GENERAL ORDER	Effective: 10-01-2021	# 05-02
	Section: Equipment & Technology	**Replaces or Modifies:** GO 14
	Title: Information Technology Systems **Issued by: Chief Deputy Mattie Provost**	

Purpose:

To establish guidelines for information technology systems owned or operated by the Fort Bend County Sheriff's Office (FBCSO).

Policy:

The FBCSO provides information technology systems to enhance the ability of the Agency and its employees to perform duties in the public interest. All employees shall only use these systems in accordance with policy and law.

Definitions:

Information Technology System (ITS) – Any FBCSO owned or operated equipment used for sending, receiving, storing, or accessing information by electronic means on wired or wireless networks. This term includes hardware (examples include but not limited to computers, telephones, laptops, and related items), software (inclusive of operating systems including but not limited to Records Management Systems, Computer Aided Dispatch Systems, Evidence/Property Management Systems,…) e-mail systems, and telephone systems. This term also includes systems such as CJIS, TCIC, NCIC, TLETS and any system where the FBCSO is the hosting agency.

Owned or Operated by FBCSO – Any ITS purchased by Fort Bend County for the operational use of the FBCSO or any part of an ITS under operational authority of the FBCSO (this term includes systems where the FBCSO is the hosting agency) regardless of purchase funding source.

Procedure:

I. Permissible Use
   A. Permissible use of an ITS is to carry forward FBCSO business. It is the responsibility of all employees to use an ITS in the most efficient and effective manner. Appropriate uses include but are not limited to:
      1. Assist in performance of specific job duties (examples include filing of reports, dispatching calls for service, entering evidence into the property room, using State and Federal systems to search for warrants/criminal history records…)
      2. Communicate information
      3. Coordinate meetings
      4. Private use of an ITS is allowed if the use does not violate any other General Order/Bureau Manual or Law, is minimal, and is not detrimental to the reputation of the FBCSO.

II. Prohibited Uses
   A. Unless the use is necessary to the performance of a particular authorized job duty

(one example includes conducting an authorized investigation into internet pornography) or by authorization of the Chief Deputy or Sheriff employees many not use any ITS in any of the following manners -

1. Sending or choosing to receive information that could reasonably be considered as being offensive, sexually explicit, abusive, threatening, or otherwise inappropriate for the workplace.
2. Sending or choosing to receive information that violates any FBCSO Policy
3. Copying or transmitting any documents, software or other information protected by the copyright laws, without proper authorization by the copyright owner. Copyright protection applies to any document, photo, software, or information unless it is specifically marked as public, not copyrighted, or freeware. In the absence of any specific copyright markings, material or information should be considered copyright protected.
4. Breaking into or attempting to break into an ITS (this includes any attempt to gain unauthorized access into an ITS) or unauthorized use/possession of a password (sharing of passwords and/or using another employee's password are examples of unauthorized use of a password).
5. Intentionally and maliciously misrepresenting the originator of any type of electronic information.
6. Supporting recreational use by sending or choosing to receive nonbusiness unauthorized software or services including games or entertainment software or services.
7. Sending or choosing to receive information related to news groups, chat rooms, instant messaging or other sources that are not clearly work-related.
8. Obtaining information that is protected by privacy laws and making this information public without authorization.

B. The FBCSO licenses software it uses. All software may be used only in accordance with the terms of the license agreement. Any unauthorized use of such software is prohibited.

C. Use that violates user agreements in systems where the FBCSO is the hosting agency (examples include but are not limited to CJIS,TCIC,NCIC,TLETS)

D. Any employee who becomes aware of prohibited use is to report this to supervisory personnel for resolution.

III. All hardware and software to be used by any ITS must have approval from the Support Services Division prior to purchase and/or installation.

IV. An employee in possession or in control of FBCSO owned or operated hardware or software shall take all reasonable efforts to insure that this property remains in good working condition. Any loss or damage shall be immediately reported to supervisory personnel for resolution.

V. All electronic information on any ITS remains the property of the FBCSO and employees have no right to privacy in the use of any ITS even if use is for personal business as authorized by this General Order. Employees are reminded that it may be within the capability of an ITS to recover previously deleted items at any time and those recovered items remain the property of the FBCSO. Recovering includes actual content and identifying information (one example is an actual e-mail message along with information on who sent it, who it was sent to, time sent, date sent, etc….)

VI. The FBCSO reserves the right, with or without notice, at any time, for any reason, to monitor the use of any ITS and to access information sent, received, or stored.

VII. Employees are reminded that information on an ITS may be subject to public disclosure per State public information laws.

VIII. The FBCSO determines who may access and the extent of access privileges on any ITS owned or operated by the FBCSO. The Chief Deputy shall by practice and/or written guidance determine access privileges and may delegate duties as he/she deems fit relating to access privileges and/or revocation of privileges.

IX. Any software from an internet source must be screened by the Support Services Division prior to any download to protect against viruses.

X. Apps on county cell phones

A. Employees may put apps on county cell phones. The content and application of any such app must not be intended for use or be used in a manner that violates Law or FBCSO policy (examples include but are not limited to apps that would be seen as offensive in violation of Section II of this General Order or are designed to compromise network security).

B. The employee downloading any app under authority of this section assumes responsibility of the reliability and trustworthiness of any such app. If the app causes issues with the function of the cell phone or any other system the employee may be liable for damages attributed to the downloaded app including but not limited to replacement cost for the cell phone and/or disciplinary action.

XI. Any person who is not an employee of the FBCSO and who is granted access to any FBCSO owned or operated ITS is expected to abide by all usage guidelines in this General Order and/or other applicable FBCSO policies. The Chief Deputy retains authority to grant, deny, or revoke access privileges in all cases.

XII. Only the Sheriff or Chief Deputy may authorize exceptions to this General Order.