FAIRFAX COUNTY SHERIFF'S OFFICE
STANDARD OPERATING PROCEDURE

SOP NUMBER: 050
SUBJECT: INFORMATION SYSTEM MANAGEMENT

I. PURPOSE

To provide guidance for the use of Sheriff's Office information systems resources on the Fairfax County Enterprise network.

II. POLICY

It is the policy of the Fairfax County Sheriff's Office that use of Sheriff's Office information systems resources must be in compliance with all applicable federal, state, and copyright law(s), Fairfax County ordinances and policies, as well as Fairfax County Sheriff's Office Standard Operating Procedures. Violations of this policy may involve disciplinary actions, up to and including dismissal and/or prosecution. Use of all computer and information resources should be to further the efficiency and effectiveness of Sheriff's Office operations; and, thereby contribute to the agency's service to the citizens of Fairfax County. Computer and information resources shall be used for business purposes, before, after, or during normal business hours relating to the performance of an employee's duties.

III. PROCEDURE

A. General Use, Confidentiality and Protection of Information

1. All data stored in Fairfax County or Sheriff's Office information systems and information contained in any reports generated from Fairfax County or Sheriff's Office information systems is property of Fairfax County or the Sheriff's Office. It is to be considered confidential, and shall be handled in accordance with SOP 010 - Research Projects, SOP 016 - Standards of Conduct, SOP 017 - Harassment in the Workplace, SOP 041 - Polygraph, SOP 530 - Dissemination, Access, Storage, and Safeguarding of Information and Records Pertaining to Inmates, and all other SOPs as applicable.

2. The use of Sheriff's Office information systems by employees, contractors and volunteers shall be in accordance with all federal, state, copyright law(s) and Fairfax County and Sheriff's Office ordinances and policies. Sheriff's Office supervisors and staff members are responsible for ensuring that the provisions of this SOP are not violated, and that when violations do occur they are documented and forwarded to the Information Technology Branch Chief.

3. Confidential information shall not be sent through the Internet unless properly encrypted or otherwise protected.

4. Authorized users have no expectation of privacy in their work-related conduct or the use of Sheriff's Office equipment, systems, or supplies.

5. Authorized users who utilize Sheriff's Office information systems equipment are advised of the following: This is a FAIRFAX COUNTY SHERIFF'S OFFICE COMPUTER SYSTEM. This computer system, including all related equipment, software, networks, and network devices (Specifically including Internet Access), are provided only for AUTHORIZED FAIRFAX COUNTY GOVERNMENT USE. Sheriff's Office computer systems may be MONITORED for all lawful purposes, including to insure that their USE IS AUTHORIZED, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. MONITORING includes active

inquiries by authorized Sheriff's Office entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this Sheriff's Office computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to disciplinary action or criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes CONSENT TO MONITORING for these purposes.

6. Authorized users shall keep their passwords to all state, Fairfax County and Sheriff's Office systems confidential. Staff members shall not share User ID's or passwords with others and will contact the Information Technology Branch to obtain new User ID's and passwords if compromised.

   a. The Information Technology Branch is responsible for resetting FFX enterprise passwords between 0700 hours and 1530 hours.

   b. FFX enterprise passwords must follow strong password guidelines:

      1) Is at least six characters long.
      2) Does not contain log on credentials, real name, or company name.
      3) Does not contain a complete dictionary word.
      4) Contains characters from each of the following groups: Uppercase letters, Lowercase letters, Numerals, and Symbols.
      5) Previous passwords may not be used.
      6) Passwords are required to be changed every 90 days.

      Network/LAN/Outlook passwords will be reset to 'Lan01!" as a temporary password. The user will be prompted to change their password at log on.

7. Authorized users are responsible for ensuring that access to the equipment and information is controlled at all times. In the event that a staff member must leave the area, computers should be locked or logged off as appropriate, and any data, documents, or other pertinent items secured. At no time, will an authorized user leave a computer logged on and unlocked while unattended.

8. Authorized users shall ensure that their equipment is properly functioning when assuming a post or starting work. Any malfunctioning or inoperable equipment will be reported immediately to the Information Technology Branch by sending an email to SHF-IT 911 or by using the SHFnet IT Issues form at: The Sheriff's Office Information Technology Issues Form.

9. Authorized users shall not attach, install, or otherwise connect any software, hardware or other device not specifically approved by the Information Technology Branch using the procedures provided in this SOP.

10. Authorized users shall not attempt to "hack" into other systems or use another user's credentials, or "crack" passwords, or breach computer or network security measures. Authorized users shall not knowingly introduce or transmit any

computer virus or otherwise damage or alter agency hardware, software or data.

11. No E-mail or other electronic communication may be sent which attempts to hide the identity of the sender or represent the sender falsely.

12. Requests for additional hardware, software, PC configuration or other changes to existing equipment must be submitted in writing by sending an email to SHF-IT 911 or by using the SHFnet IT Issues Form. All requests for new equipment must include the approval by a Division Commander and the appropriate FOCUS cost center for budget purposes.

13. Computer and information technology resources are to be used only for Sheriff's Office business purposes.

14. In addition to the general prohibitions in other sections of this SOP, the use of Sheriff's Office hardware is specifically prohibited for the following:

    a. Participating in on-line chat rooms.
    b. Engaging in on-line computer games.
    c. Engaging in on-line gambling.
    d. Viewing of pornography.
    e. Conducting personal business for profit.
    f. Installing or downloading media players.

    Notwithstanding the provisions of this SOP, staff members may utilize Information Technology Branch equipment to check personal email or utilize the Internet for legitimate, non-prohibited personal use so long as that use does not interfere with, impede, or violate any Sheriff's Office or Fairfax County policy. Use of such should be limited to times the authorized user's supervisors may deem appropriate.

15. Violations of this SOP will be handled in accordance with SOP 014 - Internal Affairs and the Administrative Investigations guidelines.

16. When a disciplinary termination occurs, the Human Resources Branch Commander shall contact the Branch Chief for Information Technology to relay the name and effective date of the termination. The IT Branch Chief shall authorize the AISC to disable the log on credentials of the terminated. All accounts will be deleted in accordance with Fairfax County guidelines.

B. Use of Computer Hardware and Software

1. Hardware

    a. Hard Disks - Data storage on computer hard disks is discouraged. Any information stored on a computer hard drive will need to be backed up by the individual user or users. The Information Technology Branch will not be responsible for any information stored on computer hard drives. It is strongly recommended that all data be stored on the appropriate network drive.

    b. Network Drives - It is highly recommended that staff members utilize

network drives to store data. This drive will be monitored to ensure data integrity. This method of data storage is preferred because the data is backed up and accessible from any networked PC.

c. Network drives are listed as follows:

1) OneDrive (Home Drive) - Each staff member has a private network drive for data storage and organization. OneDrive is to be used for Sheriff's Office business only. Personal items like photos, illegal or legal downloads of music files are not to be saved in your OneDrive. OneDrive is not to be utilized as destination for software installations. Staff members are responsible for maintaining their own OneDrive by ensuring that unneeded files are deleted or moved elsewhere, thereby maintaining space for all users.

2) X Drive (X: or Network Drive) - Each section, branch and division in the Sheriff's Office has a folder set aside for use. Each staff member has access to those folders as assigned. The purpose of X: drive is to facilitate sharing of data.

3) P Drive (P: or Public Drive) - This is a public drive accessible to all members of the agency. The purpose of this drive is to facilitate sharing of data between all agency members regardless of section, branch or division. When using P: drive to temporarily provide data to others, please ensure that all folders and files that are placed on the drive are deleted after use in order to provide maximum performance and space for all users. Also, any information that is stored on P: drive is subject to change by any other user. As a result, staff members should keep originals of any document stored elsewhere.

d. Authorized users have their network drives automatically mapped via policies.

e. DVD +/-RW drive - Agency PC's may be equipped with a DVD +/-RW drive. This drive is to be used for official business.

f. USB Encrypted Flash Drive - These portable storage devices must be of the make and model approved by the County's Information Security Office, and purchased through the County approved vendor. Any data that is classified as CONFIDENTIAL or SENSITIVE that is stored on a portable device must be encrypted and protected by a strong password. Portable storage devices that are not approved by the county are not permitted on the enterprise network.

2. Software

a. Configuration of each PC or laptop shall conform to the image made available by Fairfax County DIT.

b. Authorized Software

c. Only software authorized and approved by the Information Technology Branch will be installed on Sheriff's Office computers. All other software required by staff members in the performance of their duties must be approved by a Division.

1) Commander and reviewed by the Information Technology Branch by sending an email to SHF-IT 911 or by using the SHFnet IT Issues Form. At no time shall any staff member install software unless specifically approved.

2) Personally owned software shall not be installed on any Sheriff's Office computers.

3) At no time will unlicensed, pirated, or software that violates the concept of corporate software standardization be installed on Sheriff's Office computers.

3. Security

a. It is each staff member's responsibility to ensure that PC's and other Information Technology assets assigned to their section, branch and division are maintained in a secured and appropriate manner that prevents unauthorized access to:

1) Employee information
2) Inmate information
3) Volunteer and contractor information
4) Any other information which may be considered
5) Confidential in nature.

b. DIT shall implement and maintain a centralized anti-virus solution that provides automated protection for publicly accessible systems, perimeter devices, and internal server and client end points of the county enterprise infrastructure. Standalone and networked workstations and servers shall use the DIT approved virus protection software and configurations.

1) Anti-virus software shall maintain centralized event logging for coordinated response and analysis.
2) Web and email gateway anti-virus software shall be installed and configured for real-time active monitoring at the perimeter according to DIT approved configuration standards.
3) Email file attachments shall be scanned in real-time to inspect for viruses or other malicious code.
4) Virus protection shall be installed on Fairfax County file servers and configured to identify and clean viruses that infect files shares.

5) Internet traffic shall be scanned in real-time to ensure that transmissions and downloads do not contain viruses or other malicious code.

6) Virus protection software on County information systems shall not be disabled, bypassed, or altered in any manner.

7) Virus pattern and scan engine updates shall be current and updated. New virus patterns and anti-virus engine updates shall be centrally acquired by DIT and distributed to County information systems after release by the anti-virus software vendor.

8) The automatic update frequency of the virus protection software shall not be altered to reduce the frequency of updates. Viruses which are automatically cleaned by the virus protection software shall constitute a security incident and be reported to the Information Security Officer.

9) Security of information is each staff member's responsibility and should be in accordance with SOP 035 - Public Information, SOP 102 - Special Security Equipment, and in accordance with federal and state law, county ordinance, and Fairfax County Procedural Memorandum 70-05 - Information Technology Security Policy.

c. Relocation of computers and/or other Information Technology Branch Equipment.

1) Relocation of computers and/or equipment must receive prior approval from the Information Technology Branch. Approval for such move must be submitted and approved in advance by sending an email to SHF-IT 911 or by using the SHFnet IT Issues Form.

2) In cases of emergency or other extenuating circumstances where prior approval is impractical or impossible, staff members may move equipment to provide continued operations of key elements of the agency or to prevent damage. In such cases, the Information Technology Branch shall be notified as soon as reasonably possible.

4. Use of the Internet/Intranet/Infoweb/SHFnet on Sheriff's Office PC's.

a. Use of the Internet, Intranet, Infoweb and SHFnet is for Sheriff's Office business purposes only.

b. Site approval or restrictions on computers that have access to the Internet may be specified by individual division commanders.

c. All Internet access from the Sheriff's Office network will be through authorized Internet gateways. All other access to the Internet is prohibited.

d. The County's Information Security Officer will monitor staff usage of the

Internet.

5. Use of Outlook, Outlook for Web Access (OWA) and other e-mail Applications on Sheriff's Office PC's.

   a. Use of Outlook, Outlook for Web Access (OWA) and other e-mail Applications will be for business purposes only.

   b. The Information Technology Branch will monitor electronic mail messages when authorized by the Sheriff or a Chief Deputy.

   c. Authorized users should maintain their personal folders to ensure that they do not run out of storage space. Storage space on the network is limited. As a result, a user may not be able to receive messages when the space used by mail messages exceeds the level set by the county's Department of Information Technology.

   d. Any authorized user that wishes to send a group or mass e-mail through the county's Outlook/OWA must have approval of their Division Commander.

6. Use of Positive Identification Equipment and systems, including Livescan and Mugshot components.

   a. Use of Positive Identification Equipment and systems will be for official purposes only, including booking of prisoners and identification of persons in custody.

   b. Staff members shall adhere to procedures and policies set by the Virginia State Police in processing cases via Livescan.

   c. Staff members shall promptly notify Information Technology Branch when Livescan or Mugshot components or their peripheral devices malfunction, and provide a detailed description of the problem, including outputs where available.

C. Printers

1. Printers are provided throughout the agency for staff use. The preferred configuration for printers is to maximize agency resources by use of Xerox copy machines and network printers that serve multiple users.

2. The use of individually assigned printers is discouraged but may be needed due to special situations and work requirements. Such arrangements must be requested following the procedures outlined in this SOP and must be approved by the Chief of the Information Technology Branch.

3. Supplies for agency printers shall be obtained through the Material Management Section.

D. Requests for Equipment/Software/Configuration

1. All requests for additional equipment, software, and changes to computer

configurations must be submitted in writing to the Information Technology Branch by sending an email to SHF-IT 911 or by using the SHFnet IT Issues Form. Staff are required to obtain approval from their Division Commander, and provide the FOCUS cost center for budget purposes.

2. All computer related budget requests must be submitted through the chain of command to the Information Technology Branch. Prior to each budget submission agency staff must inform the Information Technology Branch of their

   information technology needs. Information Technology staff will review and prioritize all requests for inclusion in the budget submission.

3. Requests which have been denied due to funding shortages may be re-submitted to the Information Technology Branch for inclusion in the next fiscal year budget request.

4. County operating or capital funds will not, as a rule, be used to fund purchases for the below listed sections. Funding for purchases of new and replacement equipment and software for the following sections will be obtained from Inmate Commissary funds after approval from the Commander, Support Services Division. The Information Technology Branch will determine the appropriate configuration and purchase the equipment using Inmate Commissary funds. The Information Technology Branch retains authority over these items, and all provisions of this SOP apply to their use.

   a. Substance Abuse
   b. Programs
   c. Chaplain's Office
   d. OAR
   e. Inmate Finance Offices in the Adult Detention Center and Support Services Division

E. Requests for Assistance

1. For password reset information, see Section III., A., 6. of this SOP.

2. The County's Help Desk (703-324-HELP) is responsible for resetting the Sheriff's Office Network/LAN/Outlook passwords when our IT staff is unavailable. Instructions for changing your Outlook/ OWA password is available on the Infoweb at: Fairfax County Department of Information Technology Email and Outlook Page.

3. Normal working hours for Information Technology Branch staff are Monday through Friday, 0700 hours through 1530 hours. For assistance during those hours, please contact an Information Technology Branch staff member via e-mail at SHF-IT 911.

4. For afterhours assistance, notify the Help Desk (703-324-HELP) for any information technology problem. For issues that can only be resolved by an Information Technology Branch staff member, use the SHFnet to obtain the appropriate On-Call IT staff member.

FAIRFAX COUNTY SHERIFF'S OFFICE
STANDARD OPERATING PROCEDURE

SOP NUMBER: 050
SUBJECT: INFORMATION SYSTEM MANAGEMENT

4/30/07
DATE APPROVED
02/01/19
EFFECTIVE DATE

STACEY A. KINCAID
SHERIFF

Revised: April 2007, January 2019