CJIS METERS/NCIC Media Protection

Index Code: **1107**
Effective Date: **07/01/14 (Revised 9/6/2022)**

I. Purpose

The purpose of this directive is to ensure the protection of the Criminal Justice Information Services (CJIS) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

This directive was developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy 5.2 dated 7/01/2014. The Queen Anne's County Office of the Sheriff (QASO) may complement this policy with a local directive/policy; however, the CJIS Security Policy shall always be the minimum standard. The local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

II. Policy

It is the policy of the Queen Anne's County Office of the Sheriff to ensure that appropriate controls are in place to protect electronic and physical media containing Criminal Justice Information (CJI) while at rest, stored or actively being accessed. All controls will be in conformance with applicable policies developed by the FBI's Criminal Justice Information Services and the QASO to ensure best practices and minimum standards are applied. This directive applies to all employees of the Office of the Sheriff.

III. Media Storage and Access

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. "Electronic Media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical Media" includes printed documents and imagery that contain CJI. To protect CJI, the Queen Anne's County Office of the Sheriff personnel shall:

A. Securely store electronic and physical media within a physically secure or controlled area. A secured are includes a locked drawer, cabinet, or room.

B. Restrict access to electronic and physical media to authorized individuals.

C. Ensure that only authorized users remove printed form or digital media from the CJI.

D. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures.

E. Not use personally owned information systems to access, process, store or transmit CJI unless the QASO has established and documented the specific terms and conditions for personally owned information system usage.

F. Not utilize publicly accessible computers 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.

G. Store all hardcopy CJI printouts maintained by the QASO in a secure area accessible to only those employees whose job functions require them to handle such documents.

H. Safeguard all CJI maintained by the QASO against possible misuse.

I. Take appropriate action when in possession of CJI while not in a secure area.

J. CJI must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.

K. Precautions must be taken to obscure CJI from public view such as by means of an

opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and/or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.

L. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secured location, the data shall be protected using encryption. Storage devices include external hard drives from computer, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.

M. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

N. Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have the same CJI access permissions and users need to keep CJI protected on a need-to-know basis.

O. Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of CJI.

IV. Media Transport

A. Controls shall be in place to protect electronic and physical media containing CJI while in transport to prevent inadvertent or inappropriate disclosure and use.

1. Dissemination to another agency is authorized if the other agency is an Authorized Recipient of such equipment or media and is being serviced by the accessing agency or the other agency is performing personnel and appointment functions for criminal justice employment applicants.

2. The Queen Anne's County Office of the Sheriff personnel shall protect and control electronic and physical media during transport outside of controlled areas AND shall restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

3. The QAC Office of the Sheriff shall control, protect and secure electronic and physical media during transport from public disclosure by:

a. Use of Privacy Statements in electronic and paper documents

b. Limiting the collection, disclosure, sharing and use of CJI

c. Following the most secure privilege and role-based rules for allowing access.

d. Securing hand-carried confidential electronic and paper documents by storing CJI in a locked briefcase or lockbox. Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.

e. For hard copy printouts or CJI documents, package them in such a way as to not have any CJI information viewable and, those that are mailed, DO NOT MARK THE PACKAGE TO BE MAILED "CONFIDENTIAL". Provide complete shipping tracking, history and signature confirmation of delivery.

f. Not taking CJI home or when traveling unless authorized by the QAC Office of the Sheriff Local Agency Security Officer (LASO). When disposing confidential documents, use a shredder.

V. Electronic Media Sanitization and Disposal

The affected agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to dispose or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The affected agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media, and ensure the sanitization or destruction is witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures. For end of life media policy, refer to the DES Sanitation Destruction Policy.

IV.Breach Notification and Incident Reporting

The affected agency shall report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including, but not limited to, audit-monitoring, network monitoring, physical access monitoring and user/administrator reports.

V. Roles and Responsibilities

If CJI is improperly disclosed, lost or reported as not received, the following procedures will be immediately followed:

A. Queen Anne's County Office of the Sheriff personnel shall notify their supervisor or LASO, and an incident report will be completed and submitted within twenty-four hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident and steps taken/to be taken in response to the incident.

B. The supervisor of the affected employee will communicate the situation to the LASO, notifying them of the loss or disclosure of CJI records.

C. The LASO will ensure ISO (CJIS System Agency Information Security Officer) is promptly informed of security incident.

D. The CSA ISO will:

1. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI. 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 POCs within their area.

2. Act as a single POC for their jurisdictional area for requesting incident response assistance.

VI. Penalties

Violation of any of the requirements in this directive by any authorized personnel will result in suitable action, up to and including loss of access privileges, civil and /or criminal prosecution, and/or termination.

VII. CALEA References: None

VIII. Proponent Unit: Administrative Services

IX. Cancelation: Written Directive dated 6/23/2017

Sheriff Gary Hofmann