CHATHAM COUNTY POLICE DEPARTMENT
STANDARD OPERATING PROCEDURES

SOP# OPS-063: **EFFECTIVE DATE: 02/01/18**

SECURITY AND INTEGRITY CRIMINAL JUSTICE INFORMATION **REVISION: 02/09/22**

PURPOSE:

The purpose of this policy is to ensure the protection of Criminal Justice Information (CJI)/Criminal History Record Information (CHRI). There has been an increase in the number of accidental or malicious computer attacks against government and private agencies, regardless of whether the systems are high or low profile. The following establishes an operational incident handling policy for the agency that includes adequate preparation, detection, analysis, containment, recovery, and user response activities. As well as tracking, documenting, and appropriate incident reporting. Improper handling or release of the information to a source not authorized to receive it can have dire consequences for the individual on whom the information is released and could result in fines and/or imprisonment of the person releasing the information upon prosecution and conviction.

All agency employees, non-paid employees, and vendors/contractors with access, to include physical and logical access, to GCIC/NCIC materials, records, and information are required to ensure proper preparation, detection, analysis, containment, recovery, user response, tracking, documenting, handling and incident reporting procedures are followed for all security incidents.

POLICY:

All criminal justice documents utilized by Chatham County Police Department personnel and the information contained therein shall be handled per Department policy and applicable State and Federal laws.

Criminal fingerprint-based identification background checks shall be conducted on all CCPD personnel, volunteers, vendors, if appropriate, and custodial staff prior to employment to ensure compliance with State and Federal laws, and Department Policy. Periodic electronic criminal and driver history record checks will be performed on all personnel throughout their employment with the CCPD in order to ensure continual compliance.

Criminal justice information shall be accessed by or released to only those directly involved in criminal investigations or those who need the information for other authorized criminal justice purposes.

A Dissemination Log of all secondary dissemination of Criminal History Record Information originating from the Chatham County Police Department shall be maintained for audit purposes.

Documents utilized by Department personnel include, but are not limited to, Applicant Fingerprint Cards; Criminal Fingerprint Cards; Incident Reports; Accident Reports; Criminal History Records; Offender Based Tracking System Forms; RAP Sheets, and IQ and FQ responses.

DEFINITIONS:

Criminal History Record Information (CHRI) – Information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, accusations, information or other formal criminal charges, and any dispositions arising therefrom, including sentences, correctional supervision, and releases.

Hot File Information – Those files maintained by the FBI Criminal Justice Information System to assist the criminal justice community in performing its duties by providing a computerized filing system of accurate and timely documents relating to the following files: Vehicles; License Plates; Boats, Guns; Articles; Securities; Wanted Persons; Foreign Fugitive; United States Secret Service; Missing Persons; Unidentified Persons; Violent Gang and Terrorist Organization; Deported Felon; Protective Orders; Convicted persons on supervised release; Vehicle and Boat Parts.

Georgia Crime Information Center (GCIC) – Is established for the state, within the Georgia Bureau of Investigations, a system for the intrastate communication of vital information relating to crimes, criminals, and criminal activity.

National Crime Information Center (NCIC) – A nationwide computerized index of documented criminal justice information concerning crimes and criminal of nationwide interest and a locator file for missing and unidentified persons which can be instantly retrieved by and/or furnished by any authorized agency.

Phoenix Jail Management System – A local Records Management System owned and maintained by the Chatham County Sheriff's Department.

Local Agency Security Officer (LASO) - The LASO is an individual appointed by the Agency Head to assume ultimate responsibility for managing the security of CJIS systems within the agency.

Information Security Officer – (ISO) – an individual appointed by GCIC and serves as the security point of contact to the FBI CJIS Division ISO and is responsible for establishing and maintaining information security policies, assessing threats and vulnerabilities, performing risk and control assessments, and oversees the governance of security operations.

Physically Secure Location - A facility, a police vehicle, 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 associate information systems.

COMPUTER LAWS:

The Georgia Computer Systems Protection Act (O.C.G.A. §16-9-90 ET. Seq.) protects public and private sector computer systems, including communications links to such computer systems. The Act establishes four criminal offenses, all major felonies for violation of the Act. The Act also describes Computer Password Disclosure.

16-9-93(a)(3) Computer Theft – Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession; obtaining property by deceitful means or artful practice; or converting property to such person's use in violation of an agreement or other known legal obligation to make a specific application for disposition of such property shall be guilty of the crime of Computer Theft.

16-9-93(b)(1) Computer Trespass – Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer

program or data from a computer or computer network; obstructing, interrupting, or in any way interfering with the use of a computer program or data; or altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists shall be guilty of the crime of Computer Trespass.

16-9-93(c) Computer Invasion of Privacy – Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any person with knowledge that such examination is without authority shall be guilty of the crime of Computer Invasion of Privacy.

16-9-93(d) Computer Forgery – Any person who creates, alters, or deletes any data contained in any computer or computer network, who, if such person had created, altered, or deleted a tangible document or instrument would have committed forgery under Article 1 of this chapter, shall be guilty of the crime of Computer Forgery.

16-9-93(e) Computer Password Disclosure – Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer network in excess of $500.00 shall be guilty of Computer Password Disclosure. Violation of Computer Laws could result in Departmental sanctions, imprisonment, and fines as outlined in Georgia Law.

PROCEDURE

I. <u>RULES AND REGULATIONS</u>:

A. Agency employees, non-paid employees, and vendors/contractors with access, to include physical and logical access, to GCIC materials, records, and information are required to follow the policies, rules, and procedures set forth by GCIC, NCIC, FBI CJIS Security Policy, and the laws of the State of Georgia. Authorized personnel of the agency shall protect and control electronic and physical CJI/CHRI while at rest and in transit. The agency will take appropriate safeguards for protecting CJI/CHRI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate disclosure and/or must be reported to the Agency Head, LASO, and GCIC.

B. Personally owned information systems shall not be authorized to access, process, store, or transmit criminal justice information. All devices with access to CJI must be authorized and must meet the requirements set forth by the CJIS Security Policy.

C. <u>Security Incident Preparation, Prevention, and Handling</u>:

1. The Agency Head shall:

   (a) Ensure the perimeter of all physically secure locations are prominently posted and separated from non-secure locations by physical controls.

2. The agency's Terminal Agency Coordinator (TAC) or Point of Contact (POC) shall:

   (a) Ensure general incident response roles and responsibilities are included as part of required security awareness training.

   (b) Maintain personnel listings with authorized access to the physically secure location.

   (c) Control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

3. The agency's LASO shall:

   (a) Maintain automated mechanisms to assist in the reporting of security incidents. The agency currently employs:

      (1) Cisco Secure Endpoint software that provides comprehensive computer protection against known and new threats, network and phishing attacks, and other unwanted content. Each type of threat is handled by a dedicated configured.

      (2) Windows Security anti-virus and internet security software that prevents, detects, and removes malicious software.

   (b) Ensure proper tracking and documentation of information system security incidents on an ongoing basis.

   (c) Identify who is using approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.

   (d) Identify and document how the equipment is connected to the state system.

   (e) Ensure that personnel security screening procedures are being followed as stated in this Policy. Ensure the approved and appropriate security measures are in place and working as expected.

   (f) Ensure advanced authentication, encryption, security-related updates, official use guidance, data at rest encryption.

   (g) Be able to easily identify connected users and devices of all departmentally approved devices with access to CJI.

   (h) Track, log and manage every personally used device allowed to connect to agency technology resources for secure CJI access.

   (i) Identify individuals who are responsible for reporting incidents within their area of responsibility.

   (j) Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.

   (k) Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.

   (l) Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement point of contact within their area.

   (m) Act as a single point of contact for their jurisdictional area for requesting incident response assistance.

   (n) Track and document information system security incidents on an ongoing basis.

   (o) Maintain completed security incident reporting forms until the subsequent GCIC triennial audit or until legal action (if warranted) is complete, whichever timeframe is greater.

4. All authorized personnel of the agency shall:

   (a) Monitor physical access to the information system to detect and respond to physical security incidents.

   (b) Control physical access by authenticating visitors before authorizing escorted access to the physically secure location.

   (c) Ensure all visitors to the physically secure location are escorted by authorized personnel and continuously monitored.

   (d) Authorize and control information system-related items entering and exiting the physically secure location.

   (e) Securely store electronic and physical media within physically secure locations or controlled areas. The CCPD shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible, then the data shall be encrypted.

   (f) Protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with the transportation of such media to authorized personnel.

   (g) Utilize local device authentication to unlock mobile devices authorized by the agency for use in accessing CJI.

   (h) Use caution when downloading internet content or clicking on web-based pop-ups/windows, unknown emails, embedded objects, and email attachments or utilizing removable devices such as flash drives, CDs, etc.

   (i) Be familiar with the agency's disciplinary policy.

D. Security Incident Reporting:

1. Any security incidents that may arise shall be reported immediately to the agency's LASO. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.

2. All employees, contractors, and third-party users shall be made aware of the procedures for reporting the different types of events and weaknesses that might impact the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the LASO.

3. Once notified, the agency's LASO will notify the Agency Head and GCIC. If deemed necessary, the agency's LASO will:

   (a) Notify GCIC to relay the preliminary details of the incident.

   (b) Investigate the reported incident and submit an incident response form to GCIC once all the information has been gathered.

   (c) Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence in accordance with the agency's standard operating procedure regarding evidence procedures.

E. Security Incident Reporting for Mobile Devices:

1. 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 specialized interface.

2. All agency employees with approved mobile device access to CJI shall be made aware of the procedures for reporting the different types of events and weaknesses that might impact the security of agency assets and are required to report any information security events and weaknesses. Once notified, the LASO will notify the Agency Head and GCIC.

F. If deemed necessary, the LASO will:

1. Notify GCIC to relay the preliminary details of the incident.

2. Investigate the reported incident and submit an incident response form to GCIC once all the information has been gathered.

3. Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence in accordance with the agency's standard operating procedures regarding evidence procedures.

4. Special reporting procedures for mobile devices shall apply in any of the following situations:

(a) Loss of device control - The device is in the physical control of a non-CJIS authorized individual. The device is left unattended in an unsecured location (e.g., counter of the coffee shop). Even if the device is recovered quickly, there is a significant risk that either the device settings could be tampered with or data on the device could be illicitly accessed.

(b) Total loss of device - The device's physical location is unknown. The device has been accidentally destroyed beyond the means of information retrieval (i.e., incinerated, shredded). The device has been dropped in an area that prevents retrieval, such as the ocean or a canyon.

(c) Device compromise - This includes rooting, jail breaking, or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions).

(d) In the event of a total loss of device, loss of control, or device compromise, the LASO will:

(1) Notify GCIC to relay the preliminary details of the incident.

(2) Enable mobile device locating features if the security of the device has not been compromised. (i.e., the device has been misplaced within the department or another secure location)

5. Contact the mobile device carrier and request assistance with device tracking. If tracking for the mobile device is unsuccessful, the agency LASO will:

(a) Secure, control, or remotely erase all data on any department-issued mobile device with CJI access as deemed necessary.

(b) Utilize remote features to "lock/kill" all device hardware.

(1) Once the "lock/kill" feature has been activated, the LASO will contact the device carrier to ensure the mobile device has been successfully "locked/killed."

(2) If the remote "lock/kill" feature is unavailable, a request to disable the mobile device via the network will be made to the device carrier.

6. Notify GCIC of loss and request assigned ORI to be deactivated.

7. Complete the reported incident investigation and submit an incident response form to GCIC once all the information has been gathered.

8. Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence in accordance with the agency's standard operating procedure regarding evidence procedures.

G. All security incidents and/or GCIC violations will be reported in writing to the GCIC Division Director by the agency head, in accordance with GCIC policies and procedures.

H. Sanctions

1. Violation of any of the requirements in this policy by any authorized personnel may result in criminal prosecution by the State of Georgia and/or administrative sanctions including, but not limited to, termination of employment with the agency.

II. CRIMINAL JUSTICE INFORMATION SYSTEMS

A. The use of this information for other than the administration of criminal justice is prohibited.

B. The CCPD will handle and disseminate secret information, sensitive information, criminal history information, and restricted information in compliance with Georgia Law, the Rules of Georgia Crime Information Center (GCIC) Council, and the Georgia Criminal Justice Information System (CJIS).

C. Only the following personnel are authorized to have access to GCIC secret information, sensitive information, criminal history information, or restricted information.

1. Sworn and non-sworn personnel who are trained and certified by the Terminal Agency Coordinator (TAC) to operate and receive information from GCIC computers.

2. Sworn and non-sworn personnel who are involved in the administration of criminal justice.

3. Each person authorized to access Departmental CJIS databases shall be issued a unique username and password for each database to which they will have access.

4. Use of a user's name and password by anyone other than the authorized user is prohibited and allowing another employee to access a CJIS database is strictly prohibited.

D. State and Federal laws and GCIC Council Rules govern the use of the GCIC system. Any secret information, criminal history information, or restricted information is a "Secret of State." Secrets of State shall be divulged only as permitted by Georgia Law.

1. **GCIC Council Rule 140-2-.02(2) Security Policy for Criminal Justice Information. Amended.** Any secret information, criminal history record information, or restricted information is a "Secret of State," which is required by State policy, the interest of the community, and the right of privacy of the citizens of this State to be confidential. Such

information shall not be divulged except as permitted by Georgia Law and these rules. Criminal Justice agencies must destroy documents containing secret information, CHRI or restricted information no longer required for operations in a manner precluding access to the information by unauthorized persons.

2. **GCIC Council Rule 140-2-.02(3) Security Policy for Criminal Justice Information. Amended.** Criminal justice agencies shall disseminate Criminal History Record Information to perform duties serving the administration of criminal justice or as otherwise provided by statute. Under no circumstances will Criminal History Record Information be transmitted via the CJIS network to devices not authorized to access such information, which may exist in the GCIC computerized files, FBI Interstate Identification Index (III).
3. Criminal justice information shall never be handled in an illegal manner. Any employee found in violation of GCIC Council Rules or Department Policy regarding the handling of CJIS data shall be subject to disciplinary actions and/or criminal sanctions.
4. All violations of GCIC policy will be referred to the Local Agency Security Officer.
5. **GCIC Council Rule 140-2-.04(F) Criminal Justice Information Exchange and Dissemination.** The commercial dissemination of State or Federal Hot File records obtained from NCIC (CJIS Systems) is prohibited. Information derived for other than law enforcement purposes from national hot file records can be used by authorized criminal justice personnel only to confirm the status of a person or article, i.e., wanted or stolen. Any advertising of services providing "data for dollars" is prohibited.
6. **CIC Council Rule 140-2-.04(F) Criminal Justice Information Exchange and Dissemination.** The commercial dissemination of State or Federal Hot File records obtained from NCIC (CJIS Systems) is prohibited. Information derived for other than law enforcement purposes from national hot file records can be used by authorized criminal justice personnel only to confirm the status of a person or article, i.e., wanted or stolen. Any advertising of services providing "data for dollars" is prohibited.
7. **GCIC Council Rule 140-2-08(1) Physical Security Standards. Amended.** Criminal justice agencies, governmental dispatch centers, and other governmental agencies approved by the Director for direct CJIS network access shall provide secure areas out of public view in which criminal justice information is handled.
8. **GCIC Council Rule 140-2-08(2) Physical Security Standards. Amended.** Such agencies shall place CJIS network devices in secure areas with adequate physical security to protect at all times against any unauthorized viewing or access to computer terminals, access devices, or stored printed data. This includes locations or vehicles housing Mobile Data Terminals (MDTs) or personal/laptop computers capable of accessing criminal justice information.
9. **GCIC Council Rule 140-2-.09 Personnel Security Standards. (1)** Criminal justice agency employees and other personnel, as identified by the GCIC Director, who handles criminal justice information shall consent to an investigation of their moral character, reputation, and honesty.
10. **GCIC Council Rule 140-2-.09 Personnel Security Standards.(1)** All applicants, including appropriate information technology (IT) personnel having access to CJIS systems information, shall submit to a state and national fingerprint-based identification

check to be conducted within 30 days upon employment, assignment, or subsequent re-employment.

11. **GCIC Council Rule 140-2-.09(4) Personnel Security Standards.** All personnel directly associated with the maintenance, processing, or dissemination of Criminal History Record Information shall be specially trained.
12. **GCIC Council Rule 140-2-09(7) Personnel Security Standards.** All personnel whose jobs require them to access or process criminal justice information shall sign Awareness Statements.

E. All vendor representatives shall watch the CJIS Security Awareness Video and sign the appropriate security addendums. The security addendums will remain in the Police Department's files for audit purposes.

III. DESTRUCTION OF CRIMINAL JUSTICE INFORMATION DOCUMENTS:

A. When documents containing secret information, Criminal History Record Information, sensitive information, or restricted information are no longer required for criminal justice operations, such documents shall be destroyed by shredding.

B. Shred bins have been placed throughout the department by a department-approved vendor. The company is contracted by the department to dispose of media containing criminal justice

C. The vendor will make periodic pickups at each site where shred bins are located.

D. The vendor representative will be accompanied by an authorized department employee at all times during the removal, shredding of documents, and return of bins to the designated sites.

IV. DESTRUCTION OF HARDWARE/SOFTWARE HANDLED BY THE CHATHAM COUNTY ICS DEPARTMENT

A. A vendor approved by the Chatham County ICS Department will handle the destruction of all CCPD media handled by the ICS Department personnel,

1. The vendor will make period pickups at each site where the destruction of media is requested.
2. The vendor representative will be accompanied by an authorized department employee at all times during the removal, shredding of documents, and return of shred bins, if applicable, to the designated sites.
3. All vendor representatives shall watch the CJIS Security Awareness Video and sign the appropriate security addendums. The security addendums will remain in the Police Department's files for audit purposes.

BY ORDER OF:

Electronically Signed on PowerDMS on 02/09/2022

Jeffrey M. Hadley
Chief of Police