Policy Statement

SUBJECT: City of Detroit Workstation Usage Policy

I. Overview

A. Purpose:

The purpose of this document is to describe guidelines concerning appropriate use and security of workstations, peripheral devices, protection of confidential data and information, and securing unattended workstations to prevent unauthorized access

B. Audience/Scope

This policy applies to all City of Detroit employees, as well as contractors, and vendors or other business partners who utilize City of Detroit Workstations.

II. Policy

Workstations should only be used by authorized City of Detroit employee's business partners or vendor's representatives following the requirements of the following policies

- Data Security
- Identity Management
- Internet Usage
- Email Usage

Authentication to the City of Detroit requires a unique user ID and password unless the application captures a unique user

Users are required to follow good security practices in the selection and use of passwords according to the Identity Management policy

Screen savers with password option turned on are to be used on all Workstations unless exempted by the City Data Security Coordinator

If you are running any Remote Desktop programs, **WorkBrain and DRMS** applications cannot be accessed remotely. Any remote access by employees to these application without IT and the Department Head approval will result in discipline up to termination.

Screen savers on Workstations will be configured to automatically enable after five minutes of inactivity with the following controls

- Common workstations will be set to time out at Five (5) minutes with a password lock
- Any exceptions to the above policy will require a formal business waiver initiated by the business unit for the area represented and will require the approval of the City of Detroit IT Director.

Screen savers should be manually enabled when walking away from the Workstation or Shared Workstation, by clicking Ctrl + Alt + Delete.

For all Workstations that are not located in 24/7 departments, Users should log out of all applications, and log out of the network at the end of the business day or User workday

- Workstations dedicated to supporting a specific real-time or round the clock application or information system are not required to be logged out of the specific application, logged out of the network at the end of the business day

All Workstations will be configured according to approved ITS standards

- Unauthorized changes to the desktop hardware, file structure, or system configuration are not allowed..
- Application features are not to be disabled (e.g. virus software or auditing capabilities)

Users are not permitted to download, install, or save any unauthorized software or applications to the network or hard drives without prior approval from ITS

Work-related documents are to be stored on appropriate network drives

- Data and information should not be stored on, transferred to, or transferred from, hard drives or removable media like zip drives, floppy drives, USB devices and diskettes unless there is a legitimate business purpose

- Only data and information stored on network drives is backed up and available for restoration in the event of data loss.

- If the User's designated share on a network drive becomes full, the User is to contact ITS customer service help desk at 313-628-HELP to have the disk space extended

Physical Workstation placement should minimize the possibility of unauthorized personnel viewing screens or data

- Physical devices such as privacy guards will be utilized where needed to limit visibility of Confidential data and information to unauthorized personnel

- Workstations in high traffic areas used to access confidential data and information will be monitored during business hours.

- Business Unit managers are ultimately responsible for the physical placement and monitoring of Workstations in their areas

Always use City of Detroit's Help Desk for the completion of any of the following:

- Move desktop system (e.g. PC, telephone) or peripheral (e.g. printer) to another location
- Add/disable an employee account (e.g. network, e-mail, voicemail)
- Add/remove a service to/from an existing employee account
- Add a new employee desktop system
- Add/remove/change software or hardware to/from an existing desktop system
- Change an employee's name or other personally identifiable information in the system

.

Workstations designated for external relocation, disposal, sale, or donation will be appropriately tracked and sanitized via City of Detroit ITS Sanitation Standards and management guidelines to ensure appropriate tracking, hardware sanitizing, and disposal

All Workstations purchased by City of Detroit are considered company assets throughout the life of the asset at the City of Detroit

Workstations should not be relocated or changed by anyone other than authorized City of Detroit employees or vendors

Workstations will be protected on and off City of Detroit premises

Security locks, alarms, or tracking devices will be appropriately used to physically secure Workstations in areas that are accessible to the general public. The User and department manager are jointly responsible for securing devices and ensuring compliance

Laptops and wireless device Users are expected to follow City of Detroit policies, best practices, and industry standards to avoid laptop theft and/or breach of City of Detroit Confidential Information

Good judgment and reasonable care should be exercised to avoid damaging equipment (e.g. do not drop the device or spill liquids on equipment)

Ethical Workstation Use:

Appropriate use of resources includes maintaining the security of the system, protecting privacy, and conforming to applicable laws, including Copyright and harassment laws

Workstations are to be used primarily for the conduct of City of Detroit business

Attempts to maliciously sabotage systems or networks using City of Detroit resources are prohibited

Attempts to make a computer impersonate other systems, particularly via forged email, talk, news, etc., are prohibited

Users may not use their accounts to attempt to gain unauthorized Access to City of Detroit or non-City of Detroit systems

Users are not to interfere with or alter the integrity of the information system at large by destruction or unauthorized alteration of data or programs belonging to other users

III. Exceptions:

The City Information Technology Services Director and City Corporation Counsel must approve any exceptions to this policy