

# **City of Roanoke**

## **Information Security Policies**

**October 2008**

## Table of Contents

1. Information Security Policies, Executive Summary .....	3
2. Access Review Policy .....	4
3. Anti-Virus Policy .....	6
4. Information Security Audit Policy .....	8
5. Dial-In Access Policy .....	9
6. Electronic Investigation Policy .....	10
7. Electronic Mail (E-mail) Policy .....	12
8. Electronic Storage Media Destruction Policy .....	14
9. Electronic Security and Monitoring Policy .....	16
10. Encryption Policy .....	18
11. Incident Response Policy .....	19
12. Log-On Banner Policy .....	21
13. Partner Network Policy .....	23
14. Password Policy .....	25
15. Remote Access Policy .....	30
16. Risk Assessment Policy .....	32
17. Security Awareness, Training, and Education Policy .....	34
18. Software, Copyrights, and Licensing Assurance Policy .....	36
19. Third-Party Information Technology Service Organization Policy .....	38
20. Virtual Private Network (VPN) Policy .....	41
21. Wireless Network Communication Policy .....	42

# 1. Information Security Policies, Executive Summary

## Introduction

Today's information technology (IT) offers more complicated IT environments. IT systems have become more robust over the past few years, yet the trade off is that we begin to have disparate systems that, by design, make them more difficult to manage as a collective set of systems. Each system requires staff that have training and experience in that niche. With this variety of software and hardware, and vendor competition, IT staff have had to become experts in a whole host of systems and architectures. Include in this complexity a world of "hackers" that want to be successful in the penetration of our IT systems for financial gain or notoriety.

Employees are increasingly dependent on information technology to do their jobs, so it is important to protect technology and encourage its appropriate use. Information technology has diversified over the years providing people with new ways to communicate data via voice, video, paper, and images. Because information must be protected in whatever form it takes, it is important to have information technology security policies that address the technical methods of handling information.

These Information Technology Security Policies apply to all employees, contractors, consultants, vendors, interns, volunteers and others who use the resources that are either owned or leased by the City.

## Purpose

There are four major reasons for implementing these policies; they;

- Set the stage for appropriate behavior and awareness of acceptable IT business practices;
- Help IT staff operate information-handling systems in a secure manner;
- Assist administrators and developers in the implementation and configuration of secure information-handling systems; and,
- Provide managers a means for determining whether new requirements are adhered to, or necessitate a change in, current policy.

## **2. Access Review Policy**

### **Policy Purpose**

The access review policy is intended to establish a City-wide approach to information security and to prescribe methods to help identify and prevent the compromise of information security and the misuse of City data, applications, networks and computer systems.

### **Policy Scope**

This policy applies to all City of Roanoke departments that own or manage City information systems that require security access at the department level. This policy covers authorized users. An authorized user is an individual who has been granted access to a specific system by the system administrator. The system administrator is the person responsible and accountable for a particular system. Unauthorized users are expressly forbidden from using any City owned/operated communication or Information Technology (IT) system.

### **Policy Description**

All individuals who require access to systems and information resources shall be properly identified by means of a unique personal identifier. Appropriate access control shall be introduced into every IT system which prevents intruders from entering and misusing the system and which constrains the authorized users to their legitimate purposes. Formal procedures shall be established by the owning department to define how additions, deletions, and other modifications to user access and privileges are to be performed.

Authorized users of IT systems must be aware of their responsibilities, what they are authorized to do, and they must have an expectation of detection if they abuse their privileges. Access privileges must be removed as soon as they are no longer needed.

### **Policy**

System administrators are responsible for removing the accounts of individuals who change roles within the City of Roanoke or are no longer employed by the City of Roanoke. A documented process for periodic review of the validity of current accounts must exist at the department level. Systems are subject to independent audit review and administrators must provide a list of accounts for the systems they administer when requested by authorized City of Roanoke management. System administrators must cooperate with authorized City of Roanoke management investigating security incidents.

### **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.



### **3. Anti-Virus Policy**

#### **Policy Purpose**

The purpose of the anti-virus policy is to prevent infection of the City's computers and information systems by computer viruses and other malicious code. This policy is intended to prevent major and widespread damage to user applications, files, and hardware and to prevent financial losses resulting from such damage. Virus protection will be layered in order to protect the entire enterprise from a variety of threats.

#### **Policy Scope**

This policy applies to all City of Roanoke employees, including but not limited to full-time, part-time, temporary and volunteer employees, contractors, vendors and agents, who develop, use, operate, or manage City information systems.

#### **Policy Description**

Due to today's internet-based environment, workstations, servers, and networks are being exposed to malicious code at an ever-increasing rate. Malicious code in the form of viruses, worms, backdoors, and logic bombs all pose threats to both the City's information systems and reputation. Virus-checking programs are an integral component in today's network security architecture. Virus checkers monitor workstations and servers and look for various forms of malicious code. A common problem with a virus solution is that the entire enterprise must be protected for the anti-virus program to be completely effective. A single workstation, without anti-virus protection, could serve as a "back-door" for a malicious program and could eventually damage the entire enterprise.

The perimeter boundary of the network will be protected from viruses by installing anti-virus applications on the servers to protect the network from malicious code. Also, the City will scan e-mail and will block Internet traffic from known virus-producing sites. This way, the majority of viruses can be stopped before reaching the users.

#### **Policy**

It is City policy that:

- All systems, workstations, servers, and laptops will have virus-checking software with virus signatures designated current by the Department of Technology (DoT).
- Only the virus-checking applications approved and operated by DoT will be used.
- Only City authorized equipment will be connected to the City's network.
- Updates for the virus signatures will come from DoT. Only updates approved and delivered by DoT will be allowed on the system.
- The virus-checking program WILL NOT be disabled unless maintenance is being performed on the system or software is being installed/upgraded. Any user who disables the virus-checking program will be in violation of Administrative Procedures and Section

5.8 of the Technology Security Policy, and subject to appropriate disciplinary actions as per C.1 Human Resources, Discipline and Termination.

- Viruses could hide in executables that are downloaded from the Internet. If a software product that is only available via the Internet is required by a department for City business, the Help Desk (853-2144) should be contacted for assistance in acquiring the software.
- Removable storage media will be scanned whenever it is inserted into a workstation or server. Documents, spreadsheets, and data received from outside the City should be scanned on first use.
- All virus-related incidents shall be reported to the Help Desk (853-2144). Individual encryption systems that bypass the e-mail server's virus-checking capability are not authorized on City workstations.
- All backups will be scanned prior to restoration. Newly restored files should always be scanned with an anti-virus program with current signatures before putting the files into operation.
- No user shall knowingly store, copy, save, or transmit virus-infected files on the City's network. Infected files that are quarantined on a workstation should be removed after virus incident investigations.
- Peer-to-Peer (P2P) applications, that share files or allow access to City-owned computers from the Internet, are not allowed.

## **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

## **4. Information Security Audit Policy**

### **Policy Purpose**

To provide the policy for the Municipal Auditing Department to conduct information security audits of City of Roanoke, Virginia information systems.

Information security audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible information security incidents
- Ensure conformance to the City's information security policies
- Monitor user or system activity, where appropriate

### **Policy Scope**

This policy applies to all City of Roanoke employees, including but not limited to full-time, part-time, temporary and volunteer employees, contractors, vendors and agents, who develop, use, operate, or manage City information systems. This policy covers authorized users. An authorized user is an individual who has been granted access to a specific system by the system's administrator. This policy covers all computer and communication devices owned by the City and devices that are present on City premises. Examples of this include Telecommuting and Remote access, from home or by vendors.

### **Policy Description**

When performing an information security audit, any access needed shall be provided to Municipal Auditing and may include access to.

- Any computing or communications device at the user level and/or system level
- Information (electronic, hardcopy, etc.) that may be produced, transmitted, or stored on City equipment or premises
- Work areas (labs, offices, cubicles, storage areas, etc.)
- Interactively monitor and log traffic on any City network

### **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

## **5. Dial-In Access Policy**

### **Policy Purpose**

The purpose of this policy is to protect the City's electronic information from being inadvertently compromised by authorized personnel using a dial-in connection. Dial-in access should be the method of last resort. Alternative methods shall be used to phase out dial-in capabilities.

### **Policy Scope**

This policy applies to all City of Roanoke employees, including but not limited to full-time, part-time, temporary and volunteer employees, contractors, vendors and agents, who develop, use, operate, or manage City information systems. The scope of this policy is to define appropriate dial-in access and its use by authorized personnel. Dial-in access is defined as a type of remote access that is originated from a remote computer using a modem and telephone line to connect to the City's remote access devices.

### **Policy Description**

City employees and authorized third parties (vendors, etc.) can use dial-in connections to gain access to the City network. Dial-in access should be strictly controlled, using password authentication and, if necessary, dial-back. Modems should be disconnected at all times unless prior notice is given to allow a dial-in access connection.

Dial-In access using personal home computers or laptops will not be supported.

It is the responsibility of employees with dial-in access privileges to ensure that a dial-in connection to the City is not used by non-employees to gain access to City information system resources. Employees who are granted dial-in access privileges must remain constantly aware that dial-in connections between their location and the City are literal extensions of the City network and that they provide a potential path to the organization's most sensitive information. The employee and/or authorized third-party individual must take every reasonable measure to protect City assets.

### **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

## **6. Electronic Investigation Policy**

### **Policy Purpose**

The City of Roanoke maintains policies and procedures for the authorized use of computing resources. The Department of Technology (DoT) is charged with investigating suspected misuse of these resources by entities both internal and external to the organization. This policy outlines the method by which an investigation by DoT into suspected misuse may be requested.

### **Policy Scope**

This policy applies to all City of Roanoke employees, including but not limited to full-time, part-time, temporary and volunteer employees, contractors, vendors and agents, who develop, use, operate, or manage City information systems. A system which may be investigated includes all computer and communication devices owned or operated by the City of Roanoke.

### **Policy Description**

This policy is meant to be a general guideline. Investigations will typically be categorized as an analysis into the conduct of people or of system behavior. Any investigation requested by a department into the conduct of a person or persons will require the approval of the requesting department director. In some cases, DoT may elect to begin an investigation prior to department director approval if time is of the essence. In such instances, the department director will be informed as soon as possible.

### **Computer Evidence**

- Computer evidence is represented by, but not limited to, physical items such as chips, boards, central processing units, storage media, monitors, and printers.
- Computer evidence may be latent, and only stored in an electronic form on physical devices.
- Computer evidence is a product of the data stored, the application used to create, store and/or recover it, and the computer system that directed these activities.

### **Requesting Investigations**

- If an employee suspects misuse of the City's computing resources, he or she should have the suspected employee's department director send a written request to the Director of Technology. This may be in the form of e-mail or Inter-Office mail.
- A brief description of the suspected misuse including details of dates, times, users and systems should be included in this request.
- DoT will perform an investigation into the suspected misuse and report to the department. Depending on the findings, other City departments or external law enforcement agencies may be briefed as well.
- Any person who has concerns about the operation of a system should contact the Help Desk (853-2144).

## **Investigation Methodology**

All investigations by DoT will be performed with integrity and confidentiality. Adherence to best practices and industry standards will be maintained where possible.

## **Extracting Evidence**

Whenever possible, the examination will be conducted on copies of the original evidence, in order to protect the original evidence from accidental or unintentional damage or alteration. This principal is predicated on the fact that digital evidence can be duplicated exactly to create a copy that is true and accurate. DoT shall make a decision as to the reliability of copying, and ensure that it is true and accurate on a case-by-case basis.

## **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

## **7. Electronic Mail (E-mail) Policy**

### **Policy Purpose**

This policy defines how City e-mail communications are to be used in a professional manner for City purposes. In addition, it defines how City e-mail communications are to be secured to (1) prevent unauthorized access, (2) prevent unintended loss or malicious destruction of data, and (3) provide for the integrity and availability of all e-mail systems.

### **Policy Scope**

This policy applies to all City of Roanoke employees, including but not limited to full-time, part-time, temporary and volunteer employees, contractors, vendors and agents, who develop, use, operate, or manage City information systems.

### **Policy Description**

City information technology resources, including Electronic Mail are to be used for City business purposes. The City reserves the right to access any user's system and the information stored therein, and users should not consider any of the material transmitted via network resources or stored in network resources to be private. Agency and department directors are responsible for the appropriate use of network resources in their departments/agencies.

Access to e-mail services is a privilege that may be wholly or partially restricted without prior notice and/or without consent of the user.

All e-mail messages are the property of the City and subject to review by authorized City personnel. Staff cannot expect a right to privacy when using the City e-mail system. E-mail is subject to retention policies as stated in the Library of Virginia Records Retention and Disposition Schedule and can be reviewed at:

[www.lva.lib.va.us/whatwedo/records/sched\\_local/GS-23.pdf](http://www.lva.lib.va.us/whatwedo/records/sched_local/GS-23.pdf)

E-mail is subject to the policies concerning other forms of communication as well as all other applicable policies including, but not limited to, confidentiality, conflict of interest, general conduct and sexual harassment.

E-mail services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on the e-mail system or unwarranted or unsolicited interference with others' use of e-mail or the e-mail system. This includes misusing mailing lists, propagating chain letters, spamming or distribution of unwanted mail and resource hogging.

Encryption of e-mail may be appropriate in some instances to secure the sensitive contents of an e-mail message. Encryption must follow the City's Encryption Policy.

### **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures.

Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

## **8. Electronic Storage Media Destruction Policy**

### **Policy Purpose**

This policy establishes requirement regarding the disposal of electronic media in order to meet confidentiality and privacy requirements. The overall goal of this policy is to protect the City and the public from unauthorized release of data.

### **Policy Scope**

This policy applies to all City of Roanoke employees, including but not limited to full-time, part-time, temporary and volunteer employees, contractors, vendors and agents, who develop, use, operate, or manage City information systems. This only pertains to electronic information.

### **Policy Description**

This policy requires that all electronic storage media (i.e., floppy disks, Zip disks, optical (CD-ROM/RW/DVD, etc.), tapes, hard drives, embedded memory systems (routers, switches, PDA, key fobs, smart cards, etc.)), be erased or destroyed before any transfer, disposal, or surplus occurs. Media that contains sensitive data (privacy, financial or personal health information (PHI)) must be destroyed before disposal.

### **Destruction Procedures**

Destruction of hard drives, tapes, floppy disks, and other electronic storage media will prevent sensitive information from being obtained from equipment that is being removed from service. Acceptable means to destroy rigid magnetic media such as floppy disks, hard drives, CD-ROM, DVD-ROMs, and tapes are described below.

- Destruction by bulk degaussing. Tapes, diskettes, hard drives, and other electronic storage media can be “wiped-clean” by a degausser. Degaussing renders the media un-useable for future use. Degaussing should only be performed by individuals who are familiar with the degaussing equipment.
- Physical destruction/impairment beyond reasonable use. Floppy disks and CDs/DVDs can be shredded by DoT Operations.
- Optical mass storage media, including compact disks, optical disks, and magneto-optic disks (MO) must be destroyed by burning, pulverizing, or grinding the information-bearing surface. Burning shall be performed only in a facility certified for the destruction of materials.
- Operational computer workstations will be reimaged with a generic Operating System image and prepared for sale, donation, or disposal by any other means deemed appropriate.
- All destruction of the media covered by this policy shall be done in a manner that is consistent with all applicable laws, rules, and ordinances at the federal, state and local levels and in a environmentally safe manner.

You can contact the Department of Technology through the Help Desk (853-2144) if you require assistance in destroying electronic media.

### **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

## **9. Electronic Security and Monitoring Policy**

### **Policy Purpose**

Employees of the City are provided access to telephones, voicemail, computers, e-mail, networks, internet systems, fax machines, and electronic devices for the purpose of performing their job-related duties.

### **Policy Scope**

This policy applies to all City of Roanoke employees, including but not limited to full-time, part-time, temporary and volunteer employees, contractors, vendors and agents, who develop, use, operate, or manage City information systems.

### **Policy Description**

All City employees who are entrusted with any City facilities or equipment, including, but not limited to computers, e-mail, network, internet, electronic devices and voice systems, are prohibited from using such assets for an improper purpose.

Improper purpose includes, but is not limited to the following,

- Sexual, racial, or any other form of harassment against any person
- Pornography
- Personal use of any equipment that interferes with an employee's productivity and job performance;
- Unauthorized disclosure of the City's confidential information
- Employee theft or violation of any law
- Solicitation of any kind
- Any other use of City computers or other equipment that is not related to City business or that is deemed, in the sole discretion of the City, to be inappropriate and inconsistent with City policies.

E-mail and Internet access is provided for City business use only; use for informal and/or personal purposes is permissible only within reasonable limits. All e-mail records are considered City records and should be transmitted only to individuals who have a business need to receive them. Those who have personal/confidential matters to communicate should, to assure privacy, not use City computers or equipment, including fax machines.

Additionally, the City e-mail/internet records are subject to disclosure to law enforcement or government officials or to third parties through subpoena or other processes. Consequently, one should always ensure that the business information contained in these messages is

accurate, appropriate, and lawful.

The City reserves the right of immediate access to any City-owned equipment, including all information stored on any City computer or phone system, upon reasonable concern that the employee entrusted with such equipment is using it for an improper purpose. The City also reserves the right to conduct random reviews of employees' computers, e-mail, and voicemail systems for the purpose of ensuring that this equipment is being used for the business purposes for which it is intended and not for any improper purpose.

Consistent with the above, City employees may not expect or assert a right of privacy in connection with any City-owned assets. E-mail and voicemail messages and internet records are to be treated as shared paper files, with the expectation that anything in them is available for review by authorized City representatives.

Each employee's computer password and any other confidential access code must be kept confidential and never shared with anyone.

Employees are prohibited from accessing other employees' e-mail and voicemail files and computers, except as specifically authorized.

Providing any non-authorized person with access information or permitting such persons the use of City computer equipment is prohibited.

Entering false or unauthorized information into a computer or altering data with false and/or unauthorized information is prohibited.

Making any modification to City computer equipment, system files, or software without specific authorization is prohibited. Modification includes the installation of any software on any City equipment.

## **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

# 10. Encryption Policy

## Policy Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that proper key management is enforced for all approved crypto-systems.

## Policy Scope

This policy applies to all City of Roanoke employees, including but not limited to full-time, part-time, temporary and volunteer employees, contractors, vendors and agents, who develop, use, operate, or manage City information systems.

## Policy Description

Standard algorithms should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Symmetric crypto-system key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength.

Implementation of encryption systems must be reviewed by DoT.

## Enforcement

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

## Definitions

Terms	Definitions
Symmetric cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric cryptosystem	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

# 11. Incident Response Policy

## Policy Purpose

This plan provides policy and procedures for reporting and responding to computer security incidents and the disclosure of sensitive information. These are the minimum required policies and procedures to handle and report unauthorized network activity and security incidents. Incidents may include the disclosures of sensitive information, malicious logic, and intrusions.

## Policy Scope

This policy applies to all City of Roanoke employees including but not limited to full-time, part-time, volunteer, temporary employees, and City of Roanoke employed contractors, who develop, use, operate, or manage City information systems.

## Policy Description

Information incidents include but are not limited to:

- Attempted entry (failed or successful) to gain unauthorized access to a system or data
- Unexplained disruption or denial of service
- Unauthorized use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- Poor security practices such as exposure of passwords, etc.
- A disclosure of sensitive information

Incidents will be reported to the Help Desk (853-2144). The Help Desk will report the incident to the Security Technician and/or the Technical Support Administrator. Depending on the severity of the incident a report will be given to the Director of Technology.

## Policy Responsibilities

It is the responsibility of all staff to adhere to City of Roanoke security policy and promptly report information security incidents as defined in this policy.

## Users

- Report all unintended disclosures of sensitive information.
- Report unauthorized network activities or incidents, which includes all forms of malicious logic.
- Whenever possible, work to prevent the disclosure of sensitive information.

## **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

## 12. Log-On Banner Policy

### Policy Purpose

The purpose of this policy is to advise users of their responsibilities when accessing City and Department of Technology (DOT) systems.

### Policy Scope

This policy applies to all City of Roanoke employees including but not limited to full-time, part-time, volunteer, temporary employees, and City of Roanoke-employed contractors, who develop, use, operate, or manage City information systems. This policy covers authorized users. An authorized user is an individual who has been granted access to a specific system by the system's administrator. Unauthorized users are expressly forbidden from using all City owned/operated communication or DOT systems.

### Background

In general, legal opinion is that people have to be aware of limitations and penalties before they can be held accountable. Therefore, to establish a reasonable expectation that users have been notified of the existence of acceptable usage expectations, to limit the expectation of user privacy, and to be able to prosecute violators, the City established a Log-on Banner that notifies users of these limitations. The U.S. Department of Justice has made the following recommendations on what should be included in such a warning.

- The word WELCOME should not appear in the first log-on screen. This could imply that anyone is welcome to access and use the system. Understand, this does not mean that every screen accessing each application needs this warning, only the first screen seen by anyone accessing a City platform (e.g., stand-alone personal computers, network).
- The warning should:
  - Advise users that they are subject to having their activities monitored and that use of the system implies consent to such monitoring.
  - Inform users that information gathered may be given to law enforcement or other investigative officials for action, if warranted.
  - Inform users of the consequences of inappropriate use/access.
  - Require users to acknowledge the warning by some positive action on their part, like a keystroke.

### Policy Description

This document establishes City policy that all communications equipment capable of displaying system messages must display, as the first message seen by the user, a warning that the system being accessed is a City information system, and that access is for official use only.

The following banner contains all the necessary elements (see **Background** above). This is the

City's standard Log-on-warning banner.

*“This system of computers and networks are owned by the City of Roanoke. Its use is restricted to authorized individuals to perform official city business. By virtue of use of this system all users agree to be bound by the **Electronic Security and Monitoring Policy of the City of Roanoke**. Users have no explicit or implicit expectation to privacy of data created, stored, or transferred using this system. All users consent to data being monitored, audited, logged, recorded, and disclosed by authorized employees of the City of Roanoke.*

*Your use of this system indicates your consent and acceptance of these terms. If you do not agree to the terms set forth above you should immediately disconnect. Administrative, criminal, and civil penalties may be sought for violation of this agreement. Direct all questions concerning this agreement to the help desk of the Department of Technology.”*

## **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

## **13. Partner Network Policy**

### **Policy Purpose**

This policy governs the permanent connection of foreign networks for access to the City of Roanoke, Virginia Network. In an effort to conserve fiscal and human resources it may become necessary to allow users, systems or networks from non-City (foreign) agencies to connect to internal resources for the purpose of application and/or data sharing. The City must take appropriate precautions to protect the confidentiality, integrity and availability of its computing infrastructure. As such, each system to be connected to the Partner Network must go through a thorough analysis and review by DoT and stakeholder department(s).

### **Policy Scope**

Any system connected to the Partner Network must abide by the requirements set forth in this policy and the applicable Third Party Agreement (TPA) between the City and the partner organization. These documents must be signed on behalf of the City by the Director of Technology or the Assistant Director of Technology and the responsible authority at the connecting agency.

### **Policy Description**

To comply with this policy, prior to a system or network being connected to the City of Roanoke network, the DoT Technical Support Administrator and at least one of the following, a DoT Analyst, the DoT Assistant Director or the DoT Director, must provide written or email authorization. This authorization must be obtained prior to any system being connected to the Partner Network.

In emergency situations where primary City business will be affected, connection can be made with oral authorization. In these cases, written or email authorization must be documented within 24 hours of the incident.

### **Establishing Connectivity**

All connectivity established must be based on the least-access principle, in accordance with approved business requirements and security best practices. In no case will the City rely on the third party to protect the City network or resources.

### **Modifying or Changing Connectivity and Access**

All changes in access must be accompanied by a valid business justification and are subject to security review. Changes are to be implemented via the approved change management process. The sponsoring organization within the City is responsible for notifying DoT when there is a material change in the information originally provided so that security and connectivity evolve accordingly.

### **Terminating Access**

When access is no longer required, the sponsoring organization within the City must notify the

Help Desk (540-853-2144). This may mean a modification of existing permissions up to terminating the circuit, as appropriate.

### **Auditing Access**

Yearly, a review will be made by the DoT Security Team to ensure existing connections are still needed and the access provided meets the needs of the connection.

Connections that are determined to be no longer of value and/or are no longer being used to conduct City business will be terminated within 8 business hours. Reauthorization for all connections must be established via writing or email from the DoT Security Officer and at least one of the following, a DoT Analyst, the DoT Assistant Director or the DoT Director.

### **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

### **Definitions**

Terms	Definitions
Circuit	For the purposes of this policy, circuit refers to any method of network access, whether it is through traditional ISDN, Frame Relay, etc., via VPN/Encryption technologies, or another other technology/protocol.
Sponsoring organization	The City organization that requested the third party have access into the City's information system.
Third party	A business that is not a formal or subsidiary part of the City.

## **14. Password Policy**

### **Policy Purpose**

The password policy is intended to assist employees of the City of Roanoke in determining how to create a proper password, how and when to change passwords, and whom to contact to report problems with their password.

### **Policy Scope**

This policy applies to all City of Roanoke employees including but not limited to full-time, part-time, volunteer, temporary employees, and City of Roanoke-employed contractors, who develop, use, operate, or manage City information systems. This policy covers authorized users. An authorized user is an individual who has been granted access to a specific system by the system's administrator. Unauthorized users are expressly forbidden from using any City owned/operated communication or Information Technology (IT) system.

### **Policy Description**

In order for an individual to gain access to the City of Roanoke's Information Systems (IS), they must authenticate their identity to the system. Users identify themselves to the system through the use of a unique user identification code or UserID. The UserID can be authenticated (or proved) by providing the correct password.

All City-owned/operated IS shall require users to identify themselves before performing any actions that are governed under system security. The IS shall use a protected mechanism (i.e., password) to authenticate the user's identity. The IS shall protect authentication data so that any unauthorized user cannot access it. The IS shall be able to enforce individual accountability by providing the capability to uniquely identify each individual user. The IS shall also provide the capability of associating this identity with all auditable actions taken by that individual.

### **Policy**

#### **System-level password**

An initial user network account shall be requested from DoT (the form is available on the Lotus Notes Portal, Technology Tab). A random password will be sent via Interoffice Mail to the new user. The first time the new user logs into the network, he/she shall be forced to change the random password. The same password should not to be used for a City account that is currently being used for a personal account or those of related City business (i.e., State and Federal systems).

#### **Application password**

When assigning a password for an application, one should not use the "remember password" feature of the application. Different passwords should be set for each application accessed. All City workstations will be configured, as a default, to not store any application passwords on the system.

Certain applications assign a known-default password to allow users to start and setup the application. These default passwords should be changed the first time the user logs onto the new application.

## **Application Development Standards**

Applications developers should ensure that their programs contain the following security precautions:

- Support authentication of individual users, not groups.
- Store no passwords in clear text or an easily reversible form.
- Provide for some type of role-based management.
- Support a strong authentication process such as RADIUS, Kerberos, and/or X.509 Certificates with LDAP security retrieval whenever possible.

## **Auditing Passwords**

The DoT Security Technician may perform periodic password auditing to look for missing or easily-guessed passwords. Only DoT is authorized to perform these audits on the City's network. Missing or weak passwords will be replaced with acceptable passwords.

## **General Password Construction Guidelines**

### **Password Length**

Passwords shall be at least 7 characters in length. Passwords shall use alphanumeric characters, be case-sensitive, and shall not contain common names, dictionary words, foreign words, date of birth, or any information closely associated with the user. The network shall protect passwords and automatically perform password administration so only each user has knowledge of his own password.

### **Password Aging**

All users shall change their password at least every 60 days. Network administrators shall change their password at least every 60 days. The network administrator shall have the ability to override these defaults and change password-aging rules to meet new requirements. The network administrator shall also have the capability to expire passwords. Once expired, the system shall require the user to enter a new password if the UserID is still active. In all cases, for each password change, an audit record shall be created indicating the UserID, action (e.g., change password), time, and workstation or terminal identification. Password strings shall not be written to the audit log.

### **Account Lock-Outs**

Where possible, the system shall limit the number of consecutive incorrect access attempts by a UserID to no more than 3 and shall automatically deactivate the UserID after the 3rd unsuccessful log-on attempt. The system's action to deactivate a UserID shall affect only that UserID and shall not disable or otherwise affect the workstation or a different user who attempts to use the workstation. In recording the number of consecutive unsuccessful attempts for a specific UserID prior to reaching the lock-out threshold, the system shall reset the number

to zero (0) only after a successful log-on.

## **Password Protection**

The system shall protect passwords so an unauthorized agent cannot access them. Passwords shall not be written down nor stored in a human-readable form. System passwords shall be cryptographically protected within the system and when transmitted over a network or communications link (e.g., from workstation to the host). Only the network administrator shall have deletion rights to system-maintained password files.

## **Password Protection Standards**

Network users will enter their UserID and password when the log-on screen appears. The actual password will be masked and not appear on the screen when typed. Except for the system identification and warning banner, no information shall be displayed or other actions occur until after successful log-on.

Users shall not disclose their password to anyone. Users shall be responsible for actions attributed to the misuse of their UserID and password. If a user feels that his password has been disclosed to another individual, they shall change it immediately and notify the Help Desk. Passwords will be safeguarded so they cannot be inadvertently disclosed or retrieved. Specifically, passwords should not be part of unencrypted computer files, programmed into function keys, posted under keyboards, left in desk drawers, or any other area. Further, passwords will not be part of log-in script files, batch files, or any other method that automatically logs a user into a system. All holders of any access means may be accountable for unauthorized use of network resources due to disclosure on their part. No supervisor or IS administrator shall require a user to divulge their password. Any such request should be reported to the DoT Help Desk.

All default and initial passwords shall be changed immediately from operating systems and applications. If they cannot be changed, the account shall be rendered inactive. Passwords shall be made invalid and destroyed by the system after they have been inactive for a period of 30 days. Further, accounts will be disabled immediately if a user's access is removed for reasons of current or pending punitive action, or if the user's access is suspended. Any standard systems group or vendor-supplied default passwords shall be removed at system installation time. Accounts will be disabled as soon as employment ends.

Default passwords shall not be used. Passwords changed by the system administrator shall be invalidated at the first log-on after the change such that the user is immediately prompted for a new password.

## **Changing One's Own Password**

All users shall change and generate their own personal passwords, conforming to the guidelines in this document. When generating a new password, users shall not use a variation or something that closely resembles the previous password, such as reversing the order of characters, adding a one-digit prefix or suffix (e.g., OLDUSER becomes OLDUSER1), or variations of any UserID or user name. The new password should be completely different

from the last and not resemble any of the last 8 passwords used. The system should encrypt and store the last 8 passwords for each user. When prompted for a new password, the system should require it be entered twice.

## **Requesting a Password Change**

A user who has forgotten his password or has had his account locked will have to request that the account be unlocked or the password be changed by the Help Desk (853-2144). The user can phone in the change request, however, the Help Desk will call the user at their work number to verify their identity. If the user cannot authenticate his identity over the phone, he will have to appear in person with his City ID badge to request a password change.

## **Password Characteristics**

Passwords are used for various purposes at the City. Some of the more common uses include: user level accounts, web accounts, e-mail accounts, screen saver protection, voicemail password, and local router log-ins. Since very few systems have support for one-time tokens (i.e., dynamic passwords that are used only once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than 4 characters.
- The password is a word found in a dictionary (English or foreign).
- The password is a common usage word, such as: football
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The word <Roanoke> or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret). Strong passwords have the following characteristics:
  - Contain both upper and lower case characters (e.g., a-z, A-Z).
  - Have digits and punctuation characters as well as letters, e.g., (0-9, !@#\$%^&\*()\_+|~=\`{ } [ ] ; ' < > ? , . /). (Note: Not all systems allow for the use of these characters).
  - Are not a single word in any language, slang, dialect, jargon, etc.
  - Are not based on personal information, names of family, etc.
  - Passwords should never be written down (unless store in a locked safe for recovery purposes) or stored on-line. An attempt should be made to create passwords that can be easily remembered yet hard to guess. One way this can be done is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: “This May Be One Way To Remember” and the password could be: “TmB1w2R!” or “Tmb1W>r~” or some other variation.

## **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a

minimum, to disciplinary action in accordance with the City’s Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City’s Administrative Procedures.

**Definitions**

Terms	Definitions
RADIUS	Remote Authentication Dial-In User Service.
X.509	The most widely used standard for defining digital certificates.
LDAP	Lightweight Directory Access Protocol.

## **15. Remote Access Policy**

### **Policy Purpose**

The purpose of this policy is to define standards for connecting to the City of Roanoke's network remotely. These standards are designed to minimize the potential exposure such as loss of sensitive or confidential data and damage to City's public image, and information systems.

### **Policy Scope**

This policy applies to all City of Roanoke employees including but not limited to full-time, part-time, volunteer, temporary employees, and City of Roanoke employed contractors, who develop, use, operate, or manage City information systems. An authorized user is an individual who has been granted access to a specific system by the department of technology per individual department's approval.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, wireless, and cable modems.

### **Policy Description**

Remote access is granted for authorized City work only.

- All remote access to City's network will be accomplished via a secure remote access method (i.e., strong authentication, Virtual Private Network (VPN), controlled dial-in/dial-out, firewall demilitarized zone (DMZ).
- Access from a remote site to the City network that contains sensitive or restricted information requires extended identification and authentication procedures.
- All employees accessing the City network from remote hosts will use City-provided equipment and will exercise due diligence in ensuring that their systems (both hardware and software) are free from computer viral infection and unauthorized use.
- When an authorized user leaves City employment or transfers to another City department, office or agency, all existing remote access services will be terminated. Remote access will have to be re-justified and re-established for any new City position. City-owned hardware must be returned to the City.

Please review other chapters of the City of Roanoke Information Security policies for details of protecting information when accessing the City network remotely, and acceptable use of the City's network.

## **Policy Implementation Responsibilities**

Responsibility for implementation of this policy is as follows:

### **Department of Technology's Responsibilities:**

- Ensure that policy documents and associated guidelines for remote access usage reflect the City's mission, goals, and values.
- Provide liaison with other departments regarding remote access usage.
- Manage the infrastructure for remote access for City authorized users.
- Determine the risk of remote access and implement acceptable, approved solutions to manage the risk.

### **Departmental Responsibilities:**

- Ensure that all City and departmental remote access policies and guidelines are implemented and reviewed for compliance.
- Manage and approve end-user business case requests for remote access and resources.
- Notify DoT when remote access is no longer required for a specific employee.

### **End-user Responsibilities:**

- Follow City and departmental policies, practices, and guidelines as they relate to remote access.
- Follow City and departmental policies regarding information disclosure.

## **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

## **16. Risk Assessment Policy**

### **Policy Purpose**

The purpose of this policy is three-fold. First, the policy identifies and authorizes individuals charged with the responsibility of assessing risk for the City of Roanoke's information systems. Second, it identifies the security policies and procedures to be enforced in order to initiate appropriate remediation. Third, it requires periodic information security risk assessments for the purpose of determining areas of vulnerability for those information systems.

### **Policy Scope**

The Department of Technology may conduct risk assessments on any City of Roanoke information system. This includes but is not limited to any information system, application, server, network, facility, and/or any process/procedure by which these systems or facilities are administered and/or maintained.

### **Policy Description**

The performance of risk assessment is an important business function that identifies and secures vulnerabilities within an information system's environment.

The execution, development, and implementation of vulnerability remediation require the full cooperation of the Department of Technology and the user department. It is the joint responsibility of the Risk Assessment Team (as defined below) and those responsible for the area being assessed to perform effective remediation.

Furthermore;

- The Department of Technology and Municipal Auditing will appoint the members of the Risk Assessment Team for a specific information system.
- All risk assessment findings will be documented and provided to the parties identified at risk assessment commencement. All risk assessment findings are confidential.
- Identified vulnerabilities will be assessed for criticality. Vulnerabilities that endanger the City's resources shall be remediated immediately.

### **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.



# 17. Security Awareness, Training, and Education Policy

## Policy Purpose

Security Awareness Training and Education (SATE) is key to eliminating the City's exposure to both malicious threats and accidental errors and omissions. SATE is not only defined as industry best practices, it is also a statutory requirement for dealing with sensitive information such as defined in the Health Insurance Portability and Accountability Act (HIPAA). This policy sets forth a minimum standard for SATE to reduce the City's risk. Each department is responsible for ensuring that all employees are trained to at least this minimum standard. In certain situations it will be necessary for departments to provide additional training.

A secondary purpose of SATE is to document employees' knowledge and understanding of policies and procedures, allowing for development of good working habits and disciplinary action when required.

## Policy Scope

This policy applies to all City of Roanoke employees including but not limited to full-time, part-time, volunteer, temporary employees, and City of Roanoke-employed contractors, who develop, use, operate, or manage City information systems.

## Policy Description

The term "Security Awareness" is considered the daily "moment-by-moment" awareness level while the term "Security Training" relates to the basic training all employees need to build their basic security skills. Security Awareness is partially a by-product of training, but is also the result of environmental factors.

Most City employees only need the minimum level of security training as follows:

- Incorporate basic security training for all new hires.
- Include in the training curriculum awareness of "social engineering" techniques that hackers use to gather information.
- Explain to employees that their departments are the "owners" of the data and they need to assist DoT in its safekeeping.
- Explain to employees the difference between "public" records and the need to keep some information "confidential."
- Review Administrative Procedure #5.8 (Technology Security Policy) and explain why it is needed.
- Define user's responsibilities.
- Define how violations will be handled.

## **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

# **18. Software, Copyrights, and Licensing Assurance Policy**

## **Policy Purpose**

This document provides guidance and procedures for implementing controls over copyrighted computer software throughout the City of Roanoke, Virginia. Most software available for use on City computers is protected by federal copyright laws. The City is not exempt from the laws governing copyrights. In addition, software is normally protected by a license agreement between the purchaser and the software owner. The software provided through the City for use by employees, volunteers, and contractors may be used only on computing equipment as specified in the various software licenses.

## **Policy Scope**

These guidelines apply to all City of Roanoke, Virginia employees, City employed contractors, and volunteers, who develop, use, operate, or manage software applications on City owned or operated computers.

## **Policy Definition**

It is the policy of the City of Roanoke, Virginia to respect the copyright protections given to software owners by federal law. It is against City policy for employees, volunteers, and contractors to copy or reproduce any licensed software on City computing equipment, except as expressly permitted by the software license. Unauthorized copies of software may not be installed by individuals on City-owned computers. City-owned software may only be installed on City-owned or authorized equipment.

No software may be installed, copied, or used on City of Roanoke, Virginia information systems except as permitted by the owner of the software and by law. Unauthorized use of copyright-protected material (including, but not limited to, graphic images, movies, music, and software) is a serious matter and is a violation of federal law. Any individual who reproduces and/or distributes copyrighted material without permission and in excess of "fair use" may be at risk for the penalties of copyright infringement.

Given the above statements, the City prohibits the illegal use of software and/or violations of software license agreements.

## **General Responsibilities**

### **The Department of Technology shall:**

- Develop and implement a plan to ensure City-wide compliance with all laws covering software.
- Install software, inventory existing software, and maintain software on servers and workstations.
- Monitor the City's implementation of these procedures.
- Ensure compliance with these policies.
- Investigate reports of license violations and other infringements.

### **Users shall**

- Use software according to this policy.
- Not download or store any software products on City-owned workstations or servers, for which the City does not have a valid license to use.
- Not install any software without prior authorization from DoT.

### **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

### **Definitions**

Terms	Definitions
Copyright	A copyright is a body of legal rights that protect creative works from being reproduced, performed, or disseminated by others without permission.
Software License Agreement	A software license agreement is a legal contract between a software application author or publisher and the user of that application.

# **19. Third-Party Information Technology Service Organization Policy**

## **Policy Purpose**

This document describes information security requirements for third-party information technology (IT) service organizations that engage with the City. A third-party IT service organization is defined as an organization that manages and delivers application capabilities to multiple entities from a data center across a wide area network (WAN), such as application service providers (ASPs) and hosting service organizations (HSOs), or supports applications or systems that are physically located at City facilities through either remote access or local connections.

## **Policy Scope**

This policy applies to any use of third-party IT service organizations by any City department.

## **Policy Description**

### **Requirements of Project-Sponsoring Organization**

The project-sponsoring organization must first establish that its project is appropriate for third-party service and must confirm that the chosen vendor complies with this policy. If the system or application is to be outsourced, a risk assessment must first be completed to determine what necessary controls must be implemented.

### **Requirements of the Third-Party IT Service Provider**

The Third-Party IT Service Provider, if providing hosting services, must agree to share description of policies and controls that will be utilized to protect the City's information. The Third-Party IT Service Provider must also regularly have an independent audit performed to ensure compliance with those policies and proper implementation of controls.

All Third-Party IT Service Providers must be in compliance with existing City security policies, including the Remote Access Policy.

The Third-Party IT Service Provider will ensure that any computers or systems connected to City computers, networks or systems will be patched to the vendor's recommended level and be scanned for viruses with the most recent signatures available. The Third-Party IT Service Provider will not use any remote control software that is disallowed by City policy, unless otherwise agreed upon.

## **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

## Definitions

Terms	Definitions
Application Service Provider (ASP)	ASPs combine hosted software, hardware and networking technologies to offer a service-based application, as opposed to a City-owned and operated application.
Project-sponsoring organization	The group within the City that wishes to use the services of an ASP.

## **20. Virtual Private Network (VPN) Policy**

### **Policy Purpose**

The purpose of this policy is to provide guidelines for Remote Access through Virtual Private Network (VPN) connections to the City's trusted network. This policy will cover single connections from an individual workstation to the City's network. This policy does not cover point-to-point VPN connections (branch to branch tunnels) between two networks.

### **Policy Scope**

This policy applies to all City employees, contractors, consultants, temporary, and other workers, including all personnel affiliated with third parties using VPN to access the City's enterprise network.

### **Policy Description**

- Approved City employees and authorized third parties (visitors, vendors, etc.) may take the benefits of VPN. The user is responsible for providing the connection between the computer and the City's VPN device namely the Internet connect. Further details may be found in the Remote Access Policy.
- It is the responsibility of all users with VPN privileges to ensure that unauthorized users are not allowed access to the City owned computers or resources.
- VPN access will be controlled using assigned user IDs and passwords.
- When connected to the City network via VPN, only authorized traffic to and from City resources will travel through the VPN tunnel and all other traffic will be dropped or directed to user's Internet connection.
- VPN gateways will be set up and managed by DOT.
- All computers connected to the City's internal networks via the VPN must have up-to-date security patches and approved anti-virus software with up-to-date virus definitions.
- Only City provided VPN clients may be used.

### **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.

## **21. Wireless Network Communication Policy**

### **Policy Purpose**

The Wireless Network Communication Policy is intended to govern the connection of wireless devices to the City's network.

### **Policy Scope**

This policy covers all wireless entry points (including but not limited to 'wireless access points').

### **Policy Description**

Due to the extreme vulnerability of wireless networks, all wireless systems implementation must be approved by DOT to ensure that the correct level of protection is provided for the information and system.

### **Enforcement**

Persons who fail to comply with any of the provisions of this policy shall be subject, at a minimum, to disciplinary action in accordance with the City's Personnel Operating Procedures. Other administrative disciplinary actions may be taken in accordance with the disciplinary policy as provided in Section 5.8, Technology Security Policy, of the City's Administrative Procedures.