



ADMINISTRATIVE MANUAL

**ADM - 540 – AGENCY COMPUTER & INFORMATION TECHNOLOGY USAGE**

Amends/Supersedes: ADM-540 (09/09/2024)

Date of Issue: 12/30/2024

**I. GENERAL**

- A. Computers, networks and other technology are critical to department operations. The Public Safety Information Technology Unit, with support from the city's Information Technology Department, is responsible for ensuring that employees have access to programs and technology essential to their job functions. This policy establishes the responsibilities and requirements for all employees to maintain access to both information systems.
- B. *Computer*, as referenced, applies to all electronic resources capable of receiving and sending electronic communication, retrieving or organizing department information, and connecting to the city's wired area network (WAN). The definition will include but is not limited to, MDCs, electronic notebooks, tablets, desktop or laptop PCs, etc.

**NOTE:** Smartphone use for electronic communications will also fall under applicable sections (e.g., correspondence, privacy, games, etc.). For more information, refer to [ADM-535 Cellular Phone Use](#).

**II. POLICY**

- A. Personnel accessing department computer systems must comply with the established regulations and specific procedures regarding these systems and any rules or regulations issued by the city regarding such systems and their use as established in this policy [and PAM-1403 Use of Information Technology Policy](#). Any employee who violates these policies may be subject to disciplinary action under department policy and [PAM-1000 Standards of Conduct](#), resulting in the revocation of access rights to any or all department computing resources, as determined by the Chief of Police. [82.1.6]
- B. Employees will not use agency funds to make any information technology-related purchases (e.g., computers, monitors, external drives, software, printers, scanners, cameras, audio/visual equipment, or related peripheral devices, subscriptions or purchases of services from third-party providers, etc.) without first consulting with the Public Safety Information Technology (IT) Unit supervisor.
- C. Any employee assigned an agency computer, its related documentation, software and accessories, whether permanent or temporary, is solely responsible for its care and safekeeping.
- D. The use of obscene, profane, discriminatory, demeaning or degrading language in any electronic correspondence is strictly prohibited.
- E. While on or off duty, employees will be mindful of sending or receiving emails, viewing internet sites or web pages, or engaging in activities related to computers or information technology, potentially bringing the department into disrepute or discrediting individuals. Employees shall adhere to the [PAM-1000 Standards of Conduct](#), [ADM-210 Standards of Conduct/Disciplinary Action](#), and the department's Code of Ethics.
- F. Employees shall not use the department's electronic communications resources for personal gain (e.g., selling personal items, homes, services, etc.), whether for themselves, family members, or friends. This does not prohibit disseminating information regarding fund-raising and ticket sales for department-sponsored or sanctioned group events via email.



- G. Employees have no expectation of privacy regarding electronic or physical records, including email, personal files or official work documents, either received or generated by them while using department-owned electronic resources or connected to a city-approved network. The department reserves the right to access any content from any information technology resource without prior notice. It may require employees to provide passwords to encrypted or password-protected files upon request.
  - 1. Employees will not transmit or receive confidential or sensitive department information over their personal non-city messaging platforms (i.e., Google Mail, Facebook, Twitter, Snap Chat, Slack, etc.).
  - 2. Employees who store their personal information on department computers or peripherals do so at their own risk and are subject to city disclosure and surrender requirements.
- H. Department personnel will follow the mandates of the [Virginia Freedom of Information Act](#) (Chapter 37, Title 2.2 of the Code of Virginia) and [ADM-160 Privacy/Dissemination of Information](#), as they relate to the dissemination of information and electronic records when using computer resources in the course of their work activities. [82.1.7]
- I. Employees will observe all copyright and licensing restrictions associated with computer media and software applications.
- J. The IT Unit, in cooperation with City Information & Technology, will ensure multifactor authentication is set up on all appropriate devices to help maintain the required level of access security established by city, state and federal agencies that allow employees to access their systems, or have systems that may be accessible from the department's network.

### III. USE OF DEPARTMENT COMPUTER EQUIPMENT AND PERIPHERALS

- A. Department computer resources are designed/intended to conduct official business. The installation of games or other software for entertainment purposes is prohibited. Exceptions to official business use include: [41.3.7(c)]
  - 1. Infrequent personal use is permissible if limited in scope and frequency. Such use may not be connected to for-profit activities or promoting any product, service, or cause that the Chief of Police or designee has not explicitly approved.
  - 2. Employees may use departmental computer resources for professional and career development purposes when within this policy and with the prior approval of an appropriate supervisor.
- B. The IT Unit is responsible for coordinating employee access to systems and software as dictated by the employee's duties and responsibilities. System access may require adjustment as employees are transferred or promoted. Employees experiencing issues accessing necessary systems will notify the IT Unit. [41.3.7(a)]
- C. The assigned employee is responsible for ensuring the security of their computer against unauthorized use. Employees will not allow unauthorized personnel to use their user ID or passwords to access any department computer, city virtual private network (VPN), NNPD WAN, the city's mainframe systems, email systems, or any other secured system designated for department business. Employees are responsible for all activities that transpire under their user ID. [41.3.7(b)]
- D. To avoid breaches of security or theft, employees will utilize the following measures, as applicable:
  - 1. Set screen saver passwords.
  - 2. Close and secure the door to any private office.
  - 3. Log off of computer resources when they leave a work area.
  - 4. Ensure the computer is secured and out of public view when stored in a vehicle or at home.
  - 5. Set up and utilize the department's mandated multi-factor authentication.
- E. The system administrator or IT Unit representative must be consulted before moving department-owned computer equipment (e.g., unplugging it from the network, moving it to another office, etc.).



**NOTE:** This does not include temporarily undocking laptops and MDCs associated with regular, daily use.

**IV. USE OF PERSONALLY OWNED COMPUTER EQUIPMENT AND PERIPHERALS** [11.4.4]

- A. Connecting personally owned computer equipment, including peripheral devices such as printers, data storage devices, scanners, etc., to the department's WAN is prohibited without documented approval from the employee's chain of command and the concurrence of the IT Unit supervisor.
- B. City IT has implemented security measures to reduce the chances of an employee's account being accessed by a bad actor, which is tied to the location where access occurs. Access attempts from personal devices from locations outside the area may result in an employee's account being disabled.
  - 1. When employees travel out of the state or country and need access to their department account (including email) from any non-department-issued device, they will notify the IT Unit and provide their location.
  - 2. Employees accessing their city account from a personal device through a VPN may be disabled, as the VPN may report a different location. When an account is disabled, employees must contact the IT Unit to regain access.
- C. Employees shall not use any personally owned photography, video, or audio recording equipment, digital or otherwise (e.g., cellular phone, pocket pen camera, digital camera, etc.) to document department law enforcement-related evidence or investigative photos unless expressly set out in section III. E. of [ADM-535 Cellular Phone Usage](#).
- D. Employees using any personal device that has received written approval for attachment to the WAN is subject to network protective action by the department or city IT staff, including, but not limited to:
  - 1. Requiring the device's hardware or software to be upgraded to the requirements of the department's systems and software before the WAN connection or as a condition of continuing the WAN connection.
  - 2. The device (and user) may be subject to some or all department or city policies regarding city or department-owned technology equipment.
    - a. The device may be subject to a data wipe by department or city IT technicians in a compromised security situation (for example, theft or loss of the device), resulting in the loss of the employee's data.
    - b. The device may be subject to subpoena and the legal discovery process in connection with official use, resulting in a temporary loss of use or possession.
  - 3. The IT Unit is not responsible for responding to hardware or software support issues related to personally owned computer equipment or peripherals.
  - 4. In all cases where personally owned computer equipment or peripherals are used in department workspaces, the equipment owner shall assume complete and sole responsibility for the equipment's legal and safe operation and any liability resulting from its presence or use on or in city property.
  - 5. Neither the city nor the department is liable for any personally owned computer equipment, software, or peripheral devices that may be stolen, damaged, or otherwise made inoperable while in department workspaces.
  - 6. Any media (e.g., USB drives, external HD, DVDs, CDs, etc.) not owned or supplied by the department and used with or intended to be used with any device will be scanned before files are transferred into a department computer.

**NOTE:** Employees wishing to upload information into a department-owned system must contact the IT Unit so the media can be virus-scanned.



7. If department or city computer equipment becomes infected with a virus and the infection is traced to a personally owned computer system or media device, the individual who transferred the virus to the system may be held liable for the costs of removing the virus.

**V. ACCOUNTABILITY AND AUDITING**

[C6.8.5, 82.1.6(D)]

- A. The IT Unit will perform a documented quarterly audit of all computer systems for verification of passwords, multifactor authentication, access codes, and user accounts for possible violations and improper use. The will: [T 7.3.5]
  1. Verify all user accounts on all computer platforms currently used by employed users or ensure that all such accounts for former employees have been disabled. [T 7.3.7(b)]
  2. Verify system password requirements are applied to all active directory accounts,
  3. Review all permissions to verify that users may access only the information required to perform their duties as supervision approves. [T7.3.7(b)]
  4. Review network security measures as appropriate.
  5. Personnel will change their system password every 90 days when logging into the network, adhering to the following password rules. [T7.3.7(a), T7.3.8]
    - a. Passwords must contain at least fourteen (14) characters, with at least one of the following:
      - 1) Number
      - 2) Uppercase letter
      - 3) Lowercase letter
      - 4) Special character (e.g., !, @, #, \*, ?)
    - b. Passwords should not contain any word, proper name, or phrase spelled completely using letters unless used as part of a passphrase.
    - c. Passwords cannot contain the username or a combination of characters in the username.
    - d. Users should not modify the old password by adding a single character when changing passwords.
  6. Personnel will create a multifactor authentication pin to access city devices.
    - a. A minimum of six (6), non-repeating characters, either numeric or letters.
    - b. The pin must not contain the employee's active directory username or password.
- B. The system administrator will ensure that the internal inventory records for all departmental computer resources are kept current and available for inspection.
- C. System Backups [82.1.6(a,b)]
  1. The system administrator will ensure that all dynamically changing computer files are backed up daily to a secure location with an active, non-corrosive fire suppression system. Daily incremental backup tapes will be stored in a climate-controlled, secure area. [TA 7.3.6(a)]
  2. The system administrator shall ensure that the agency's complete data storage system is backed up no less than weekly. Weekly backup tapes are stored off-site in the climate-controlled, secure building. [TA 7.3.6(b,c)]
  3. Requests to review or restore data from backup tapes or stored computer files shall be made in writing to the system administrator. [TA 7.3.6(a,c)]
  4. Computer files ported to tape for backup purposes shall remain viable and retrievable for up to six months. At that time, the backup tapes will be overwritten and reused. [TA 7.3.6(d)]



**NOTE:** The amount of online storage shall be increased, as necessary, to ensure that all active user files remain available and accessible on the agency's network, regardless of the agency's backup capability.

**VI. IMPORTING/DOWNLOADING INFORMATION AND SOFTWARE**

[11.4.4; 41.3.7(A,B)]

A. The IT Unit will approve all software loaded onto department computers or provided through cloud access.

**NOTE:** Software includes any that enables the user to perform tasks using computer resources (i.e., programs, routines, scripts, applications, firmware, grayware, freeware, open-source, sound and video files, attachments to emails, Internet files, or other external sources), whether cloud-based or requiring a hard installation.

B. Employees who request to purchase and load software onto department computers will consult with their supervisors first, then the IT Unit, to ensure that the software does not interfere with other programs and systems.

C. The IT Unit will inventory all software loaded into a system to maintain the license record. Depending on the individual company's licensing requirements, the software will be licensed to the Newport News Police Department or the specific user.

**VII. MOBILE DATA COMPUTERS (MDCS) AND SIMILAR MOBILE TECHNOLOGY**

A. The IT Unit may install additional security measures on MDCs and laptops to prevent unauthorized access. Employees are prohibited from disabling or bypassing access security measures on their issued devices. [41.3.7(d)]

B. MDCs (and similar mobile technology) allow communications personnel to communicate and retrieve routing information. Officers shall use this technology for non-emergent communications. Supervisors are expected to monitor these communications during their shifts and immediately address policy violations. [41.3.7 (e)]

**NOTE:** As used, the term "MDC" also refers to tablets or similar mobile devices.

C. All personnel operating a vehicle equipped with an MDC shall comply with the general computer rules and regulations and specific procedures regarding the use and care of the MDCs, as provided to them. Non-compliance will be brought to the attention of the officer's supervisor for corrective action.

D. Dispatcher instructions via radio or phone take precedence over information forwarded and displayed on the MDC.

E. All MDC entries, including emails, talk messages, and conference messages, are recorded and electronically saved, falling under the Commonwealth of Virginia's Freedom of Information Statutes, for review by the department, the public, and the media.

F. Officers will observe proper MDC safety use protocol and will not compromise their safety or the safety of others (e.g., do not type while driving, perform an NCIC/VCIN check while trying to initiate a traffic stop, *et cetera*).

**VIII. SOCIAL MEDIA AND SOCIAL NETWORKING SITES (PAM-1410 - SOCIAL MEDIA POLICY)**

A. Development of Personal Webpages, Social Media Sites, And Social Networking Sites

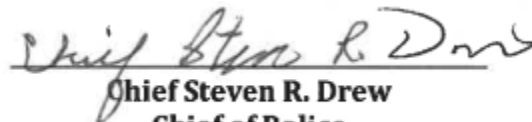
1. Personnel will not portray themselves as representatives of the department, the city, or its affiliated programs on their personal web pages, Facebook accounts, Twitter messages, or any other social media or networking sites without the express written permission of the Chief of Police or designee.

2. For safety reasons, employees are cautioned not to disclose their employment with the department or post any information about any other agency member without that individual's permission.



B. Development of Agency Webpages, Social Media Sites, And Social Networking Sites

1. The city Communications Department shall approve all department social media sites or webpages after receiving approval from the Chief of Police or designee before posting them for viewing.
2. Any such site, blog, or webpage used to promote the city, or the agency shall clearly indicate:
  - a. They are maintained by the city and prominently display city contact information.
  - b. The city's posting policy regarding appropriate content, if applicable for the social media type. Posted comments will be monitored for adherence to the posting policy, and violating content may be removed, rejected, deleted, or disabled.
  - c. Content removed from a social media site shall be retained according to Virginia Records Retention requirements, along with a description of the reason the content was removed.
  - d. Any opinions expressed by visitors to the site(s) do not necessarily reflect those of the Newport News Police Department or the City of Newport News.
  - e. Any content posted or submitted for posting is subject to full public disclosure (i.e., FOIA, e-discovery), storage and media management laws.
  - f. Questions regarding the appropriateness of a prospective post shall be made before posting to the employee's supervisor or the department's Public Information Office.

  
**Chief Steven R. Drew**  
**Chief of Police**