547.1 COMPUTER USAGE & PORTABLE ELECTRONIC DEVICES

I. PURPOSE: The purpose of this policy is to establish clear guidelines for the appropriate use of department-issued computers, portable electronic devices, and software by employees. These tools are provided to support the department's mission of reducing crime and enhancing the quality of life for city residents. Adherence to this policy ensures responsible, secure, and ethical use, aligns with legal requirements and Florida Statutes, and promotes operational effectiveness. This policy supplements all City of Tampa policies covering the same subject(s).

II. DEFINITIONS:

A. Criminal Justice Information (CJI): Sensitive data collected, stored, or shared by criminal justice agencies (e.g., arrest records, warrants, biometric data). CJI requires strict access controls and security measures.

B. Electronic Mail (Email): A system for sending and receiving electronic messages, files, or data. Emails created or received in connection with official business are public records subject to retention under Florida's Public Records Law.

C. Mobile Data Terminal (MDT): Portable computing devices in vehicles or carried by personnel for secure access to organizational systems and data.

D. Non-Transitory Messages: Messages with long-term or permanent value that must be retained (e.g., those related to official decisions, policies, or criminal justice matters). These records are subject to retention and public access under Florida's Public Records Law.

E. Passwords: A secure combination of characters used to restrict access to systems, accounts, or data.

F. Personal Identification Information (PII): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other data. PII includes, but is not limited to, an individual's name, social security number, date of birth, driver's license / state identification number, and contact information.

G. Portable Electronic Device (PED): Mobile devices capable of storing or transmitting data, such as smartphones, tablets, and notebook computers.

H. Security Incident: Events compromising the confidentiality, integrity, or availability of organizational systems or data (e.g., unauthorized access, malware, or data breaches).

I. Social Media: Online platforms for sharing content and interacting with others (e.g., Facebook, Instagram, TikTok).

J. Software: Programs or applications enabling devices to perform tasks (e.g., operating systems, communication tools).

K. Text Messages: Short electronic messages sent via mobile phones or other devices. Text created or received in connection with official business are public records subject to retention under Florida's Public Records Law.

L. Transitory Messages: Short-term communications (e.g., reminders, drafts) without long-term value and not subject to record retention. They do not set policy, establish guidelines or procedures, certify a transaction, or become a receipt.

M. Virtual Private Network (VPN): A system that allows employees access to the department's computer network via the Internet from any location.

III. DEPARTMENT-ISSUED COMPUTERS AND PORTABLE ELECTRONIC DEVICES:

A. Access:

1. Devices will be issued through the City of Tampa's Technology & Innovation (T&I) Department and may only be used by authorized employees for designated purposes.

2. Employees are prohibited from using department-issued devices for personal purposes.

   To prevent unauthorized access to the department's network, employees utilizing the VPN outside police facilities – including, but not limited to, School Resource Officers and Task Force Officers - must remain with their device at all times that it is connected to the network. If employees need to step away from their devices while connected to the department's network, they must ensure they have "locked" access to the device prior to stepping away from it, ensuring the device itself is not readily accessible to unauthorized personnel.

3. Remote access shall only be for official use only. This includes sworn members remoting into the agency's network via Absolute Secure Access Client VPN. Authorized vendors may be granted access to the agency's network only if they are virtually escorted by authorized personnel at all times.

B. Authorized Use:

1. Employees must keep issued devices charged and operational during their shift.

2. Usage of issued devices is restricted to official purposes only and in the capacity for which it was designated.

3. Additional instances when the use of these devices is unacceptable include, but are not limited to, the following:

   a. Violating laws or departmental policies.

   b. Using offensive, harassing, or profane language.

   c. Downloading unauthorized software.

   d. Accessing social media or streaming platforms for personal use.

   e. Actions that degrade network performance or constitute unauthorized system access.

4. Employees must not attach personal equipment to devices or download unauthorized applications/software prior approval of T&I.

5. Disabling device features (e.g., OneDrive or wireless functionality) is prohibited without prior approval from T&I.

6. Devices may not be loaned or transferred to another employee without first obtaining approval from the employee's division/bureau commander and T&I.

C. Loss/Damage:

1. Employees shall immediately report loss of or damage to their devices to their immediate supervisor and T&I so that security measures can be taken to disable that device's access to secure networks.

2. Damage from normal use is covered under the manufacturer's warranty. However, damage caused by employee carelessness or negligence may result in disciplinary action and/or financial responsibility for repairs, in accordance with the prevailing collective bargaining agreement.

IV. ELECTRONIC MAIL (EMAIL) AND TEXT MESSAGES:

A. Official Use:

1. The City of Tampa's email system and text messaging tools are for official purposes only. All messages are property of the city and subject to public records law.

B. Monitoring:

1. Employees possess no expectation of privacy for any communication that occurs on department-issued devices or through department-controlled systems.

2. The City of Tampa retains the right to monitor emails and text messaging tools at any time, without notice to the employee.

C. Appropriate Use:

1. Employees must maintain professionalism and courtesy in all written communications.

2. Appropriate uses include but are not limited to:

a. Job-related communication.

b. Coordinating meetings or resources.

c. Inter-departmental or external communication.

D. Prohibited Use:

1. Employees must understand that the unauthorized use of the City of Tampa's electronic mail or text messaging tools can reflect negatively, both on the individual employee and on the department.

2. Inappropriate uses include but are not limited to:

a. Illegal activities.

b. Harassment, threats, defamatory, or derogatory remarks.

c. Political endorsements.

d. Commercial activities or solicitations.

e. Misrepresentation of one's identity, unless it's part of an approved undercover investigation.

f. Transmission of programs or information in violation of copyright laws.

V. <u>INTERNET USE:</u>

A. General Use:

1. All employees may use the internet provided that the usage does not interfere with the employees' established duties or violate the City of Tampa's policies.

B. Restricted Websites:

1. Employees are not permitted to use the internet to visit the following website categories unless the activity is part of a legitimate law enforcement investigation and/or serving a legitimate law enforcement purpose:

a. Pornographic or gambling sites.

b. Gaming, streaming media, or personal business websites.

c. Social media websites for personal use.

d. Any other website that may be deemed as inappropriate to visit in a workplace setting.

C. Monitoring:

1. The department reserves the right to track or audit an employees' internet usage, including sites visited and downloads.

VI. COMPUTER SOFTWARE:

A. Standardization:

1. All computers and devices will have a standardized software suite installed on it, appropriate for the employee's specific work assignment.

B. Prohibitions:

1. Employees are prohibited from manipulating, altering, or deleting software that has been installed on computers and devices.

2. No computer software and/or portable electronic device applications will be downloaded or installed on computers or devices without permission from T&I.

C. Criminal Justice Information (CJI) Compliance:

1. To comply with the Florida Department of Law Enforcement's security requirements, all employees are prohibited from viewing and/or submitting

documentation containing Criminal Justice Information (CJI) unless they are being sent in a secure facility, with appropriate safeguards or encryption.

a. For purposes of this procedure, a secure facility includes all police buildings and/or all police vehicles.

D. Computers utilized for forensic analysis and/or covert investigations may have additional approved software.

VII. PASSWORDS:

A. Confidentiality:

1. Employees are responsible for all activity that occurs under a password protected computer, device, or software application.

2. Passwords should never be shared with other employees.

B. Guidelines:

1. Passwords must, at a minimum, adhere to the following guidelines:

a. Be at least 8 characters long.

b. Avoid dictionary words or proper names.

c. Does not contain the account's username.

d. Change every 90 days and be different from the last 10 passwords.

C. Compromised Passwords:

1. Any suspected password compromises must immediately be reported to your immediate supervisor and T&I.

VIII. CRIMINAL USE OF PERSONAL IDENTIFICATION INFORMATION (FSS 817.568):

A. Prohibited Acts:

1. It is unlawful to willfully and fraudulently use or possess another person's personal identification information (PII) without authorization. This personal identification information includes names, social security numbers, dates of birth, bank account details, and other identifying data.

B. Penalties:

1. Violations range from third-degree felonies to first-degree felonies, depending on the severity of the offense and the value of benefits obtained or attempted. Enhanced penalties may apply for crimes involving minors, elderly individuals, or repeat offenses.

2. Victims are also entitled to restitution and assistance in recovering their stolen identities. Courts may order offenders to pay damages or assist victims in correcting their records.

C. Organizational Implications:

1. Employees must provide reasonable safeguards for another person's personal identification information (PII) and report any unauthorized use, theft, or breaches to their immediate supervisor to mitigate liability and protect affected individuals.

2. Employees shall comply with laws governing the handling of another person's personal identification information (PII) and must avoid engaging in activities that could constitute identity theft or fraud.

Supersedes SOP 547.1, dated 8/22