
	<b>Florida State University Police Department</b>	
<b>Utilization and Security of Computer Hardware and Software</b>		
Revision Effective Date: 06/29/2020	<b>General Order 1109</b>	Attachments: None
Rescinds/Amends: 1109 (09/05/17), 10-34C (9/14/10), 08-100-137	Distribution: Department-Wide	CFA Reference: 26.04, 32.01
	Pages: 4	

**Policy - Utilization and Security of Computer Hardware and Software**

It is the policy of the FSU Police Department to regulate the use of computer hardware and software that is utilized, owned, or leased by the Department. Personal software is not allowed on Department computers. Any download or add-on software must be approved by the IT (Information Technology) Manager.

**Procedure**

Employees of the FSU Police Department, sworn and non-sworn, are authorized to utilize the Department’s computer resources subject to the procedural provisions of this general order and pertinent University policies for use of information technology resources. In certain circumstances, other University and/or law enforcement personnel, as specified in subsequent sections of this general order, may be permitted to access and utilize this Department’s informational technology resources on an as needed and restricted basis.

**A. E-Mail, Internet, and Intranet Usage and Access**

All sworn and non-sworn employees of the Department are authorized to use desktop and laptop computers - individually assigned at workstations or general Departmental use areas for e-mail, internet, and intranet purposes directly associated with their individual job responsibilities. [CFA 32.01A, B and E]

1. The IT (Information Technology) Manager (hereafter referred to as “Coordinator”), as the designee of the Chief, shall assign unique usernames. Users select passwords that must be at least 6 alpha/numeric characters. This username and password enables police users to log on to the Department’s applications, as well as the intranet (FSUPD Net) and email.
2. For sensitive or confidential information access to the Records Management System (RMS), the Coordinator, upon explicit approval from the Chief or other member of the command staff, shall further assign specific user names and passwords to those individuals, within and external to the Department, e.g., officials from the Office of Student Rights and Responsibilities, that have a need for such information.
3. The Coordinator shall be responsible for maintaining a current list of authorized Departmental internet, intranet, and e-mail account holders. The list shall include their names, Department (if external to the FSUPD), username, password, and any limitations, e.g., time expiration, on their access. In addition, the Coordinator shall further be responsible for performing an annual audit to verify only authorized members have access.

**B. Authorized Usage [CFA 32.01E]**

Authorized usage of e-mail and the internet is restricted as discussed in Section A., above, of this general order. In addition, there shall be no public access to any Departmental computers within the FSU PD facility unless designated specially for public use. However, upon express approval by the Chief or other member of the command staff, members of other criminal justice agencies or University departments may access and use Departmental computer resources for official purposes only. Department members shall further adhere to electronic communication restrictions discussed in University Policy No. OP-H-5, "Information Security". For the purpose of this general order, the most pertinent restrictions include, but are not limited to:

1. For personal financial or commercial purposes.
2. To impersonate another person or misrepresent authorization to act on behalf of others.
3. To access or view pornographic or obscene materials unless necessary for the investigation of a criminal or administrative complaint.
4. To harass another person or transmit text, pictures, or sound that might be perceived by a reasonable person as being offensive or harassing.
5. To send or create junk mail, spam, chain letters, computer viruses, or other disruptive material.
6. For purely personal use. This specifically includes the use of entertainment/games that are available from the internet, sent by e-mail, or loaded as a CD by the employee. However, employees may very briefly use the e-mail and internet resources of the Department during their breaks or lunch periods.

**C. Access to and Authorized Usage of Special Software(s)**

1. For access to written directives online (general orders), each employee is assigned a unique username, and password. This allows users the ability to access and sign general orders.
2. Each user is assigned a unique username and password that will enable access to Spillman, the department's records management system. Rights are assigned to individual users depending on job tasks, and responsibilities.
3. Access to ARMS, the department's automatic records management system prior to December 2007, can be accessed by specific individuals depending on job task and responsibilities.

**D. General Restrictions to Computer Usage**

In addition to the restrictions on e-mail and internet usage discussed above, the following general restrictions apply regarding all types of computer usage:

1. No devices of any kind may be attached or added to any Departmental computer equipment without the express authorization of the Chief, member of the command staff, or Coordinator, e.g., modems, sound cards, scanners, printers, etc.)
2. The installation or use of any copyrighted software without an approved license agreement is strictly prohibited. All approved software shall be installed by the Coordinator, only. Before copying software or installing software on a computer other than the one for which it was originally licensed, the Coordinator must ensure that the license terms permit the copying or installation. [CFA 32.01C]
3. No Departmental employee, other than the Coordinator, shall attempt to repair or configure any computer, related equipment, or network configurations. Needed repairs shall be

communicated to the Coordinator, who, in turn, shall either remedy the problem, himself or herself, or communicate with appropriate officials from the Office of Technology Integration or a business with which the University has a contract for computer repairs.

4. Only the Coordinator, upon express approval of the Chief or member of the command staff, may give out any Departmental computer's configurations or network setting.
5. Employees must use extreme caution when eating or drinking at a computer workstation. If any liquid is spilled on the system, the user should logout immediately, turn of all power, wipe up the spill, and advise the Coordinator.
6. All employees at the end of the workday should logout from the network and properly shut down their computers. This does not apply to shared computer or to any computer with a designated task to be performed by a later hour.

**E. Virus Control**

1. All computer workstations and servers will have the latest version of the approved anti-virus software installed by the Coordinator or employees from the Office of Technology Integration.
2. Anti-virus software shall be run at all times and is not to be removed, disabled, or its scanning parameters modified.
3. Virus definition updates will be made automatically as soon as they are posted by the Office of Technology Integration.
4. Any floppy disks, CDs, DVDs, USB storage media, or other removable media including new, formatted ones shall be scanned for viruses before being used in the computer.

**F. Violation Penalties**

1. Copyright statutes do not preclude the position of legal liability for copyright infringements on government agencies or their staff. Illegal reproduction of software can subject the violator to civil damages and criminal penalties.
2. Violations of the provisions of this general order and University policies regarding computer access and utilization may subject Departmental employees to disciplinary actions discussed in General Order, titled, "Standards of Conduct."

**G. Mobile Data Terminals (MDTs)**

A complete discussion of the use of MDTs is provided in General Order, titled, "Mobile Data Terminals (MDT's) Systems."

**H. Computerized Central Records**

1. Security. The Server Room is located in a secure temperature-controlled room. This room is only accessible by command staff units and will not be entered without the express authorization of Chief, member of command staff, or Coordinator. [CFA 26.04A, B]
2. Maintenance, Back-up, and Retention [CFA 26.04B]. All Departmental information technology resources and processes (hardware, software, servers, security, licensing, etc.) are maintained by a full-time Technical Specialist. Backups are performed daily by the University Computing Service (UCS) a division of the Office of Technology Integration. In addition, the University Computing Services saves and backs-up any files that have been changed within a 24-hour period to an off-site system.

3. The Coordinator will remove unauthorized personnel from the electronic records system within 10 business days after electronic notice of termination is received from the Chief of Police or designee. [CFA 26.04C]

**Glossary**

**Coordinator** – The agency’s Information Technology (IT) Manager.

**Intranet** – A private network inside a company or organization, which uses software like that used on the Internet, but is for internal use only, and is not accessible to the public.


**Information Technology Services (ISI)** – The University department that coordinates the University information technology resources and processes.

**RMS** – Records Management System.

**University Computing Services** – The unit within OTI that provides technical support services, e.g., security, back-up, and recovery, to FSU departments.

**Attachments**

None

CAA 06/29/2020	Filed: General Order 1109
Title: Utilization & Security of Computer Hardware and Software	
Approved:	 Terri S. Brown, Chief
Effective Date:	06/29/2020