Siskiyou County Mobile Use Policy

Approved by the Siskiyou County Board of Supervisors on December 5, 2023.

Table of Contents

1. Overview

This policy applies to all Siskiyou County employees and contractors. Mobile devices represent an ever-increasing demographic in modern computing environments. Their mobility and remote access pose a different set of security risks to be addressed with this policy.

2. Purpose

The purpose of this policy is to define the standards, procedures and protocols for the use of mobile devices in relation to Siskiyou County, or related California State networks, data, websites, web applications, cloud storage and other systems.

3. Scope

This policy applies to all Siskiyou County staff who use mobile devices for County business purposes. Personal use of County-owned equipment is prohibited. Additional policies from State or County departments may apply further requirements.

4. Definitions

Mobile devices include the following categories:

a. Laptop/Notebook,

b. Convertible devices such as Microsoft Surface Pro,

c. Tablets such as iPads,

d. Mobile/cellular phones,

e. Smartphones.

f. PDAs,

g. And any other mobile device capable of connecting to managed systems and/or storing County data.

5. Policy

A. GENERAL

All mobile devices, whether owned by Siskiyou County or owned by staff, that have access to County systems and applications are governed by this policy. Applications accessible remotely by staff on their own personal devices are also subject to this policy. The following general procedures and protocols apply to the use of mobile devices:

1. Mobile computing devices must be protected with an approved authentication method required at the time the device is powered on and on every subsequent login.

2. Authentication methods must meet the requirements outlined in the Siskiyou County Access Control and Authentication Policy.

3. All data stored on mobile devices shall be encrypted.

4. Wireless encrypted security and access protocols shall be used with all wireless network connections.

5. Staff shall refrain from using public or unsecured network connections while using a mobile device for work.

6. Staff shall adhere to all related HIPAA and confidentiality or other State and County requirements regarding forms of communication.

7. Staff whose job duties require regular or occasional driving are expected to refrain from using a mobile device while driving and abide by all Federal and State laws.

    a. Staff who are charged with traffic violations resulting from the use of mobile devices while driving will be solely responsible for all liabilities that result from such actions. Staff will be subject to disciplinary action, up to and including termination of employment.

8. Staff shall not use County owned devices for any personal use and may not store any personal data on the device.

9. Personal mobile computing devices that require network connectivity must conform to all applicable Siskiyou County policies.

10. Personal devices used for business shall be registered with the respective IT Team as well as the Communications Department and must be approved for use by their department head in coordination with Risk Management. Use of personal devices for County business is not recommended.

11. Unattended mobile computing devices shall be physically secured.

12. Devices that access the County network shall have active and up-to-date anti-virus, firewall, and Mobile Device Management (MDM) software installed.

13. Lost or stolen devices shall have locations services enabled and the units locked or wiped of all information, so they are unusable until recovered or destroyed.

B. USER DEVICE RESPONSIBILITIES

The following procedures and requirements shall be followed by all users of mobile devices:

1. Staff shall immediately report any lost or stolen devices.

2. Unauthorized access to a mobile device or County data must be immediately reported.

3. Mobile devices shall not be “rooted” or have unauthorized software/firmware installed.

4. Staff shall not load illegal content or pirated software onto any mobile device.

5. Only approved applications are allowed on mobile devices that connect to the County network.

6. Mobile device operating systems and applications shall be kept up to date (within 30 days of release).

7. All mobile device physical storage partitions shall be encrypted.

8. Firewalls shall be installed and active where applicable.

9. Staff shall use the County email system when sending or receiving County data.

10. Staff shall not store any County data directly on the device where possible, instead using provided cloud storage.

11. Staff understands that Mobile Device Management (MDM) will be used to enforce common security standards and configurations on devices including personal devices.

12. Staff shall not modify configurations without express written authorization from their respective IT Team.

13. Staff are expected to follow applicable local, state, and federal laws and regulations regarding the use of mobile devices at all times.

14. Driving while using mobile devices is not permitted.

15. When using visual and audio options, such as a video conference call service, staff are required to ensure that they are in a secure environment and that no confidential or sensitive information are in view or can be heard while utilizing the video call or conference call service.

C. ADMINISTRATIVE RESPONSIBILITIES

Siskiyou County IT Team shall implement procedures and measures to strictly limit access to sensitive data moving to and from mobile computing devices since these devices generally pose a higher risk for incidents than non-portable devices.

Respective Siskiyou County IT Team shall ensure:

1. Specific configuration settings shall be defined for personal firewall and malware protection software to ensure that that this software is not alterable by users of mobile and/or employee-owned devices.

2. Use of MDM software to manage risk, limit security issues, and reduce costs and business risks related to mobile devices. The software shall include the ability to inventory, monitor (e.g., application installations, issue alerts) (e.g., disabled passwords, categorize system software operating systems, rooted devices), and issue various reports (e.g., installed applications, carriers).

3. Use of MDM software to enforce security features such as encryption, password, bricking, and key lock on mobile devices.

4. Use of MDM software to include the ability to distribute applications, data, and global configuration settings against groups and categories of devices.

5. Completion of regular reviews and updates of security standards and strategies used with mobile computing devices.

6. Development of procedures and policies exist to manage requests for exemptions and deviations from this policy.

6. Audit Controls and Management

Documented procedures and evidence of practice must be in place for this operational policy. Examples of evidence and compliance include, but are not limited to:

1. User training for compliance with mobile device computing policies,
2. Readily available policies and procedures for staff use of mobile devices,
3. Configuration and support guidelines and procedures for mobile devices,
4. And device logs showing appropriate protocols are in place.

7. Enforcement

Staff members found in violation of this policy will be subject to disciplinary action, up to and including termination of employment.

8. Distribution

This policy is to be distributed to all Siskiyou County staff and contractors through email, or intranet portals.