MYRTLE BEACH POLICE DEPARTMENT

ADMINISTRATIVE REGULATIONS AND OPERATING PROCEDURES

Subject: Physical Protection of CJI	***Number: 128-A***
Effective Date: January 10, 2019	***Revised Date: October 16, 2026***
Rescinds: 128 – Physical Protection Policy	***Dated: 01-10-2019***

Approved By:

I. PURPOSE

The purpose of this policy is to provide guidance for agency personnel, support personnel, and private contractors/vendors for the physical, logical, and electronic protection of Criminal Justice Information (CJI). All physical, logical, and electronic access must be properly documented, authorized, and controlled on devices that store, process, or transmit unencrypted CJI. This Physical Protection Policy focuses on the appropriate access control methods needed to protect the full lifecycle of CJI from insider and outsider threats.

II. PROCEDURE

A. Physically Secure Location

A physically secure location is 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 the FBI CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted non-public areas in the Myrtle Beach Police Department shall be identified with a sign at the entrance.

B. Visitors' Access

1. A visitor is defined as a person who visits the Myrtle Beach Police Department facility temporarily who is not employed by

the Myrtle Beach Police Department and has no unescorted access to the physically secure location within the Myrtle Beach Police Department where FBI CJI and associated information systems are located. For agencies with jails with CJI terminals, additional visit specifications need to be established per agency purview and approval.

2. Visitors shall:

    a. Check in before entering a physically secure location by:

        i. Completing the visitor access log, which includes: name and visitor's agency, purpose for the visit, date of visit, time of arrival and departure, name and agency of person visited, and form of identification used to authenticate visitor.

        ii. Document badge number on visitor log if visitor badge issued. If Myrtle Beach Police Department issues visitor badges, the visitor badge shall be worn on the visitor's outer clothing and collected by the agency at the end of the visit.

        iii. Planning to check in or sign in multiple times if visiting multiple physically secured locations and/or building facilities that are not adjacent or bordering each other and each has its own individual perimeter security to protect CJI.

        iv. The log shall be kept for a minimum of one year, and the LASO shall review it quarterly for anomalies.

    b. Be accompanied by a Myrtle Beach Police Department escort at all times, including delivery or service personnel. An escort is defined as an authorized person who accompanies a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

    c. Show Department personnel a valid form of photo identification.

d. Follow Myrtle Beach Police Department policy for authorized unescorted access.

   i. A Noncriminal Justice Agency (NCJA), such as city or county IT, that requires frequent unescorted access to restricted area(s) will be required to establish a Management Control Agreement between the Myrtle Beach Police Department and the NCJA. Each NCJA employee with CJI access will appropriately have a state and national fingerprint-based record background check before this restricted area access is granted.

   ii. Private contractors/vendors who require frequent unescorted access to restricted area(s) will be required to establish a Security Addendum between the Myrtle Beach Police Department and each private contractor personnel. Each private contractor personnel will appropriately have a state and national fingerprint-based record background check prior to this restricted area access being granted.

e. Not be allowed to view screen information, mitigating shoulder surfing.

f. Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified or call 911.

g. Not be allowed to sponsor another visitor.

h. Not enter into a secure area with electronic devices unless approved by the Myrtle Beach Police Department Local Area Security Officer (LASO), including cameras and mobile devices. Photographs are not allowed without permission of the Myrtle Beach Police Department assigned personnel.

i. All requests by groups for tours of the Myrtle Beach Police Department facility will be referred to the proper

agency point of contact for scheduling. In most cases, these groups will be handled by a single form, to be signed by a designated group leader or representative. Remaining visitor rules apply for each visitor within the group. The group leader will provide a list of names to front desk personnel for instances of emergency evacuation and accountability of each visitor while on agency premises.

C. Authorized Physical Access

1. Only authorized personnel will have access to physically secure non-public locations. The Myrtle Beach Police Department will maintain and keep current a list of authorized personnel. All physical access points into the agency's secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display media of CJI. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical, and electronic breaches.

2. All personnel with CJI physical and logical access must:

    a. Meet the minimum personnel screening requirements before CJI access.

        i. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.

        ii. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

        iii. Before granting access to CJI, the Myrtle Beach Police Department on whose behalf the contractor is retained shall verify identification via a state of

residency and national fingerprint-based record check.

iv. Refer to the CJIS Security Policy for handling cases of felony convictions, criminal records, arrest histories, etc.

b. Complete security awareness training.

i. All authorized Myrtle Beach Police Department, Noncriminal Justice Agencies (NCJA) like city or county IT, and private contractor/vendor personnel will receive security awareness training before being granted duties that require CJI access. The training must have been completed within six months of initial access and be renewed annually thereafter.

ii. Security awareness training will cover areas specified in the CJIS Security Policy at a minimum.

3. Be aware of who is in their secure area before accessing confidential data.

a. Take appropriate action to protect all confidential data.

b. Protect all terminal monitors with viewable CJI displayed on the monitor and do not allow viewing by the public or escorted visitors.

4. Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc.

a. Report loss of issued keys, proximity cards, etc. to authorized agency personnel.

b. If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call the Myrtle Beach Police Department POC to have authorized credentials like a proximity card deactivated and/or door locks possibly rekeyed.

c. Safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e., Smartcard), and all other facilities and computer

systems security access procedures. See the Penalties Section of this Procedure.

5. Properly protect from viruses, worms, Trojan horses, and other malicious code.

6. Do not use personally owned devices on the Myrtle Beach Police Department computers with CJI access. (Agency discretion). See Personally Owned Policy.

7. Use of electronic media is allowed only by authorized Myrtle Beach Police Department personnel. Controls shall be in place to protect electronic media and printouts containing CJI while in transport. When CJI is physically moved from a secure location to a non-secure location, appropriate controls will prevent data compromise and/or unauthorized access.

8. Encrypt emails when electronic mail is allowed to transmit CJI-related data, as such in the case of Information Exchange Agreements.

9. If CJI is transmitted by email, the email must be encrypted, and the email recipient must be authorized to receive and view CJI.

10. Report any physical security incidents to the Myrtle Beach Police Department's LASO, including facility access violations, loss of CJI, loss of laptops, cellphones, thumb drives, CDs/DVDs, and printouts containing CJI.

11. Properly release hard copy printouts of CJI only to vetted and authorized personnel in a secure envelope and shred or burn hard copy printouts when no longer needed. Information should be shared on a "need-to-know" basis. (See MBPD 130 Disposal of Media)

12. Ensure data centers with CJI are physically and logically secure.

13. Keep appropriate Myrtle Beach Police Department security personnel informed when CJI access is no longer needed. In the event of ended employment, the individual must surrender all property and access managed by the local agency, state, and/or federal agencies.

14. Know which door to use for proper entry and exit of the Myrtle Beach Police Department and only use marked alarmed fire exits in emergency situations.

15. Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped open, and take measures to prevent piggybacking entries.

D. Roles and Responsibilities

1. Terminal Agency Coordinator (TAC)

   The TAC serves as the point of contact at the Myrtle Beach Police Department for matters relating to CJIS information access. The TAC administers CJIS systems programs within the agency and oversees the agency's compliance with FBI and state CJIS systems policies.

2. Local Agency Security Officer (LASO): Each LASO shall:

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

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

   c. Ensure that personnel security screening procedures are being followed as stated in this policy.

   d. Ensure the approved and appropriate security measures are in place and working as expected.

   e. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

3. CJIS System Agency Information Security Officer (CSA ISO). The CSA ISO shall:

   a. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

   b. Document technical compliance with the CJIS Security Policy to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.

c. Document and assist in implementing the security-related controls for the Interface Agency and its users.

d. ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASO's institute the incident response reporting procedures at the local level. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the ISO, the affected criminal justice agency, and the FBI CJI Division ISO major incidents that significantly endanger the security or integrity of CJI.

E. Information Technology Support

In coordination with the above roles, all vetted IT support staff will protect from compromise at the Myrtle Beach Police Department by performing the following:

1. Protect information subject to confidentiality concerns - in systems, archived, on backup media, and until destroyed. Know where CJI is stored, printed, copied, transmitted, and planned end of life. CJI is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, DVDs, thumb drives, mobile devices, and internet connections as authorized by the Myrtle Beach Police Department. For agencies that submit fingerprints using Live Scan terminals, only Live Scan terminals that receive CJI back to the Live Scan terminal will be assessed for physical security.

2. Be knowledgeable of required Myrtle Beach Police Department technical requirements and policies, taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit, and at the end of life.

3. Take appropriate action to ensure maximum uptime of CJI and expedited backup restores by using agency-approved best practices for power backup and data backup means such as generators, backup universal power supplies on CJI-based terminals, servers, switches, etc.

4. Properly protect the Myrtle Beach Police Department's CJI system(s) from viruses, worms, Trojan horses, and other malicious code (real-time scanning and ensure updated definitions).

a. Install and update antivirus on computers, laptops, MDTs, servers, etc.

b. Scan any outside non-agency-owned DVDs, thumb drives, etc., for viruses.

5. Data backup and storage-centralized or decentralized approach.

    a. Perform data backups and take appropriate measures to protect all stored CJI.

    b. Ensure any media released from the Myrtle Beach Police Department is properly sanitized and destroyed.

6. Timely application of system patches, which are a part of configuration management.

    a. The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

7. Access control measures

    a. Address least privilege and separation of duties.

    b. Enable event logging of:

        i. Successful and unsuccessful system log-on attempts.

        ii. Successful and unsuccessful attempts to access, create, write, delete, or change permissions on a user account, file, directory, or other system resource.

        iii. Successful and unsuccessful attempts to change account passwords.

        iv. Successful and unsuccessful actions by privileged accounts.

        v. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.

c. Prevent authorized users from utilizing 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.

8. Account Management in coordination with TAC

   a. Agencies shall ensure that all user IDs belong to currently authorized users.

   b. Keep login access current, updated, and monitored. Remove or disable terminated, transferred, or associated accounts.

   c. Authenticate verified users as uniquely identified.

   d. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs.

   e. Do not use shared generic or default administrative user accounts or passwords for any device used with CJI.

   f. Passwords

      i. Be a minimum length of eight (8) characters on all systems.

      ii. Not be a dictionary word or proper name.

      iii. Not be the same as the User ID.

      iv. Expire within a maximum of 90 calendar days.

      v. Not be identical to the previous ten (10) passwords.

      vi. Not be transmitted in the clear or plaintext outside the secure location.

      vii. Not be displayed when entered.

viii. Ensure passwords are only reset for authorized users.

9. Network infrastructure protection measures.

    a. Take action to protect CJI-related data from unauthorized public access.

    b. Control access, monitor, enable, and update configurations of boundary protection firewalls.

    c. Enable and update the personal firewall on mobile devices as needed.

    d. Ensure confidential electronic data is only transmitted on secure network channels using encryption and advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear text.

    e. Ensure any media that is removed from a physically secured location is encrypted in transit by a person or network.

    f. Do not use default accounts on network equipment that passes CJI, like switches, routers, firewalls.

    g. Make sure law enforcement networks with CJI are on their own network accessible by authorized personnel who have been vetted by the Myrtle Beach Police Department. Utilize Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city and/or county agencies using same wide area network.

10. Communicate and keep the Myrtle Beach Police Department informed of all scheduled and unscheduled network and computer downtimes, all security incidents and misuse. The ultimate information technology management control belongs to the Myrtle Beach Police Department.

F. Front Desk and Visitor Sponsoring Personnel

1. Administration of the Visitor Check-In/Check-Out procedure is the responsibility of identified individuals in each facility. In

most facilities, this duty is done by the Front Desk or Reception Desk.

2. Prior to visitor gaining access to a physically secure area:

    a. The visitor will be screened by the Myrtle Beach Police Department personnel for weapons. No weapons are allowed in the agency except when carried by authorized personnel as deemed authorized by the Myrtle Beach Police Department.

    b. Escort personnel will acknowledge being responsible for properly evacuating visitors in cases of emergency. Escort personnel will know appropriate evacuation routes and procedures.

    c. Escort and/or Front desk personnel will validate that the visitor is not leaving the agency with any agency-owned equipment or sensitive data before Visitor departure.

3. All Myrtle Beach Police Department personnel and supporting entities are responsible for reporting any unauthorized physical, logical, and electronic access to the Myrtle Beach Police Department officials. For the Myrtle Beach Police Department, the points of contact to report any non-secure access are:

    a. Local contact-LASO: Cathie Rhodes
    Myrtle Beach Police Department
    Phone: 843.918.1341

    b. State contact-CSA ISO: Major Jennie Temple
    SLED
    Phone: 803.896.7008

G. Penalties

1. 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.

2. Violation of any of the requirements in this policy by any visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

III. 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.