Administrative Regulations
Office of the Mayor
Title: ELECTRONIC INFORMATION SECURITY
A.R. Number: 2.6 **Effective Date:** 2/1/2009 **Page:** 1 of 7
Supersedes: N/A **A.R.:** N/A **DATED:** N/A

I. PURPOSE

In recognition of the critical role that electronic information systems play in City of Richmond (COR) business activities, this policy defines the rules and other requirements necessary for the secure and reliable operation of the COR electronic information systems infrastructure.

There are information security roles and duties for every employee of the COR. For example, it is an employee's duty to report information security problems. The system designers at the COR are required to include necessary security measures such as user access restrictions based on the need to know.

The COR critically depends on continued customer confidence. This confidence has been gradually increased and is the result of many years of dedicated effort on the part of COR employees. While it is slow to grow, this confidence can be rapidly lost due to problems such as hacker intrusions causing system outages. The trust that customers have in the COR is a competitive advantage that must be nurtured and grown with efforts such as this information security initiative.

The intent of this policy is to provide an overview of security concerns and to define roles for every employee. This policy defines baseline control measures that everyone at the COR is expected to be familiar with and to consistently follow. This is the minimum required to prevent a variety of different problems including: fraud and embezzlement, industrial espionage, sabotage, errors and omissions, and system unavailability. They also define the minimum controls necessary to prevent legal problems such as allegations of negligence, breach of fiduciary duty, or privacy violation. This policy document details both reasonable and practical ways for everyone at the COR to prevent unnecessary losses.

II. POLICY

A. General Use and Ownership

1. Information Owners—Directors in user departments must be designated as the Owners of all types of information used for regular business activities. Each type of "production system information" must have an Owner. When information Owners are not clearly implied by organizational design, the City CAO will make the designation. Information Owners do not legally own the information. They are instead members of the COR management team who make decisions on behalf of the organization. Information Owners or their delegates must make the following decisions and perform the following activities:

   a. Approve information-oriented access control privileges for specific job profiles.

   b. Approve information-oriented access control requests that do not fall within the scope of existing job profiles.

   c. Select a data retention period for their information, relying on advice from the Legal department.

   d. Designate an original source for information from which all management reports will be derived.

   e. Select special controls needed to protect information, such as additional input validation checks or more frequent backup procedures.

   f. Define acceptable limits on the quality of their information, such as accuracy, timeliness, and time from capture to usage.

   g. Approve all new and different uses of their information.

h. Approve all new or substantially-enhanced application systems that use their information before these systems are moved into production operational status Review reports about system intrusions and other events that are relevant to their information.

i. Review and correct reports that indicate the current production uses of their information.

j. Review and correct reports that indicate the job profiles that currently have access to their information.

k. Select a sensitivity classification category relevant to their information, and review this classification every five years for possible downgrading.

l. Select a criticality category relevant to their information so that appropriate contingency planning can be performed.

Information Owners may designate their automation coordinators to act as a back-up person to act if they are absent or unavailable. Owners may not delegate ownership responsibilities to third-party organizations such as outsourcing organizations, or to any individual who is not a full-time COR employee. When both the Owner and the back-up Owner are unavailable, immediate Owner decisions may be made by the designated manager in charge.

2. City Departments—An employee's immediate manager or automation coordinator must approve a request for system access by submitting a system access request form (SAPR) via the city intranet. When an employee leaves the COR, it is the responsibility of the employee's immediate manager or automation coordinator to promptly inform the Department of Information Technology (DIT) that the privileges associated with the employee's user ID must be revoked. User IDs are specific to individuals, and must not be reassigned to, or used by, others.

3. Information Custodians—Custodians are in physical or logical possession of information and information systems. Like Owners, Custodians are specifically designated for different types of information. In many cases, a manager in DIT will act as the Custodian. If a Custodian is not clear, based on existing information systems operational arrangements, then the Chief Information Officer (CIO) will designate a Custodian. Custodians follow the instructions of Owners, operate systems on behalf of Owners, but also serve users authorized by Owners. Custodians must define the technical options, such as information criticality categories, and permit Owners to select the appropriate option for their information.

   Custodians also define information systems architectures and provide technical consulting assistance to Owners so that information systems can be built and run to best meet business objectives. If requested, Custodians additionally provide reports to Owners about information system operations and information security problems. Custodians are responsible for safeguarding the information in their possession, including implementing access control systems to prevent inappropriate disclosure, and developing, documenting, and testing information systems contingency plans.

4. Information Users—Users are not specifically designated, but are broadly defined as any employee with access to internal information or internal information systems. Users are required to follow all security requirements defined by Owners, implemented by Custodians, or established by DIT.. Users must familiarize themselves with, and act in accordance with, all COR information security requirements. Users also must participate in information security training and awareness efforts. Users must report all suspicious activity and security problems to their supervisors.

5. Department of Information Technology (DIT)—DIT is the central point of contact for all information security matters at the COR. Acting as internal technical consultants, it is this department's responsibility to create workable information security compromises that take into consideration the needs of users, Custodians, Owners, and selected third parties. Reflecting these compromises, DIT defines information security standards, procedures, policies, and other requirements applicable to the entire organization. DIT must handle all access control administration activities, monitor the security of the COR information systems, and provide information security training and awareness programs to COR employees.

   DIT is also responsible for periodically providing management with reports about the current state of information security at the COR. While information systems contingency planning is the responsibility of information Custodians, DIT must provide technical consulting assistance related to emergency response procedures and disaster recovery. DIT is also responsible for organizing a computer emergency response team to promptly respond to virus infections, hacker break-ins, system outages, and similar information security problems.

6**.** Internal Audit Department—The COR's Auditor Office periodically performs compliance checks to ensure that all parties are performing their assigned duties, and to ensure that other information security requirements are being consistently observed. The Auditor's Office acts as the eyes and ears of top management at the COR, ensuring that internal controls, including those related to information security, are consistent with both top management expectations, organizational goals, and with the Code of the City of Richmond - Charter, Section 4.18 City Auditor.

B. Information Sensitivity Classification

1. Reasons for Classification—To assist in the appropriate handling of information, a sensitivity classification hierarchy must be used throughout the COR. This hierarchy provides a shorthand way of referring to sensitivity, and can be used to simplify information security decisions and minimize information security costs. One important intention of a sensitivity classification system is to provide consistent handling of the information, no matter what form it takes, where it goes, or who possesses it. For this reason, it is important to maintain the labels reflecting sensitivity classification categories.

   The owner of information must designate an appropriate label, and the user or recipient of this information must consistently maintain an assigned label. Labels for sensitive information must be used in the subject field of electronic mail messages or paper memos. Labels for sensitive information must appear on the outside of floppy disks, magnetic tape reels, CD-ROMs, audiocassettes, and other storage media. If a storage volume such as a compact disk contains information with multiple classifications, the most sensitive category should appear on the outside label. When creating a collection of information from sources with various classifications, the collection must be classified at the highest sensitivity level of the source information.

   The COR uses four sensitivity classification categories: Public, Internal Use Only, Confidential and Secret. If information is not marked with one of these categories, it will default into the Internal Use Only category. If information falls into the Internal Use Only category, it is not necessary to apply a sensitivity label. Information that falls into the Confidential or Secret categories is designated Sensitive.

a. **Public**—Public information has been specifically approved for public release by Public Relations department or Marketing department managers. Unauthorized disclosure of this information will not cause problems for COR, its customers, or its business partners. Examples are marketing brochures and material posted to the COR web page. Disclosure of the COR inform - public requires the existence of this label, the specific permission of the information Owner, or long-standing practice of publicly distributing this information.

b. **Internal Use Only**—Internal Use Information is intended for use in the COR, and in some cases in affiliated organizations, such as COR business partners. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may cause problems for the COR, its customers, or its business partners. This type of information is already widely distributed in the COR, or it could be so distributed in the organization without advance permission from the information Owner. Examples are the COR telephone book and most internal electronic mail messages.

c. **Confidential**—Confidential information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Unauthorized disclosure of this information to people without a business need for access may be against laws and regulations, or may cause significant problems for the COR, its customers, or its business partners. Decisions about the provision of access to this information must be cleared through the information Owner. Examples are customer transaction account information and worker performance evaluation records.

d. **Secret**—Secret information is the most private or otherwise sensitive, and must be monitored and controlled at all times. Unauthorized disclosure of this information to people without a business need for access may be against laws and regulations, or may cause severe problems for the COR, its customers, or its business partners. Decisions about the provision of access to this information must be cleared through the information Owner. An example is legal information protected by attorney-client privilege.

C. Privacy

1. Expectations of Privacy—Users must have no expectation of privacy when using information systems at COR. To manage systems and enforce security, COR may log, review, and otherwise utilize any information stored on or passing through its systems. COR may capture user activity such as telephone numbers dialed and web sites visited. The COR may use any and all software, hardware, or device to monitor all material utilizing the COR's network or devices. Examples of this may include, but is not limited to, sniffers, key logging, content filtering, audit logs, et. Al.

2. Collecting Information—the COR does not collect information that is unnecessary for business purposes. COR does not collect information from third parties such as customers unless these parties are notified about the collection activities before they occur.

3. Third-Party Information Privacy—A wide variety of third parties have entrusted their information to the COR for business purposes, and all workers at COR must do their best to safeguard the privacy and security of this information. Customer account data is Confidential and access must be strictly limited based on business need for such access. Customer account information must not be distributed to third parties without advance authorization by the customer. Exceptions will be made in the case of customer incapacitation or death.

D. Viruses, Malicious Software, and Change Control

1. Virus Checking Required—Virus-checking systems approved by DIT must be in place on all PCs with operating systems susceptible to viruses, on all firewalls with external network connections, and on all electronic mail servers. All files coming from external sources must be checked before execution or usage. If encryption or data compression has been used, these processes must be reversed before the virus-checking process takes place. Users must not turn off or disable virus-checking systems.

2. If a Virus Is Detected—If users obtain virus alerts, they must immediately disconnect from all networks and cease further use of the affected computer, and call the DIT help desk for technical assistance. Users must not remove viruses on their own. If users believe they may have been the victim of other malicious software, they must immediately call the help desk to minimize the damage. User possession or development of viruses or other malicious software is prohibited.

3. Change Control—Users must not install new or upgraded operating systems or application software on PCs or other machines used to process COR information. Systems used to process COR information may be owned by the COR, but have been specifically recognized as systems used for regular business activities. This approach permits the COR to perform automatic software distribution, automatic software license management, automated remote backup, and related functions on a centralized and coordinated basis. While change control will be maintained through the above-mentioned access control packages, users can, however, change the preferences on software packages, such as the fonts for a word processing package.

E. Intellectual Property Rights

1. Legal Ownership—With the exception of material clearly owned by third parties, the COR is the legal Owner of all business information stored on or passing through in its systems. Unless the Chief Administrative Officer has signed a specific written agreement, all business-related information developed while a user is employed by the COR is COR property.

2. Making Copies of Software—Users must not make copies of or use software unless they know that the copies are in keeping with the vendor's license to the COR. If a system that is used to process COR information has been set up by the DIT, users can rely on the fact that all software on this system is licensed and authorized. Questions about licensing must be directed to DIT, which maintains documentation reflecting software licenses throughout the COR. Making regular backups of software for contingency planning purposes is permissible. DIT must remove all software that is not authorized on systems that are used to process the COR information.

3. Labeling—Users must maintain information about source, date, and usage restrictions for all information provided by third parties. These labels will be important for management decision-making purposes, and will demonstrate that the COR observed appropriate copyright and other intellectual property laws. Users must assume that all materials on the Internet are copyrighted unless specific notice states otherwise.

F. Systems Development

1. Production System Definition—Information systems that have been designated production systems have special security requirements. A production system is a system that is regularly used to process information critical to COR business. Although a production system may be physically situated anywhere, the production system designation is assigned by the DIT Operations Manager.

2. Special Production System Requirements—All software developed in-house that runs on production systems must be developed according to the DIT project management methodology. This methodology must ensure that the software will be adequately documented and tested before it is used for critical COR information. The SDM also must ensure that production systems include adequate control measures. Production systems also must have designated Owners and Custodians for the critical information they process. Information Security must perform periodic risk assessments of production systems to determine whether the controls employed are adequate. All production systems must have an access control system to restrict who can access the system and restrict the privileges available to these users.

3. Separation between Production, Development, and Test Systems—Where resources permit, there must be a separation between the production, development, and test environments. All production software testing must proceed with sanitized information where Confidential or Secret information is replaced with dummy data. All security fixes provided by software vendors must go through the systems development methodology testing process, and must be promptly installed.

   A formal and documented change control process must be used to restrict and approve changes to production systems. All application program-based access paths other than the approved user access paths must be deleted or disabled before software is moved into production.

4. User Programming—Users must not write production computer programs unless specifically authorized by the Chief Information Officer. The construction of spreadsheet formulas, automatic execution scripts that are run when a system is booted, or databases are not considered programming for purposes of this document. Both users and programmers must be careful never to embed user IDs, readable passwords, encryption keys, or other security parameters in any file.

III. RESPONSIBILITIES

All employees must promptly report to DIT any loss of, or severe damage to, their hardware or software. Workers must report all suspected compromises to the COR DIT Help Desk information systems. All serious information security vulnerabilities known to exist must be reported. All instances of suspected disclosure of Confidential or Secret information also must be reported. .All reports should be sent via email to the DIT Help Desk or called into the DIT Help Desk at 646.6367. All reports must be investigated before any action is taken. If the violation is sensitive it is to be reported DHR and to DIT Security.

Non-compliance with these and other information security requirements can result in disciplinary action up to and including termination. In rare cases, a business case for non-compliance can be established. In all such cases, the non-compliance situation must be approved in advance through a risk acceptance process. This process requires a risk acceptance memo signed by a department director and approved by the DIT CIO and the Auditor’s Office.

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

IV. DEFINITIONS

Terms	Definitions
Employees	For this policy, employees include all individuals who use the city's electronic information systems/network. e.g. but not limited to, employees, contractors, vendors, temporary agency staff, and state agencies.
Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.
Forwarded email	Email resent from an internal network to an outside point.
Chain email or letter	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Messages	This term includes e-mail (electronic-mail), Intranet bulletin boards, electronic subscription services, electronic documents, and any other forms of electronic communication.
Sensitive information	Information is considered sensitive if it can be damaging to the COR or its customers' reputation or market standing.
Virus warning	Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people, both inside and outside the COR, who do not have a need to know that information.

V. REGULATION UPDATE

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

APPROVED:

Dwight C Jones

MAYOR