SEMINOLE COUNTY SHERIFF'S OFFICE GENERAL ORDER	NUMBER: G - 45
	RESCINDS:
SUBJECT:	**Information Systems and Services**
EFFECTIVE:	**February 7, 2000**
REVISED:	**February 18, 2025**

Table of Contents:

I. PURPOSE:

This policy gives direction for the effective management and security of electronic systems and services of the Sheriff's Office.

II. SCOPE:

It is the policy of the Seminole County Sheriff's Office to deliver and support technology solutions to meet the needs of its diverse workforce in support of its official mission. This directive provides appropriate controls to protect the information to which it has been entrusted. It provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of data. This directive applies to every individual - employee, contractor, private entity, noncriminal justice agency representative, volunteer, intern, reserve, etc. with access to, or who operate in support of, SCSO's criminal justice information and systems.

III. DEFINITIONS:

A. *Criminal Justice Information (CJI):*
CJI is defined as any information derived, in whole or part from any state or federally controlled source, such as FCIC/NCIC or CJNet. This includes partial information that might otherwise be gained from

publicly available resources. For example, an address gained from running a person in DAVID is CJI, even though that information may be gleaned from property records. A statement saying that a person does not have a criminal history comprises CJI. Only the following types of data are exempt

from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

B. *Criminal History Record Information (CHRI):*
A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges, when obtained in whole or part from any state or federally controlled source. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI.

C. *Personally Identifiable Information (PII):*
PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Most Restricted Systems provided or maintained by the agency include an individual's PII.

D. *Restricted Systems:*
Restricted records systems are systems that contain CJI or PII. They are also systems that contain any information otherwise considered confidential or exempt by state or federal law. Examples of these systems include, but are not limited to; NCIC/FCIC, CJNet, David, CAFEWeb, XCAD/MiCAD, TUCSON, ELVIS, Finder, Jail Management, CorrecTek, Human Resources and Payroll systems.

E. *Computer:*
Any device running a full featured operating system (e.g. Microsoft Windows, Apple OS X). This definition includes desktop computers, towers, and servers. It also includes laptops such as MCT's and certain tablet computers like the Surface Pro. This definition does not include smartphones.

F. *Limited Operating System Devices:*
Limited-feature operating systems devices are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers (e.g. Apple iOS, Android, Windows RT/Phone, Blackberry OS, etc.). For the purposes of this policy, the term "smartphone" may be used interchangeably with the phrase "limited operating system device." Any policy covering smartphones also applies to other handheld devices such as limited operating systems devices such as iPads and Android tablets.

G. *Mobile Device Management (MDM):*
Security rich software deployed on smartphones. MDM software allows the agency to administer the security of the device, containerizes and protects agency data and allows secure access to agency networked resources.

H. *Spam:*
Unsolicited or inappropriate email messages, especially advertising.

I. *Phishing:*
To try to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one.

J. *Physically Secure Location:*
A physically secure location is a facility, a criminal justice conveyance (such as an enclosed, secured automobile), or an area, a room, or a group of rooms within a facility with both the physical and personnel

security controls sufficient to protect CJI and associated information systems.

IV. GOVERNING AUTHORITY:

A. The FBI's Criminal Justice Information Services (CJIS) Security Policy version 5.5 or higher governs minimum security standards that must be met when processing or storing criminal justice information.

B. The Criminal Justice User Agreement between the Florida Department of Law Enforcement and the Seminole County Sheriff's Office defines the terms and conditions under which access to FCIC/NCIC/CJNet is granted.

C. Chapter 119, Florida Statutes provides for general state policy on public records, including confidentiality, retention, inspections and exemptions.

D. Chapter 316, Florida Statutes, State Uniform Traffic Control, section 316.305 governs the use of wireless communication devices while driving.

E. The Privacy Act of 1974 prohibits the disclosure of personally identifiable information maintained by agencies is a system of records without the consent of the subject individual, subject to twelve codified exceptions.

F. Health Insurance Portability and Accountability Act (HIPAA) protects certain individually identifiable health information.

G. Title 28, Part 20, Code of Federal Regulations (CFR) defines CHRI and provides the regulatory guidance for dissemination of CHRI.

H. Title 18, Part I, Chapter 47, § 1030, United States Code (USC) criminalizes fraud and related activity in connection with computers.

I. Florida Statute 817.568 Criminal use of personal identification information

J. Florida Statute 943.125 (4)(o) Access and use of personal identification information

V. NO EXPECTATION OF PRIVACY:

A. By authorizing use of the electronic equipment (computers, smartphones, programs, network, etc.) by its personnel, the Sheriff's Office does not relinquish control over materials on the systems or contained in system files.

B. Users should not expect privacy in the content of files, emails, texts, call logs, electronic messages or any other data residing on or processed by Sheriff's Office owned equipment. Agency systems should not be used as repositories for personal documents, images or records. All information stored on agency systems is subject to release in accordance with provisions set forth in state public records law and in response to court orders.

C. Information systems are provided as tools for official business purposes and all information created, accessed or stored using these systems are subject to monitoring, auditing or review.

D. Unencrypted electronic communication should never be considered secure. Email could potentially be stored indefinitely on any number of computers. Copies of your message may be forwarded either electronically or on paper. In addition, email sent to nonexistent or incorrect accounts may be delivered to persons that that were not intended to receive it.

E. Unless exempted by Chapter 119, Florida Statutes and/or other provisions of state law the Sheriff's Office treats all records in any format created or sent in connection with the transaction of official

business as public record.

F. Internal review of an individual user's data such as system usage logs, email, cell phone records, etc. is authorized in the following circumstances:

1. By Records personnel to fulfill public records requests.

2. By Professional Standards to conduct investigations.

3. By Technology Solutions personnel to ensure the efficient operations of systems, compliance with policy and directives such as the CJIS Security Policy, and to assist an individual with their own account or equipment.

4. By Financial Services to process invoices and bill agency members for excess or unauthorized services.

5. By request of another agency member via chain of command, approved at the rank of Chief or above. The request will then be addressed to the Director of Technology Solutions for processing.

6. By court order for production of records.

7. Exceptions exist for items where custom reports have been made readily accessible to users of certain agency systems. This includes the CAFEWeb Incident Audit Report and the XCAD/MiCAD Audit User Messages Report.

G. Custom signatures or footers on emails must be limited to contact information. No verbiage relating to public records laws, disclosure, distribution, privacy, confidentiality or similar language should be included. All emails sent to recipients outside of the seminolesheriff.org domain will automatically get a standard disclaimer attached to them.

VI. INFORMATION AND EQUIPMENT HANDLING:

A. The integrity of Sheriff's Office information systems are critical to the effective delivery of law enforcement, corrections, and support services. Users are responsible for guarding the system against unauthorized users, protecting confidential information, safeguarding hardware, conforming to legal requirements, the FBI CJIS Security Policy and written directives.

B. Agency controlled buildings are monitored by security cameras. All ingress and egress to agency buildings (except for those areas within the facility officially designated as publicly accessible) are controlled via smart card coded access systems and guarded by law enforcement or security guards when appropriate. Physical access to information systems and networking equipment within the physically secure location are further protected by additional permissions on the access control system, electronic keypads or physical lock and key depending on the facility. Individual access authorization must be verified before access is granted.

C. Restricted systems are to be used to conduct official Sheriff's Office business only. Users are prohibited from using any restricted system for personal or private reasons.

D. Sheriff's Office systems contain a wide array of confidential and exempt information. Many records and files, in both electronic and paper formats, contain protected CJI and PII for which special handling is required.

E. PII may be extracted from CJI systems for official business only. Approved examples including searching for a person in FINDER or eAgent to extract additional information to complete a warrant, running a tag to learn the vehicle's owner then populating XCAD or CAFEWeb with the corresponding information. PII may also be supplied to agency representatives by other means. This includes situations

like an applicant completing a job application or a citizen verballing providing details for investigate report. All policies and procedures that relate to the handling of CJI are applicable to the handling of PII and are detailed below.

F. Physical access to information system devices that display CJI or PII (i.e. computer monitors or laptops) must be controlled and positioned in such a way as to prevent unauthorized individuals from accessing and viewing CJI or PII.

G. Visitors must be authenticated before being authorized to have escorted access to the physically secure locations (except for those areas designated as publicly accessible). Visitors must be escorted by an SCSO employee at all times and their activity must be monitored.

H. Data containing CJI or PII that is transmitted or transferred electronically outside of the Sheriff's Office network, via email or other methods (with the exception of facsimile), is required to be encrypted to FIPS 140-2 standards. The Technology Solutions Division ensures that the hard drives of mobile computers are properly encrypted. In addition, the MDM on agency issued smartphones ensures agency information is secured when accessed in that method.

I. Paper files containing CJI, CHRI or PII must be stored within the physically secure area accessible only to users authorized to use the information. When not needed for immediate use, paper records will be placed into locked filing cabinets inside the physically secure area.

J. Electronic media containing CJI, CHRI or PII while in transport (physically moved from one location to another) shall be encrypted. The Technology Solutions Division issues encrypted thumb drives for this purpose.

K. Any media containing CHRI that are removed from the physically secure area will be recorded on the secondary dissemination log.

L. Paper files transported between locations must be transported in a sealed envelope or locked briefcases.

M. All media in transport must remain in the possession of the user until re-secured. At no time will the media physical media be released to an unauthorized person or left without proper documentation. If at any time a user knows or suspects they have lost control of media, even temporarily, this must be reported immediately to Technology Solutions via 407-665-6900.

N. Under no circumstances will CJI, PII, exempt or confidential information in the custody of the Sheriff's Office be communicated via any means to an unauthorized person or entity.

O. Users must maintain personal control of their computers and smartphones whenever they leave the confines of the controlled area. If at any time a user knows or suspects they have lost control of their device, even temporarily, this must be reported immediately to Technology Solutions via 407-665- 6900. Use of Sheriff's Office technology equipment and network by family members or friends is prohibited. Use of agency systems by the public or an outside agency member is also prohibited unless it has been expressly configured for that purpose by Technology Solutions (for example, computers located in Community Rooms).

P. User must maintain the security of their passwords and any credentialing tokens. If users know or suspect credentials have been lost, compromised, or they are the target of an unauthorized attempt to gain credentials (phishing), they shall contact Technology Solutions via 407-665-6900 for assistance.

Q. The use of PKI (Public Key Infrastructure) to gain access to CJI or PII is prohibited.

R. Access to and use of personal identification information is in accordance with Florida Statute.

VII. SECONDARY DISSEMINATION AND CHRI/CJI:

A. CHRI data is typically state arrest records searched through e-Agent. In addition to arrest and criminal charge information, CHRI also consists of the following restricted files:

1. Gang Files
2. Known or Appropriately Suspected Terrorist Files
3. Supervised Release Files
4. Immigration Violator File
5. National Sex Offender Registry Files
6. Historical Protection Order Files of the NCIC
7. Identity Theft Files
8. Protective Interest Files
9. Person with Information (PWI) data in the Missing Person Files

B. CHRI is disseminated only as a part of the user's criminal justice duties on a need to know, right to know basis. Voice transmission of CHRI should be limited, and details should only be given over a radio or cell phone when an officer's safety is in danger or the officer determines that there is a danger to the public. A facsimile machine may be used to send CHRI providing both the sending and receiving agencies have an ORI and are authorized to receive criminal history information.

C. CHRI is constantly changing and should only be kept until a case file is closed, the record is superseded, obsolete or the administrative value is lost. Documents that have not lost their value and are still being kept must be stored in a manner to prevent unauthorized or unintended access. CHRI information must never be cut and pasted or stored in agency records management systems such as CAFEWeb or Jail Management. Neither shall it be included as part of a criminal case packet sent to the State Attorney's Office.

D. CHRI may be disseminated to other authorized criminal justice agencies. When the person requesting and/or in the possession of the criminal history shares any part of that information with another criminal justice professional outside of their agency, physically or verbally, that action is considered secondary dissemination.

E. Logging is encouraged anytime CJI is released, however logging is REQUIRED when releasing CHRI. Any user that shares criminal history information with a member of another criminal justice agency must maintain a Secondary Dissemination Log. Secondary Dissemination Logs must be maintained for at least four years for audit purposes. All Secondary Dissemination Logs must be approved by the FCIC Agency Coordinator (Communications Manager) prior to use. Unauthorized request, receipt or release of CHRI/FCIC/NCIC material could result in criminal proceedings or loss of agency access to state and federal systems.

F. Users are required to validate that the requestor of the information is an employee or authorized contractor of a law enforcement agency requiring the information to perform their mission before dissemination. If the requestor is not personally known to the user as being employed by a law enforcement agency, that user must independently verify the requestor's credentials. This can be accomplished by viewing someone's enforcement credentials, identification badge, conducting an employment verification with the requestor's agency, or via teletype.

G. The Secondary Dissemination Log must include the following information:

1. The date the criminal history was released.

2. The subject (name) of the criminal history request.

3. Any numeric identifiers used to obtain the complete criminal history (e.g., FBI numbers and/or SID numbers).

4. Who the information was released to (the requestor).

5. The name of the requestor's agency, this field is mandatory for secondary dissemination logs.

6. Who released the information (the operator).

7. The reason the criminal history was requested (e.g., incident number, case number, type of investigation).

8. The purpose code used to run the criminal history. It is essential the correct purpose code is utilized. Some common purpose codes include:

   a. F - Release a gun to the owner,

   b. J - Employment Applications, and

   c. C - Individuals not administration of criminal justice such as Janitorial, maintenance and vending personnel.

VIII. MOBILE DEVICE:

A. The Sheriff's Office recognizes the importance of mobile technologies such as cellular telephones, smartphones or other limited-feature operating system devices (collectively referred as a "mobile device") that employ wireless telecommunications as a tool in conducting law enforcement business with residents, visitors, businesses, and governmental agencies located within and outside Seminole County. Their mobility, functionality, ease of use, reliability and low cost make them indispensable time saving law enforcement tools.

B. Many agency issued mobile devices have the ability to access restricted systems. Due to their small size and portable nature, users must take extreme care to ensure the security of the device.

C. Use of Mobile Devices:

1. Mobile devices are used to supplement existing telecommunication systems and should not be used to circumvent the Sheriff's Office 800 MHz radio system.

2. Using a mobile device for texting while driving is governed by Chapter 316.305 Florida Statutes.

3. Users are responsible for voice and data usage on their assigned device.

4. The mobile device is for the express use of the person to whom it has been issued (and who is accountable for its use). Use of an assigned device by family members and friends is prohibited.

5. Mobile devices should not be used when confidential voice communication is desired.

6. Mobile phone numbers are the property of the Sheriff's Office. Agency members who retire from the agency in good standing may be eligible to port their assigned number to a personal device. Requests should be made via chain of command, approved at the rank of Captain/Director or higher, and forwarded to the Director of Technology Solutions for review and processing.

D. Request for a Mobile Device:

1. Requests for issuance of a mobile device shall be made via chain of command, approved at the

rank of Chief or higher, and forwarded to Technology Solutions for processing.

E. Calling Plans (Use of Mobile Device for Personal Business):

1. The Sheriff's Office currently contracts for a pooled minute calling plan that also provides for additional services such as free nights and weekend calling and free mobile to mobile calling and nationwide roaming. Pooled minutes purchased by the Sheriff's Office are then shared within the Agency.

2. Contracted plans are obtained based upon billing management reports, which indicate calling patterns of users assigned to specific functions. These reports are reviewed by Technology Solutions and Financial Services and changes made to plans as necessary.

3. Minutes not used under the Sheriff's Office pooling plan do not result in cost savings to the Sheriff's Office. For this reason, and the fact there may be other reasons during the work day which necessitates personal use of the telephone (family emergency, late work day, etc.), the issued cell phone may be used for personal business subject to the following:

   a. During working hours, but should be limited to emergencies or calls of short duration to ensure productivity and adherence to work place protocol.

   b. During time periods, or under other circumstances, when the Sheriff's Office is not contractually charged for the call. Examples include "free nights and weekend" periods and "free mobile to mobile" calling. Such calling shall not occur when the user is on duty except for emergency situations or calls of short duration.

   c. Users may be held financially responsible for excess minutes if the Sheriff's Office exceeds its pooled monthly minute allocation, thereby incurring additional monthly costs, and the excess minutes incurred by the user cannot be justified as work related. Exceptions to this allocation of costs are based upon extenuating circumstances (all work related calls, multiple assignments, major case, etc.) and may be approved by the user's Lieutenant or equivalent rank supervisor.

   d. Users are responsible for paying any monthly expense that is not business related and not provided for under the Sheriff's Office mobile device contract. Exceptions may be made for items such as international roaming or mobile application purchases preapproved by the Director of Technology Solutions.

4. Users are allowed minimal personal use of the devices internet and mobile application capabilities where such use does not result in any additional charges to the Sheriff's Office, or interfere with official duties in any way.

5. Financial Services will send usage bills to users who incur excess or unauthorized expenses and who must reimburse the Sheriff's Office. Reimbursement must be remitted to Financial Services within ten days of receipt of the bill.

F. *Care and Security of Equipment:*

1. Mobile devices such as cell phones or smartphones are issued in protective cases to help prevent accidental damage. When a device has been issued in a case, it must remain in that case at all times, unless instructed to remove it by Technology Solutions.

2. Users are responsible for the care and upkeep of their assigned mobile device, case and accessories and may subject to reimbursing the Sheriff's Office for the cost of repairs/replacement.

3. Users are prohibited from modifying the operating system or firmware of their assigned mobile device (rooting or jail-breaking).

4. Users are prohibited from removing, tampering with, or circumventing the MDM software.

G. *Loss/Compromise/Repair of Mobile Device:*

1. User's must immediately notify Technology Solutions and their supervisor if their mobile device is lost, stolen or its security potentially compromised. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or website as Technology Solutions may be able to remotely locate a device if notified right away. If loss of the device is determined the fault of the user or the loss was not reported in an immediate fashion, the user may be responsible for reimbursing the Sheriff's Office for any financial losses.

2. Requests for mobile device repair shall be directed to the Technology Solutions Help Desk. If damage to the repair is determined to be the fault of the user, the user may be subject to reimbursing the Sheriff's Office for the cost of repairs/replacement of the device.

H. *Mobile Applications Use:*

1. One of the major benefits of using a limited feature operating system device such as smartphones and tablets is the ability to install and use mobile applications. Ubiquitous access to Sheriff's Office resources such as email, calendars and applications create a much more efficient operational environment. However, it also increases the risks for unauthorized access to Sheriff's Office resources or PII due to malicious or poorly written applications.

2. Mobile Device Management software (MDM) is preloaded on agency smartphones. MDM software is required to comply with the FBI CJIS Security Policy.

3. Applications may only be downloaded from standard applications stores, specifically the Google Play Store, the Apple App Store or the Amazon App store. Authorized applications may also be available from the MDM application catalog or pushed directly to the device. Installation of unauthorized Applications is prohibited unless preapproved by the Director of Technology Solutions.

4. Users must review and comprehend permissions granted to applications that they elect to install. Excessive permissions can compromise the security of the device and any personal information it contains. For example, applications that can access geolocation (GPS) can track the phone's location and could potentially cause a threat to a user's personal safety or to operations in which they are involved, so discretion should be used when enabling this feature.

5. Six digit pins are required for device access.

I. *Text Messaging:*

1. The Sheriff's Office does not have the ability to electronically archive text messages. Text message should be used for transient messages only. Users that inadvertently make or receive a text message in connection with official agency business must forward that message to their Sheriff's Office email account for retention in accordance with Chapter 119 Florida Statutes.

IX. SHERIFF'S OFFICE INFORMATION SYSTEMS:

A. *Legal Use of Software/Databases:*

1. The Sheriff's Office licenses the use of computer software from a variety of vendors, and does not own this software or related documentation. Licensed software (Microsoft Word, Excel, etc.) is only used on one computer at a time and only upon authority of the Technology Solutions Division. Any unauthorized duplication of licensed software, except for backup or archival purposes, is a violation of federal law and this policy.

2. Use of Sheriff's Office internally developed databases or databases accessible via the Sheriff's Office computer system through contractual agreements are predicated upon an user's job function and associated need to know. The use of such databases containing information not subject to public disclosure by users not normally authorized access to said databases and for uses not pertaining to official Sheriff's Office business is prohibited.

B. *Purchase/Installation of Computer Hardware or Software:*

1. All computer software and hardware will be purchased by the Technology Solutions Division. Requests for software or hardware are submitted through email to 6900@seminolesheriff.org. Technology Solutions will obtain the necessary quotes, write the requisition and place the order. Software and hardware will be installed only by Technology Solutions staff after ensuring it is registered with the appropriate licenser, if required. Exceptions to the above can only be made with special permission from the Technology Solution's Director.

2. The introduction, installation, modification or removal of software or hardware on any Sheriff's Office computer, device or network infrastructure without the prior approval of Technology Solutions is prohibited unless expressly allowed in this policy.

C. *Movement of/Tampering with Equipment:*

1. Seminole County Sheriff's Office Technology Solutions equipment (computers, servers, routers printers, UPS boxes, projectors, wall/ceiling mounted screens, etc.) shall not be moved or tampered with by non-Technology Solutions personnel unless specifically authorized by email from 6900@seminolesheriff.org.

2. Only Technology Solutions personnel or persons specifically authorized by its supervisors are permitted to access rooms or areas that house Sheriff's Office server systems.

3. Users may not alter Sheriff's Office computer hardware and/or peripheral equipment or accessories without prior authorization from Technology Solutions. Altering includes, but is not limited to, defacing, marring, inscribing, painting or affixing items or stickers to the equipment.

4. Users are responsible for returning agency equipment in the condition in which received, normal wear and tear excepted. Users may be held financially liable for altering or damaging agency equipment, the results of which impacts the value of the equipment, negates warranty protection and/or causes said equipment to be unfit for repurposing.

D. *Disaster Preparedness:*

1. Central computer records are routinely backed up in case of system failure.

a. The Technology Solutions Director (or designee) is responsible for ensuring Sheriff's Office computer records are backed up on a regular and consistent basis, and for ensuring that backup media is stored in such location(s) so as to be able to effectively restore the agency's records in the event of a catastrophic event.

b. Central computer records are automatically backed up to electronic storage media.

c. Storage media is also backed-up on a weekly and monthly basis, and is stored off-site

at a secure location determined by the Technology Solutions Director.

2. Users should routinely backup agency records stored on local computers to the agency network to ensure they get automatically backed up through the central computer system.

E. *Acceptable and Unacceptable Uses of the Sheriff's Office Information Equipment and Systems:*
The ability to access information systems and networks is essential to enhancing a user's work performance, and they are provided with access to Sheriff's Office computer systems for this purpose. Any suspected misuse of the Sheriff's Office computer system including hardware, software, databases, CJI, PII, network, reports or internet must be reported to Professional Standards for evaluation. Misuse of Sheriff's Office systems will be recorded in the user's record. Depending on the nature of the violation, it may also be reported to the Florida Department of Law Enforcement, the Department of Highway Safety and Motor Vehicles or the Criminal Justice Standards and Training Commission and may result in disciplinary action up to and including termination.

1. Acceptable Uses:

a. Personnel are permitted to access the Internet and other Sheriff's Office systems to conduct authorized investigations, supervisory required quality assurance reviews, further Sheriff's Office business, or enhance educational goals consistent with the Sheriff's Office mission, except as otherwise prohibited.

b. Personal use of unrestricted Sheriff's Office systems, such as the Internet and phones is limited to short periods of time such as during break or lunch periods or occurring before/after normal working hours and is subject to monitoring by the Sheriff's Office to ensure conformance with acceptable use policies and duration limits.

2. Unacceptable Uses:

a. Access, review, upload, download, store, print, post, or distribute pornographic, obscene, or sexually explicit material, except for authorized law enforcement purposes.

b. Transmit obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language, except for authorized law enforcement purposes.

c. Access, review, upload, download, store, print, post, or distribute materials using language or images inappropriate to a business setting or disruptive to the business process, except for authorized law enforcement purposes.

d. Access, review, upload, download, store, print, post, or distribute materials that use language or images advocating violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination, except for authorized law enforcement purposes.

e. Knowingly or recklessly post false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

f. Engage in any illegal act or violate any local, state, or federal statute or law.

g. Vandalize, damage, or disable the property of another person or organization or make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means. Furthermore, users shall not

tamper with, modify, or change the agency system software, hardware, or wiring or take any action to violate the agency system's security, and shall not use the agency system in such a way as to disrupt the use of the system by other users. Gain unauthorized access to information resources or to access another person's materials, information, or files without authorization.

h. Post or share private or personally identifiable information about another person including, but not limited to, addresses, telephone numbers, identification numbers, account numbers, access codes or passwords, except for authorized law enforcement purposes.

i. Attempt to gain unauthorized access to any agency system, attempt to log in through another person's account, or use computer accounts, access codes, or network identification other than those assigned to the user.

j. Violate copyright laws, or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any agency computer, and shall not plagiarize works they find on the Internet.

k. Conduct a personal business or conduct transactions for financial gain unrelated to the mission of the agency.

l. Knowingly put the agency computers or software programs at risk by opening a suspected email, email attachment, or load files that may contain a virus or spam. If the user suspects that they have an infected email or file, the user shall immediately notify Technology Solutions for instructions.

m. Knowingly pass infected email files or damaging software to anyone in the agency or outside the agency that could cause the Sheriff's Office to be potentially liable for damages to other computer systems.

n. Disguising your identity when sending email except for authorized law enforcement purposes.

o. Knowingly initiating or forwarding chain mail. Chain mail is a message sent to a number of people asking each recipient to send copies with the same request to a number of others.

p. Use agency email or messaging systems to create or send unprofessional and inappropriate statements that could negatively impact the Sheriff's Office or interfere with its core mission and values.

q. Allow non-agency members to access agency systems or utilize any Sheriff's Office issued equipment or network without prior authorization from Technology Solutions, unless it has been expressly configured for that purpose (for example, computers located in Community Rooms).

r. Conduct or participate in a political campaign.

s. Use of restricted Sheriff's Office and other law enforcement databases for personal or unauthorized use is strictly prohibited.

t. Access, review, upload, download, store, print, post, or distribute materials stored in the Axon or Panasonic digital evidence recording systems. Access to those systems shall be restricted to those members who have direct involvement in any piece of

digital evidence captured using those two systems.

u. Live Streaming in-car or body worn cameras without an operational need.

X. DATA BREACH INCIDENT RESPONSE

A. A data breach is an incident in which sensitive, protected or confidential data is exposed to an unauthorized individual. Data breaches can occur in a variety of ways, including through hacking, phishing, social engineering, and malware attacks. The following is to outline the steps that will be taken by the Seminole County Sheriff's Office in the event of a data breach. The goal of this policy is to minimize the impact of a data breach and to protect the Sheriff's Office data and reputation

B. *Responsibilities*

1. The Director of Technology Solutions is responsible for developing and maintaining the organization's data breach incident response plan.

2. The Data Breach Response Team (DBRT) is responsible for carrying out the organization's data breach incident response plan. The DBRT is comprised of the agency LASO (Local Agency Security Officer) and System and Network Administrators

3. All employees are responsible for reporting any suspected data breaches to the Director or the DBRT immediately

C. Any data breach or security incident will follow specific response according to the nature of the breach.

1. Identify the breach. The first step is to identify the breach. This may involve determining the type of data that was exposed, the number of individuals affected, and the potential impact of the breach. Once identified, an Incident ticket will be opened in the Sheriff's Office ticketing system. The ticket should have the following information, to be filled in for the lifecycle of the incident:

a. Where the breach occurred. Workstation IP or device ID.

b. When the breach occurred. This may not be accurate at the start of the incident.

c. What data was exfiltrated

d. Who was affected.

e. How was the breach manifested. Root cause and kill chain.

2. Contain the breach. The next step is to contain the breach. This may involve taking steps to prevent further unauthorized access to the data, such as disabling user accounts, changing passwords, blocking IP addresses and isolating systems up to and including total network shutdown.

3. Investigate the breach. The next step is to investigate the breach. This may involve determining how the breach occurred, who is responsible, and what data was exposed

4. Notify affected individuals. The next step is to notify affected individuals of the breach. This notification should include information about the type of data that was exposed, the potential impact of the breach, and steps that individuals can take to protect themselves.

5. Report the breach. The LASO will inform FDLE of all breaches immediately. At the same time once a breach has been discovered, the Agency Cyber Insurance Company will be notified via the Director.

6. Take corrective action. The final step is to take corrective action to prevent future breaches. This may involve implementing new security measures, training employees, and review and conduct security audits. A post mortem or root cause report (RC) and a corrective action (CA) report will be generated.

D. *Communication of an Incident*

1. The Agency will communicate with affected individuals and the public about the data breach in a timely and transparent manner. The communication will include information about the type of data that was exposed, the potential impact of the breach, and steps that individuals can take to protect themselves.

E. *Training*

1. The organization will provide training to employees on how to identify and report data breaches. The training will cover the following topics:

a. The definition of a data breach

b. The signs of a data breach

c. How to report a data breach

d. The importance of reporting data breaches

e. The mandatory Security Awareness Training is to be done annually. In addition, the agency will conduct tabletop exercises to improve incident response at the very least annually if not more based on environment and need.

F. *Testing*

1. The Sheriff's Office will test its data breach incident response plan on a bi-annual basis to ensure that it is effective. The testing will include the following steps:

a. Identifying potential data breach scenarios

b. Developing response plans for each scenario

c. Testing the response plans

d. Making improvements to the response plans as needed

XI. EMAIL:

A. As CJI and PII must be encrypted while in transit, users shall not send data containing CJI or PII via unencrypted email, including via the Sheriff's Office Exchange (Outlook) email system. Encrypted email service is available via CJNet at http://www.flcjn.net/Email.aspx and the FBI's Law Enforcement Enterprise Portal (LEEP).

B. As state and federal law governs the retention of public records, the Sheriff's Office's systems archive emails to ensure compliance. Email messages regarding official Sheriff's Office business shall not be sent from personally owned electronic devices (such as a home or public computer or a user owned smartphone) to any email address other than one that belongs to the Sheriff's Office (the seminolesheriff.org domain), except as noted above. Use of outside equipment to conduct official agency business subjects that equipment to searches to preserve evidence or respond to public records requests.

C. Unsolicited Emails:

1. Emails containing spam should be deleted without being opened.

2. If an unsolicited email is inadvertently opened, users should not click on an embedded links users or open any attachments without verifying the authenticity of the sender.

3. If a user suspects an email contains a virus or is a phishing attempt, they shall contact Technology Solutions at 407-665-6900 for assistance.

4. Unsolicited emails regarding offered products/services should be sent for review to the Human Resources Division before being sent out to all mail users.

D. Any member may send email that is Sheriff's Office business to "All Mail Users."

E. Email Forwarding:

1. Users may not auto forward email from the seminolesheriff.org domain to an account outside our domain (i.e. to a personal email account or to another agency). Exceptions may be granted on a case by case basis with approval of a Chief or higher.

2. Nothing in this policy prohibits a user from explicitly sending email to an external email account, provided precautions are taken with regard to protected information.

XII. VOICE OVER IP

A. Voice over IP (VoIP) is provided by Seminole County Information Technology Services. The county installs and managed the network and the devices that comprise the VoIP system.

B. Use and Restrictions:

1. Use of the VoIP system is strictly for Voice service. No data services shall be interfaced over the VoIP network.

2. Transmission of CJI over the VoIP network shall be limited to voice only and only when needed and conveyed to known and authorized recipients.

3. Voicemail on the VoIP system must be devoid of CJI, PII, PHI (Private Health Information), or HIPAA (Health Insurance Portability and Accountability Act). Voicemail is not private and is discoverable for legal and investigative purposes.

4. All VoIP devices have the default administration password changed and are only accessible by County authorized representatives.

5. All VoIP devices are located on a network that is physically separate from the Sheriff's Office data network, or where shared, a VLAN is used to segment the VoIP traffic from data traffic.

6. Users are prohibited from connecting any device other than the County-supplied telephone to the VoIP network.

7. Unused ports are automatically inactivated and additional monitoring contracts are employed to prevent the operation of a foreign device connecting to the VoIP network.

8. A softphone is a software program for making telephone calls over the Internet. Softphone use is prohibited from the County VoIP system and must never be used to convey CJI or PII.

9. Users are required to establish a PIN to access features of the VoIP system such as voicemail and single device configuration.

XIII. PERSONALLY OWNED DEVICES:

A. Personally owned devices, including, but not limited to, computers, tablets, routers, thumb drives, printers and cell phones may not be used to access, process, store or transmit CJI (or PII obtained in the course of conducting official business).

B. No personally owned devices may be connected to any portion of the Sheriff's Office network with the exception of network areas completely segregated and designated for general public use. This includes Community Rooms and guest Wi-Fi.

C. Connecting to Exchange (Outlook email) server via ActiveSync from personally owned devices is prohibited. Users may retrieve email and calendar events using the Microsoft web application (via https://webmail.seminolesheriff.org/owa/) as email never contains CJI or PII.

D. Wireless printing is not secure and should not be used. Connecting to a home printer should be done via a USB or similar cable. Printing to a public printer is not allowed. CJI or sensitive materials should not be printed while outside of the agency's physical secure location. If unavoidable, these items must be secured in a locked container or location when left unattended, and should not be viewed or accessed by unauthorized individuals.

XIV. CLOUD COMPUTING:

A. The National Institute of Standards and Technology defines cloud computing as: "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." In general terms, cloud computing means anything that involves delivering hosted services over the Internet.

B. Some examples of cloud computing services include internet mail clients such as Gmail, Yahoo and Microsoft; internet storage such as OneDrive, Dropbox, iCloud Drive; virtual office products like Google Docs and Office 365; video storage systems like YouTube and any other internet based system that where Sheriff's Office data or records could be stored.

C. Due to the inherent risks of these technologies and strict CJIS Security requirements and accreditation standards governing the use of these systems, any use of cloud or internet computing services used to conduct Sheriff's Office business must be preapproved by the Director of Technology Solutions. The Director will certify that security, privacy, licensing, auditing, public records and other management requirements have been adequately addressed prior to approving use of cloud computing services.

XV. WI-FI AND HOTSPOTS:

A. *Agency Issued Hotspots:*
Wi-Fi hotspots provide mobile wireless access to the internet and SCSO systems. These include MiFis, Jetpacks, air cards and wireless hotspot functionality on smartphones. CJIS Security Policy dictates that Wi-Fi hotspots may only be utilized by equipment issued by the Sheriff's Office. Personal use is prohibited. In special circumstances where operational requirements dictate internet access by outside entities, Technology Solutions will assist by providing services with connectivity distinct from that of SCSO systems.

B. *Agency Provided Wi-Fi:*
The Sheriff's Office has provided a limited number of agency secured network wireless access points.

These are configured, monitored and logged to conform to strict security guidelines.

C. *Public/Private Wi-Fi:*
There are significant risks to connecting to non-agency controlled wireless access points (Wi-Fi) such as those at home, coffee shops, hotels and similar locations. However, it is also a realization that working from home brings a necessity to the ability to users to connect to private/public Wi-Fi. While the agency has, at great expense, supplied MiFi and allowed hotspots, it is also a reality that the agency cannot supply everyone with a device.

When a supplied hotspot or aircard is not available or practical, users may connect to public/private Wi-Fi if the following compensating controls are in place:

1. The mobile computing device meets current policy specifications (see D: Netmotion). Agency devices already meet that specification and require advanced authentication and encryption before user can access the device.

2. Firewalls will be active and monitored. By-pass or disabling of the firewall is prohibited

3. Mobile device will only allows access to WPA2 Wi-Fi.

4. Public or Private Wi-Fi that requires an agent installed are prohibited.

5. Users should use a unique username and password for any Public/Private Wi-Fi access. Users shall not use their Sheriff's Office network username or password.

6. As part of its review of security issues and warning, Technology Solutions may from time to time blacklist a wireless access point.

7. Ad-Hoc wireless access is prohibited and will be disabled

D. *NetMotion:*
When connected to agency network resources remotely, issued laptops and tablets are required to run NetMotion. NetMotion encrypts network traffic and ensures our data flows through our enterprise grade security tools and filters and must not be bypassed unless the device is connected to an agency issued network port or agency issued Wi-Fi. Exceptions are made for devices specifically designed to run outside the agency network, such as undercover devices.

XVI. BLUETOOTH TECHNOLOGY:

A. Bluetooth Earpiece/Speakers:
Agency issued smartphones may be connected to Bluetooth or wired ear pieces or speakers by users in uniform or plain clothes while in nonpublic spaces such as cars and private agency offices. As earpieces can detract from a professional image, discretion shall be used when employing them.

B. Other Uses:
The Agency does employ Bluetooth connected RAPID-ID devices in the field for identification purposes. The RAPID-ID device is paired to each laptop by Technology Solutions before being deployed to the user. All other Bluetooth configurations and uses are prohibited.

XVII. INTERNATIONAL TRAVEL:

A. *Preauthorization:*
Sheriff's Office issued information systems equipment, including computers, smartphones and Wi-Fi hotspots may not be taken out of the country without the prior approval of the Technology Solutions Support Manager or Director.

B. *International Calling Plans:*
International roaming charges are exorbitant so agency issued cell phones should not be taken out of the country or onto cruise ships except in very limited circumstances. If your job assignment makes it imperative that the agency be able to contact you while you are travelling, arrangements for international calling must be approved at the Captain/Director level or higher and sent to the Technology Solutions Support Manager or Director at least three weeks prior to your departure. Technology Solutions will attempt to secure a plan appropriate for your travel plans, but cannot guarantee plan availability or coverage in your travel destination.

C. *Pre and Post Travel Equipment Inspections:*
Certain internal functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a "trusted" entity by the device. Technology Solutions must perform an inspection to ensure that all controls are in place and functioning properly in accordance with the policies prior to and after deployment outside of the country.

XVIII. MEDIA DISPOSAL:

A. *Physical Media:*
Physical media (printed reports and other physical hard copies) containing CJI, PII or other sensitive information that can be disposed of in accordance with G-10 Records Management shall be disposed of by shredding using a cross cut shredder provided for this purpose. The record destruction must be carried out personally by Sheriff's Office employees only. Where secure cross cut shredders are not available or the volume is very large, the Director of Technology Solutions authorizes one or more vendors to support cross cut report shredding. Destruction of records by the authorized contactor is witnessed personally by a Sheriff's Office employees.

B. *Electronic Media:*
Electronic media (hard drives, USB drives, tapes, CD's, copier drives, etc.) that ever contained or processed CJI, PII or other sensitive information that can be disposed of in accordance with G-10 Records Management are destroyed by overwriting it (at least 3 times). Where the volume of media is very large, the Director of Technology Solutions authorizes one or more vendors to support media destruction by a cross cut media shredder. Destruction of media by the authorized contactor is witnessed personally by a Sheriff's Office employee.