

STATE OF HAWAII
Office of Enterprise Technology Services Policy No. 508.01
Secure Device Standards
Effective Date: December 1, 2017
Revision No./Date: September 18, 2018

Category	Minimum Standard	Comments
Operating systems	Operating systems must have mainstream support by the vendor	This is typically the current or immediately prior generation, i.e., "N-1" (e.g., Windows 8 and 10)
Operating system and application updates	Enabled	When manual updates are required, reasonable effort should be made to stay current
Device management platform compatibility	Microsoft Intune (if supported)	Mobile device management software with enabled remote location and erase services
Device passwords	Desktop/Laptop: 10 characters Mobile device: 6 characters All passwords must be unique	
Device biometric security	Acceptable (provided the overriding device password meets standard above)	Examples of biometrics include thumb print and facial recognition
Multi-factor authentication (MFA)	Enabled for remote access	Also known as 2-factor authentication and login verification
Host-based firewall	Enabled on the endpoint (if supported)	Also known as personal firewall
Screen lock	Manual and auto screen lock functionality enabled (users must manually lock device screen when intentionally leaving the device unattended, in addition to enabling auto screen lock timer) Desktop/Laptop: Auto lock after 15 minutes Mobile device: Auto lock after 5 minutes	Device shall require reentry of password or biometrics after specified time
Full-Device/Disk encryption	AES 128-bit or higher (if supported)	Effective immediately for existing devices, if supported, and all NEW devices, without exception Effective July 1, 2018, for all devices
Device endpoint protection	Anti-Malware/Virus enabled and updating regularly (excluding Apple iOS)	
"Jailbroken" or "rooted" devices	Prohibited	Jailbreaking or rooting refers to mechanisms that involve overriding manufacturer controls and permissions