Administrative Regulations
Office of the Mayor
Title: USE OF COMPUTER SOFTWARE
A.R. Number: 2.9 **Effective Date:** 2/1/2009 **Page:** 1 of 2
Supersedes: N/A A.R.: N/A DATED: N/A

I. PURPOSE

The purpose of this policy is to assure compliance with the United States Copyright Act. This act prohibits companies and individuals from downloading software onto personal computers (PC) and protects the authors and publishers of software. It is the responsibility of the City of Richmond (COR) to adhere to all copyrights and licensing terms of all computer software issued to employees.

II. SCOPE

This policy covers all COR employees, temporary agency staff , contractors, visitors or other agents and any computer equipment owned by the COR. Unauthorized installing or copying of computer software is illegal and is considered an act of theft. Copyright and intellectual property laws protect the rights and property of authors and publishers of computer software. Unauthorized installing or copying of software whether from the Internet or disk or other means, legally and operationally threatens the security and integrity of the COR's computer system and its overall compliance with the US Copyright Act.

Computer viruses and malware can be easily introduced by employees who bring in software from outside the company. Viruses and malware can spread from one machine to another, destroying critical data.

Unauthorized duplication of software is unethical because it disregards the work and creativity of others. Unauthorized installation or copying of software may also subject employees and the COR to both civil and criminal penalties under the US Copyright Act and/or software licensing agreements.

III. POLICY

A. Guidelines

1. Employees may not install any software licensed by a third party including duplicates intended for use at work, at home, or by an outside party. All installations must be coordinated through the DIT Help Desk.

2. Employees may not use a personally-owned computer to run COR-owned software without appropriate authorization from the Department of Information Technology (DIT).

3. Employees may use software on the network or on multiple machines only in accordance with applicable license agreements (EULAs).

4. Employees should not acquire or purchase any software or use any software on any COR PC without the prior approval of DIT.

5. All new software must be registered with the End User Services (EUS), Desktop Team. The Desktop Team will provide support for approved software applications.

6. Proof of software licenses must be provided to the DIT, EUS, Desktop Team. The Desktop Team will keep a record of all authorized licenses.

IV. RESPONSIBILITY

It is the responsibility of all COR PC users to adhere to this policy. All COR Managers/Automation Coordinators must communicate this policy and assure compliance in their departments.

DIT End User Services will audit PCs for unauthorized or illegally installed software, regularly audit software looking for unauthorized software on PCs, monitor PCs remotely using a management tool which enables the inventory of all hardware and software configurations for any COR-networked PC.

Unauthorized software will be immediately removed by DIT without notification and reported to the user's supervisor and the Chief Information Officer (CIO). The failure to follow the policy may create a serious liability for the COR.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

V. DEFINITIONS

Terms	Definition
Malware	Comes in many forms and can be any program or source code producing output that the computer owner does not need, want, or expect. For example, malware can be a remote access Trojan horse that can not only open a back door to a remote computer but also control someone computer or network from a remote location. Malware includes viruses, worms, Trojan horses (that can, for example, spy on the system and display ads when the user least expects it), and malicious active content arriving through email or Web pages visited. These forms of malware normally run without the knowledge and permission of the user.

VI. REGULATION UPDATE

The Department of Human Resources and the Department of Information Technology shall be responsible for modifications to this Policy.

APPROVED:

MAYOR