



MYRTLE BEACH POLICE DEPARTMENT ADMINISTRATIVE REGULATIONS AND OPERATING PROCEDURES

Subject: Computer Misuse Policy

Number: 127-A

Effective Date: January 10, 2019

Revised Date: October 26, 2023

Rescinds: 127 – Computer Misuse Policy

Dated: 10/10/2019

Approved By:

I. Purpose:

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

II. Procedure:

In support of 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, SCIEEX, 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 of 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.

1. 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 for search. Where follow-up actions against a person or agency after an information security incident involves 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.

Examples of Misuse with access to FBI CJI

- Using someone else's login that you are not the owner.
- Leaving 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.
- Allowing 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.
- Allowing remote access of Myrtle Beach Police Department issued computer equipment to FBI CJIS systems and/or data without prior authorization by Myrtle Beach Police Department.
- Obtaining a computer account that you are not authorized to use.
- Obtaining a password for a computer account of another account owner.
- Using the Myrtle Beach Police Department's network to gain unauthorized access to FBI CJI.
- Knowingly performing an act which will interfere with the normal operation of FBI CJIS systems or any departmental software.
- Knowingly propagating a computer virus, Trojan horse, worm and malware to circumvent data protection or compromising existing security holes to FBI CJIS systems.
- Duplication of licensed software, except for backup and archival purposes that circumvent copyright laws for use in Myrtle Beach Police Department, for home use or for any customer or contractor.
- Deliberately wasting computing resources to include streaming audio, videos for personal use that interferes with Myrtle Beach Police Department network performance.
- Using electronic mail or instant messaging to harass others.
- Masking the identity of an account or machine.
- Posting materials publicly that violate existing laws or Myrtle Beach Police Department's codes of conduct.
- 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.

- 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.
- 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.
- Using Myrtle Beach Police Department's technology resources and/or FBI CJIS systems for personal or financial gain.
- Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy.
- Using personally owned devices on Myrtle Beach Police Department's network to include 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.

****The above listing is not all-inclusive and any suspected technology resource or FBI CJIS system or FBI CJI misuse will be handled by 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.**

2. Privacy Policy

All agency personnel utilizing agency-issued technology resources funded by Myrtle Beach Police Department expressly acknowledges and agrees 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 are under the control and management of Myrtle Beach Police Department.

3. Personal use of Agency Technology (City Handbook)

Personal Use of Agency Technology (Taken from the City Handbook – Section 11)

Electronic Communications

The City's workplace privacy policy discourages the use of City issued electronic devices (including laptop computers and phones) for personal business without the express written permission of the City. The City consents to the "reasonable" use of its computers for personal business as determined in the sole discretion of the City. The only sure way to avoid violating the City's policy on personal computer use is not to use the City's computers for any personal purpose.

The following personal computer use is absolutely forbidden:

- To access any material which the City considers to be pornographic.
- To transmit or knowingly accept receipt of any communication which is pornographic, obscene, or in the City's opinion might contribute to a hostile work environment in that it demeans individuals on the basis of race, sex, age, national origin, disability or some similar distinction.

Social Networking:

The City recognizes that employees may use social networking websites or similar media including, but not limited to, blogs, chat rooms, Facebook, MySpace, Twitter, etc. (hereinafter referred to as "personal websites").

Employees may not post on a personal blog or web page or participate in a personal social networking site during working time or at any time with City equipment or property, unless such postings and participation is part of the employee's job. Working time is your scheduled time of work, not including lunch hour, breaks or time prior to or after your shift.

All other City rules and policies regarding discrimination and harassment apply in full force to personal websites and social networking. The City is firmly committed to its equal employment opportunity policies and does not condone or tolerate discrimination. The City also prohibits all forms of unlawful harassment. Employees are prohibited from engaging in any conduct, activities, communication or postings which violate City policies regarding discrimination and harassment. No messages with derogatory or inflammatory language about any legally protected characteristic shall be transmitted or retrieved. No abusive, profane or offensive language is to be transmitted. Any conduct which is impermissible under the law if expressed in any other form or forum is also impermissible if expressed through blogs, social networks, text messages or other electronic means.

You should not represent yourself as a representative of the City on personal websites. Personal websites, which indicate your place of employment, should include a disclaimer that the opinions provided do not represent the views of the City.

If an employee believes that a blog or other online communication violates any City policy, the employee should immediately report the blog or online communication to the Public Information Officer. The City may investigate the matter, determine whether such blog, posting, website, or communication violates City policies, and take appropriate action.

Any employee who violates this policy may be subject to disciplinary action, up to and including termination. Additionally, violations of this policy may result in criminal prosecution, reimbursement of expenses incurred as a result of the violation, and additional legal action.

IMPORTANT NOTICE: The City has the capability to examine the computer usage of individual employees in detail. Even though an item has been "deleted" and the employee cannot retrieve it, this does not mean that the City cannot do so. It is also possible to generate a report of every Internet connection made by each user and the amount of time was spent at each web site. The City explicitly reserves the right to examine City computers to ensure that they are used appropriately.

Misuse Notification

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.

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.

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.

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

Jim Smith
City of Myrtle Beach IS Analyst
Phone: 843.918.1445

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