MYRTLE BEACH POLICE DEPARTMENT

ADMINISTRATIVE REGULATIONS AND OPERATING PROCEDURES

Subject: Computer Misuse Policy	***Number: 127-B***
Effective Date: January 10, 2019	***Revised Date: October 16, 2026***
Rescinds: 127 – Computer Misuse Policy ***127-A – Computer Misuse Policy***	***Dated: 10-10-2019*** ***10-26-2023***

Approved By:

I. PURPOSE

To establish procedures for the proper use of computer resources within the Department.

II. POLICY

A. In support of the Myrtle Beach Police Department's mission of public service to the City of Myrtle Beach citizens, the Myrtle Beach Police Department provides the needed technological resources to personnel to access FBI CJIS systems and information in support of the agency's mission. All agency personnel with access to FBI Criminal Justice Information (CJI) or any system with stored FBI CJI have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care, and maintenance of the information. Use of all technology equipment: computers, laptops, software, copiers, printers, terminals, MDTs, mobile devices, live scan devices, fingerprint scanners, software to include RMS/CAD, operating systems, etc., used to process, store, and/or transmit FBI CJIS is a privilege allowed by Myrtle Beach Police Department, state CSO, and the FBI. All software includes, but is not limited to, SunGard OSSI, SCIEX, GangNet, CrimeNTel, Rapid ID, and ALPR.

To maintain the integrity and security of the Myrtle Beach Police Department's and FBI's CJIS systems and data, this computer use privilege requires adherence to relevant federal, state, and local laws, regulations, and contractual obligations. All existing laws and Myrtle

Beach Police Department regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply to personal conduct.

B. Privacy Policy - All agency personnel utilizing agency-issued technology resources funded by the Myrtle Beach Police Department must expressly acknowledge and agree that such service, whether for business or personal use, shall remove any expectation of privacy. Use of Myrtle Beach Police Department systems indicates consent to monitoring and recording. The Myrtle Beach Police Department reserves the right to access and audit any and all communications, including electronic and physical media at rest, in transit, and at end of life. Myrtle Beach Police Department personnel shall not store personal information with an expectation of personal privacy that is under the control and management of the Myrtle Beach Police Department.

III. PROCEDURE

A. Misuse

Misuse of computing, networking, or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statutes. All files are subject to search. Where follow-up actions against a person or agency after an information security incident involve legal action (either civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Complaints alleging misuse of Myrtle Beach Police Department's computing and network resources and FBI CJIS systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

B. Examples of Misuse of access to FBI CJI

1. Using someone else's login that you are not the owner.

2. Leaving a computer logged in with your login credentials unlocked in a physically unsecure location, allowing anyone to access Myrtle Beach Police Department systems and/or FBI CJIS systems and data in your name.

3. Allowing an unauthorized person to access FBI CJI at any time for any reason. Note: Unauthorized use of the FBI CJIS systems

is prohibited and may be subject to criminal and/or civil penalties.

4. Allowing remote access of Myrtle Beach Police Department-issued computer equipment to FBI CJIS systems and/or data without prior authorization by the Myrtle Beach Police Department.

5. Obtaining a computer account that you are not authorized to use.

6. Obtaining a password for a computer account of another account owner.

7. Using the Myrtle Beach Police Department's network to gain unauthorized access to FBI CJI.

8. Knowingly performing an act that will interfere with the normal operation of FBI CJIS systems or any departmental software.

9. Knowingly propagating a computer virus, Trojan horse, worm, or malware to circumvent data protection or compromise existing security holes in FBI CJIS systems.

10. Duplication of licensed software, except for backup and archival purposes, that circumvents copyright laws for use in Myrtle Beach Police Department, for home use, or for any customer or contractor.

11. Deliberately wasting computing resources, including streaming audio or videos for personal use, that interferes with Myrtle Beach Police Department network performance.

12. Using electronic mail or instant messaging to harass others.

13. Masking the identity of an account or machine.

14. Posting materials publicly that violate existing laws or Myrtle Beach Police Department's codes of conduct.

15. Using Myrtle Beach Police Department's technology resources to advance unwelcome solicitation of a personal or sexual relationship while on duty or through the use of official capacity.

16. Unauthorized possession of, loss of, or damage to Myrtle Beach Police Department's technology equipment with access to FBI CJI through unreasonable carelessness or maliciousness.

17. Maintaining FBI CJI or duplicate copies of official Myrtle Beach Police Department files in either manual or electronic formats at his or her place of residence or in other physically non-secure locations without express permission.

18. Using Myrtle Beach Police Department's technology resources and/or FBI CJIS systems for personal or financial gain.

19. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy.

20. Using personally owned devices on Myrtle Beach Police Department's network, including personally owned thumb drives, CDs, mobile devices, tablets on Wi-Fi, etc. Personally owned devices should not store Myrtle Beach Police Department data, State data, or FBI CJI.

C. The above listing is not all-inclusive, and any suspected technology resource or FBI CJIS system or FBI CJI misuse will be handled by the Myrtle Beach Police Department on a case-by-case basis. Activities will not be considered misuse when authorized by appropriate Myrtle Beach Police Department officials for security or performance testing.

D. See the City Handbook for the Acceptable Use Policy regarding the rules for the personal use of Department technology and social networking.

E. Misuse Notification

1. Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, Myrtle Beach Police Department shall: (i) establish an operational incident handling capability for all information systems with access to FBI CJIS systems and data. This includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

2. LASO's have been identified as the POC on security-related issues for their respective agencies. LASO's shall institute the CSA incident response reporting procedures at the local level.

3. All Myrtle Beach Police Department personnel are responsible to report misuse of Myrtle Beach Police Department technology resources to appropriate Myrtle Beach Police Department officials.

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

    b. State contact-CSA ISO: Lauren P. Barwick, CISA, CRISC
    Phone: 803.995.3374

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.