ORANGE COUNTY SHERIFF'S OFFICE

GENERAL ORDER

Effective Date: October 20, 2017	☒ **Amends** - GO 13.1.4 (December 19, 2011)	**Number:** 13.1.4
Distribution: All Personnel	**Review Month:** November	**Reviewing Authority:** Undersheriff / Information Technology
Subject: Computer Security		

This policy consists of the following:

1. Purpose
2. Policy
3. Definitions
4. Procedures

1. Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of the agency's information as well as the security of the technology that is used to store and transmit it.

2. Policy

It is the policy of the agency to protect the rights of the citizens and employee safety by following security protocols for the storage and dissemination of electronic information.

3. Definitions

A. Advanced Authentication (AA) - provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based public key infrastructure (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, or "Risk-based Authentication" that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

B. CJIS Security Policy (CSP) – Federal Bureau of Investigation compliance document containing information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI).

C. Criminal Justice Information (CJI) – FDLE and FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data.

D. Logical Security – The specific use of passwords and user names intended to block access to a computer network for which a user's need has not been proven, and

authorization has not been approved.

E. Mobile Device Management (MDM) – information technology system capable of the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers.

F. Network Permissions – Specific rights given to individual users or groups of users, which allow the users to access network resources.

G. Network Resources – Shared folders, printers, active directory structure or other device or object created within the agency computer network.

H. Personally Identifiable Information (PII) - 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.

I. Personally Owned Information Devices – any technology device that was purchased by an individual and was not issued by this agency. List of devices can be found in the CJIS Personally Owned Device policy.

J. Physical Security – Preventing unauthorized persons from accessing a computer network.

K. Physically Secure Location - a facility 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

L. Remote Access - temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

M. Remote Connection – Accessing the agency computer network from a computer system not directly connected to the agency computer network via a phone line, cable modem or wireless device.

N. Removable Media – Electronic storage media such as tapes, platters, CD's, DVD's, USB flash drives, or floppy disks.

4. **Procedures**

A. Security Measures

Physical security measures for computers and network workstations are the responsibility of the office or unit where those systems are installed and located. The individual unit Lieutenant or office supervisor is responsible for providing physical safeguards for the hardware, software and data to the same extent as is provided for other agency property in the unit. All computers and workstations will use both logical and physical security as preventative measures.

B. Physical Access

Computers will be kept in areas not easily accessible to the public or unauthorized personnel. Agency personnel shall control access to computers, servers, attached hardware, network equipment. This does not include outside agencies that have requested and been granted access to agency data. It is the responsibility of the requesting agency to confirm compliance with appropriate security measures. Access can also be considered the unintentional viewing of information on a computer screen. All computers must be placed in such a manner as to prevent viewing by unauthorized personnel. Computers will not be removed from the United States unless the purpose is agency business and approved by the IT Security Manager or designee.

C. User Accounts and Access

Positive control will be maintained at all times to prevent access to information by unauthorized personnel. The supervisor of each unit shall be responsible for requesting network access for personnel under their direct control. At no time will any individual be allowed to access information without specific authorization of the supervisor.

1. For access to the agency network a request must be submitted to Information Technology (IT) listing the name and ID number of the individual or individuals for whom access is being requested. Each individual that is allowed network access shall have a user name consisting of their first initial followed by their last name and an identifying numeric character in the event of duplicate naming (i.e. jsmith01). The new user shall be advised of his/her initial password. Only one logon will be allowed with this password. Subsequent problems with passwords must be submitted to the IT Service Desk, 407-254-7300.

2. Users shall be allowed access to resources of the agency computer network based upon their business needs. For access to restricted resources of the network the unit supervisor shall request access by supplying the IT Security Manager with the user's name the business need for access and the proper access requested. Employees shall not attempt to gain access to unauthorized resources of the network. Employees shall not make unauthorized changes to the network permissions that would allow them or other users' access to unauthorized resources of the network. If an employee finds his or her user account has been given access to unauthorized resources of the network, the employee shall notify the agency IT Security Manager at once. It will be the responsibility of the unit supervisor to notify the Service Desk when an employee status change results in that employee's network permission's changing. The Service Desk shall then open a work order assigning it to the IT Security Manager with the permissions information included.

3. To access the agency network via a remote connection the employee shall make the request, via their immediate supervisor, to the IT Security Manager detailing the reasons the remote access is required. Upon approval by the IT Security Manager, remote access will only be allowed through agency owned devices. No remote access from personally owned devices will be allowed. The employee shall be required to sign the remote user agreement prior to a

remote access account being established. No users shall access the agency network from outside the United States unless it is for agency business and the access is approved by the IT Security Manager or designee.

The use of remote access by IT personnel and designated vendors is for the support and maintenance of agency information systems.

Automated mechanisms will be employed to facilitate the monitoring and control of remote access methods. All remote accesses will be controlled through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but will document the rationale for such access in the security plan for the information system.

a. Personally owned information systems are not authorized to access, process, store or transmit CJI. This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).
b. Publicly accessible computers will not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

4. IT shall redirect the user's "My Document" folder to a network share and implement file synchronization to provide a secure redundant storage location for user files.

5. Access to secured systems must be requested through the user's supervisor to IT.

6. Employees shall log off or lock the operating system of any computer that contains or has access to the agency computer network, mail system, files or software whenever they are no longer in physical control of the computer.

7. Multiple concurrent active sessions for one user identification are not permitted, unless the agency grants authority based upon operational business needs. Request for this access must be submitted through the chain of command to the IT Security Manager or designee. IT personnel are permitted multiple logon sessions, utilizing their unique credentials, for support and maintenance tasks.

D. Software Security

1. Copyrighted software purchased by the agency is considered confidential in nature and will not be reproduced or released to persons or groups not employed by the agency for any reason. Software and programs developed by the agency will be subject to the rules and regulations contained in Public Access Laws.

2. Federal law allows copyrighted software to be copied for backup purposes. The making of unauthorized copies of software products is prohibited.

3. IT shall retain and file all software media and licensing for such software. All software retained by the agency will be stored in a secure area with IT and only those individuals authorized shall have access to such software.

4. The agency reserves the right to access any information contained in agency owned software or devices and may require personnel to provide passwords to files that have been encrypted or password protected.

5. Only legally obtained and licensed software, with proof of licensing for each instance of use, will be installed on agency owned computer hardware. IT personnel shall not install, support or maintain any other software. The IT Security Manager shall notify the involved person's Division Commander via chain of command, reporting all instances of:
   a. Installation of unlicensed or unauthorized software on agency owned equipment.
   b. Security incidents on agency owned equipment including but not limited to, serious virus infections, sensitive information released to unauthorized person(s), password compromise, etc.
   c. Any alterations to agency owned hardware and software without the consent of IT.

E. Data Security
   1. Backups
      a. Files stored on local hard drives will not be backed up and are the responsibility of the individual unit as to the safety and integrity of such data.
      b. Backup schedules will be determined and implemented by IT.
      c. It will be the responsibility of IT to provide back up services to the Communications Center and Central Operations.
      d. Backup media will be stored in a secure area. If required back up data may be sent off site to a secure location.

   2. Sensitive or Confidential Data
      Sensitive or confidential data will be protected by storage on removable media and locked in a designated physically secure location. It will be the responsibility of each unit and IT to determine what constitutes sensitive or confidential data as well as provide storage for such data. Electronic media containing CJI or PII will be encrypted before it is moved outside of a secure location.

   3. Electronic Media Sanitization and Disposal
      The agency will sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media will be destroyed in a manner that prevents the data from being read. The IT Security team shall maintain written documentation of the process used to sanitize or destroy electronic

media. The agency will confirm the sanitization or destruction is witnessed or carried out by authorized personnel. Outside organizations assisting or contracted to carry out the sanitization and disposal process will be required to complete CJIS security training, security addendums and proper background checks consistent with the current CSP.

4. Unauthorized Access by Individuals
   a. Unauthorized individuals shall be denied access to any computer system, system password, individual's password, or system procedures that will allow the changing of access or system passwords. IT shall conduct regular audits of the access log files to identify access violations.
   b. A text-based computer use policy will be displayed on each computer within the agency at boot up. By accepting the terms of the policy all personnel are responsible for adhering to the stated terms.

5. Passwords
   a. Passwords will be known only to the assigned person and will not be shared.
   b. Passwords should be memorized.
   c. Passwords will not be stored in data files, printed on reports, taped to work stations, or under keyboards, or programmed on function keys.
   d. A password will be created or changed with a minimum of eight (8) characters. The password will consist of upper and lower case alpha characters and numeric characters, no part of the user's name will be used in the password. The password should not be a dictionary word or proper name.
   e. Passwords should be sufficiently difficult to prevent unauthorized users from guessing the correct password. The names of children, pets, spouses, favorite teams, favorite bands, telephone number(s), anniversary dates, birth dates, etc. should not be used.
   f. Passwords and Usernames will not be the same.
   g. Passwords will be changed periodically or immediately if a security breach should arise. Passwords will be changed when a supervisor requests, in writing, the removal of a subordinate's password.
   h. Compromised passwords will be changed immediately by contacting the IT Service Desk.
   i. IT shall implement password complexity to confirm password requirements are met.
   j. Passwords will be set to expire within a maximum of 90 calendar days.
   k. Passwords will not be identical to any of the previous 10 passwords.
   l. Passwords will not be transmitted in the clear (e.g. using unencrypted communications through http instead of encrypted communications through https) outside of a designated secure location.
   m. Systems will be configured to confirm passwords are not displayed when entered.

6. Advanced Authentication

Advanced Authentication (AA) will be used with any computer used or located outside of a designated physically secure location. Methods of AA will be determined and configured by IT.

7. Encryption
   a. Encryption will be a minimum of 128 bit.
   b. When CJI is transmitted outside the boundary of a physically secure location, the data will be immediately protected via cryptographic mechanisms (encryption).
   c. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data will be protected via cryptographic mechanisms (encryption).
   d. When encryption is employed, the cryptographic module used will be certified to meet FIPS 140-2 standards.
   e. For use of a public key infrastructure technology, the agency will develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate will:
      1) Include authorization by a supervisor or a responsible official.
      2) Be accomplished by a secure process that verifies the identity of the certificate holder.
      3) Confirm the certificate is issued to the intended party.

8. Email
   Agency email is by default unencrypted. Agency email will not be used to transmit either CJI or PII.

9. Voice over Internet Protocol
   Usage of Voice over Internet Protocol (VoIP) technologies on agency networks requires approval by IT. Passwords on VoIP devices will be changed from the default password. Virtual Local Area Network (VLAN) technology will be used to segment VoIP traffic from data traffic.

10. Wi-Fi
    a. The agency provides an internal and guest wireless Wi-Fi network. Guest wireless access is for the use of OCSO guests. Internal wireless is for use of agency devices only. The two networks will be segmented from each other.
    b. Agency Wi-Fi will use Cryptographic algorithms meeting the requirements for FIPS 140-2. Encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
    c. Annual validation testing will be conducted to verify rogue Access Points do not exist in the Wireless Local Area Network.
    d. A complete inventory of all Access Points will be maintained.
    e. Access Points will be placed in secured areas to prevent unauthorized physical access and user manipulation.
    f. Access Point range boundaries will be tested to determine the extent of the wireless coverage. Access Point wireless coverage will be limited to the coverage area to only what is needed for operational

purposes.

g. User authentication and encryption mechanisms will be enabled for the management interface of Access Points.

h. All Access Points will have strong administrative passwords and confirm that all passwords have been changed from the manufacturers default password.

j. The reset function on Access Point will be used only when needed and is only invoked by authorized personnel. The device will be reconfigured to proper security settings before returning the device to production.

j. The internal Wi-Fi default service set identifier (SSID) will be set in a manner to disable its broadcast and such that the network is not identified as belonging to the agency.

k. Ad hoc mode will be disabled.

l. All nonessential management protocols will be disabled on the Access Points.

m. Logging will be enabled on wireless systems.

n. Logs will be reviewed monthly.

11. Bluetooth

Use of Bluetooth on agency systems with access to CJI must be approved by the IT Security Manager or designee before use.

F. Termination/Disabling of User Accounts

1. When an employee, volunteer or intern separates from the agency, Human Resources shall confirm that IT is informed. Once IT personnel have been notified, the user account of the individual in question will be immediately disabled.

2. The employee's immediate supervisor shall be provided "read" access to the contents of the employee's network user folder.

3. The immediate supervisor shall review the files in the user's folders and shall be responsible for the proper disposal or retention of those files.

4. Thirty days after the employee's termination, the IT Security Manager may delete the users account and the user folder.

5. In the event an employee is relieved of duty or suspended, the employee's immediate supervisor shall notify the IT Security Manager. The IT Security Manager and employee's manager shall determine the appropriate access levels to network resources.

6. An employee's chain of command, or Professional Standards, may cause a user's account to be temporarily disabled by request. Such request should be directed to the IT Security Manager. The user account will remain disabled until the requesting authority advises the account may be reactivated.

7. Agency domain user accounts will be reviewed on an annual basis. Unauthorized user accounts identified will be disabled.

G. Computer Viruses

1. Virus detection software is required for all computers within the Orange County Sheriff's Office, networked or stand-alone.

2. All computers attached to the Sheriff's Office networks must have virus detection software installed by IT.

3. IT shall update virus software as required to confirm protection against new threats.

4. If a virus is detected, the individual must immediately do the following:
   a. Stop all work on the affected workstation.
   b. Do not power off or reboot the affected workstation.
   c. Carefully write down the complete error message, if any.
   d. Notify his/her supervisor immediately.
   e. Notify the IT Service Desk at 407-254-7300.
   f. IT shall assist in the removal of the virus, if possible, or reloading of software if necessary.

5. To confirm that the latest up-to-date malware signature is available, all Laptops must be connected to the agency network and logged on once every 30 days. IT shall disable the user accounts of any laptop user who does not keep the anti-virus (malware) signature file up to date.

H. Tampering and Repair of Computers

1. Only IT employees or agency personnel authorized by IT are allowed to:
   a. Install or remove any hardware or software.
   b. Make any connections to the network.
   c. Install any printers and associated hardware or software.
   d. Make any changes to computers either internally or externally.
   e. Make any type of cable attachments.
   f. Perform any type of maintenance or repair (this does not include changing toner cartridges, ink cartridges, or ribbon for printers).

2. Outside agencies may not perform any type of action to any computer unless specifically authorized by the agency.

I. Lost or Stolen Information Technology Equipment

1. In the occurrence of lost or stolen agency devices, the employee assigned the device(s) or their supervisor shall immediately notify the IT Service Desk at 407-254-7300 or the on-call IT representative if the IT Service Desk is closed.

2. The IT Service Desk or on call representative shall reset the users Active Directory account password in an effort to prevent unauthorized access from the lost or stolen device(s).

3. In the occurrence of a lost or stolen mobile aircard, IT Service Desk shall contact the service provider and have the device disabled.

4. In the occurrence of a lost or stolen agency phone, the phone will be remotely wiped through the use of the agency's Mobile Device Management system.

J. Patch Management

Scheduled monthly patch management will occur in an effort to mitigate vulnerabilities on computer systems and electronic devices. IT Change Management entries will be created, reviewed and approved before patching occurs.

K. Security Alerts and Advisories

The agency will subscribe to and review information system security alerts/advisories on a regular basis. Whenever possible automated mechanisms will be used for notification. If relevant alerts/advisories are identified they will be communicated to appropriate personnel. Actions taken to mitigate vulnerabilities will be documented and approved through the IT Change Management process.

L. Incident Response

1. In the occurrence of an Information Security event effecting multiple agency systems, the unauthorized extraction of agency data or the inaccessibility of agency systems IT shall follow a formalized incident response process. IT shall establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities.

2. If an employee suspects an information security incident occurred, the employee shall contact the IT service desk at 407-254-7300. In the case of sensitive events the reporting employee may ask that a member of the Security Team contact them directly.

3. IT shall track, document, and report incidents to appropriate agency officials and/or authorities.

4. In the situation where CJI systems or data are effected the FDLE CJIS Information Security Officer shall be notified via the FDLE designated process.

5. The agency will confirm general incident response roles and responsibilities are identified.

6. Information security event incident response will be conducted.

7. The agency will track and document security incidents on an ongoing basis.

M. CJIS Security Policy

FBI CSP is the minimum standard for information security on systems, personnel and infrastructure capable of accessing CJI. Agency policy may augment, or increase the standards, but will not detract from the CSP standards.

N. Personally Identifiable Information

Any FBI CJIS provided data maintained by the agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. PII will be extracted from CJI for the purpose of official business only. PII data will be handled with the same information security standards as CJI.