CITY OF PLANO POLICIES AND PROCEDURES

224.000

Department Name: Human Resources Manual
Procedure: PC Use

Effective Date: 11/01/00
Revision Date(s): 04/30/01, 04/01/06, 04/01/09

I. Purpose

The purpose of this policy is to provide guidance to the employees of the City of Plano concerning their use of personal computers (PC), both "desktop" and mobile (laptop), and related peripheral equipment (e.g., printers, modems, hubs, switches, devices attached to a PC, etc.). Personal computers provided by the City are City owned resources. They are provided to enable City employees to work more efficiently and effectively. When it improves an employee's productivity and effectiveness, use of a PC is encouraged. In ALL circumstances the PC must be used in accordance with City policies and procedures. City employees do not have a right to use or possess this equipment; it is a benefit provided by the City.

II. Definition

A. Authorized user

An authorized user is a current employee or contractor who can lawfully access the City of Plano network and/or PeopleSoft system through a unique network login.

B. Password "Reset"

Reset means enabling the default setting to log onto PeopleSoft.

III. Policies and Procedures

These policies and procedures shall apply to all employees.

A. Property of the City

All personal computers (PC), the network, server, and related equipment are the property of the City of Plano. The City has unilateral right to access all stored electronic files and data to ensure proper use. Therefore, any information transmitted over or stored on this equipment is public property and subject to disclosure and public access as provided by law. In order to protect its interests, the City retains the right to monitor all of its PC systems at its discretion and as allowed by law. By using these systems, employees consent to monitoring by the City.

B. General Computer Use

All use of the PC must be in compliance with this policy and other applicable procedures and rules.

Objectionable/improper materials unrelated to City business such as pictures, posters, calendars, graffiti, objects, promotional materials, reading materials or other materials which are sexually explicit, demeaning or pornographic are not to be transmitted or stored via a City computer.

Any employee using a City PC does so knowing the following:

1. The City of Plano shall not be responsible for any illegal or objectionable/improper use of any aspect of the City's computer system by its employees;

2. Users shall not share passwords for any computer with any unauthorized person, nor obtain any other password by any unauthorized means;

3. Unauthorized use of another staff member's password may result in disciplinary action up to and including termination;

4. All PeopleSoft password reset requests must be made by the authorized user of the account, or the authorized user's current division manager or department manager in writing via e-mail to the helpdesk. If the authorized user does not have a City email account, the supervisor may submit the request for the authorized user;

5. Upon termination from employment, or discontinued computer use authorization, an employee shall not attempt to use or access the City of Plano computer system(s);

6. Files and records created and/or stored on City computers may be subject to State of Texas Open Records laws. Therefore, files may be accessed to the fullest extent allowed by law;

7. Without prior written permission, the PC and related peripherals shall not be used for the transmission or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (viruses and/or self-replicating code), political material, or any other unauthorized use;

8. No PC may contain, store, or operate any software not authorized by City policy or the city manager or his/her designee. Unauthorized software, electronically stored materials, data, and files are subject without notification to immediate removal by the City;

9. Management has the right of access to each City PC and its associate files as consistent with municipal policies, all applicable laws, and individual user's job responsibilities - regardless of the physical location of the PC;

10. Any City files or data stored upon an employee owned PC or related equipment is subject to this policy;

11. Upon separation from City employment all City files and data shall be removed from the employee's equipment. The City specifically retains the right to inspect the equipment to verify the removal;

12. No personal files may be stored on a City computer or network server. Employees must store personal information, both e-mails and data files, on personally owned storage medium (e.g., floppy, zip disk, CD, etc.).

C. Software Duplication

The City has defined a standard software configuration for each PC. Modification of the standard requires the written authorization of the Director of Technology Services and either a deputy city manager or the city manager.

No software shall be installed on a City of Plano computer without a review and authorization of said system by an authorized staff member of the Technology Services Department. Only software that follows the process outlined in the City's Long Range Technology Plan will be supported by the Technology Services Department. All other software is the responsibility of the department in which it is installed.

Department directors shall keep and monitor a record of authorized computer software for all individual users within their department. A current list shall be provided to the City's Technology Services Department at all times.

Personal files on City equipment are subject to being viewed by others. Objectionable or inappropriate material on personal files is prohibited. Files kept on City personal computers for the purposes of personal private business are also prohibited. Individual users should use their best judgement as to files kept on personal computers, as files kept on this equipment can be considered public record and subject to review by the City and others.

Loading of any software that causes technical problems or difficulty to the maintenance and operation of the City's technology infrastructure is prohibited. When identified, notice will be e-mailed to the user and the user's

department director. Additionally, Technology Services can immediately remove the software. Encryption software is specifically prohibited without the written permission of the city manager or a deputy city manager. A copy of the encryption software and "key" will be provided to the City's Director of Technology Services within two (2) business days of approval for use.

All authorized software must be maintained as defined by the City's computer standards. These standards mandate the software be either at a current release level or one back. Any older version will not be allowed to operate on the City's technology infrastructure. It is the responsibility of the operator's department to budget for and maintain all authorized, but non-I.S. supported software. Technology Services will be responsible for budgeting and maintaining all City standard PC software.

D. Computer Maintenance

Departments shall be responsible for ensuring that all computer users know and understand safe computing practices. This shall include, but not limited to:

1. Performing frequent backups on data files consistent with City policy;

2. Using anti-virus software to scan for viruses on all files that are downloaded to disc from the Internet, or any other outside source.

Immediately reporting instances of malfunctioning computer equipment that extends beyond one personal computer shall be reported to the City's director of Technology Services or his/her designated representative. If the event is determined a virus outbreak, it will be logged along with the eradication method used by the Technology Services Department.

Other departments shall immediately be notified. In the event of a serious virus outbreak, or in the case of a continued break of this policy by a department, that department will be disconnected from the Internet and the City's other computer systems until such time as it again complies with the City's computer policy.

Computer equipment installed, moved, changed, or modified without the authorization of Technology Services and either a deputy city manager or city manager shall be the responsibility of the operator's department. Any unauthorized equipment not supported by Technology Services that creates or causes technical problems or malfunctions of the City technology infrastructure shall be immediately removed by Technology Services.

E. Department Director's Responsibilities

Each department director or his/her designee is responsible for:

1. Maintaining an updated list of staff having Internet access, plus communicating the list in writing to the appointed representative of the City's Technology Services Department;

2. Maintaining a list of approved personal computer software for each user within the department;

3. Ensuring that each computer-using member of the department has reviewed and understands this policy; and

4. Maintaining a hard copy of each staff member's written verification that they have reviewed and understand this policy. A copy of the verification is on file with the City's Human Resources Department.

F. Policy Violation

Violation of this policy shall result in disciplinary action. Specifically, any suspected violation will be communicated to that person's department director. The director will follow disciplinary procedures identified in the most current version of the City's "Human Resources Policies and Procedures" manual.

IV. Appendices

None referenced.