



INFORMATION SECURITY AND TECHNOLOGY USE POLICY

Adopted:

Amended:

POLICY CONTENTS

A. Purpose.....	1
B. Scope.....	1
C. Definitions	2
D. Policy.....	2
E. Enforcement.....	9
F. Evaluation and Renewal Requirements.....	9
G. Roles and Responsibilities.....	9

A. Purpose

City of Shakopee maintains and communicates an Information Security Program to protect the confidentiality, integrity and availability of City of Shakopee information and information systems.

This program is established and supported by City of Shakopee executive management. The IT Director is responsible for implementation, support and ongoing management of the Information Security Program. All City of Shakopee users are required to understand and comply with this Information Security Policy. Security is everyone's responsibility.

The Information Security Program consists of the Information Security Policy (this document), Security Standards and supporting processes and procedures that:

- Support the implementation of information security best practices.
- Provide value to the way we conduct business.
- Support our organizational objectives.
- Serve to minimize risk to our organization.
- Allow for compliance with relevant legal, regulatory and compliance requirements.

B. Scope

This policy applies to users who have access to City of Shakopee information or information systems, including, but not limited to, elected officials, employees, vendors and contractors.

C. Definitions

- Information: any communication or representation of knowledge in any medium or form (i.e. electronic, physical, verbal).
- Information Security: the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.
- Information System / System Resources: individual resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposal of information (i.e. devices, network equipment, file management systems, software, messaging systems).
- User: any individual (or process acting on behalf of an individual) that has access to an information system (i.e. employees, contractors, suppliers).

D. Policy

1. Acceptable Use

- You have been provided access to City of Shakopee system resources based on your job responsibilities.
 - Do not attempt to access systems you have not been authorized to access.
 - Do not share your access (including passwords, tokens, access cards, remote access credentials) with anyone.
- You are provided access to system resources to enable you to do your job.
 - Use of system resources must be conducted in a productive, ethical and lawful manner.
 - Use of system resources must be in compliance with City of Shakopee's security standards set within this document.
 - Non-business activity must be limited, not interfere with work and not compromise City of Shakopee information.
 - The following activities are prohibited at any time on city resources for either business or personal use:
 - For any illegal or unethical activities
 - Adult or explicit material
 - Material advocating intolerance of other people, races or religions
 - For profit or commercial activities
 - For any other public office or employment incompatible with city employment responsibilities
 - For online wagering, betting or selling chances
 - For annoying or harassing individuals internally or externally

- Full-time employees are expected to conduct all electronic city business through their city-assigned email account, xxxx@ShakopeeMN.gov.
- Elected officials are provided with a City of Shakopee email account and is recommended to use those accounts for all city related correspondence.
- If a city related email communication is received from a full-time employee's personal email account, a city employee response should include the recipient's xxxx@ShakopeeMN.gov email address if available.
 - Part-time, paid-on-call, and seasonal employees who are not assigned a ShakopeeMN.gov email address can communicate with their supervisors through a personal email account for the purposes of schedule coordination and general communications of activities and information. Supervisors must still conduct all communications through their official ShakopeeMN.gov email if assigned.
- The internal business use of commercial email accounts, such as Gmail, is limited and is required to be documented with IT. The use of such accounts are limited to cases where the website, such as Youtube, or application, such as Google Analytics, requires the use of only a proprietary account.
- The city reserves the right to restrict all employees access to any website or an individuals' access to specific websites.
- We actively monitor our information system to protect the confidentiality, integrity, and availability of our information and information systems and your activity on system resources (including email, web browsing and instant messaging). All electronic communication is subject to monitoring with or without notification.
- If we suspect unauthorized activity, the city is obligated to take action. We may disconnect, wipe or quarantine any resource, including non-City of Shakopee resources that contain City of Shakopee information, to protect City of Shakopee information and/or information systems.
- Upon termination of employment or agreement, you must return all assets, including data, to City of Shakopee.
 - If you have City of Shakopee resources or information on personally owned devices, this information must also be removed upon termination of employment or agreement.

2. Data Protection, Security, and Privacy

- The City provides multiple networks to protect city data. Networks are designed for public use, employee use, and for protected CJIS information. Only approved authenticated users are provided access to the employee and CJIS networks. Users of the CJIS network must also be CJIS certified and approved through the Police Department TAC(Terminal Agency Coordinator).

- Computers installed in public locations or unescorted access by the public will not be joined to the city domain. This includes kiosks, certain conference and training rooms, and other general areas. These computers will only access internet resources through our public network.
- The work you do for the City of Shakopee is considered City of Shakopee property.
 - Do not share, sell or transfer City of Shakopee information outside of the organization unless you have been authorized to do so.
 - Do not use unapproved resources (i.e. unapproved online storage, unapproved applications, unapproved devices) to store or transmit information.
 - Do not post sensitive City of Shakopee information online (i.e. social media, publicly accessible websites) unless you have been authorized to do so. See Social Media Policy available internally on CityNet.
 - Any email, documents, Web search/history and written material has the potential of being part of a public data request.
- Many of the devices issued by the city contain device tracking functionality. Location and device usage tracking can be activated at any time with or without notification.
- You will access data of varying sensitivity and are responsible for complying with City of Shakopee's requirements for creation, transmission, storage or destruction of information and information systems based on sensitivity.
- The local data on your computer, laptop, or mobile device is not backed up by our automated backup software. You are responsible for saving all data to a network share, Laserfiche, or other approved application for long-term or permanent storage. This includes documents, photos, desktop items, and any locally stored databases. IT may not be able to restore locally stored items due to device theft, computer crash, or virus.
 - You are responsible for being aware of the City of Shakopee Data Practices and Records Retention policies and ensuring your actions are in compliance with the procedures put forth by the City Clerk's office. See Data Practices Policy available internally on CityNet.
- Your passwords provide protection against unauthorized access to information and, therefore, must be protected.
 - Do not share your passwords with others.
 - Make sure all passwords, including passwords to external systems not managed directly by City of Shakopee, follow password best practices, which include making passwords long, use passphrases, hard to guess, and not using common passwords.

- Weak passwords, such as **Summer2019**, can easily be guessed or cracked using very basic methods and should not be used. IT can scan periodically for weak passwords and will notify users to change their password immediately. Many data breaches occur due to cracked, weak, or stolen credentials,
- Use different passwords for your work accounts than you do for your personal accounts. Using duplicate passwords for multiple accounts increases the risk of a breach and malicious activity.
- If you think your account or password may be compromised, or is communicated by IT you may have been compromised, you are required to change your password immediately. If you are unavailable IT may change your password for you or disable your account until we can work with you on the incident.
- Third party vendors are not allowed direct unsupervised access to our managed IT systems. To gain access to a control system, such as HVAC, the vendor must be supervised by an employee familiar with that area or someone from IT.
 - This section does not apply to LOGIS. LOGIS is a trusted partner and has access to our systems.

3. Physical Security

- Be sure not to leave sensitive Personally Identifiable Information(PII) around your workspace, at printers, in meeting areas (including any dry erase boards or visuals), or in other areas that would allow for unauthorized access to information.
- When you step away from your device, lock your device screen.
 - If you take your device off-site, you must maintain physical control of the device at all times.
 - Do not leave devices unattended in public spaces.
 - Do not leave your device in a visible location in unattended vehicles (put it in the trunk or take it with you).
 - Make sure your screen is not easily displaying sensitive information to unauthorized people (i.e. shoulder-surfing).
 - If your device is lost or stolen, contact IT immediately.
- Access to IT datacenters and closets is restricted by job function and certification. In many cases, authorization is enforced by policies set by the BCA and FBI. Access to all IT data centers and closets is monitored, recorded and controlled centrally by Administration and IT.
- Do not prop doors open to locked employee workspaces and data centers.

- Be aware of your surroundings and visitors within your buildings. Report any strange activity that does not feel or look normal.

4. Device and Data Destruction

- All city of Shakopee computers will be reused internally, recycled or destroyed after they are taken out of service. All device hard drives slated for destruction will be stored in a locked environment for security purposes. Prior to any recycling, all hard drives within computers, tablets, laptops, and phones will be physically destroyed internally, or other approved method, and witnessed by IT staff through a consistent documented method. Recycled and destroyed computers are logged within an inventory system.
- Any physical devices, such as a USB stick, no longer needed with critical data should be given to IT for disposal. IT will destroy the device and data in the same manner as other drives.

5. Tools and Technology

- In order to protect City of Shakopee information, all devices and equipment must be approved for internal employee network access to system resources. Do not purchase any IT device for internal city use without approval from IT staff.
 - Do not physically connect unauthorized hardware to our City of Shakopee employee internal network. This includes vendor computers for presentations or system work.
 - Use of the guest Wi-Fi is for these non-approved devices.
 - On the rare occasion a vendor needs a physical network connection, IT will need to reconfigure the network jack for the public network. This configuration change will require advanced notice for IT.
- Mobile Device Management(MDM) is required and enforced on all city and personal mobile devices connecting to our email system. Do not attempt to override this protection on your mobile phone.
 - Use of personally owned devices, such as cell phones, is approved for city email access. Personal devices are not supported by IT and are not guaranteed to be compatible with current security standards and may be blocked by MDM.
- Multi-Factor Authentication(MFA) is required for external access to email and multiple other applications on externally connected devices and networks. You will be prompted and required to setup MFA before access is granted.

- Only authorized removable media is allowed to be plugged into City of Shakopee information systems. USB devices should not be shared and plugged into computer systems outside of the City of Shakopee. See IT for scanning of devices you obtain from outside sources.
 - Never plug in a USB device which has been found randomly. Intentionally dropped USB sticks are a well-known tactic for distributing malicious files. The USB sticks may even have something enticing written on them to raise curiosity.
- Do not attempt to override any of the City of Shakopee implemented security features of your device and/or the network.
 - Unless you have been explicitly authorized to do so, do not attempt to test, break, remove or otherwise penetrate our security features and/or system resources.
- You are required to use approved applications to perform city functions. This includes applications to transmit, store or process City of Shakopee information.
 - Do not download or install unauthorized or unlicensed software.
 - Do not illegally copy material protected under copyright law or make that material available to others for copying.
- Practice electronic communication best practices.
 - Log out of applications when you are no longer using them.
 - Do not open an attachment from unknown sources or known sources if the message was not expected.
 - Do not click on links in messages from unknown sources or known sources if the message was not expected.
 - Think before you click on anything.

6. Patch Management

- Employee workstations are set to automatically update Microsoft operating system security patches monthly. If patches do not automatically install, users are asked to install and reboot the computer system you are using as prompted. Follow up by IT staff will be required if computer systems are not patched.
- All Shakopee servers will be patched every month by IT staff.
- Any Hotfix , patch, or action that is deemed critical for immediate installation will be released to all machines within the city and installed. Computers within the domain will be tracked for compliance. Machines and devices not on the domain will be completed manually.

- Patching local workstations is one of the critical first lines of defense to a more secure environment. Do not bypass patching of computers for sake of convenience.

7. Wireless Connectivity

- Wireless connectivity is provided for the convenience of mobility and the flexibility of employees and other users. There is not an expectation of wireless functionality in every facility or every space within a facility.
- The segmented employee WIFI network is for authenticated users and the public network is for all non-authenticated users.
- All wireless traffic is monitored for content and goes through a filter for appropriate viewing of sites. All traffic is recorded and logged for auditing purposes and can be reviewed at any time.
- City devices should not be connected to public external WIFI networks outside of your home network. It is highly recommended if you are going to need a public external WIFI connection off-site to use your mobile phone or a city mobile hotspot. Public places like coffee shops and hotels are not guaranteed safe wireless access points and are not recommended as a safe practice. IT has a mobile hotspot for loan and should be used as available.

8. VPN Connections

- VPN(Virtual Private Network) connectivity will be provided on an as needed basis for specific job functions. VPN allows users to connect to internal resources when at a remote location. VPN authorization is not set by default and must be formally requested. VPN access is only approved for use on city owned devices.
- VPN users that have access to critical, restricted, and sensitive information are required to use MFA(Multi-Factor Authentication) to connect to the internal network. IT will provide the method of VPN MFA to the approved user and connection to city resources are not available without it.
 - If the MFA Token is lost you must contact IT immediately so the device can be disabled/revoked. A new token will be provided as soon as possible.

9. Training and Awareness

- You are required to participate in a Security Training and Awareness program as required by HR.
 - New users must participate in information security training as part of onboarding.
 - All users must participate in ongoing awareness training.

- You may be assigned role-based training depending on your job responsibilities.

10. Reporting

- You should report any potential security incidents or concerns as soon as possible.
 - Incidents may include but are not limited to: lost/stolen devices, policy violations, unauthorized access, unusual activity on your device or on company property.
 - You are required to report the incident to your supervisor and directly to IT.
- If you suspect a computer virus, worm or other malicious content infection has infected your device, disconnect the device from the network (if able) and report it immediately to IT.

11. Incident Response

- Incident response to any IT situation is taken with great seriousness. Everyone should feel the responsibility to report any issue they feel necessary to management and IT.

E. Enforcement

All City of Shakopee users are responsible for complying with this Information Security Policy.

A violation of this policy or supporting standards may result in disciplinary action, up to and including termination. Violators may also be subject to legal action, including criminal prosecution. City of Shakopee also reserves the right to take any other action it believes is appropriate.

F. Evaluation and Renewal Requirements

The City of Shakopee will evaluate the effectiveness of the Information Security Program no less than annually.

G. Roles and Responsibilities

1. Management – Management will demonstrate leadership and commitment with respect to the Information Security Program by:
 - Ensuring the Information Security Program is established and compatible with the strategic direction of City of Shakopee.
 - Ensuring the integration of the Information Security Program requirements into the City of Shakopee's processes.

- Ensuring that the resources needed for the Information Security Program are available.
 - Communicating the importance of effective information security and of conforming to the Information Security Program requirements.
 - Ensuring that the Information Security Program achieves its intended outcome(s).
 - Directing and supporting persons to contribute to the effectiveness and continued improvement of the Information Security Program.
2. IT Director - The IT Director will have responsibility and authority working with HR for:
- Ensuring that the Information Security Program conforms to security requirements and standards.
 - Maintaining documentation to support the Information Security Program and making information available to related personnel.
 - Monitoring, measuring, analyzing and evaluating the Information Security Program for continued effectiveness and improvement.
 - Overseeing internal audits to verify the City of Shakopee is meeting information security requirements.
 - Maintaining appropriate contacts with relevant authorities (i.e. law enforcement) and special interest groups (security forums, professional associations).
 - Addressing information security in organizational projects.
 - Reporting on the performance of the Information Security Program to executive management.
3. All Users - City of Shakopee employees, contractors, elected officials and suppliers are in the scope for the Information Security Program. Everyone is responsible for the safety and security of information, computer systems, physical assets, and devices within the City. Practicing safe computer use and thinking before you click will decrease malware infections, alleviate the loss of credentials, and lessen the possibility of information loss.

CITY OF SHAKOPEE
INFORMATION SECURITY AND TECHNOLOGY USE POLICY

**Please return a signed copy of this signature page
To the Human Resources Office**

Employee signature

I have received and read the above Information Security and Technology Use Policy and have had an opportunity to ask any questions. I understand that my failure to follow these policies may result in disciplinary action including revocation of system privileges.

Print Employee Name

Print Department Name

Employee Signature

Date