Mobile Device Use for City Business Policy

Committee on Information Technology

The City and County of San Francisco (City) is dedicated to building an effective cost management and strong cybersecurity program to support, maintain, and secure critical infrastructure and data systems.

PURPOSE AND SCOPE

Chapter 22I of the City Administrative Code establishes the City Chief Information Security Officer's duty to develop and update citywide cybersecurity requirements to mitigate the City's risk and comply with legal and regulatory cybersecurity requirements. The purpose of these requirements is to establish a policy for both secure and cost-effective management of mobile devices, such as smartphones and tablets, used for City business.

The requirements identified in this document apply to digital information and technology operated by or for the City and County of San Francisco and its departments and commissions. Elected officials, employees, contractors, partners, bidders, and vendors working on behalf of the City and County of San Francisco are required to comply with this policy.

Cybersecurity Officers, Liaisons, Information Technology (IT) Professionals, and Finance/Budget Professionals have a joint responsibility to implement the following technical and fiscal requirements. Departments should subsequently develop departmental policies or processes that should be equivalent to or greater than these Citywide requirements to encompass department-specific practices, promote cost-effectiveness, and reduce potential risks.

POLICY REQUIREMENTS

All City departments must adopt the following minimum requirements:

Issuance and Decommissioning of City-Owned Mobile Devices

- *New Device Procurement* – Telecommunication carriers often offer beneficial pricing for device models released 12-24 months prior to the latest device model. These earlier models have substantially similar technical capabilities with the latest models, and departments should strongly consider procuring these earlier device models to maximize potential cost benefits and minimize potential equipment charges in the event of early termination of services.

- *Issuance Approval* - A departmental process and criteria for requesting, reviewing, and approving or rejecting the issuance of City-owned mobile device(s) must be established. See Appendix A for sample approval form.
- *Record of Devices* - Issuance and approval of City-owned mobile devices must be recorded with appropriate business justification and information regarding the requester, approver, and device.

- *Replacement of Lost or Damaged Devices* – Departmental approval and issuance processes should track and manage requests for replacement devices.

COIT Policy Dates
Approved: September 21, 2023

- *Review of Device Inventory* - Inventory of City-owned mobile devices must be reviewed quarterly, at a minimum, to affirm that devices are necessary for City business, identify mobile devices with no activity, and to facilitate the suspension of City payments for mobile devices no longer needed for City business.

- *Return and Decommissioning* – City-owned mobile devices must be returned to the City when no longer in use or not required for City business for re-issuing or decommissioning. City-owned devices must be wiped and re-imaged prior to re-issuing or decommissioning the device.

- *Separation from the City* – City data on City-owned mobile devices must be deleted upon separation of staff from City employment or contract.

Configuration of City-Owned Mobile Devices

- *Device Version and Model* – City-owned mobile devices must meet minimum version(s) and type(s) of operating system and minimum device model(s) that support City technical safeguards. **Note:** minimum device models are not necessarily the newest available model.

- *Security Configuration* - City-owned mobile devices must be configured with approved safeguards (e.g., approved mobile apps for City data) before being used for City business.

- *Updated Operating System* – City-owned mobile devices must be updated to the latest patch level of a supported operating system no later than 14 days of the update being issued by the operating system manufacturer.

- *Device Lock Required* – City-owned mobile devices must require a passcode, at a minimum, to unlock the device.

- *Deleting City Data* - City data on City-owned mobile devices must be automatically deleted if an incorrect passcode is repeatedly entered, upon detection of tampering with device's operating system (i.e., jailbreaking), or if the mobile device does not connect with City systems for a designated period of time.

Data and Legal Protection

- *City Data and Document Storage* - City data and documents must be stored and accessed using approved and protected mobile applications.

- *Public Records Laws* - City data and documents are subject to public records laws.

- *Information Security Records* - Information security records, such as data generated by mobile authentication apps or security codes and passwords sent to mobile devices, are generally exempt from public records disclosure under California Public Records Act exemptions.

Physical Security Protection

- *Theft or Loss Protection* – City-owned mobile devices must be protected from loss due to theft or vandalism and must remain in the possession of a person to whom the device is issued, unless they have been deposited in a secure location such as a locked City office, locked location at home, trunk of a car, or a hotel safe.

- *Immediate Reporting Lost Devices* – Lost or stolen City-owned mobile devices must be reported immediately. City data must be deleted from these devices and City-owned mobile devices must be disabled.

ROLES AND RESPONSIBILITIES

City Chief Information Security Officer (CCISO) shall:

- Support departments' implementation of these requirements, including providing centralized cybersecurity capabilities and a citywide cybersecurity toolset for the departments to leverage.
- Revise Citywide cybersecurity requirements upon changes in the City risk profile, regulation, or legislation.

Departmental IT Leaders/ Chief Information Security Officers (CISOs)/ Information Security Officers (DISOs) shall:

- Adopt and implement requirements in this standard. Department-specific policies and requirements must be equivalent to or greater than these Citywide requirements.
- Implement requirements by utilizing citywide cybersecurity toolset and Department resources.

Department Telecom Authorized Contacts (TACs) and Procurement Staff shall:

- Ensure device requests (see Appendix A for an example) include:
    1) Requesting employee's name and job class,
    2) justification for use of City-owned mobile devices,
    3) departmental approver's name and job class,
    4) type/model of requested devices, and
    5) the estimated cost.
- Support the administration of and adherence to department-specific mobile device management policy or process.

Department Chief Financial Officer (CFOs) / Finance or Budget Directors / Departmental Leadership shall:

- Develop department-specific process for reviewing business needs for mobile devices, manage device requests for new or replacement devices.
- Consider the costs and benefits of providing City-owned mobile devices to optimize the use of City general funds.
- Evaluate the rate plan and usage of each mobile device to ensure optimal cost-effectiveness for all use cases when the rates are updated or at least annually.
- Inform department TAC, as needed, to disconnect or deactivate underutilized mobile devices, or provide written justification to the Department of Technology to maintain existing lines and devices.

IMPLEMENTATION GUIDANCE

Requirements in this COIT policy will come into effect 90 days after the publication date. Departments should prepare for implementation of requirements by analyzing existing CCSF technology platforms and developing a risk-based implementation plan.

Departments should consider utilizing a City-wide platform to support implementation of this policy.

Procured or implemented CCSF technology platforms must meet requirements in this policy.

EXCEPTIONS

Exceptions, whether related to security or fiscal requirements, to the standards shall by approved on a case-by-case basis by each Departmental CISO/ISO, who shall record all such expectations with the City CISO, and review said exceptions at least annually.

Citywide cybersecurity and fiscal requirements shall not supersede State or Federal requirements that may apply to certain specific City departments.

Appendix A

CITY AND COUNTY OF SAN FRANCISCO

JUSTIFICATION FOR ACQUISITION AND USE OF MOBILE DEVICE REQUEST

The purpose of this form is to request a City-owned mobile device (cell phone, tablet, or hotspot).

USER INFORMATION

NAME:		CLASS		TITLE	
DEPT:		OFFICE PHONE:			

DEVICE INFORMATION

□New Device □Upgrade □Replacement □Transfer From: _________to: ___________

Device Phone #

Use Existing Phone #: □Yes □No

I am requesting approval for a:

□ Smartphone

□ Tablet

□ Hotspot

Time frame for anticipated use:

□Indefinite

□Intermittent project work

□Other (specify):

Cellular Provider:

□AT&T □T-Mobile □Verizon

□FirstNet *Justification*: *Only first responders and public safety personnel, such as dispatchers, are eligible to use FirstNet. The reserved bandwidth and frequency preemption (right of first use during emergencies) make the eligibility requirements strict.*

JUSTIFICATION: Job responsibilities require (check all that apply):

□ Constant access to data sources, network resources and/or other systems to conduct official Government business when routinely out of the office (e.g., telecommuting, attending meetings, serving customers and patients, traveling)

□ Provide technical assistance to customers and be immediately available to receive their request(s)

□ Engage in extended communications and/or monitor projects to support mission-related activities beyond the standard workday/workplace.

□ Have a back-up communication resource to use in the event of network disruptions that could negatively impact operations.

□ Have access to vital and frequently automated information when there is no other immediate means.

□ Other (please specify):

SIGNATURES:

Immediate Supervisor: ______________________________________ Date:________________________

Department Head: ______________________________________ Date:________________________

DECISION:

□ Approved □Disapproved

Comments: