City of Madison, Wisconsin
Information Technology

Network Security Policies and Procedures

Table of Contents

Introduction

The City of Madison seeks to enhance constituent support and service through a secure, reliable network of data systems. These systems are interconnected via high-speed switches, routers, and firewalls that allow for appropriate access to City information stored on multiple file servers and databases. The goal is to maintain all of these components, including backup devices and supported client devices, in a manner consistent with industry standards and best practices. Through employing industry best practices that are reinforced by proprietary processes, Information Technology (IT) strives to maintain the confidentiality, integrity, and availability of the City's data resources.

Purpose

The purpose of this document is to establish policies, processes, and procedures for maintaining and securing data within enterprise network. These policies provide an enforceable governance model around how the City's network is managed and maintained to keep data secure and accessible.

This endeavor is truly a partnership, as all parties involved have a significant stake and responsibility to comply with all agreed-upon policies and procedures to ensure the highest level of security. A single security breach, whether from the largest server to an individual user, could compromise the integrity of confidential data or create a catastrophic loss. Malicious applications can be inadvertently or deliberately run on a device, and cause the destruction or disruption of service to others on the network. IT is constantly working to reinforce systems against such attacks, and to implement services to screen out hostile mobile code and viruses. However, it is still up to each individual user to comply with all revisions to published policies and procedures. All network users should follow the security mantra, "risk assumed by one is shared by all."

Scope

These policies and procedures cover all City network resources and associated data. This version of the document is intended for internal IT Department use only.

User Responsibility

Each employee is entirely responsible for their user ID and password, and should not share them with anyone else. Every file server and piece of networking equipment has its own protection mechanisms through access codes.

Consequences for Non-Compliance

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

Revision Process

Providing network security is an ongoing refinement process as situations change and new vulnerabilities develop. IT will conduct a review of this document and make revisions as necessary.

Acceptable Use Policy

Data Privacy

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

Incidental Personal Use

Incidental personal use of City computer resources is outlined in the City of Madison Appropriate Use of Computer Network Resources Policy (APM 3-9) outlines the guidelines for the use of computer resources for incidental personal use.

Internet and/or Email Usage

Internet and email usage is governed by the City of Madison Appropriate Use of Computer Network Resources Policy (APM 3-9).

All incoming email attachments will be scanned using virus scanning software and those that may be infected, or pose a threat of being infected, will be quarantined.

Internet Content Filtering

The City of Madison Internet Content Filtering Policy outlines the internet filtering security protocols for the City network.

Ownership of Network, PC, and Data Resources

All hardware and software are the property of the City of Madison. All workstations, telephones, servers, and other networking devices must be approved by IT and Purchasing, per the City of Madison Policy for the Procurement and Disposal of Electronic Products (APM 4-7), before being connected anywhere on the network.

Privacy Rights Waiver

Employees should not expect privacy with respect to information transmitted, received, or stored on the City's network resources. By accessing the City network, the employee authorizes the City to access, inspect, monitor, and disclose material. IT will never ask for employees' passwords.

Usage Prohibitions and Restrictions

Computer resource usage prohibitions and restrictions are outlined in the City of Madison Appropriate Use of Computer Network Resources Policy (APM 3-9).

Network Infrastructure

Backup Systems

The City of Madison Backup Systems Policy outlines the standards of backing up files on the network as a means to restore information in the event of a disaster or incident.

File Storage

Files that need to be shared by multiple employees or with other City agencies, or need to be stored in a secure, disaster 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.

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 an authorized contact from the customer's agency.

Use of a common directory (e.g., ITCOMMON) 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 HIPAA-related information should not be stored in these directories.

On each file server resides a common directory as 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.

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 contact may request to have this structure created through the Help Desk.

Virtual Desktop Infrastructure (VDI)

Approved City employees and authorized third-parties (e.g., customers, vendors, etc.) may utilize the benefits of VDI and virtual machines (VMs). A person may receive permission to access this environment through approval from an authorized contact. City employees must obtain permission from an authorized contact within their agency. An agency may request that IT provide an audit trail of employees that access VDI.

There are two use cases for VDI as designated by IT: (1) remote access into a City-owned device that is connected to the City network; and (2) connecting to a VM.

Virtual Private Network (VPN)

Approved City employees and authorized third-parties (e.g., customers, vendors, etc.) may utilize the benefits of VPNs, which are classified as 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 City of Madison Network Connection Policy.

Additionally, the following should be noted on VPNs:

- It is the responsibility of employees to ensure that unauthorized users are not allowed access to City internal networks.
- External vendors are required to use a two-factor authentication method.
- 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.
- Gateways will be set up and managed by Network Operations (e.g., GlobalProtect).
- 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 network after four (4) hours of inactivity.
- The VPN session is limited to an absolute connection time of seventy-two (72) hours.
- All City employees must use a City-owned laptop and have a business need to access the City's internal network via VPN.
- Only City-approved VPN clients may be used.
- By using VPN technology with personal equipment, users must understand that their devices 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-owned equipment (i.e., their devices must be configured to comply with the City's Network 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's internal networks. Wireless devices and/or networks without any connectivity to the City'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 IT standard, is required.

All wireless access points and base stations must be registered and approved by IT. All wireless network interface cards (NIC) (i.e., PC cards) used in City devices must be registered and approved by IT. 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.

Workstations

Only workstations approved and setup by IT may be connected to the City network. The Help Desk is responsible for deploying patches to workstations on a monthly basis. All workstations must comply, at a minimum, with standard workstation types and configurations established by IT.

All software running on City workstations must be properly licensed, and any new software must follow the New Software Request Process (APM 3-20).

Workstation software categories are outlined in APM 3-9 Attachment A. All workstation software standards are inventoried in the City of Madison Technology Standards Directory.

Network Security

Formal IT Permissions Approval

Written approval from an authorized contact in the owner agency must be attained to add new network accounts and/or devices, grant network file rights, search archived emails, or install new application software on a work device. A list of all authorized contacts is available on the City's EmployeeNet.

Physical Security

Every City employee is responsible for maintaining physical security in City 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. Employees also carry valuable information and equipment with them – laptops, smart phones, and customer hardware.

City-owned work areas

- All City employees should have an employee ID badge to access City-owned work areas.
- When not in public areas of City-owned facilities, City employees and guests should carry their identification badge in a visible location.
- When stepping away from your computer workstation (either in a City office or elsewhere), lock the console of your workstation.

Conference rooms

Wireless access points in all conference rooms will be located on a network separate from the internal City network, but still behind a firewall. If City employees need to access the internal network from a conference network connection, they must use VPN. All conference rooms in all City offices will be configured in this manner. Many conference rooms have Wyse terminals for direct employee access to the City network.

Portable devices

City 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.

Primary and secondary Network Operations Centers

- No food or beverages are allowed in any of the Network Operations Centers.
- All doors to the Network Operations 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 Operation Centers.
- 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.

User IDs and Passwords

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

- Every customer must use a unique user ID that is associated with their name alone (i.e., no generic/shared user IDs are allowed).
- Network user IDs must comply with the City's standard naming conventions for network login names.
- Wherever possible, applications should use SLDAP or other approved and secure authentication methods. This is to validate user ID and password information that is stored in the City's enterprise network directory.
- City staff should not share their password with anyone. If an instance arises where someone requires access to another person's files, an authorized contact in the owner agency should contact the Help Desk to request a change in access rights for the account.
    - If a customer forgets their password, they should contact the Help Desk to request that a new, temporary password be assigned. The Help Desk will assign a new short-term password that will expire upon the user's next network login, and prompt the user to change their password.

- Passwords must meet or exceed the following rules in accordance with the City of Madison Password Policy:
    1. Must be at least 14 characters.
    2. No complexity required.
    3. Passwords expire every 180 days.
    4. Passwords may not contain the owner's email or any part of their name.
    5. Passwords cannot be a "common" word (e.g., it should not be a word in the dictionary or slang in common use).
    6. Should not contain words from any language.
- Only IT personnel, or security consultants contracted by IT, are authorized to run any form of security assessment tools with written approval from the IT Director.