Mobile Device Standards

Contents

Subject	Effective Date	Division / Area	Approval:	Signature
Mobile Device Standard	Effective Date: 03/27/2024 Issue Date: 03/27/2024 Review Date: 03/27/2025	Business & Finance / Office of Information Technology	Rose McAuliffe VP Business & Finance/CFO 3/25/2024 Al Speckens Interim Deputy CIO 3/25/2024	 

Revision History

Standard	Effective Date	Email	Version	Contact	Phone
OIT-SEC	March 27, 2024	security@csustan.edu	1.0	ASpeckens@csustan.edu	209.667.3894

Executive Summary

Mobile devices are often used to access and sometimes store sensitive university data. Whether university or personally owned the devices need protection and to be used appropriately. This standard outlines the controls applied to university owned mobile devices and expected to be used on personally owned devices used to conduct university business.

Introduction and Purpose

This standard defines the requirements for the use of mobile devices at Stanislaus State with the goal of safeguarding the confidentiality, integrity, and availability of information stored, processed, and transmitted by mobile devices while doing Stanislaus State business.

Scope

This standard applies to all Stanislaus State, Self-Funded, and Auxiliary ("campus") computer systems and facilities (including Stanislaus State remote network locations), with a target audience of Stanislaus State Office of Information Technology (OIT) employees. For the purposes of this document, mobile devices include but are not limited to cellular phones, cellular WiFi hotspots, smartphones, tablets, any portable computing device, smart watches, etc. These devices will either be university owned or personally owned, both are in-scope for these standards since they may be used to conduct university business and access to university systems and data.

Standard

Secure Configuration

University owned devices must be enrolled in appropriate mobile device management platforms and configured to accept configuration changes from it.

The ability to side-load or use 3rd party app stores should be disabled. Settings the enforce the use of applications from known developers should be applied.

Regular backup of devices will be enabled and scheduled.

Device Encryption

To the extent supported by the device encryption will be used to secure the data, applications, and operating system.

Locking

Auto-locking with passcode or passphrase needed

Anti-malware

Device appropriate anti-malware should be installed, up to date, and operating. Applications from unknown developers and 3rd party app stores are not permitted on university owned devices.

Secure Wireless Communications

WiFi networks used by devices should be secured with encryption. If appropriate for the work being done from a mobile device the VPN client should be installed and used.

University owned devices will be enrolled in mobile devices management tools appropriate to the device by OIT.

Physical Security

Mobile devices tend to be small and easily forgotten or left behind. At airports, in public spaces be sure your device is with you before leaving. Do not leave devices unattended or in vehicles.

Device Disposal

Mobile device disposal will follow all asset management processes as outlined by Property Management. Devices will be wiped before transfer to a new user. At the end of the device's useful life, they will be wiped and recycled.