MYRTLE BEACH POLICE DEPARTMENT

ADMINISTRATIVE REGULATIONS AND OPERATING PROCEDURES

Subject: Media Protection	***Number: 129-B***
Effective Date: January 10, 2019	***Revised Date: September 18, 2026***
Rescinds: 129 – Media Protection Policy ***129-A Media Protection Policy***	***Dated: 01-10-2019*** ***10-26-2023***

Approved By:

I. PURPOSE

The intent of the Media Protection Policy is to ensure the protection of the Criminal Justice Information (CJI) 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 report data), or is purged or destroyed in accordance with applicable record retention rules.

II. POLICY

1. The scope of this policy applies to any electronic or physical media containing FBI Criminal Justice Information (CJI) while being stored, accessed, or physically moved from a secure location of the Myrtle Beach Police Department. This policy applies to any authorized person who accesses, stores, and/or transports electronic or physical media. Transporting CJI outside the agency's assigned physically secure area must be monitored and controlled.

2. Authorized Myrtle Beach Police Department personnel shall protect and control electronic and physical CJI while at rest and in transit. The Myrtle Beach Police Department will take appropriate safeguards for protecting and to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate disclosure and/or use will be reported to the Myrtle Beach Police Department Local Agency Security Officer (LASO). Procedures shall be defined for securely handling, transporting, and storing media.

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

III. PROCEDURE

A. Media Storage and Access

1. 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.

2. To protect CJI, the Myrtle Beach Police Department personnel shall:

    a. Ensure system media is properly marked to include the distribution limitations, the handling caveats, and the applicable security markings required for said information.

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

    c. Restrict access to digital and non-digital media to authorized individuals.

        i. Digital media examples include flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid-state, magnetic), compact discs, and digital versatile discs.

        ii. Non-digital examples include paper and microfilm.

    d. Ensure that only authorized users remove printed forms or digital media from the CJI.

    e. Physically protect CJI until media end of life. End-of-life CJI is destroyed or sanitized using approved

equipment, techniques, and procedures. (See MBPD 130 Disposal of Media)

f. Not use personally owned information systems to access, process, store, or transmit CJI. There are no exceptions. (See Personally Owned Device Policy)

g. 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.

h. Store all hardcopy CJI printouts maintained by the Myrtle Beach Police Department in a secure area accessible to only those employees whose job function requires them to handle such documents.

i. Safeguard all CJI by the Myrtle Beach Police Department against possible misuse by complying with the Physical Protection Policy, Personally Owned Device Policy, and the enforcement provisions in the Policy Section of this procedure.

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

    i. Ensure that the media containing CJI is marked to include the distribution limitations, the handling caveats, and the proper security markings for the information.

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

    iii. 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.10. When CJI is at rest (i.e. stored electronically) outside the boundary of

the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, backup tapes, mobile devices, laptops, etc.

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

l. 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 need to keep CJI protected on a need-to-know basis.

m. Establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of CJI. (See Physical Protection Policy)

B. Media Transport and Marking

1. Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. "Electronic media" means electronic storage media including 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.

2. The Department shall:

a. Protect and control media during transport outside of controlled areas.

b. Maintain accountability for information system media during transport outside of controlled areas.

c. Document activities associated with the transport of information system media.

d. Restrict the activities associated with the transport of information system media to authorized personnel.

C. Media Use – The Department shall:

1. Restrict the use of digital and non-digital media on agency-owned systems that have been approved for use in the storage, processing, or transmission of criminal justice information (CJI) by using technical, physical, or administrative controls (examples below); and

2. Prohibit the use of personally owned digital media devices on all agency-owned or controlled systems that store, process, or transmit CJI; and

3. Prohibit the use of digital media devices on all agency-owned or controlled systems that store, process, or transmit CJI when such devices have no identifiable owner.

4. Examples of technical controls: port disabling, access control lists (ACL), security groups, group policy objects (GPO), mobile device management (MDM).

5. Examples of physical controls: locked server cage, disconnect the CD-ROM drive in the PC, remove the USB port.

6. Example of administrative controls: the agency's electronic media policy defining how flash drives are to be used within the agency rules of behavior

D. Dissemination to Another Agency is Authorized if:

1. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or

2. The other agency is performing personnel and appointment functions for criminal justice employment applicants.

E. The Myrtle Beach Police Department personnel shall:

1. Protect and control electronic and physical media during transport outside of controlled areas.

2. Restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel.

3. Not store, download, or transport CJIS data on personally owned devices or media.

F. The Myrtle Beach Police Department personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents.

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

3. Following the least privilege and role-based rules for allowing access. Limit access to CJI to only those people or roles that require access.

4. Securing hand-carried confidential electronic and paper documents by:

    a. Storing CJI in a locked briefcase or lockbox.

    b. Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.

5. For hard copy printouts or CJI documents:

    a. Package hard copy printouts in such a way as to not have any CJI information viewable.

6. For packages that are mailed or shipped, the agency must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.

7. Not taking it home or when traveling unless authorized by the Myrtle Beach Police Department LASO. When disposing of confidential documents, use a shredder.

G. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and exempt digital and non-digital media containing CJI from marking if the media remains within physically secure locations or controlled areas.

H. Electronic Media Sanitization and Disposal:

The agency shall 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 shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall 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. See MBPD 130 (Disposal of Media) for approved disposal and destruction methods as well as the department responsible for each. The documentation and witnessing requirements apply.

I. Breach Notification and Incident Reporting:

The agency shall promptly 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.

J. Roles and Responsibilities:

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

1. Myrtle Beach Police Department personnel shall notify his/her supervisor or LASO, and an incident-report form must be completed and submitted within 24 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.

2. The supervisor will communicate the situation to the LASO to notify of the loss or disclosure of records.

3. The LASO will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of security incidents.

4. The CSA ISO will:

    a. 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 CJI Division ISO major incidents that significantly endanger the security or integrity of CJI.

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

K. LASO Responsibilities:

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

2. Ensure policies and procedures are reviewed and updated annually for compliance or in the event of a security incident involving digital and/or non-digital media.

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

M. LASO Name: Cathie Rhodes Phone: 843.918.1341

IV. REVIEW

The LASO shall review this procedure annually. The Chief of Police will approve any modifications or affirm the procedure as written by affixing their signature.