Information and Technology

.01 Policy

It is the policy of the Bladensburg Police Department to maximize the efficiency of our personnel, and to enhance the quality of their work, to encourage employees to use computer systems and databases. In order to protect Department hardware, software, and the records stored in databases from unauthorized access and computer viruses, it is necessary for the Department to implement and enforce certain security measures and procedures. Relaxed security measures could result in severe damage to operating systems, data, software and hardware.

All correspondence, including files and documents produced, transmitted or received on any department electronic database or messaging system, regardless of content, is the property of the Town of Bladensburg.

.02 Terms

Local Area Network: Also known as a "LAN," it is a computer network limited to a specific group of computers enabling the sharing of information and resources.

Electronic Messaging System: Any department computer, terminal, or network, internal electronic messaging, Internet, and facsimile (Fax) technologies.

.03 Governing Legislation and Reference

Governing Legislation:

Electronic Communications Privacy Act.

Maryland Code, Criminal Procedures Article, Section 7-202, 8-606, and 10-213 through 10-228.

COMAR 12.15.01.15.

CFR Title 28, Chapter 1, Part 20.

Forms:

Criminal Record Request Log (Form #609).

.04 Procedure

No employee will use access to e-mail, the Internet, or any computer program for any purpose other than those reasonably necessary for the performance of his or her work assignment. Members are specifically prohibited from using e-mail or Internet accounts to access information reasonably considered offensive or disruptive to any member. Offensive content includes, but is not limited to, sexual comments or images, racial slurs, gender-specific comments, or any comments that would reasonably offend someone on the basis of age, sexual orientation, religious or political beliefs, national origins or disability.

Username and Passwords

All access to computer use and the data contained within is protected by the use of individual user names and passwords issued to an employee by the Department. Employees will not access any Department computer for any purpose by using a user name and password other than those issued to the employee by the Department.

Employees will maintain the confidentiality of their Department-issued user name and password. Members will not disclose their username and password to any other person with the following exceptions:

- IT Manager; and,
- Upon the request of an officer conducting an administrative investigation.

  Employees are responsible for all computer access logged under their user name.

Equipment

Only Town-owned or acquired computer equipment will be maintained and operated within Departmental facilities, except the following:

- personally owned portable units removed at the end of the tour of duty ;
- Computing equipment held as evidence;
- Visitors using their own personal equipment; or,
- Exceptions authorized by the Chief of Police or their designee.

Local Area Network (LAN) computers will not be detached from the network at any time.

Absent IT Manager authority, employees are prohibited from making hardware repairs, software additions, or adjustments to Town-owned computers.

Employees will not attempt to modify any computer start up routine or operating system files.

Employees will not password-protect the boot (start up) process of any Town computer.

Employees will not use Town computer resources to produce personal material.

Absent the affected employee's expressed permission, employees will not knowingly move, copy, encrypt, destroy, modify, delete or tamper with the electronic data files of other employees.

Employees will not knowingly place a computer virus onto a Town computer, onto the LAN, or in any manner deliberately abuse computer resources.

Except in cases of operational necessity, employees will not divulge their network log-on password to others.

Computer resources are fixed assets and will not be moved from the area to which they are assigned without IT Manager's authority.

Software

Only software purchased or acquired by the Town will be operated on Departmental computers. All software must be installed in accordance with United States copyright laws. All software not Town-owned will be removed.

Electronic Files

All files contained on Departmental hard drives, floppy disks or other storage media are considered work products. Therefore, employees have no expectation of privacy regarding these files. Electronic files may be administratively accessed or monitored for various reasons, including, but not limited to, any of the following:

- System maintenance;
- Internal investigations;
- Subpoena process; or,
- Public record inspection.

Files will not be encrypted without the consent of the Commander of Operations. In the event files are encrypted, both the employee supervisor and Commander of Operations will be made aware of the encryption password.

Computer Removal

When a computer has been designated as non-serviceable or when a hard drive on a computer fails, the Department will retain the hard drive for destruction.

When a computer is removed from service, the IT Manager will ensure that the computer is removed from the Town's fixed asset inventory, along with the termination of all associated maintenance fees. The computer will be disposed of in accordance with Town policy.

Removable Storage Media Destruction

When removable storage media (floppy disks, tape back up, etc.) containing confidential information or criminal history record information (CHRI) become unusable, employees will forward the media to the IT Manager for destruction.

Criminal Justice Information System (CJIS)

CJIS can be accessed via LAN-connected computers and mobile data computers. The system offers detailed information concerning the personal and physical identity of defendants, prisoners and arresting officers, pending charges, bond arrangements and trial dates.

Dissemination of CJIS Information

Information obtained through CJIS is for official government use only. Secondary dissemination of information will be limited to the following:

- Other government criminal justice agencies when a signatory to a Secondary User Agreement; or,
- As administrative and/or law enforcement responsibilities require.

The disseminating employee will ensure that the recipient identity is recorded by completing the Criminal Record Request Log when the data is retrieved from the terminal.

Maryland law prohibits secondary dissemination of CJIS information for other than official purposes. This restriction applies to motor vehicle and licensing information obtained through CJIS. Employees will direct requests for such information to the MVA. Any employee disseminating criminal history record information to unauthorized recipients is subject to federal and state criminal and civil sanctions.

Electronic Mail (E-Mail)

E-mail shall not be used to send abusive, demeaning, harassing, or threatening messages.

Information and Technology

Department's Official Web Site

Any employee requesting the addition of any information to the Department's Web Site will submit the request by memorandum through the chain of command to the Chief of Police.

Web Pages and Other Internet Services

Employees will not convey official Department information, or make any representation, actual or implied, that he or she is conveying official Department information on any web site or in any other form through the Internet, other than through the Official Department Web Site.

HISTORY: Adopted May 16, 2008

This General Order supersedes all other orders and memoranda in conflict therewith.

Authority:

Charles L. Owens
Chief of Police