



Office of the City Auditor Policies and Procedures

Number: 5.2.4**Title:** Information Technology Security

Original Date:**Revision Date:****Approved by:**

10/02/2001

I. Policy

The security of City-owned information technology resources is the responsibility of all employees.

II. Purpose

To define security requirements for City-owned information technology resources.

III. Definitions

City owned information technology resource is any technological device owned by the City and provided to the employees to conduct their work. Examples include desktop computers, software, printers, laptops, etc...

IV. Procedures

- A. OCA staff should either log off of their desktops or implement a screen saver password if they are going to be away from their desktops for an extended period of time (30 minutes or more). If a resource is shared (e.g. common room computer, intern and audit team, etc.), then only the log-off should be used when leaving the workstation, since a screen saver password would block access of others to resources.
- B. OCA staff should not install software or execute downloaded software. This includes freeware, shareware, and personal software. For more information on how to request that additional software be placed on your workstation, refer to Policy 5.2.1, Legal Software.

- C. OCA staff who have checked out a laptop, projector or other IT equipment are responsible for its security. Such equipment should not be left unsecured but should be returned, if possible, or locked up when not in use. Both extreme heat and extreme cold can cause damage to IT equipment. OCA staff who are negligent while IT equipment is in their care will be fiscally accountable for replacing lost, stolen, or damaged equipment.
- D. Passwords should not be posted anywhere in the vicinity of IT equipment and should not be shared with others. In addition, OCA staff should use passwords that consist of a mix of letters, numerals and symbols and be of at least six characters in length. (Example: de26my*%.)

V. Responsibilities

- A. Each **OCA staff member** is responsible for:
 - 1. Following the City of Austin IT policy(ies). Information technology related policies are on the Intranet under the Information Systems Department.
 - 2. Acquainting themselves with these policies and review them periodically to maintain an understanding.
 - 3. Notifying management of any security violations they become aware of.
 - 4. Accessing only those systems they are authorized to access.
 - 5. Managing their passwords in accordance with this policy.
- B. The **Administrative Specialist** is responsible for notifying the appropriate system administrator(s) when an OCA staff person leaves OCA employment.