SUBJECT	Number	Issue	Page
	90.66	2	1 of 6
MOBILE DEVICE SECURITY	Effective Date January 17, 2020		

1. PURPOSE

1.1. To establish rules that govern the use of *smartphones*, *tablets*, and other *mobile devices* used for City of San Diego (City) business.

1.2. To protect the confidentiality and integrity of data and applications, and the availability of services.

1.3. To protect the *mobile devices* and the data residing on them, as well as maintain continuity of the services that the City provides.

1.4. The City's information and communications technologies are provided for the benefit of *users* in providing public services.

2. SCOPE

2.1. This administrative regulation applies to City-owned and personally-owned *smartphones*, *tablets*, and other *mobile devices* that access City systems or internal City network resources. The compatibility matrix can be found on CityNet at https://citynet.sandiego.gov/it/services/cell-phone-service.

2.2. This administrative regulation applies to *users* using *mobile devices* with City *Computer systems* or internal City network resources.

2.3. The standards set forth in this regulation are minimum standards for City employees, volunteers, contractors, consultants, and other City agents. Additional information can be found in the City's Information Security Standards and Guidelines available on CityNet.

2.4. Departments may develop rules and procedures regarding department-specific use of information and communications technology resources in order to implement this administrative regulation. Departments may also develop more restrictive rules when required to comply with state or federal laws or regulations; however, department-specific policies may not conflict with, circumvent, or supersede this or any other administrative regulation or other information security policies. Department-specific rules or procedures are to be forwarded to the Chief Information Security Officer (CISO) for review before implementation.

(Supersedes Administrative Regulation 90.66, Issue 1, effective December 7, 2012)

Authorized

Signature on File
CHIEF OPERATING OFFICER

3. DEFINITIONS

3.1. *Automated Security Policy* - A standard set of security settings that are automatically applied to *mobile devices* that connect to the City *email* system.

3.2. *Bluetooth and Infrared* - Wireless technologies that enable wireless communication between compatible devices. These technologies are used for short-range connections between desktop and laptop computers, *mobile devices*, digital cameras, scanners, wireless headsets, and printers.

3.3. *Computer System* - Includes a network system or any other system that is not publicly accessible which requires City authentication, interconnected computer equipment (e.g., servers and storage devices), software package, or other City IT resources.

3.4. *Email (Electronic Mail)* - A method of composing, storing, sending, and receiving electronic messages, memoranda, and attached documents from a sender to one or more recipients using a telecommunications network.

3.5. *Compromised* - An event that has the potential to expose confidential or protected data or sensitive information to unauthorized individuals.

3.6. *Mobile Devices* - City *smartphones*, *tablets*, and other electronic devices that are City-owned or personally-owned electronic devices, used for City business, and have access to *email* or other applications over the Intranet or Internet usually via a wireless connection.

3.7. *SANNET* - The City's internal network (Intranet) and technical infrastructure.

3.8. *Smartphone* - A wireless phone that has the ability to access *email* and City applications over the Internet via a carrier's wireless network or via *Wi-Fi*. *Smartphones* can access network resources via Web browsers or over synchronization technologies.

3.9. *Tablet* - A wireless, portable, personal computer with a touch screen interface, which typically has a form factor that is smaller than a notebook computer but larger than a *smartphone*.

3.10. *Users* - City employees, volunteers, contractors, consultants, interns, and other approved agents who have approval to access City resources from a *mobile device*.

3.11. *Wi-Fi* - A mechanism for connecting electronic devices wirelessly.

4. POLICY

4.1. Mobile Devices Accessing City Systems or Internal City Network Resources

4.1.1. *Mobile devices* within the City or accessing internal City network resources must adhere to City security policies as described in the City's Information Security Standards and Guidelines.

4.1.2. The City reserves the right to disable or deactivate access to the City network to protect the integrity of the City's services. Reasons may include unauthorized user; unauthorized *mobile device*; *mobile device* is not complying with security policies; *mobile device* poses a security threat to the City or City services; or *mobile device* is having a negative impact on the confidentiality, integrity, or availability of the City network or services.

4.1.3. The act of connecting any City-owned or personally-owned *mobile device* to City technical infrastructure assumes the *user's* consent to City security policies. This includes the authorization to wipe any City data (i.e. remove data from) the *mobile device* in the event that it is lost, stolen, or *compromised*. When possible, the City's Chief Information Security Officer, or a member of his or her cyber security team, will inform users prior to wiping any device.

a. In the event a personally-owned *mobile device* is lost, stolen or *compromised*, users are required to take all necessary actions and work with the City Cyber Security team, which may include working with users' mobile device provider (e.g. AT&T, Verizon Wireless, Sprint, etc.) to ensure City data has been wiped from user's *mobile device*. These actions may include wiping all user data from the *mobile device*. The impacted user will complete a statement of compliance confirming the data has been wiped from their *mobile device*.

4.1.4. *Users* accessing City systems from *mobile devices* must adhere to acceptable use guidelines as outlined in A.R. 90.62, titled "Information and Communications Technology Acceptable Use."

4.1.5. All services on *mobile devices* must be configured in compliance with City security policies.

4.1.6. *Users* may install City-approved software on City-owned or personally-owned *mobile devices*. Installing other software on City-owned *mobile devices* requires written approval from the Department of Information Technology. Failure to comply with this administrative regulation may result in discipline that may lead to termination. Unauthorized actions are outlined in A.R. 90.63, titled "Information Security Policy."

4.1.7. Installation and download of applications for *mobile devices* must be done from the official mobile application store for that device. Unless otherwise approved in

writing by the Information Security Team, the *mobile device* configuration shall prohibit installs from untrusted or third-party sources.

4.2. Mobile Devices Containing City Data

4.2.1. *Users* should refer to the City of San Diego A.R. 90.64, "Protection of Sensitive Information and Data," for procedures regarding handling sensitive information. *Users* should be aware that City information on City-owned or personally-owned *mobile devices* is subject to the California Public Records Act (California Government Code sections 6250 et seq.). The City must comply with the California Public Records Act and respond appropriately to any request by a member of the public for a public record.

a. Text messages and *mobile devices* are not intended to be a permanent storage medium for public records or a medium for transmitting public records. (See A.R. 95.20, "Public Records Act Requests and Civil Subpoenas; Procedures for Furnishing Documents and Recovering Costs," and A.R. 90.25, "Wireless Communication Services.")

b. Text messages determined to be public records, whether transmitted on a City-owned or personally-owned *mobile device*, must be saved in accordance with A.R. 85.10, "Records Management, Retention and Disposition," and A.R. 85.30, "Vital Records Retention and Preservation." Users must transfer and save the messages to their permanent storage location as outlined by the employee's respective Department Records Disposition Schedule.

4.2.2. *Users* must change their network password immediately if their City-owned or personally-owned *mobile device* used for City business is lost or stolen. Changing the network password ensures that *mobile devices* can no longer access City resources. Passwords can be changed from any computer that is connected to *SANNET*, or by calling the City's Information Technology Help Desk.

5. RESPONSIBILITY

5.1. Information Technology Department

5.1.1. Establish *mobile device* policy, review the policy yearly, and update as appropriate.

5.1.2. Develop, deploy, manage, and audit *mobile device* security policy to ensure that approved devices have appropriate security controls in place.

5.1.3. Develop and maintain a list of *mobile device* operating systems that support deployment of automated security settings.

5.2. City Departments

5.2.1. City departments, through their designated Cell Phone Coordinator(s), are responsible for billing, activation, de-activation, inventory management, and audit of the department's use of Wireless Communication Services, including *mobile devices* that are used for City business, whether City-owned or personally-owned. Refer to A.R. 90.25, "Wireless Communication Services," for more information relating to mobile device management.

5.3. Users

5.3.1. Call Help Desk and ensure that the Information Security Team is informed within 24 hours if *mobile device* is lost, stolen, or compromised.

5.3.2. Notify department's Cell Phone Coordinator or supervisor within 24 hours if *mobile device* is lost or stolen.

5.3.3. Adhere to *mobile device* and acceptable use policies.

5.3.4. Ensure destruction of City data and settings on a City-owned or personally-owned *mobile device* prior to recycling, disposing, or returning of the *mobile device* to the vendor. This can be done by user performing a "factory reset" to remove all content and settings. If help is needed, contact your mobile service provider or IT liaison.

5.3.5. Non-exempt employees must not access any City applications via a *mobile device* to perform any City work, including but not limited to payroll time entry and approvals, and preparation of leave requests and approvals outside of their normal working schedules. In addition, supervisors must not direct employees to access any electronic or mobile City applications outside of their normal work schedules. See A.R. 95.01, "Overtime Compensation."

APPENDIX

Legal References

City of San Diego City Clerk Administrative Guidelines
Administrative Regulation 85.10 – Records Management, Retention and Disposition
Administrative Regulation 85.30 – Vital Records Retention and Preservation
Administrative Regulation 90.25 – Wireless Communication Services
Administrative Regulation 90.62 – Information and Communications Technology Acceptable Use
Administrative Regulation 90.63 – Information Security Policy
Administrative Regulation 95.01 – Overtime Compensation

Forms

Statement of Compliance

Subject Index

Mobile Device Security Policy
Acceptable use of Technology on Mobile Devices

Administering Department

Department of Information Technology

The City of
SAN DIEGO

ATTACHMENT 1

Administrative Regulation 90.66 - Mobile Device Security

STATEMENT OF COMPLIANCE REGARDING THE DELETION (WIPE) OF ALL CITY DATA FROM A PERSONAL MOBILE DEVICE THAT BECOMES LOST, STOLEN OR COMPROMISED BELONGS TO:

_____
Print or type name of official or employee

I, _____, state as follows:
Print name

1. I am an official or employee of the City of San Diego. In accordance with A.R. 90.66 – Mobile Device Security, I have notified the Department of Information Technology (DoIT) Cyber Security Team, that my personally-owned *mobile device* which contains City data has been lost, stolen, or *compromised*.

2. I am the owner or authorized user of the following personal *mobile device(s)* containing City Data that has been lost, stolen, or *compromised*:

_____
Insert description of personal mobile device(s) – i.e. tablet, cell phone, laptop, etc.

3. On _____, the DoIT Cyber Security Team has requested me to:
Date

_____
Insert details to wiping personal mobile device

4. I have taken all necessary actions and worked with my *mobile device* provider (i.e. AT&T, Verizon Wireless, Sprint, etc.) to ensure all City data has been wiped from my personal *mobile device* which was lost, stolen, or *compromised*.

Check the applicable box:

☐ I certify that to the best of my ability, I have taken all necessary actions to remove all City data from my personal *mobile device* which was lost, stolen, or *compromised.*

☐ I certify that I cannot reasonably wipe my personal *mobile device* which was lost, stolen, or *compromised* because of the following reasons:

_____

_____

_____

_____

_____

Executed this _____day of_____20____,

in_____, California.

Signature: _____ Print Name: _____

City Position/Title:_____