Administrative Regulations
Office of the Mayor
Title: USE OF COMPUTER EQUIPMENT
A.R. Number: 2.7 **Effective Date:** 2/1/2009 **Page:** 1 of 3
Supersedes: N/A **A.R.:** N/A **DATED:** N/A

I. PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at the City of Richmond (COR). These rules are in place to protect the employee and the COR. Inappropriate use exposes the COR to risks including virus attacks, compromise of network systems and services, and legal issues.

The Use of Computer Equipment Policy is not to impose restrictions that are contrary to the COR's established culture of openness, trust, and integrity. The COR is committed to protecting its employees, partners, and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP are the property of the COR. These systems are to be used for business purposes in serving the interests of the organization and of our clients and customers in the course of normal operations.

II. SCOPE

This policy applies to all employees. The term "employees" includes employees, contractors, consultants, temporary agency staff, vendors, and other individuals who may have the occasion to operate the COR computer equipment, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the COR.

III. PROCEDURE

A. General Use and Ownership

1. While the COR's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the COR. There is NO expectation of privacy per Administrative Regulation (AR) 2.5.
2. The COR recommends that any information that users consider sensitive be encrypted.
3. For security and network maintenance purposes, authorized individuals in the COR may monitor equipment, systems, and network traffic at any time using any and all means needed to accomplish such actions, per AR 2.5. Examples of this may include, but is not limited to, sniffers, key logging, content filtering, audit logs, et. Al.
4. The COR reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy, per AR 2.5, using any and all software, hardware, or devices necessary to accomplish this task.

B. Security and Proprietary Information

1. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete) when the host will be unattended.
2. All hosts used by the employee which are connected to the COR Internet/Intranet/Extranet, whether owned by the employee or the COR, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

C. Unacceptable Use

Employees may be exempted from certain restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of the COR authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing COR-owned resources. The list below is by no means exhaustive, but an attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited with no exceptions:

1. Violations of the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the COR.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the COR or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a COR computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws as outlined in Administration Regulation 4.13 – Violence in the Workplace..
7. Making fraudulent offers of products, items, or services originating from any COR account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to the COR is made.
11. Circumventing user authentication or security of any host, network or account.
12. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
13. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
14. Providing information about, or lists of, COR employees to parties outside the COR without receiving the appropriate authorization.

IV. RESPONSIBILITIES

Employees must report any suspicious, illegal, or offensive activities to supervisors immediately**.** Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

V. DEFINITIONS

Term	Definition
Blogging	A blog is a personal online journal that is frequently updated and intended for general public consumption.
Employees	For this policy, employees include all COR employees, contractors, consultants, temporary agency staff, vendors, and other individuals who may have the occasion to operate the COR computer equipment, including all personnel affiliated with third parties

VI. REGULATION UPDATE

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

APPROVED:

MAYOR