

751.2. SUBJECT: COMPUTER SYSTEMS SECURITY

- :1 OBJECTIVE:
To establish policies and procedures relating to the security of computer facilities, software, and data.
- :2 AUTHORITY:
This procedure amended by City Council September 15, 2003.
- :3 DIRECTION:
Systems & Networks Senior Manager, as an Appointed Official, serves at the pleasure of the Mayor and receives direction from the Chief Information Officer.
- :4 FUNCTIONS:
- A. Computer Rooms
1. Physical computer facilities (those areas that house the network equipment, midrange computers, peripherals or data storage) will be secured from unauthorized access. Access will be restricted by locked doors. Keys or combinations to those doors will only be granted to City personnel that have a need to enter the facility on a continual basis or senior management staff, as appropriate. A list of those having such access to each facility will be approved by the Systems & Networks Senior Manager and the Chief Information Officer. Other personnel having a need to enter the facility may do so by being granted access by the Computer Operations Supervisor on duty.
 2. Visitors to a computer facility, whether City employees or not, will be escorted by a Technology Management Division employee.
 3. Individuals entering a computer facility who are not authorized keys and/or access by combination locks will sign IN and OUT on a visitor log.
 4. The Technology Management Division Security Officer is responsible for the development, maintenance, and periodic review of procedures to assure adherence to this policy.
- B. Security Officer
1. Systems security administration is the responsibility of the Technology Management Security Officer as appointed by, and under the direction of the Systems & Networks Senior Manager.
 2. The Security Officer is responsible for:
 - a. Developing and administering procedures to carry out security policies.
 - b. Recommending changes to and the development of new security policies to the Chief Information Officer.
 - c. Conducting periodic reviews of security practices to assure compliance with established procedures.
- C. Software/Data Security

1. *Definitions*

Data/Software Owner - Although data and software are corporate assets of the City, an individual is responsible for a specific set of data and/or software resident on a computer system. All data and software in the computer environment will be owned by a specifically identified individual. The data owner is responsible for granting or denying access to data and software and for insuring data integrity (except as provided for under the Florida Public Records Law). A list of the data/software owners will be maintained by the Systems Security Officer.

Data/Software Custodian - The Technology Management Division will act as the data custodian for all data and software resident on computers within their direct control. As the data and software custodian, the Technology Management Division is responsible for assuring that access to the data is limited to those individuals having permission from the data owner (except as provided for under the Public Records Law), and for safeguarding of the data and software assets. Data/software outside the direct control of Technology Management Division is the responsibility of the individual owner to safeguard.
2. *Specific Direction*
 - a. All data and software will be owned by a designated "data owner." This designation will be established through the Chief Information Officer. Data and software physically resident on a personal computer is owned by the individual responsible for the personal computer hardware asset.
 - b. The Technology Management Security Officer is responsible for activating access to data upon receipt of the appropriate authority from the data owner.
3. *Password Security*
 - a. Data will be physically secured by passwords. Passwords will be randomly generated utilizing both alpha and numeric characters.
 - b. Passwords will normally be specific to a single user. However, group passwords (a single password for multiple people) will be permitted under the following conditions: (1) access to data is for display only, (2) the data is not confidential, and (3) such access is granted and approved by the data owner and the Chief Information Officer.
 - c. Passwords will be given to the individual user by the Technology Management Security Officer. It is the responsibility of the individual users to keep their password confidential.
 - d. In order to identify unauthorized attempts to access any midrange or network system, a maximum of three attempts at entering the password will be granted. Upon the fourth attempt, the system will render the sign-on device unusable. The Technology Management Security Officer must then be contacted in order to re-activate the device to sign on. The Technology Management Security Officer will be notified if a security breach is suspected.

- e. As a matter of good security practices, passwords will be changed on a periodic basis to reduce the risk of unauthorized access.

:5 FORMS:
None.

:6 COMMITTEE RESPONSIBILITIES:
None.

:7 REFERENCE:
This procedure adopted by City Council February 4, 1991, Item 3/50; amended December 9, 1991, Item 6/NN; amended April 19, 1993, Item VV; amended March 20, 1995, Item SS; amended August 31, 1998, Item 3K; amended April 3, 2000, Item 2PPP; amended September 15, 2003.

:8 EFFECTIVE DATE:
This procedure effective September 15, 2003.