Network Security Policies and Procedures

Version 5.0

ISSUED BY:
Information Technology
September, 2015

Network Security Policies and Procedures

TABLE OF CONTENTS

INTRODUCTION

Background

Security must be an integral thread running through every aspect of the enterprise. Just as physical security for employees has been provided with policies, guards and metal detectors, we must also provide for security of the City of Madison's data using a multi-layered approach.

Each employee is entirely responsible for his or her user ID and password. No one else should share these. Every file server and piece of networking equipment has its own mechanisms of protection through access codes as well. Security is everyone's business, and is an ongoing refinement process as situations change and new vulnerabilities develop.

The City of Madison has set a vision and is progressing on a path into the future of enhanced constituent support and service by maintaining a secure and available network of electronic data systems. These systems are interconnected via high-speed switches, routers and firewalls to allow appropriate access to City of Madison information stored on multiple file servers and databases. The goal is to maintain all of these components, along with the backup devices and supported client devices, in a manner consistent with industry best practices.

Contained in this document are the policies that direct the processes and procedures by which the City of Madison strives to maintain a secure and available data enterprise. By employing industry best practices along with proprietary processes, we are working to provide due diligence in our best efforts to maintain the confidentiality, integrity and availability of the City of Madison's data resources.

This endeavor is truly a partnership, in that all parties involved have a significant stake and responsibility to comply with all agreed-upon policies and procedures to ensure the highest possible level of security. A single weak link anywhere in the chain, from the largest server to any individual user running an unauthorized program, could compromise the integrity of confidential data or create a catastrophic loss. There are "hostile" applications that can inadvertently or deliberately be run on a device and cause data destruction or disruption of service to others. Information Technology (IT) is constantly working to harden systems against such attacks, and to implement services to screen out hostile mobile code and viruses, but it is still up to each individual user to comply with all revisions of published policies and procedures. Risk assumed by one is shared by all.

The latest version of the "Network Security Policies and Procedures" will always be posted on the City of Madison's EmployeeNet for quick reference.[1] As all City of Madison network users carefully follow operational and security guidelines we have a good opportunity to continue providing the best possible services to the employees, residents and businesses of the City of Madison.

Scope

This document contains multiple sections that are in many ways inter-related. Several concepts, with security being foremost, become threads that run through the entire document and are common to

[1] www.cityofmadison.com/employeeNet/IT/policies

multiple areas of discipline. The overall objective is to guard the City of Madison's vital electronic data resources that contain confidential employee records, payroll information, customer information and much more. All of these records are stored in electronic data systems and must be treated in a manner consistent with current best practices to ensure their confidentiality, integrity and availability.

This document strives to define methodologies to support the three essential principles for guarding electronic data systems:

- Confidentiality: Ensuring that only authorized users can access confidential or sensitive information. By precisely defining groups of users, and regularly auditing the accuracy and consistency of those groups, we can limit and control who has access to which data. Through a variety of policies, practices and systems, we work to ensure that only those who are authorized will access any given data resource.
- Integrity: Ensuring that data has not been tampered with, either on the network or in storage. Our goal is to ensure that data integrity is maintained at all levels.
- Availability: Data must be available to those who are authorized to use it. Denial-of-Service attacks are becoming common, and our goal is to ensure that users can access the data they need.

Target Audience

The policies and procedures described in this document cover various groups of people. Some policies cover every user of the City of Madison's network and its resources, and others apply to specific groups who administer or manage the network. This is not discriminatory; it is simply a function of roles and responsibilities. The identified groups are listed below:

- City of Madison Employees
- Third-Party Vendor Employees
- City of Madison Information Technology Staff
  - Managers
  - Network Operations Section
  - HelpDesk Support Section
  - Software Development Section
- Each and every individual person who uses any portion of the network or its resources.

Enforcement

Any employee found to have violated any of these policies might be subject to disciplinary action, up to and including termination of employment.

ACCEPTABLE USE SECTION

Ownership of Network, PC and Data Resources

All hardware and software are the property of the City of Madison. Although there are numerous "personal computers" provided for use by staff members they are owned by, are to be used for conducting business for, the City of Madison. All workstations, telephones, servers and other networking devices must be approved by Information Technology, per APM 4-7, before being connected anywhere on the network.

No Privacy of Data

All electronic data, communications and information, including information transmitted or stored on the electronic systems of the City, remain the property of the City. The City retains the right to access, inspect, monitor or disclose any material transmitted or received on its electronic systems, including information downloaded from the Internet, or received or sent via e-mail.

Privacy Rights Waiver

Employees should not expect privacy with respect to information transmitted, received or stored on the City's computing resources. By accepting the grant of access to City of Madison electronic systems, the employee shall be deemed to have authorized the City to access, inspect, monitor and disclose material. Consequently, an employee's manager and other authorized individuals shall have the right to know employees' passwords.

Prohibitions and Restrictions on Use

The use of computer resources including the Internet and/or e-mail, whether in-house or external, for any of the following purposes is strictly prohibited:

- To create or transmit material which is designed or likely to threaten, disturb, intimidate or otherwise annoy or offend another, including, but not limited to, broadcasting unsolicited messages or sending unwanted mail after being advised it is unwanted.
- To create or transmit defamatory material.
- To gain unauthorized access to facilities or services accessible by the City network and intended to be used for official City business or to use such facilities or services in an unauthorized manner.
- To conduct business or engage in any "for profit" communications or activities.
- To access, view or obtain any "adult entertainment," pornographic or obscene material unless it is for work-related investigatory purposes and with the approval of the department head.
- For political campaign purposes, including, but not limited to, using e-mail to circulate advertising for political candidates or relating to political campaign issues.
- Placing one's City-issued Internet e-mail address on any ListServ for other than business purposes. If an employee becomes aware that his/her City-issued Internet e-mail address is on a non-business related ListServ, he/she should promptly request that it be removed and/or unsubscribe.
- To gain commercial or personal profit or advantage, including, but not limited to, selling lists of names, addresses, telephone numbers or other information generated from City files.

- To create or transmit material in violation of APM 3-5.
- To represent oneself directly or indirectly as conducting City business when using such equipment for incidental personal purposes.
- To create web pages - No personal web pages may be created, regardless upon what server they may reside. Web pages representing official City information may be created in coordination with Information Technology.
- To print lengthy documents except for business purposes.
- To use the Internet and speakers or headsets for the purpose of listening to audio or viewing video unless it is for City business.
- For any purpose which would be a violation of any City work rules, City ordinance or state or federal law.

Internet and/or E-mail Usage

The Internet and e-mail, whether in-house or external, shall be used in an appropriate and professional manner at all times. The use of language inappropriate to the work place is prohibited. Offensive messages, including racial slurs or sexual slurs, obscene, vulgar and other inappropriate language in violation of APM 3-5 are strictly prohibited.

Access to electronic mail (e-mail), whether in-house or external, and access to the Internet is only granted by approval of the agency head. Reception and transmission of e-mail, while connected to the City network, is permissible only through the City of Madison enterprise e-mail system.

Transmission of any material in violation of U.S. or state laws or regulations is prohibited.

While the Internet is an effective network for its purpose, it is not and should not be considered a secure network and should not be relied on for the transmission of confidential or sensitive data or messages.

Downloading software from the Internet to City PCs without authorization from Information Technology is prohibited. Doing so could put the City in jeopardy of breaking software piracy rules and/or could contaminate the network with viruses.

Attempt to limit the downloading of large files from the Internet unless absolutely necessary. If it is necessary, try to schedule for off-peak hours (before 7:30 a.m. or after 4:30 p.m.). Remove downloaded files when you are finished with them.

Unless approved by IT, do not connect directly to the Internet or to any other external computer system using any other connection type not underwritten by the Information Technology.

Employees must use the City's Internet gateways, i.e., e-mail through the City's enterprise e-mail system and the Internet through a browser on the City's network. This is in order to prevent the City's network from being compromised by external factors.

All incoming e-mail attachments will be scanned using virus checking software and those that may be infected, or pose a threat of being infected, will be quarantined.

Internet Content Filtering

The "Prohibitions and Restrictions on Use" policy of this document describes how the Internet may and may not be used. Note that this section tolerates the occasional and limited personal use of computers, and goes on to list how such computers may not be used.

An Internet content filtering appliance has been installed on the City network in order to facilitate the implementation of the policies contained in the "Prohibitions and Restrictions on Use" policy of this document. This appliance provides the ability to filter out a wide variety of websites based on their category/content, and based on bandwidth usage. Decisions regarding the extent to which Internet content filtering will take place will be made by the Director of Information Technology, after consulting with other appropriate staff in IT and in other agencies.

The Internet content filtering appliance has been implemented in order to:

1. Decrease the amount of staff time spent inappropriately being spent using the Internet.
2. Reduce the amount of staff time spent on investigating situations involving the inappropriate use of the Internet.
3. Minimize the amount of network bandwidth being used for non-business related Internet browsing.

Information Technology routinely monitors network traffic, including Internet traffic, for bandwidth utilization and for security purposes. If in the normal course of reviewing logs, IT staff should come across what appears to be the inappropriate use of network resources, that occurrence will be brought to the attention of IT management staff for necessary remedial action.

Incidental Personal Use

Although occasional and limited personal use of computers is tolerated, subject to the limitations, conditions, and regulations contained in this policy, employees may not use any information technology resources in any way that:

- Directly or indirectly interferes with City operations of computing facilities or e-mail services.
- Is contrary to or damages the City's interest.
- Results in any incremental costs to the City.
- Interferes with the employee's work duties, performance or other obligations to the City. Examples include, but are not limited to, excessive use of games, excessive "surfing" of the Internet, etc.

Any personal use shall be at the risk of the person engaging therein. The City is not responsible or liable for the consequences. Such use shall be limited to individualized personal communications and not mass distribution of material. Using computer resources for incidental personal purposes to transmit material to "all e-mail users" is strictly prohibited. Use of computer resources for such incidental personal purposes is a privilege and can be withdrawn by a supervisor at any time.

NETWORK SECURITY SECTION

Formal Information Technology Permissions Approval

Written permission, e-mail or otherwise, from an authorized contact person in the owner agency, must be attained in order to add new network accounts and/or devices, grant network file rights, search archived e-mail, or install new application software on a PC. A list of all Authorized Contacts by Department[2] is available on the City of Madison's EmployeeNet.

User IDs and Passwords

Individual user accounts and passwords are issued to create security for the systems and data belonging to the City of Madison. The purpose of a User ID and password is to create security from unauthorized access to the City of Madison's systems or confidential data. User ID's and passwords must conform to the following criteria:

- Every customer must use a unique User ID that is associated with his or her name alone. No generic/shared User ID's are allowed.
- Network User ID's must comply with the City of Madison standard naming convention for network login names.
- Wherever possible, applications should use LDAP to validate User ID and password information that is stored in the City's enterprise network directory.
- It is permissible to use the same User ID and password for each system or application that a user accesses. In all cases, each user is entirely and personally responsible to maintain the complexity and secrecy of his or her password.
- Under normal circumstances, City staff should not share their password with anyone. However, some departments may require employees to share their passwords with their supervisor and/or department head. If an instance arises where someone requires access to another person's files, an authorized contact person in the owner agency should contact the HelpDesk to request a change of access rights for the account.
  - Passwords should be complex but easy to remember; e.g. msi5!yold (My son is 5 years old) OR ihlimf5#yn (I have lived in Madison for 5 years now).
  - If a customer forgets his or her password, they should call the HelpDesk to request that a new, temporary password be assigned. The HelpDesk will assign a new short-term password that will expire upon the user's next network login, at which time the customer will be prompted to change their password.
  - All accounts must have a password that meets or exceeds the following rules:
    1. Must be at least 8 and not more than 14 characters long.
    2. No more that 3 consecutive characters are allowed (i.e., aaa) and no more than 5 of the same characters are allowed (i.e., 1aaabaa).
    3. Must expire every 60 days.
    4. Will not reuse the previous eight passwords.
    5. May not contain the owner's e-mail name or any part of their full name.
    6. Cannot be a "common" word (for example, it should not be a word in the dictionary or slang in common use).
    7. Should not contain words from any language.

[2] www.cityofmadison.com/employeenet/it/authorizedcontacts

8. Must contain characters from each of the following 4 classes:

Description	Examples
Upper-case English Letters	A, B, C, ... Z
Lower-case English Letters	a, b, c,.....z
Westernized Arabic Numerals	0, 1, 2, ...9
Non-alphanumeric ("special characters")	For example, punctuation, symbols: ({}[],.<>;:'"?/|\`~!@#$%^&*()_-+=)

- Only Information Technology personnel, or security consultants hired by Information Technology, are authorized to run any type of password cracking tool.

NETWORK COMPONENT PASSWORDS – CONTINGENCY ACCESS

Network Operations related Passwords (Servers, Apps, switches and equipment) are to be stored in a secure and password protected management application.

In the event that the appropriate Network Support or Server Administrators are not available in an emergency access to the password vault files, access can be provided by one of the following people:

- Information Technology Director
- Technical Services Manager
- Network Operations Team leader
- HelpDesk Supervisor

NETWORK COMPONENT PASSWORDS – CHANGE CYCLE

Passwords on infrastructure components must be changed at the following times:

- At least once every 180 days.
- In the event that a password or system becomes compromised all infrastructure passwords are to be changed as soon as possible.

Physical Security

Every City of Madison employee is responsible for maintaining physical security in City of Madison offices. While the need for physical security is obvious for locations such as the network operation centers, other areas are just as sensitive. There is valuable equipment on desks and other storage areas, and there is sensitive business information on desks and laptops. Even how we handle disposing of sensitive materials has an effect on our physical security. The need for physical security extends beyond the walls, too. Employees carry valuable information and equipment with them—laptops, smart phones and customer hardware.

CITY-OWNED WORK AREAS

- It is highly recommended that City-owned offices appoint a front door "gatekeeper." In the event that the primary "gatekeeper" must leave the area of the front door, someone should be designated as "gatekeeper" in his or her absence. Ideally, the "gatekeeper" will sit at a receptionist's desk. Alternatively, someone with a view of the entrance area from his or her desk is acceptable.

- When not in public areas of City-owned facilities, City of Madison employees and guests should carry their identification badge in a visible location. Badge pulls and neck lanyards are available from the receptionist.
- If a City of Madison employee sees an unfamiliar person without a badge or escort in a City of Madison facility, the employee should politely inquire if they can be of any help.
- When stepping away from your computer workstation (either in a City of Madison office or elsewhere), lock the console of your workstation.
- Set a password on the screensaver of your workstation and set the inactivity timer to at most 15 minutes.

PORTABLE DEVICES

Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

City of Madison employees traveling with computer hardware (laptops, smart phones, tablets) should take steps to minimize the likelihood of theft or loss. For example: Encryption software and hardware must be used to secure very sensitive data on traveling computers. Keep your bags with you at all times. When waiting to board a plane, loop the handle of the laptop case around your arm or leg.

CONFERENCE ROOMS

Network interface jacks and wireless access points in all conference rooms will be located on a network separate from the internal City of Madison network, but still behind a firewall. If City of Madison employees need to access the internal network from a conference network connection, they must use VPN.

All conference rooms in all City of Madison offices will be configured in this manner.

PRIMARY AND SECONDARY NETWORK OPERATIONS CENTERS (NOC)

- No food or beverages are allowed in any of the Network Operations Centers.
- All doors to the Network Operation Centers must remain closed and locked. Emergency exit doors must remain locked and may only be used in the event of an emergency.
- Access to any of the Network Operations Centers is restricted to authorized personnel only. (Authorized personnel must wear their City-issued ID card/lanyard while in the Network Operations Centers.)
- Access keys to all of the network equipment facilities will be kept in a key management system. A key management system will be located at both the primary and secondary Network Operations Centers.
- Access to any of the Network Operations Centers, by an individual not on the authorized personnel list (visitor), will require:
  - The person acting as a project leader (sponsor), or another member of the project leader's team, for the visitor's project, must sign the person into the NOC. The visitor will provide the following information on the sign in sheet:
- Visitor's Name (Printed)
- Visitor's company

- Date/time of entry into the NOC
- City sponsor
- Estimated time of departure
- Badge number
  - In instances where the City employee is not familiar with the visitor, a photo ID will be required to be shown by the visitor.
  - The visitor will be issued a visitors pass and will be required to wear the pass for the duration of their visit. When the visitor leaves the NOC for the day, the badge must be returned to City staff.
- Tailgating (following an authorized person into the operations center without signing in and out) is prohibited.
- Whenever possible, gear should be unpacked and staged in a designated setup area. The gear should be positioned and racked immediately, and all packing materials must be removed immediately.
- All network operation centers must be kept in an orderly and professional manner. Any material, which constitutes an environmental hazard or diminishes the professional appearance of the data center, must be removed immediately.

WIRING CLOSETS

In all new City-owned facilities and facilities being remodeled, wiring closets and test labs should be located in a controlled and monitored area that would allow access to authorized personnel only. Wherever possible, an effort should be made to improve the security of existing facilities that house City-owned network devices.

Network Connection

To ensure that a secure method of connectivity is provided between the City of Madison and contracted vendors, and to provide guidelines for the use of network and computing resources associated with the network connection as defined below.

- The City's connectivity options listed below are the standard methods of providing a third party network connection. Anything that deviates from these standard methods must have a waiver sign-off by the City.
  - Leased line (i.e., T1): Leased lines for third parties will be terminated on the partner's network.
  - ISDN/FR: Dial-leased lines will terminate on a third party-only router located on the ECS or IT partners network. Authentication for these connections must use the Partners Authentication database and Token Access System. Currently, RSA SecureID is the token access system in use.
  - Encrypted Tunnel: Encrypted tunnels must be terminated on the partner's network whenever possible. In certain circumstances, it may be required to terminate an encrypted tunnel on the dirty subnet, in which case the normal City perimeter security measures will control access to internal devices.
  - Third-party browser-based SSL (i.e., WebEx): All connections via browser-based SSL must be initiated and terminated by the City. All connections via browser-based SSL must be terminated by the initiating City employee at the conclusion of the business transaction.

- Contractor will complete a "Network Connection Policy" agreement prior to connection to the City network.
- Contractor will allow only Contractor's employees approved in advance by the City to access the Network Connection. Contractor shall be solely responsible for ensuring that Authorized Employees are not security risks, and upon the City's request, Contractor will provide the City with any information reasonably necessary for the City to evaluate security issues relating to any Authorized Employee.
- Contractor will promptly notify the City whenever any Authorized Employee leaves Contractor's employ or no longer requires access to the Network Connection.
- Each party will be solely responsible for the selection, implementation, and maintenance of security procedures and policies that are sufficient to ensure that (a) such party's use of the Network Connection is secure and is used only for authorized purposes, and (b) such party's business records and data are protected against improper access, use, loss alteration or destruction.
- Contractor shall notify the City in writing promptly upon a change in the user base for the work performed over the Network Connection or whenever in Contractor's opinion a change in the connection and/or functional requirements of the Network Connection is necessary.
- Contractor shall notify City within five (5) days of the change in name, address, phone, fax, e-mail of its contact person. It is Contractor's responsibility to ensure that Contractor has provided all of the necessary information and that such information is correct.
- When existing Third Party Network Connections do not meet all of the guidelines and requirements outlined in this policy, the City reserves the right to have Contractor re-engineer those connections as needed.
- All requests for third party connections must be made via the Technical Services Manager.
- When possible, third party (Partner) Access Points (PAPs) should be established in locations such that the cost of the access is minimized. The City will determine each PAP router, protocol and line type.
- In general, services provided over Third Party Network Connections should be limited only to those services needed, and only to those devices (hosts, routers, etc.) needed. City shall not provide blanket access. The City's default policy position is to deny all access and then only allow those specific services that are needed and approved by the City pursuant to the established procedure.
- In no case shall a Third Party Network Connection to the City be used as the Internet connection for the third party.
- The standard set of allowable services is:
  - File Exchange Via FTP: Where possible, file exchange via FTP should take place on the existing City FTP servers (ftp.cityofmadison.com).
  - Electronic Mail Exchange: Business-related e-mail exchange between the City and third parties may be conducted over the Network Connection as needed. Mail from third party websites to non-City addresses will not be allowed over the Network Connection.
  - Telnet Access: Telnet access will be provided to specific City hosts, as needed. Employees from third parties will only be given accounts on the specific City hosts that are needed as determined by the City. Where possible, router ACLs and static routes will be used to limit the paths of access to other internal City hosts and devices. Note: NIS accounts and directory services are not to be established for employees of third parties who have accounts on City hosts.
  - Web Resource Access: Access to internal web resources will be provided on an as-needed basis. Access to the City's public web resources will be accomplished via the normal Internet access for the third party.

- Access to Source Code Repositories: The City shall determine this access on a case-by-case basis.
- Print Services: The City shall determine this access on a case-by-case basis.
- SQL*Net Access: The City shall determine this access on a case-by-case basis.
- ERP Access: The City shall determine this access on a case-by-case basis.

- Third Party Network Connections made via remote dial-up using PPP/SLIP or standard telnet over the Internet will be authenticated using the Partners Authentication database and Token Access System. Currently, RSA SecureID is the token access system in use.
- All right, title and interest in and to confidential information shall remain the exclusive property of the City and the confidential information shall be held in trust by Contractor for the benefit of the City. Contractor shall not, directly or indirectly, use or exploit the confidential information for any operational, commercial or other purpose whatsoever or in any manner detrimental to the City or disclose, disseminate, impart or grant access to the confidential information to any person for any purpose.
- Contractor shall not copy, reproduce in any form or store in any retrieval system or database the confidential information without the prior written consent of the City, except for such copies, reproductions and storage as may be reasonably required internally by Contractor for the purpose for which Contractor receives the confidential information.
- Contractor agrees that at no time shall Contractor, its employees or agents, authorize a third party to have access to the City's network.
- Security of third party connections will be achieved by implementing "Access Control Lists" on the Partner Gateway routers to which the third party websites are connected. The ACLs will restrict access to pre-defined hosts within the internal City network. The ACLs will be determined by the appropriate support organization. A set of default ACLs may be established as a baseline.
- The City shall not have any responsibility for ensuring the protection of third party information. The third party shall be entirely responsible for providing the appropriate security measures to ensure protection of their private internal network and information.
- All materials relating to the business and affairs of the City, including, without limitation, all manuals, documents, reports, equipment, working materials and lists of customers or suppliers prepared by the City or by Contractor in the course of Contractor's employment are for the benefit of the City and are and shall remain the property of the City.

Terminated Employees

Network accounts for terminated employees need to be removed from the network in a timely manner. The following groups or individuals are responsible for completing the tasks identified, in order to complete the account removal process.

HUMAN RESOURCES AND/OR PAYROLL

- Notifies Information Technology via e-mail that an employee has terminated employment with the City of Madison.
- Provides the HelpDesk with the employee's name, department and last day of employment.

HELPDESK

- Verifies that the terminated employee had a network account.

- Notifies the authorized security contact for the employee's department via e-mail.
- Generates a call in the IS call tracking system and assigns the call to the appropriate queue(s).

DEPARTMENTAL AUTHORIZED SECURITY CONTACT

- Completes the "terminated employee" form on the EmployeeNet.

NETWORK OPERATIONS TEAM

- Removes enterprise directory account.
- Identifies application group membership for the development staff (if required).
- Revokes and retrieves network security token (if required).

TELEPHONE ADMINISTRATION

- Removes voicemail and telephone accounts. (if required)

SYSTEMS & PROGRAMMING MANAGER

- Coordinates the removal of appropriate applications accounts (if required).

NEW WORLD SECURITY GROUP

- Removes New World account (if required).

Risk Assessment

Risks are those factors that could affect confidentiality, availability and integrity of the City of Madison's key information assets and systems. Information Technology is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

Information Technology will contract with a third party vendor that will perform periodic information security risk assessments for the purpose of determining areas of vulnerability. The Technical Services Manager will be responsible for initiating appropriate vulnerability remediation. A risk assessment can be conducted on any information system, to include applications, servers and networks, and any process or procedure by which these systems are administered and/or maintained.

The execution, development and implementation of remediation programs are the joint responsibility of Information Technology and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any risk assessment being conducted on systems for which they are held accountable. Employees are further expected to work with the Technical Services Manager in the development and implementation of a remediation plan.

Security Incident Reporting

The Incident Response Team (IRT) serves as the focal point for computer security incidents in City of Madison. The IRT is made up of the Situation Manager, the HelpDesk Supervisor, the Network

Operations Team Leader, and the Madison Police Computer Forensics Unit Supervisor or their designees.

The IRT identifies computer security incidents, characterizes the nature and severity of incidents, and provides immediate diagnostic and corrective actions when appropriate. A security incident is defined as a compromised or suspected compromised system; any type of attack levied on or from a City of Madison computer resource; or misuse of IT resources (such as chain letters, virus hoaxes, etc.)

The IRT receives incident reports from its customers via the HelpDesk, from its intrusion detection device(s), from proactive scans, from law enforcement officials, from other outside sources, or from IT Support and Development staff. The IRT then informs the appropriate technical staff.

Incidents are either identified as **possible** or **active.**

POSSIBLE INCIDENTS INCLUDE (BUT ARE NOT LIMITED TO)

Pre-attack probes, unauthorized access attempts, denial of service attempts, or vulnerabilities identified as a result of a SARA scan. This could also include notification by an outside source that they are being attacked from a City of Madison IP address.

For a possible incident, the only action necessary to close the incident is for the Situation Manager to notify the appropriate technical staff. If however, while investigating the potential incident a compromise is found, the Situation Manager should treat this as an active incident, and should follow the steps below.

ACTIVE INCIDENTS INCLUDE (BUT ARE NOT LIMITED TO)

Confirmed unauthorized access, denial of service, and successful exploits of vulnerabilities; these incidents should be reported as such:

- Technical staff who suspects and/or identifies an active incident, notifies the IRT,
- The IRT confirms incident,
- The Situation Manager notifies IT Management,
- Technical IT staff informs IRT and then resolves the incident, or
- Technical IT staff requests assistance from IRT to resolve incident; IRT resolves incident and informs the Situation Manager. (Corrective actions may include upgrading or reinstalling operating systems, installing patches, or modifying system access.)

For inappropriate e-mails, such as virus hoaxes, chain letters, or pornography, the individual who identified the incident should report it to the Situation Manager. If the incident is reported to the IRT, the IRT will notify the Situation Manager. If the incident is contained within the one device, the Situation Manager does not need to report back to the IRT. If the incident has spread to more than one device, the Situation Manager should follow the steps for reporting an ACTIVE incident.

NETWORK INFRASTRUCTURE SECTION

Routers and Switches

All routers and switches connecting to the City of Madison network or used in a production capacity at or on behalf of the City of Madison must meet or exceed minimal security configuration standards. All routers and switches connected to the City of Madison network are affected. Routers and switches within DMZ areas fall under the Internet DMZ Equipment Policy.

Every device must meet the following configuration standards:

- No local user accounts are configured on the device. Devices must use TACACS+ for all user authentications.
- The enable password on the device must be kept in a secure encrypted form. The device must have the enable password set to the current production device password from the device's support organization.
- Disallow the following:
  - IP directed broadcasts
  - Incoming packets at the device sourced with invalid addresses such as RFC1918 address
  - TCP small services
  - UDP small services
  - All source routing
  - All web services running on device
- Use standardized SNMP community strings.
- Access rules are to be added as business needs arise.
- Services and applications not for general access must be restricted by access control lists.
- Each device must have the following statement posted in clear view:
  "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

Internet DMZ Equipment

All equipment owned and/or operated by the City of Madison located outside the City of Madison's Internet firewalls must comply with standards that are designed to minimize the potential exposure to the City of Madison from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of the City of Madison resources.

Devices that are Internet facing and outside the City of Madison firewall are considered part of the "de-militarized zone" (DMZ) and are subject to this policy. All equipment or devices deployed in a DMZ owned and/or operated by the City of Madison (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by the City of Madison must follow this policy. This policy also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the "cityofmadison.com" domain or appears to be owned by the City of Madison.

All equipment must comply with the following configuration policy:

- The Technical Service Manager, as part of the pre-deployment review phase, must approve hardware, operating systems, services and applications.
- Operating system installation and configuration must be done according to the *Routers and Switches* and/or *Servers* policy.
- All patches/hot-fixes recommended by the equipment vendor must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Services and applications not serving business requirements must be disabled.
- Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by the Technical Services Manager.
- Access control lists must restrict services and applications not for general access.
- Insecure services or protocols (as determined by the Technical Services Manager) must be replaced with more secure equivalents whenever such exist.
- Remote administration must be performed over secure channels (e.g., encrypted network connections using SSL or IPSEC) or console access independent from the DMZ networks.
- All host content updates must occur over secure channels.
- Security-related events must be logged and audit trails saved to Information Technology-approved logs. Immediate access to all equipment and system logs must be granted upon demand. Security-related events include (but are not limited to) the following:
  - User login failures.
  - Failure to obtain privileged access.
  - Access policy violations.
- The Technical Services Manager will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.
- Network interfaces must have appropriate Domain Name Server records (minimum of A and PTR records).
- The Technical Services Manager must be invited to perform system/application audits before the deployment of new services.

The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented.

Virtual Private Network (VPN)

Approved City of Madison employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the Network Connection Policy.

Additionally:

- It is the responsibility of employees to ensure that unauthorized users are not allowed access to City of Madison internal networks.
- Authentication must use a two-factor authentication method provided by the City of Madison.
- When actively connected to the City network, VPNs will force all traffic to and from the PC over the VPN tunnel. All other traffic will be dropped.
- Client software must provide an embedded firewall feature, which must be active.

- Gateways will be set up and managed by Information Technology Network Operations section.
- All computers must use up-to-date anti-virus software.
- All computers must have the most current operating system security patches applied.
- Users will be automatically disconnected from City of Madison's network after 60 minutes of inactivity.
- The VPN session is limited to an absolute connection time of 24 hours.
- All City employees, with the exception of authorized Information Technology Support Staff, must use a City-owned laptop and have a bona fide business need to access the City's internal network via VPN.
- Users of computers that are not City of Madison-owned equipment must configure the equipment to comply with City of Madison's *VPN* and *Network Connection* policies.
- Only City-approved VPN clients may be used.
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of City of Madison's network, and as such are subject to the same rules and regulations that apply to City of Madison-owned equipment, i.e., their machines must be configured to comply with City of Madison's Security Policies and Procedures.

Wireless Communication

Includes all wireless communication devices capable of transmitting packet data (e.g., personal computers, wireless phones, smart phones, etc.) connected to any of the City of Madison's internal networks. Wireless devices and/or networks without any connectivity to the City of Madison's networks do not fall under the purview of this policy.

All point-to-point (building-to-building) wireless devices must use City-approved vendor products and security configurations. A data encryption method, which meets or exceeds the Information Technology standard, is required.

All wireless access points and base stations must be registered and approved by Information Technology. All wireless LAN access must use City-approved vendor products and security configurations. A data encryption method, which meets or exceeds the Information Technology standard, is required. Client authentication must be accomplished using a two-factor authentication method.

All wireless network interface cards (NIC) (i.e., PC cards) used in City laptop or desktop computers must be registered and approved by Information Technology. If a mobile device contains both a LAN NIC and wireless NIC, the wireless NIC must be disabled while the device is connected to the internal network via the LAN NIC.

Servers

Only servers, approved by and setup by Information Technology may be connected to the City network. Servers should be physically located in one of the City's data centers. No server will be connected to the operational network until it has been sufficiently hardened. Hardening of the server includes application of all current OS and security-related patches, removal of all unnecessary services and components, installation of anti-virus software with the current signature file and engine, installation of virus prevention software, and adherence to account and password standards.

Trust relationships between servers will not be used.

All servers will be managed using the City's enterprise server management software.

Root and Admin passwords will be assigned and retained as confidential by the Network Operations Team leader and/or Network Operations Team members as designated by the Network Operations Team leader.

All servers will be configured with a hardware device that provides for remote access. These devices will be accessed using industry standard browsers using the SSL protocol to encrypt communications with the server.

All security-related events on critical or sensitive servers must be logged and audit trails kept online for a minimum of 1 week.

The Network Operations Team will be responsible for applying patches monthly to all City servers. Patches for new threats will be evaluated and applied when necessary.

Workstations

Only workstations, approved by and setup by Information Technology may be connected to the City network. No workstation will be connected to the operational network until it has been sufficiently hardened. Hardening of the workstation includes application of all current OS and security-related patches, removal of all unnecessary services and components, installation of anti-virus software with the current signature file and engine, and adherence to account and password standards. The City desktop management tool will be employed to facilitate the deployment of standardized workstation setups. Information Technology will install the enterprise power management software on all city-owned workstations and laptops.

The HelpDesk will be responsible for deploying patches to workstations on a monthly basis. Patches for new threats will be evaluated and deployed when necessary.

All workstations must comply, at a minimum, with the standard workstation type and configuration, as established by Information Technology. If software in the "other acceptable" category should cause the standard workstation's resources, e.g., memory, processing speed, disk storage, etc., to be exhausted, the agency will be responsible for expanding the workstation to meet the needs of the software. If this software should have a negative impact on the overall City network, the software may be removed, or the workstation may be removed from the network, or the workstation may need to be expanded—at the agency's expense.

All software running on City workstations must be properly licensed and proof of this licensing must be available.

PC software falls into one of the following three categories:

- **Standard Software:** This is software that is fully supported by Information Technology. Any new software that is proposed for City-wide use must first be approved by Information Technology.

- **Other Acceptable Software:** This software is defined as being of benefit for a particular agency or section. The department head of the owner-agency and Information Technology must approve purchase of this software. An important guideline to follow when purchasing this type of software is that there should be a business reason to use the software, rather than just personal preference. Support from IT will only be on a "familiarity" basis. Primary software support responsibility belongs to the agency where the software is used. Consideration should be given to the possible need to share data, which is created using this software, with others.
- **Unauthorized Software:** This is software that is not included in either of the above two categories. If any software of this type is found to reside on a City-owned computer, the agency head will be notified and the software may be removed. If this software is running on a networked computer, that computer may be removed from the network until the situation is corrected.

Portable Computing Devices

This section covers all City-owned and supported portable computing devices, which consist of smart phones, laptops, and notepads (contact the HelpDesk for specific brands and models supported). Only portable computing devices, approved by and setup by Information Technology may be used to access network resources. City authorized and supported virus protection, intrusion prevention, and device management software must be installed. Portable device users are responsible for keeping this software updated and shall not disable its facilities. Portable computing devices must require authentication. A two-factor authentication method is preferred, but passwords that meet the City of Madison *Password Policy* are acceptable. Users of portable computing devices must comply with the City of Madison *Physical Security Policy.* City of Madison data, that is not part of the public record, should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive City of Madison data (e.g. juvenile information, Police reports, HIPAA related information, employee SSAN) must be encrypted using approved encryption techniques. City of Madison data being transmitted via wireless to or from a portable computing device must comply with the City's *Wireless Communication Policy.* Transmission of any information that is not part of the public record is prohibited.

Network Storage

Files that need to be shared by multiple employees or with other City agencies, or need to be stored in a secure, disaster proof (resistant) environment, should be written to one of our network file servers. Usually these file servers are annotated by a drive letter of F: or higher (G:, H:, I:, etc.).

A "USER" directory will be maintained for each customer account on a network file server and access to this directory will be exclusive to the customer, unless otherwise requested by on authorized security contact from the customer's agency.

Use of a common directory (e.g., ISCOMMON), with full rights granted to all employees in a given agency, is a common practice and provides a convenient place for agencies to share files with fellow agency employees. However, it should be noted that sensitive information such as juvenile or HIPPA related information should not be stored in these directories.

On each file server resides a COMMON directory, which is an ideal place to temporarily store files that need to be shared between agencies. Full rights to ALL employees have been granted for this directory, so it is important that no sensitive information is stored in this directory at any time.

Any data that requires encryption, by state, federal or local statutes, will be stored in separate folders on the network and encrypted using an encryption method that meets or exceeds legal requirements.

All sensitive information should be stored in a secure area of the file server for which only those employees who are authorized have access. If an area does not already exist on the network that is suitable to store this sensitive information, the agency's authorized security contact may request, via the HelpDesk, to have this structure created.

City of Madison Data Backup and Restore Policy

Files that fall under the City of Madison records retention guidelines are the responsibility of the user and department. Such files must be maintained in a retrievable form independent of back-ups. Although backup media may contain files that fall under record retention policies, back-ups are intended to restore files, not to maintain them for long-term use.

Backups of all data on the network servers are done daily during non-peak network utilization times. These non-peak periods occur between the hours of 5:00 PM and 7:00 AM Monday through Friday and on weekends from 5:00 PM on Friday until 7:00 AM on Monday. Incremental backups (files that have been modified since the last Full backup) are done on weekdays (Monday through Thursday). Incremental backup will also be done on Fridays when a weekend full backup is not scheduled for those particular servers. Full backups (all files on the network servers) are done on the weekend. Full backups that occur on the last weekend of the month are copied to tape and taken to offsite storage.

Daily incremental backup media will be retained for one week and then overwritten. Weekly backup media will be retained for (4 weeks) and then overwritten. Monthly backup tape copies will be retained for 3 months and then overwritten.

Requests to restore data should be directed to the HelpDesk via e-mail. Restore requests involving data that is not normally accessible to the requestor such as another user's or agency's files must be made by submitting a written request from an authorized agency contact to the HelpDesk**.**