CITY OF SPOKANE
ADMINISTRATIVE POLICY

ADMIN 5300-21-08
LGL 2021-0033

TITLE: MOBILE DEVICE MANAGEMENT
EFFECTIVE DATE: 12/21/2021
REVISION EFFECTIVE DATE:

1.0 GENERAL

1.1 The purpose of this policy is to define the requirements for all city-owned mobile devices. This policy shall include devices issued by the city that are used for business purposes and vendor-provided/required devices.

1.2 TABLE OF CONTENTS

2.0 DEPARTMENTS/DIVISIONS AFFECTED

Applicable to all departments and divisions of the City of Spokane.

3.0 REFERENCES

City of Spokane’s Information Security Policy – ADMIN 5300-17-06

City of Spokane’s City and personally owned communication devices (including cell phones) and city and personally owned email and social media accounts Policy – ADMIN 5600-17-06

Center for Internet Security - Top 20 Critical Security Controls for Effective Cyber Defense Guidelines

Criminal Justice Information Systems. Policy Area: 13: Mobile Devices

National Institute of Standards and Technology (NIST) Cybersecurity Framework Guideline - Version 1.1

National Institute of Standards and Technology: Special Publication 800-124, Revision 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise

Office of the Chief Information Officer, Washington State – Standard No. 141.10: Securing Information Technology Assets Standards

RCW 19.255.020 - Liability of Processor, businesses, and vendors

RCW 19.255.101 - Disclosure, notice

RCW 42.56.420 - Security

The Health Insurance Portability and Accountability Act of 1996. Pub. L. 104-191.

4.0 DEFINITIONS

4.1 "Bring-Your-Own-Device" (BYOD) is personally owned devices but not limited to, cellphones, computers that could be used for work purposes.

4.2 "Information Technology Resources" or "IT Resources" means hardware, software, and communications equipment including, but not limited to, personal computers, email, internet, mainframes, wireless, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services or facsimile machines. In addition, technology facilities (including but not limited to: data centers, dedicated training facilities, and switching facilities), and other relevant hardware and software items. In addition, personnel tasked with the planning, implementation, and support of technology.

4.3 "Jailbreak or rooted" of a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software. "Rooting" is the process of gaining root access to a device. This is generally performed on Android devices.

4.4 "MDM" is mobile device management which is a type of security software used by the City of Spokane's Innovation and Technology Services Division (ITSD) Help Desk, Spokane Police Department's (SPD) Technical Assistance Response Unit (TARU), Spokane Fire Departments (SFD) Information Technology (IT) and Public Works ITSD (PWITSD) staff to monitor, manage and secure city-owned mobile devices.

4.5 "Mobile device" is a portable computing device such as a smartphone or tablet computer. This definition does not include computer laptops.

4.6 "Sideloading" is the name used for installing applications directly on a mobile device rather than using the App Store.

4.7 "USB debugging" is a developer mode on devices that allows newly programmed applications to be copied via USB to the device for testing.

5.0 POLICY

5.1 Requirements

5.1.1 In accordance with the City of Spokane's City- and Personally-owned communication devices (including cellphones) and City- and Personally-owned email and social media Policy (ADMIN 5600-17-06), using a personal device for City business may result in personal records being subject to a public records request.

5.1.2 The City of Spokane will protect Protected Health Information and Criminal Justice Information in transit, at rest, and stored on portable technology devices from the threat of loss, theft or unauthorized access.

5.1.3 City-owned technology devices capable of connecting to a city-managed network must have MDM software installed and utilized at all times. An exemption may be granted for certain devices used for investigative purposes by SPD. Devices exempted from the MDM requirement shall not connect to the city-managed networks.

5.1.4 Users may only load corporate data that is essential to their role onto their mobile device(s).

5.1.5 All city-deployed mobile devices shall be managed to ensure security configuration compliance.

5.1.6 All city deployed mobile devices shall have the default device name changed for tracking and monitoring purposes.

5.1.7 All mobile devices shall be kept up to date with manufacturer Operating System (OS) provided patches.

5.1.8 All personal use is subject to public records requests.

5.1.9 Debugging mode shall be permitted for business purposes only.

5.1.10 Personal Apple or Google accounts shall be restricted from city-deployed devices. A city-issued Apple or Google account will be provided.

5.2 Bring-Your-Own-Device

5.2.1 The connection of personally owned devices is not allowed on the city managed network

5.2.2 City managed MDM software shall not be permitted on any personally owned devices.

5.3 Lost/stolen & Remote Wipe/Sanitation Requirements

5.3.1 City staff must report all lost or stolen city-owned devices to their assigned Help Desk immediately.

a. City staff should contact the ITSD Help Desk

b. Spokane Police Department staff must report all lost or stolen city-owned devices to TARU immediately.

c. Spokane Fire Department staff must report all lost or stolen devices to their assigned help desk immediately.

d. Public Works staff must report all lost or stolen devices to their assigned PWITSD support group immediately.

5.3.2 If a device is lost or stolen, the data on the device shall be remotely erased and the device shall be reset to its default factory settings.

5.4 WIFI Regulations

5.4.1 City-owned devices are allowed to access city wireless networks and other work-related wireless networks.

5.4.2 Outside of the City of Spokane's internal networks, auto-connect Wi-Fi shall be restricted.

5.5 Password Requirements

5.5.1 Devices shall be configured with a secure password.

5.6 Software Installation Guidelines

5.6.1 Unauthorized software shall be restricted.

a. A list of authorized software shall be maintained within each IT Support group that is unique to their compliance requirements.

5.6.2 Requested software will be reviewed and approved by the ITSD Help Desk in coordination with SPD TARU, SFD-IT and PW ITSD when needed.

5.6.3 Prevention of sideloading of non-market application installations shall be enforced.

5.7 Jailbroken or rooted devices

5.7.1 Devices must not be “jailbroken” or “rooted” or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

5.7.2 Such devices shall be denied access to the City’s network and returned to the appropriate support organization.

5.8 Violation

5.8.1 Failure to comply with this policy, processes, and procedures may lead to disciplinary or remedial action.

6.0 RESPONSIBILITIES

6.1 ITSD Director

6.1.1 The ITSD Director shall administer this policy.

6.2 ITSD Security Office

6.2.1 The ITSD Security Office shall be responsible for providing guidelines to ensure the effectiveness of this policy. In addition, at any time to ensure compliance, the ITSD Security Office may audit implementations of this policy.

6.3 ITSD Help Desk

6.3.1 The ITSD help desk shall implement technology to enable this policy to be effective and are responsible for ensuring the effectiveness of this policy for their divisions.

a. The ITSD Help Desk will coordinate with PWITSD for ensuring effectiveness of this policy with Public Works requirements.

6.4 Spokane Police TARU

6.4.1 SPD's TARU unit shall be responsible for ensuring the effectiveness of this policy for their division and managing MDM software for SPD staff.

6.5 Spokane Fire Department Help Desk

6.5.1 Fire IT help desk shall be responsible for ensuring the effectiveness of this policy for their division and managing the MDM software for SFD staff.

7.0 APPENDICES

7.1 None.

APPROVED BY:

DocuSigned by:
Eric Finch
295098100B81411...
Eric Finch
Chief Innovation & Technology Officer

12/21/2021
Date

DocuSigned by:
James Richman
59DFB076D0684D7...
James Richman
City Attorney

12/20/2021
Date

DocuSigned by:
Johnnie Perkins
I96A908C563754B1...
Johnnie Perkins
City Administrator

12/21/2021
Date