



MYRTLE BEACH POLICE DEPARTMENT

ADMINISTRATIVE REGULATIONS AND OPERATING PROCEDURES

Subject: *Departmental Computer Resources*

Number: *109-E*

Effective Date: *January 1, 2001*

Revised Date: *November 10, 2023*

Rescinds: *109-D Departmental Computer Resources*
109-C Departmental Computer Resources
109-B Departmental Computer Resources
109-A Department Computer Resources
049

Dated: *January 14, 2019*
September 11, 2008
January 8, 2008
September 22, 2003
March 9, 2000

Approved By: _____

I. PURPOSE

To establish procedures for the use of computer resources within the Department and to outline parameters for use of software, hardware and data to protect the interests of the Department and its employees.

II. DEFINITIONS

- A. Computer System - All internal and external hardware components of the Departmental computer resources (PC stand alone, PC network, AS/400 mainframe, laptops, cabling, hubs, printers, servers, etc.)
- B. Software - Programs used by a computer to perform any of its functions (i.e., DOS, MS Office Word, Excel, Access, Publisher etc.).
- C. Authorized Software - Computer programs that the Department or city has paid for or is otherwise licensed. Also, public domain software approved by the Chief of Police or his/her designee for use on a Departmental computer.
- D. Data File - Word processing, spreadsheet, database or other file containing information, as opposed to software, which acts on a data file.
- E. PD IT - A city employee(s) approved by the Chief of Police to work with all departmental computer equipment and ensure functional operating systems as well as guaranteeing proper job related application of the related hardware and software.

III. PROCEDURE

- A. This Department will maintain and use all available computer resources in accordance with all applicable Federal, State and Local laws, software manufacturer licensing agreements and departmental rules and regulations.
 - 1. At no time shall any software be installed or used on any departmental computer system in violation of copyright laws or this policy.
 - 2. According to the U.S. Copyright law, illegal reproduction of software or use of illegally copied software is subject to civil damages of \$50,000.00 or more in addition to criminal penalties that can include fines and/or imprisonment.
 - 3. Any employee who knowingly makes, acquires or uses unauthorized copies of computer software licensed to the Department or who places or uses unauthorized software on Departmental computer equipment shall be subject to immediate disciplinary action up to and including termination.
 - 4. The Myrtle Beach Police Department cannot condone and specifically forbids the unauthorized duplication of software.
 - 5. The intentional corruption of any information stored in the City computers or the unauthorized documentation of information shall result in disciplinary action.
 - 6. At no time will any employee sign on or allow someone to sign onto ANY computer using any log on name & password other than their own unless authorized by PD IT for maintenance or auditing purposes. The only exception to this will be when an employee's supervisor uses the employee's name and password to sign on to their workstation computer for authorized departmental business.
- B. The PD IT employee(s) will be approved by the Chief of Police and will work in coordination with the Local Agency Security Officer (LASO). PD IT will be responsible to:
 - 1. Establish guidelines for the procurement of computer hardware, software, and supplies; maintenance of computer hardware/software; use of computer hardware/software; and inventory of all computer resources.
 - 2. protect the central records computer system through data backup and storage,
 - 3. Ensure secured system access;
 - 4. Require all employees with access to department computer systems to change their password at least every ninety days.
 - 5. Review requests/acquisitions from command staff for computer systems hardware/ software and make appropriate recommendations.
 - 6. PD IT will make daily backup copies of all data stored on departmental servers and maintain these in a secure location.
 - 7. Coordinate the installation, use, inspection, and support of Departmental computer systems. Conduct random inspections of computer resources used by Departmental employees.
 - 8. Coordinate requests for computer training, information and assistance.

C. Responsibilities:

1. All Department Supervisors:

- a. Ensure that all Department members comply with all applicable statutes, software manufacturers' licensing agreements and Departmental rules and regulations concerning the use of all computer resources used by employees.
- b. Review requests to contact on call IT and complete the phone call.
- c. Enter any requests for vehicle IT equipment repair or body camera repair on the appropriate SharePoint site.
- d. Report any damaged or vandalized computer equipment to PD IT.
- e. All damage must be logged on a Loss Report and forwarded through the chain of command with a copy forwarded to PD IT. The form should include, but is not limited to, the damage incurred, the serial number, model, brand name, city ID number, and location of the equipment.

D. Computer Users:

1. Must comply with all State and Local Laws, software manufacturers' licensing agreements, FBI CJIS Security Policy and Departmental rules and regulations.
2. Notify a supervisor in the event of a system hardware or software problem for appropriate resolution.

E. Utilization of Computer Resources

1. All computer equipment is provided for Departmental business and other uses that are approved by the City's Computer Use Policy. Any use for personal or financial gain, outside of these specific guidelines, is prohibited and may result in disciplinary action.
2. All information stored within Departmental computer systems shall be considered official business and therefore is the property of the Myrtle Beach Police Department. All information within the computers is subject to inspection and will be audited randomly.
3. All data created or stored on Departmental computer systems will be used solely for law enforcement purposes and other activities that are expressly authorized by City policy.
4. Employees will make every reasonable attempt to ensure that no software which is to be used in a departmental computer is contaminated with a virus. At any time that an employee does identify or suspect a virus has infected his/her workstation, he/she will immediately shut down the computer and promptly notify a supervisor.

F. Transfer or Separation from Employment

1. When an employee, for any reason, separates from employment with the Department, the employee will surrender all externally stored (flash drive, external drive) data files to PD IT that are produced and/or maintained by said employee.

2. Any employee who transfers within the Department will release any and all data, files, etc. within their possession relating to the previous position to the employee's immediate supervisor.
3. When an employee separates from employment with the Department, on the date of separation, Police Administration will send correspondence to Information Systems (IS) notifying them of the separation and place a copy of this correspondence in the employee's personnel file for documentation purposes.

G. Transfer of Computer Equipment

1. All transfer of computer equipment must be coordinated through PD IT.

H. Online Services

1. Employees may not access any online service with a Departmental computer or under a Departmental issued address or authorization, or incur online service charges, without proper specific or implied authorization from the Chief of Police or PD IT. All online activity will comply with guidelines outlined throughout this policy, FBI CJIS policy and the City's Computer Use Policy.
2. Employees may not access nor download any data, graphics, photos, websites, etc., from any internet or intranet website with any departmental computer or any computer under the direct control of the department unless required for investigative, intelligence or work related research. Downloads of material designed to improve the function of the assigned computer, or its components, must be approved by PD IT.
3. No information gained from any Criminal Justice database such as NCIC, Gang Net, SCIEX, SC DMV and others will be used for anything other than official departmental purposes.