DUBLIN POLICE DEPARTMENT

**STANDARD OPERATING PROCEDURE**

**SECTION: C-004 GCIC Security Incident Reporting/**

 **Handling Policy**

**EFFECTIVE DATE: 16 NOV 2016 NUMBER OF PAGES: 6**

**REVISED DATE: 16 NOV 2016 DISTRIBUTION AUTHORIZATION:**

#### STANDARD COVERED *CHIEF KEITH MOON*

**N/A**

**Subject:**

Security Incident Reporting/Handling Policy for information derived from the Georgia Crime Information Center (GCIC) Criminal Justice Information (CJIS) Network

**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 both 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.

All agency employees, non-paid employees, and vendors/contractors with access include

Physical and logical access, to GCIC/NCIC materials, records, and information is required to ensure proper preparation, detection, analysis, containment, recovery, user response, tracking, documenting, handling, and incident reporting procedures are followed for all security incidents.

**Definitions**:

**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, assesses threats and vulnerabilities, performs 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.

**Rules and Regulations:**

Agency employees, non-paid employees, and vendors/contractors with access, including 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.

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.

**Security Incident Preparation, Prevention and Handling**:

**The Agency Head shall:**

Ensure the perimeter of all physically secure locations is prominently posted and separated from non-secure locations by physical controls.

**The agency’s Terminal Agency Coordinator (TAC) shall:**

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

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

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.

**The agency’s LASO shall:**

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

(Name of Software) 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 component. Components can be enabled or disabled independently of one another, and their settings can be configured.

(Name of Anti-Virus) anti-virus and internet security software that prevents, detects, and removes malicious software.

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

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

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

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.

Ensure advanced authentication, encryption, security-related updates, official use guidance, data at rest encryption, and prevention of data compromise are utilized for all departmental-approved mobile devices with access to CJI.

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

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

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

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

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

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.

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

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

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

**All authorized personnel of the agency shall:**

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

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

Ensure all visitors to the physically secure location are escorted by authorized personnel and monitored at all times.

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

Securely store electronic and physical media within physically secure locations or controlled areas. The agency 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.

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

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

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.

Be familiar with the agency’s disciplinary policy.

**Security Incident Reporting:**

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 that allows timely corrective action to be taken.

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 have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the LASO.

Once notified the agency’s LASO will notify the Agency Head and GCIC.

If deemed necessary the agency’s LASO will:

Notify GCIC to relay the preliminary details of the incident.

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

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 agency’s standard operating procedure regarding evidence procedures.

**Security Incident Reporting for Mobile Devices:**

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.

All employees of the agency 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 have an impact on 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.

If deemed necessary the LASO will:

Notify GCIC to relay the preliminary details of the incident.

Investigate the reported incident and submit an incident response form to GCIC once all the

Information has been gathered.

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.

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

**Loss of device control** - The device is in the physical control of a non-CJIS authorized individual or the device is left unattended in an unsecured location (e.g., the 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.

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

**Device compromise** -This includes rooting, jailbreaking 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).

In the event of a total loss of the device, loss of control, or device compromise, the ASO will:

Notify GCIC to relay the preliminary details of the incident.

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)

Contact the mobile device carrier and request assistance with device tracking.

If tracking for the mobile device is unsuccessful the agency ASO will:

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

Utilize remote features to “lock/kill” all device hardware.

Once the “lock/kill” feature has been activated, the ASO will contact the device carrier to ensure the mobile device has been successfully “locked/killed”.

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.

Notify GCIC of the loss and request the assigned ORI be deactivated.

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

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.

All security incidents and/or GCIC violations will be reported in writing to the GCIC Deputy Director by the Agency Head, in accordance with GCIC policies and procedures.

**Sanctions:**

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.