



MYRTLE BEACH POLICE DEPARTMENT ADMINISTRATION REGULATIONS AND OPERATING PROCEDURES

Subject: Acceptable Use Policy

Number: 143

Effective Date: October 26, 2023

Revised Date:

Rescinds:

Dated:

Approved By:

I. Purpose:

The purpose of this policy is to outline the acceptable use of computer equipment at Myrtle Beach Police Department. These rules are in place to protect the employees and Myrtle Beach Police Department. Inappropriate use exposes Myrtle Beach Police Department to risk including virus attacks, compromises of the network systems and services, and legal issues.

II. PROCEDURE:

- A. Employees are to adhere to the City's workplace privacy policy on the personal use of agency technology.
- B. Electronic Communications
 - i. 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:
 - 1. To access any material which the City considers to be pornographic.
 - 2. 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.

C. Social Networking:

- i. 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").
- ii. 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.
- iii. Working time is your scheduled time of work, not including lunch hour, breaks or time prior to or after your shift.
- iv. 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.
- v. 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.
- vi. 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.
- vii. 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.
- viii. 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.

- ix. **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.

- D. The Myrtle Beach Police Department security department recommends that any information that a user considers sensitive or vulnerable (etc. residual NCIC information on a computer terminal that has access to the internet and CJIS information) be encrypted.
- E. For security and network maintenance purposes, authorized individuals within City of Myrtle Beach may monitor equipment, systems and network traffic at any time.
- F. Myrtle Beach Police Department reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy.

III. Security and Proprietary Information

- A. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or non-confidential, as defined by agency confidentiality guidelines. Examples of confidential information include, but are not limited to: NCIC information, state criminal history information, agency personnel data, etc. Employees should take all necessary steps to prevent unauthorized access to this information.
 - i. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
 - ii. All personal computers, laptops, and workstations should be secured with password-protected screen savers with an automatic activation feature, set at ten minutes or less, or by logging off (control-alt-delete) when the computer is unattended.
 - iii. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in

accordance with "Laptop Security Policy".

- iv. All devices used by employees that are connected to the Myrtle Beach Police Department Internet/Intranet/Extranet, whether owned by the employee or Myrtle Beach Police Department, shall be continually executing approved virus-scanning software with a current database.
- v. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

IV. Unacceptable Use

A. The following activities are, in general, prohibited.

- i. Under no circumstances is an employee of Myrtle Beach Police Department authorized to engage in any activity that is illegal under local, state, federal, or international law utilizing Myrtle Beach Police Department owned resources. The list below are by no means exhaustive, but attempts to provide a frame work for activities which fall into the category of unacceptable use.

V. System and Network Activities

A. The following activities are strictly prohibited, with no exceptions:

- i. Unauthorized access, copying, or dissemination of classified or sensitive information (e.g., NCIC information, state criminal information, etc.).
- ii. Installation of any copyrighted software for which Myrtle Beach Police Department or end user does not have an active license is strictly prohibited.
- iii. Installation of any software without preapproval and virus scan is strictly prohibited.
- iv. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, logic bombs, etc.).
- v. Revealing your account password to others or allowing use of your account by others.
- vi. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For the purpose of this policy, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information

for malicious purposes.

- vii. Port scanning or security scanning is expressly prohibited unless prior notification has been given to Myrtle Beach Police Department Security administration.
- viii. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- ix. Circumventing user authentication or security of any host, network, or account.
- x. Interfering with or denying service to any user other than the employee's host.
- xi. Using any program/script/command or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- xii. Providing information about NCIC information to parties outside Myrtle Beach Police Department.

VI. Enforcement

- A. Violations of this policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law; inappropriately modifying or destroying data; inadequately protecting restricted data. Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, civil or criminal prosecution, and termination of employment.