of the Utah State Board of Education	
Policy #	05-10
Subject:	Malware Defense
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 10	

1) Purpose and Scope

a) The purpose of this policy is to set a base line for the prevention and control of the installation, spread, and execution of malicious applications, code, or scripts on Utah State Board of Education (USBE) assets.
   i) This document should be expanded upon with additional policies and USBE operating procedures created in tandem with relevant USBE parties.

2) Policy

a) Anti-Malware software must be deployed and maintained on all USBE assets.
   i) Anti-Malware signature updates should be configured to automatically update on all USBE assets.
b) Anti-Malware Software
   i) Anti-malware software should be managed centrally.
   ii) Behavior-based anti-malware software should be used in tandem with signature based anti-malware software.
c) Anti-exploitation features should be enabled on all USBE assets and software, where possible.
   i) Examples include Microsoft Data Execution Prevention (DEP), Windows Defender Exploit Guard (WDEG), and Apple System Integrity Protection (SIP).
d) Removable Media
   i) Autorun and Autoplay for removable media should be disabled.
   ii) Anti-malware software should be configured to automatically scan removable media.

3) Change History

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