CALIFORNIA STATE UNIVERSITY
FULLERTON

Division of Information Technology
800 N. State College Blvd., LH 700
Fullerton, CA 92831
657-278-8500

Mobile Device Policy

Division:

Information Technology Services

Contact Information:

Berhanu Tadesse / *Associate Vice President for Information Technology/ Academic Technology Services* Division of Information Technology / 657-278-8748

Effective Date:

June 1, 2022

Revised Date:

May 23, 2022

Authority:

ICSUAM 8045.S400 - Mobile Device Management Standard
ICSUAM 8050 - Configuration Management
ICSUAM 8060 - Access Control - Appendix A
ICSUAM 8065.S02 - Information Security Data Classification
ICSUAM 8075 - Information Security Incident Management
ICSUAM 8105 - Responsible Use Policy

Objective:

The purpose of this policy is to secure university mobile computing devices that access or store CSUF sensitive data. The measures specified herein must be followed by all CSUF Employees and Faculty to protect university data and ensure compliance with Federal and State laws and regulations, and CSU and CSUF policies and procedures governing security of information. Only CSUF-issued owned devices are approved for use with sensitive data.

Definitions:

Mobile device: Mobile computing devices such as laptops, tablets, and smartphones excluding traditional Internet of Things (IoT) devices such as sensors or cameras.
Sensitive data (Levels 1 and 2): Campus data is classified according to its potential risk which is governed by federal and state laws. Sensitive data includes confidential (Level 1) and internal use (Level 2) data classifications. See the CSU Data Classification for more information.
Confidential data (Level 1 - Encryption Required): Level 1 data is considered confidential must be appropriately secured. If Level 1 data is lost, stolen or accessed by unauthorized individuals, it must be reported to ISO@fullerton.edu and may require a formal breach notification to impacted individuals under state and federal law.
Internal Use data (Level 2 – Encryption Strongly Recommended): Level 2 data is for internal use and may only be released under prescribed conditions. If Level 2 data is lost, stolen or

accessed by unauthorized individuals, it must be reported to ISO@fullerton.edu immediately and may require formal breach notification under state and federal law.

Statement:

User Practice for Securing Devices

Sensitive data (Levels 1 and 2) must not be accessed from or stored on mobile devices unless:

1. The device is university-owned
2. There is a documented business need for the sensitive data to be accessed or stored by the mobile device
3. Effective security measures have been implemented to protect the data
4. Full-device or container encryption is enabled.

Required Mobile Device Security Measures

General security measures for mobile devices used for university business:

- Contact the IT Help Desk if a mobile device is compromised, lost or stolen
- Frequently check for and install any available security updates & patches
- Only download and install apps from trusted app stores (Apple App Store, Google Play, Microsoft Store, etc.)
- Remove or refrain from downloading and installing unverified apps
- Do not leave mobile devices unattended
- Follow the CSUF Mobile Device Passcode Policy and or CSUF Password Policy

Device Access Security Measures

- Mobile devices that access or store sensitive data must be screen locked during inactivity
- Unlocking requires strong authentication, such as: a passcode, or password, or biometric functionality

Required Sensitive Data Security Measures

Sensitive data security measures apply to mobile devices that access or store data classified as confidential level 1 and internal use level 2.

- Use wireless networks that support reliable encryption (802.1x)
- Auto-wipe device after 10 failed login attempts
- Configure device to be remotely wiped in the case it is lost or stolen
- Wipe or securely delete data from mobile devices before disposing, reselling, or trading them in.
- Wireless encrypted security and access protocols shall be used with all wireless network connections. Staff shall refrain from using public or unsecured network connections while using their mobile device.

Required Confidential (level 1) Data Security Measures

Security measures for securing mobile devices that access or store confidential level 1 data:

- Limit access to the device to those that need to access the confidential data
- Disable Bluetooth and wireless access when not needed
- Use CSUF's VPN when accessing confidential (level 1) data
- Advance approval is required for storing confidential (level 1) data on a mobile device.

User Responsibilities

- Employee shall immediately report any lost or stolen devices to IT Help Desk
- Unauthorized access to a mobile device or data must be immediately reported
- Only approved applications are allowed
- Employees are responsible for ensuring all important files stored on the mobile device are backed up on a regular basis.
- Employee shall not modify configurations
- Employee shall ensure to maintain physical security at all times (locked and stored away and not in plain sight)

Implementation

Responsibility for implementing this Policy will rest with the Division of Information Technology. Submit any apparent violation of Password Policy to the appropriate administrative authority (vice president, dean, director, department, or program chair) or to ISO@fullerton.edu.

Non-Compliance

Noncompliance with applicable policies and/or practices may result in suspension of network and systems access privileges. In addition, disciplinary action may be applicable under other University policies, guidelines, implementing procedures, or collective bargaining agreements.