Section 1: **Purpose**

The purpose of this policy is to establish the technical guidelines for Information Technology (IT) security, and to communicate the controls necessary for a secure network infrastructure. The network security policy will provide the practical mechanisms to support the City's comprehensive set of security policies. However, this policy purposely avoids being overly specific in order to provide some latitude in implementation and management strategies. The City wishes to provide a secure network infrastructure in order to protect the integrity of City data and mitigate risk of a security incident. While security policies typically avoid providing overly technical guidelines, this policy is necessarily a more-technical document than most.

Section 2: **Scope**

This policy covers all IT systems and devices that comprise the City network or that are otherwise controlled by the City.

Section 3: **Policy**

1. Network Device Passwords

A compromised password on a network device could have devastating, network-wide consequences. Passwords that are used to secure these devices, such as routers, switches and servers, must be held to higher standards than standard user-level or desktop system passwords.

a. Password Construction

The following statements apply to the construction of passwords for network devices:

- Passwords should be at least 8 characters
- Passwords should be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols)
- Passwords should be comprised of a mix of upper and lower-case characters
- Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary
- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
- Passwords should not include "guessable" data such as personal information like birthdays, addresses, phone numbers, locations, etc.

b. **Failed Logons**
Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the City must lock a user's account after 10 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the IT Manager.

In order to protect against account guessing, when logon failures occur, the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

c. **Change Requirements**
Passwords must be changed according to the City's Password Policy. Additionally, the following requirements apply to changing network device passwords:

- If any network device password is suspected to have been compromised, all network device passwords must be changed immediately.

- If a City network or system administrator leaves the City, all passwords to which the administrator could have had access must be changed immediately. This statement also applies to any consultant or contractor who has access to administrative passwords.

- Vendor default passwords must be changed when new devices are put into service.

d. **Password Policy Enforcement**
Where passwords are used an application must be implemented that enforces the City's password policies on construction, changes, re-use, lockout, etc.

e. **Administrative Password Guidelines**
As a general rule, administrative (also known as "root") access to systems should be limited to only those who have a legitimate business need for this type of access. This is particularly important for network devices, since administrative changes can have a major effect on the network, and, as such, network security. Additionally, administrative access to network devices should be logged.

2. **Logging**
The logging of certain events is an important component of good network management practices. Logging needs vary depending on the type of network system, and the type of data the system holds. The following sections detail the City's requirements for logging and log review.

a. **Application Servers**

Logs from application servers are of interest since these servers often allow connections from a large number of internal and/or external sources. These devices are often integral to smooth business operations.

Examples: Web, email, database servers

Requirement: At a minimum, logging of errors, faults and login failures is required. Additional logging is encouraged as deemed necessary. No passwords should be contained in logs.

b. **Network Devices**
Logs from network devices are of interest since these devices control all network traffic, and can have a huge impact on the City's security.

Examples: Firewalls, network switches, routers

Requirement: At a minimum, logging of errors, faults and login failures is required. Additional logging is encouraged as deemed necessary. No passwords should be contained in logs.

c. **Critical Devices**
Critical devices are any systems that are critically important to business operations. These systems may also fall under other categories above - in any cases where this occurs, this section shall supersede.

Examples: File servers, lab or manufacturing machines, systems storing intellectual property

Requirements: At a minimum, logging of errors, faults and login failures is required. Additional logging is encouraged as deemed necessary. No passwords should be contained in logs.

d. **Log Management**
Logs should be retained in accordance with the City's Retention Policy. Unless otherwise determined by the IT Manager, logs should be considered operational data.

3. Firewalls

Firewalls are arguably the most important component of a sound security strategy. Internet connections and other unsecured networks must be separated from the City network through the use of a firewall.

a. **Configuration**
The following statements apply to the City's implementation of firewall technology:

• Firewalls must provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.

• No unnecessary services or applications should be enabled on firewalls. The City should use 'hardened' systems for firewall platforms, or appliances.

• Clocks on firewalls should be synchronized with the City's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

• The firewall ruleset must be documented and audited annually. Audits must cover each rule, what it is for, if it is still necessary, and if it can be improved.

• For its own protection, the firewall ruleset should include a "stealth rule," which forbids connections to the firewall itself.

• The firewall should log dropped or rejected packets.

b. **Outbound Traffic Filtering**

Firewalls are often configured to block only inbound connections from external sources; however, by filtering outbound connections from the network, security can be greatly improved. This practice is also referred to as "Egress Traffic Filtering."

Blocking outbound traffic prevents users from accessing unnecessary, and many times, dangerous services. By specifying exactly what outbound traffic to allow, all other outbound traffic is blocked. This type of filtering would block root kits, viruses, and other malicious tools if a host were to become compromised. This will also prevent remote desktops from accessing the internal network.

The City encourages outbound filtering if possible, but it is not required. If filtering is deemed possible, only the following known "good" services should be permitted outbound from the network: 21, 22, 23, 25, 53, 80, 110, 443, and 995 or others at the discretion of the IT Manager.

4. Networking Hardware

Networking hardware, such as routers, switches, hubs, bridges and access points, should be implemented in a consistent manner. The following statements apply to the City's implementation of networking hardware:

• Networking hardware should provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.

• Clocks on all network hardware should be synchronized using NTP or another means.

Among other benefits, this will aid in problem resolution and security incident investigation.

- If possible for the application, switches are preferred over hubs. When using switches, the City should use VLANs to separate networks if it is reasonable and possible to do so.

- Access control lists should be implemented on network devices that prohibit direct connections to the devices. Exceptions to this are management connections that can be limited to known sources.

- Unused services and ports should be disabled on networking hardware.

- Access to administrative ports on networking hardware should be restricted to known management hosts and otherwise blocked with a firewall or access control list.

5. Network Servers

Servers typically accept connections from a number of sources, both internal and external. As a general rule, the more sources that connect to a system, the more risk that is associated with that system, so it is particularly important to secure network servers. The following statements apply to the City's use of network servers:

- Unnecessary files, services and ports should be removed or blocked. If possible, follow a server-hardening guide, which is available from the leading operating system manufacturers.

- Network servers, even those meant to accept public connections, must be protected by a firewall or access control list.

- If possible, a standard installation process should be developed for the City's network servers. This will provide consistency across servers no matter what employee or contractor handles the installation.

- Clocks on network servers should be synchronized with the City's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

6. Intrusion Detection/Intrusion Prevention

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technology can be useful in network monitoring and security. The tools differ in that an IDS alerts to suspicious activity whereas an IPS blocks the activity. When tuned correctly, IDSs are useful but can generate a large amount of data that must be evaluated for the system to be of any use. IPSs automatically take action when they see suspicious events, which can be both good and bad, since legitimate network traffic can be blocked along with malicious traffic.

The City neither requires nor prohibits the use of IDS or IPS systems. The decision to use

IDS/IPS systems is left to the discretion of the IT Manager.

7. Security Testing

Security testing, also known as a vulnerability assessment, a security audit, or penetration testing, is an important part of maintaining the City's network security. Security testing can be provided by IT staff members, but is often more effective when performed by a third party with no connection to the City's day-to-day Information Technology activities. The following sections detail the City's requirements for security testing.

a. Internal Security Testing

Internal security testing does not necessarily refer to testing of the internal network, but rather testing performed by members of the City's IT team. Internal testing should not replace external testing; however, when external testing is not practical for any reason, or as a supplement to external testing, internal testing can be helpful in assessing the security of the network.

Internal security testing is allowable, but only by employees whose job functions are to assess security, and only with permission of the IT Manager. Internal testing should have no measurable negative impact on the City's systems or network performance.

b. External Security Testing

External security testing, which is testing by a third party entity, is an excellent way to audit the City's security controls. The IT Manager must determine to what extent this testing should be performed, and what systems/applications it should cover.

External testing must not negatively affect network performance during business hours or network security at any time.

As a rule, "penetration testing," which is the active exploitation of City vulnerabilities, should be discouraged. If penetration testing is performed, it must not negatively impact City systems or data.

The City requires that external security testing be performed annually.

8. Disposal of Information Technology Assets

IT assets, such as network servers and routers, often contain sensitive data about the City's network communications. When such assets are decommissioned, the following guidelines must be followed:

- Any asset tags or stickers that identify the City must be removed before disposal.

- Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.

- Physical destruction of the device's data storage mechanism (such as its hard drive or solid state memory) is required. If physical destruction is not possible, the IT Manager must be notified.

9. Network Compartmentalization

Good network design is integral to network security. By implementing network compartmentalization, which is separating the network into different segments, the City will reduce its network-wide risk from an attack or virus outbreak. Further, security can be increased if traffic must traverse additional enforcement/inspection points. The City requires the following with regard to network compartmentalization:

a. **Higher Risk Networks**
Examples: Guest network, wireless network

Requirements: Segmentation of higher-risk networks from the City's internal network is encouraged but not required.

b. **Externally-Accessible Systems**
Examples: Email servers, web servers

Requirements: Segmentation of externally accessible systems from the City's internal network is encouraged but not required.

c. **Internal Networks**
Examples: Finance, Administrative Services

Requirements: Segmentation of internal networks from one another can improve security as well as reduce chances that a user will access data that he or she has no right to access. The City encourages, but does not require, such segmentation.

10. Network Documentation

Network documentation, specifically as it relates to security, is important for efficient and successful network management. Further, the process of regularly documenting the network ensures that the City's IT staff has a firm understanding of the network architecture at any given time. The intangible benefits of this are immeasurable.

At a minimum, network documentation must include:

- Network diagram(s)
- System configurations
- Firewall ruleset
- IP Addresses

- Access Control Lists

The City requires that network documentation be performed and updated on a yearly basis.

11. **Antivirus/Anti-Malware**

Computer viruses and malware are pressing concerns in today's threat landscape. If a machine or network is not properly protected, a virus outbreak can have devastating effects on the machine, the network and the entire City. The City provides the following guidelines on the use of antivirus/anti-malware software:

- All City-provided user workstations must have antivirus/anti-malware software installed.

- Workstation software must maintain a current "subscription" to receive patches and virus signature/definition file updates.

- Patches, updates and antivirus signature file updates must be installed in a timely manner, either automatically or manually.

- In addition to the workstation requirements, virus and malware scanning must be implemented at the Internet gateway to protect the entire network from inbound threats.

12. **Software Use Policy**

Software applications can create risk in a number of ways, and thus certain aspects of software use must be covered by this policy. The City provides the following requirements for the use of software applications:

- Only legally licensed software may be used. Licenses for the City's software must be stored in a secure location.

- Open source and/or public domain software can only be used with the permission of the IT Manager.

- Software should be kept reasonably up to date by installing new patches and releases from the manufacturer.

- Vulnerability alerts should be monitored for all software products that the City uses. Any patches that fix vulnerabilities or security holes must be installed expediently.

13. **Maintenance Windows and Scheduled Downtime**

Certain tasks require that network devices be taken offline, either for a simple re-boot, an upgrade, or other maintenance. When this occurs, the IT staff should make every effort to perform the tasks at times when they will have the least impact on network users.

14. **Change Management**

Documenting changes to network devices is a good management practice and can help speed resolution in the event of an incident. The IT staff should make a reasonable effort to document hardware and/or configuration changes to network devices in a "change log." If possible, network devices should bear a sticker or tag indicating essential information, such as the device name, IP address, Mac address, asset information, and any additional data that may be helpful, such as information about cabling.

15. **Suspected Security Incidents**

When a security incident is suspected that may impact a network device, the IT staff should refer to the City's Incident Response policy for guidance.

16. **Redundancy**

Redundancy can be implemented on many levels, from redundancy of individual components to full site-redundancy. As a general rule, the more redundancy implemented, the higher the availability of the device or network, and the higher the associated cost. The City wishes to provide the IT Manager with latitude to determine the appropriate level of redundancy for critical systems and network devices. Redundancy should be implemented where it is needed, and should include some or all of the following:

- Hard-drive redundancy, such as mirroring or RAID
- Server-level redundancy, such as clustering or high availability
- Component-level redundancy, such as redundant power supplies or redundant NICs
- Keeping hot or cold spares onsite

17. **Manufacturer Support Contracts**

Outdated products can result in a serious security breach. When purchasing critical hardware or software, the City must purchase a maintenance plan, support agreement, or software subscription that will allow the City to receive updates to the software and/or firmware for a specified period of time. The plan must meet the following minimum requirements:

Hardware: The arrangement must allow for repair/replacement of the device within an acceptable time period, as determined by the IT Manager, as well as firmware or embedded software updates.

Software: The arrangement must allow for updates, upgrades and hotfixes for a specified period of time.

18. **Applicability of Other Policies**
This document is part of the City's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as needed.

Section 4: Enforcement

This policy will be enforced by the IT Manager and/or executive team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more-severe penalties up to and including termination of employment.

Section 5: Definitions

ACL: A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.

Antivirus Software: An application used to protect a computer from viruses, typically through real-time defenses and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware and other malware.

Firewall: A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.

Hub: A network device that is used to connect multiple devices together on a network.

IDS: Stands for Intrusion Detection System. A network monitoring system that detects and alerts to suspicious activities.

IPS: Stands for Intrusion Prevention System. A networking monitoring system that detects and automatically blocks suspicious activities.

NTP: Stands for Network Time Protocol. A protocol used to synchronize the clocks on networked devices.

Password: A sequence of characters that is used to authenticate a user to a file, computer, network or other device. Also known as a passphrase or passcode.

RAID: Stands for Redundant Array of Inexpensive Disks. A storage system that spreads data across multiple hard drives, reducing or eliminating the impact of the failure of any one drive.

Switch: A network device that is used to connect devices together on a network. Differs from a hub by segmenting computers and sending data to only the device for which that data

was intended.

U.S. DoD Standards: Stands for United States Department of Defense Standards. Standards on data destruction detailed in DoD 5220.22M. Most data-wiping software packages provide an option for wiping to this standard.

VLAN: Stands for Virtual LAN (Local Area Network). A logical grouping of devices within a network that act as if they are on the same physical LAN segment.

Virus: Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.