STAFF REPORT

DATE: December 12, 2023
WORKSHOP

TO: Mayor and City Council
FROM: Karissa Goers, Administrative Services Director
AGENDA ITEM: Telework and AI Policy

BACKGROUND:
Currently, the City of Lake Elmo has no telework or artificial intelligence usage policy.

ISSUE BEFORE COUNCIL:
Does the council have any questions or recommendations regarding the proposed personnel policies?

DISSCUSSION:
A telework policy is a good workplace and business strategy to attract new talent and improve retention of current employees. This policy is intended to provide a flexible work location for eligible employees to maintain productivity and enhance job satisfaction.

In preparing to add a telework policy, it was found that a computer and internet use policy was also missing from the City personnel policies. A computer and internet use policy outlines expectations and permitted uses that need to be followed by staff in order to protect the integrity of the City's information system.

Metro-INET has created an acceptable use policy that will go into effect on 1/1/2024 and all employees of cities obtaining IT services through Metro-INET will be expected to follow the policy. Their policy aligns with the proposed computer and internet use policy and staff found it efficient to present them at the same time.

Additionally, artificial intelligence (AI) enhanced services have become increasingly popular and mainstream. Many software applications now have embedded AI tools including Microsoft 365, which is the software the City uses. Staff recommends implementing an AI policy to lay out expectations and acceptable uses for AI for city staff.

FISCAL IMPACT:

None

ATTACHMENTS:

- Telework policy
- Telework agreement
- Computer and internet use
- Metro-INET acceptable use
- AI policy
- AI Flowchart

TELEWORK

It is the policy of the City of Lake Elmo to permit employees, under certain circumstances, to conduct work remotely. Telework is intended to provide a flexible work location for eligible employees and business-related benefits to the City, including attracting and retaining a skilled workforce, supporting continuity of operations, and maximizing efficiency and cost savings. Telework arrangements are a business and workplace strategy, not an employee benefit or employee right, and approval or denial is at the sole discretion of the City. Telework may not be an option for all employees depending on factors that may include but not be limited to, employee job performance and current job duties, the business needs of the department and its customers. This policy guides the practice of working from locations other than City office buildings or properties and provides standards and expectations for all City telework arrangements.

Teleworkers will always be cognizant of the public's expectation of efficient, effective, and responsive service from all City employees. Both actual and apparent conflicts with this expectation must be avoided and the existence of any such conflicts will result in termination of the telework arrangement and/or disciplinary action.

DEFINITIONS

Telework: A work arrangement approved by the department director and city administrator that permits employees to work offsite in their homes or other approved location other than City buildings or properties.

City work conducted by employees at a non-City work site as required by their functional job responsibilities is not considered telework (e.g., building inspectors at a building site, firefighters on a call). Exempt staff performing incidental tasks (e.g., checking email, responding to voicemails, etc.) while on unpaid time (e.g., Paid time off, or after work hours) is not considered telework.

Teleworker: An employee who is authorized to work remotely. No employee may telework exclusively.

Onsite worker: An employee whose job cannot be performed from a telework location and/or who is not authorized to telework, or chooses not to telework.

Telework location: An approved location other than City buildings, typically an employee's home, at which the employee is authorized to telework.

Primary work location: The City building which is the employee's assigned work location when working onsite. All employees will have a primary work location and must be prepared to work at that location when required.

Telework Schedule: Work arrangement, including hours and days of work, agreed to by the teleworker and the department director, reflected in the *Telework Agreement*, during which the employee will be working remotely. Telework schedules may vary by job or employee but will generally be consistent with those of their department and colleagues.

TELEWORK OPTIONS

Routine/Long-Term – a telework arrangement that lasts for more than four (4) weeks where employees may work remotely up to two (2) days per week. Telework days are regular, scheduled agreed upon days that do not vary from week to week (e.g. every Tuesday).

Situational/Intermittent – May be planned or unplanned. Telework days are approved by the supervisor on an as-needed basis. Employees wishing to have this telework arrangement must complete the telework agreement prior to requesting any intermittent telework days. For example, an employee may work from home when there is inclement weather, they have a repair service coming to the home, or they want uninterrupted work time for a special project.

Generally, an employee will choose between a routine or situational telework option. All telework options require approval by the supervisor, department head, Administrative Services Director, and City Administrator and must meet all requirements as defined in this policy.

TELEWORK

ELIGIBILITY

To be eligible to telework, the employee's job must be suitable to telework, and the employee must meet the following criteria:

- Must have and maintain a satisfactory performance.
- Have been employed with the City for three (3) or more months.
- Maintain a reliable high-speed, broadband internet connection. The internet connection speeds must be verified, and the employee shall provide a screenshot of the speed test results with the *Telework Agreement* form, showing both the download and upload speeds.

Department Directors are responsible for determining if a job is suitable for telework and if an employee is capable of teleworking. Each telework agreement will be determined on a case-by-case basis using the following criteria:

- The business needs of the department.
- Ensuring business coverage is maintained - a minimum of one employee from each department will be available on site at the primary work location during business hours.
- The employee's duties and responsibilities.
- The employee's ability to perform job duties from a remote location, e.g., customer facing, providing office coverage, etc.
- Ability to perform job duties during approved work schedule and be available during normal work hours.
- Employee's current and past job performance.
- Expectations for future performance by the employee and how performance will be measured.
- Positive or negative effects on quality customer service.
- Positive or negative effects on the department, division, and City of Lake Elmo as a whole.
- Availability of high-speed internet at the remote work site.
- Whether the employee has demonstrated essential work skills, such as time management, organization skills, self-motivation, and the ability to work independently.
- Other potential distractions to the teleworker should be considered and conflicting demands resolved in advance of commencing a teleworking agreement.

APPROVAL PPROCESS AND TELEWORK AGREEMENT

1. Employees shall complete and submit to their supervisor the *Telework Agreement* form along with a screenshot of their internet download and upload speeds.
2. The supervisor and the employee will schedule a meeting to discuss the telework arrangement. This meeting is an opportunity to ask clarifying questions and ensure that both the supervisor and the employee have a mutual understanding about the expectations for the arrangement.
3. If the supervisor approves the request, they are responsible for consulting with the Administrative Services Director to ensure all technology requirements are met before signing the agreement and obtaining Department Head and City Administrator approval.
4. Completed forms will be placed in the employees' personnel file in the administration department.

Modifications to the telework agreement or a change in the employee's position require a newly completed *Telework Agreement* form. Telework agreements shall be reviewed by the supervisor and renewed (at a minimum) annually.

TERMS AND CONDITIONS OF EMPLOYMENT

An employee has no automatic right to telework, and the City has the right to refuse or deny any teleworking request from an employee. The City and/or the employee may terminate a telework agreement at any time for any reason.

Teleworking does not change the terms and conditions of employment such as salary, benefits, or job responsibilities and work tasks. When working from a telework location, that location will be considered

the temporary place of reporting. Teleworkers work at an approved location during work hours as agreed upon by the teleworker and supervisor and will not do work at any other time or anywhere else unless approved by their supervisor.
Teleworkers do not receive a special commuting allowance when working at the telework location. Overtime, compensatory time, or leave provisions contained in City policies are not altered to accommodate a telework arrangement.

Teleworkers are responsible for having a designated workspace suitable for completing the work assigned. The area should be free of health and safety hazards and/or obstructions. Teleworkers are responsible for all expenses necessary to set up their telework location, including expenses associated with establishing, maintaining, and modifying workspaces and internet connectivity. Additionally, teleworkers will not receive any mileage reimbursement for commuting between their telework location and primary work location.

PERFORMANCE STANDARDS AND EXPECTATIONS OF TELEWORKERS

Performance standards for teleworkers are no less than those of employees working in City offices or buildings doing the same work. If modifications to the standards are necessary, they must be discussed with and approved by the supervisor.

Employees entering a telework agreement will generally have a telework schedule consistent with their work schedule and provisions of the telework arrangement. Work schedules for onsite and offsite work hours are pre-approved by the employee's supervisor if different from the arrangement specifications.

Teleworkers will be as accessible and available as their onsite counterparts during their agreed upon telework schedule, regardless of work location. Teleworkers are expected to be available and working during all hours of their telework schedule. They must be available by telephone, email, Microsoft Teams, and video conferencing at a minimum. This includes, without limitation, attending scheduled meetings using applicable technology or onsite and being available to customers, clients, coworkers, supervisors, and others. Business meetings and vendor/client visits in the employee's home are prohibited.

There will be times when teleworkers will be expected to be at the primary work location on days when they have scheduled telework hours, such as for mandatory meetings and training, and when the need to conduct city business in person is necessary. Supervisors may recall teleworkers back to the primary work location during emergency situations to assist in mitigating the situation. In these circumstances, the employee can resume normal teleworking once the meeting, training, or emergency is over.

Non-exempt (hourly) employees must report actual hours worked and may not work overtime or additional hours, without advance approval by their supervisor.

Teleworkers must comply with all applicable City rules and regulations as well as any applicable departmental rules, policies and procedures. All Teleworkers must comply with time reporting and overtime procedures as outlined in the personnel policies manual.

The employee shall inform their supervisor of any absences from the teleworking location during scheduled work hours. Paid time off should be utilized as usual for illnesses, appointments, etc. as noted in Annual Leave policy. If a teleworker is found to be unavailable during their telework hours, it may be grounds for disciplinary action including termination of the telework agreement.

In Accordance with Worker's Compensation Insurance, in the event of work-related injury while teleworking, the employee is required to notify their supervisor and the Administrative Services Director and complete all necessary reports for reporting an accident/incident.

Telework is not:
- A viable work arrangement for all positions or well suited to all employees.
- An accommodation to complete personal or other non-City endeavors during work hours.
- Telework is not for the purpose of allowing an employee to provide dependent care. Teleworkers who

work at home will manage dependent care and personal responsibilities in the same way they meet these responsibilities while working at their primary work location and in a way that allows them to successfully meet job responsibilities.
- Telework is not a substitute for using paid time off (PTO).
- Considered a contract or guarantee of continued employment.

DATA MANAGEMENT AND SECURITY

City owned equipment shall be treated the same as if it was in the primary work location. Internet usage on City owned equipment may still be tracked. No rogue or outside software shall be installed and the devices shall be encrypted. Software installations may only be completed by Metro-INET. Telework computers will receive standard windows and antivirus updates over the approved network connection.

Teleworkers must take all necessary precautions to keep City data and information secure and to prevent unauthorized access to any City system or information from the telework location. The City's normal data privacy and security policies and procedures apply equally to telework. Teleworkers are also responsible for complying with all federal and state laws and regulations that apply to their work.

Each employee shall complete cyber security training twice annually.

TELEWORK SCHEDULE AND LOCATION

Telework schedules must be consistent with the Hours of Work policy. Department Directors are responsible for developing telework schedules for each teleworker on their team by balancing their department's business needs and the teleworker's desire for flexibility. Telework schedules should generally occur during normal work hours as defined in the Hours of Work Policy. Teleworkers are responsible for complying with all City policies, including specifically the provisions of the Payroll and Compensation Policy regarding time tracking.

Travel to and from the primary work location for purposes of meetings or other work requirements shall not be considered compensable hours and mileage will not be reimbursed.

A teleworker who is scheduled to work remotely on a day that is declared to be an emergency closing is expected to work remotely as scheduled.

All telework locations must have an identified workspace, free from distractions, be approved in advance by the teleworker's supervisor, and be maintained by the employee. Prior to approval of telework, the telework location may be assessed for compliance with applicable requirements. This includes home and other telework locations.

The City has the right to make a site visit to the telework location to ensure proper procedures are being followed including, but not limited to, employee and work site suitability, protection of data, the assurance that safe working conditions exist, and to maintain, repair, inspect, or retrieve City owned equipment as necessary. Teleworkers must allow access to their remote workspace for the purpose of performing work site inspections as requested.

For regulatory reasons, staff are not generally allowed to telework from any location outside of Minnesota or Wisconsin unless specifically traveling for a work purpose (e.g., work conference) and approved to do so by their department head. The City Administrator, at their discretion, may approve limited telework outside of Minnesota or Wisconsin to meet City business needs.

EQUIPMENT

The City will provide equipment and related supplies for use by the teleworker. Any equipment supplied by the City for the use at a telework location may not be used for personal purposes by the employee or non-city employees as outlined in the Computer and Internet Use policy.

Teleworkers shall promptly notify their supervisor of equipment malfunction, failure, theft, or damage of City owned equipment. In the event of delay in repair or replacement of equipment or any other circumstance under which it would be impossible for the employee to telework, the employee will return to the primary work location to work.

Equipment, hardware, software, supplies, documents and other information or property remain the property of the City no matter where it is located and shall be returned prior to termination of employment or at the request of the City.

DISCLAIMER

Telework agreements can be modified or terminated by the City at any time. Failure of the teleworker to comply with all relevant laws, policies, provisions, requirement or expectations, or the terms of the telework arrangement may result in the loss of telework privileges and/or disciplinary action as necessary or appropriate.

Telework Agreement Form

Employee Name: Position:

Supervisor: Date:

Requested start date: Telework location:

Is this the employee's home: ☐ Yes ☐ No If no, where is the telework location:

Type of Telework Arrangement requested: ☐ Routine ☐ Situational

If routine, what day(s) of the week you are requesting to work remotely:

☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday

Which of your job tasks and percentage of time for each could be done remotely?

_____

_____

By signing below, I confirm that I have read and understand the Telework Policy. I understand that prior approval is required and my telework arrangement can be cancelled at any time for any reason, by the City or myself.

Employee Signature Date

Frequency and type of contact between employee and supervisor on remote days will be:

_____

_____

Supervisor Approval Date

To be completed by the Administrative Services Director

Criteria for consideration:

☐ Employee has been employed with the City for at least three (3) months.

☐ Employee has a satisfactory work performance.

☐ Employee has a reliable broadband internet connection and a screenshot of speed test (completed by www.highspeedinternet.com) is attached.

Equipment Provided by the City:

☐ Laptop ☐ Desktop ☐ Monitor ☐ Keyboard ☐ Mouse ☐ Other_____

Administrative Services Director Approval Date

Department Director Approval Date

City Administrator Approval Date

*Return completed form to the Administrative Services Director to be kept in the employee's personnel file. *

COMPUTER & INTERNET USE

The purpose of this policy is to protect the quality and integrity of, while minimizing the risks to, the City's information system. This system is vital to performing City functions. The City's Administrative Services Director is responsible for developing and maintaining procedures that best serve these purposes. In addition to this policy, City staff are required to follow the Metro-INET Acceptable Use policy.

DATA MANAGEMENT AND PROTECTION

Data Storage:

1. **Back-Up**: All data shall be stored on the network server. This ensures that all data is backed up daily.

2. **Agency Access**: All network users will have rights to the "Shared" directory. This directory should be used for sharing files with other departments.

3. **Department Access**: Each department may have additional access to directories of the file server and each user within the department will have a sub-directory under the department directory. The department directory will be accessible to all users within that department.

Management of Files

The storage capacity of the network server is limited. Therefore, all users are responsible for deleting their own outdated files.

Portable Files

Only appropriate files may be copied to City computers. Under no circumstances may a user copy to or from an agency computer, any program files or any executable files (e.g., games, screensavers, etc.). Users bringing files home and back are responsible for following this policy and should **pay special attention to the virus protection guidelines herein.**

Work Product Ownership

All information developed on the City computer system or introduced to the City computer system becomes the property of the City, regardless of where it was created. All information developed by city employees on computers outside the city, if in conjunction with their employment at the city, is the property of the City. Copies of all such files must be provided to the city, which has exclusive rights to retain, maintain and modify these files.

USE OF EQUIPMENT

General Use

The primary purpose for use of the City's computer equipment is agency business.

Only City employees may use the City's computer equipment. Use by any other party requires prior approval of the City Administrator. City employees must use their assigned login identification (ID) when connecting to the network. Users should never login under another employee's ID.

Portable Equipment

Only portable equipment (e.g., laptop computers, tablets, phones, computer accessories) may be removed from City buildings. This equipment must be checked out through the Administrative

Services Director and may only be used for City business. Employees are expected to provide appropriate protection against theft, accidental breakage, environmental damage and other risks, for any equipment in their possession.

Desktop computers and attached devices shall not be removed from City buildings.

INSTALLATION OF HARDWARE AND SOFTWARE

Installation

All hardware and software shall be installed or downloaded by Metro-INET. Users who wish to run product demonstrations or download information from bulletin boards or the Internet should contact the Administrative Services Director/City Clerk prior to doing so.

Configuration

Individual workstations are configured to operate in a complex network environment. Users shall not change their system's set-up files. Users who have a concern about the configuration of their set-up files should contact the Administrative Services Director.

Licensed Software

The City complies with all software copyrights and terms of software licenses. City employees shall not duplicate licensed software or related documentation. Any such duplication may subject employees and/or the City to both civil and criminal penalties under the United States Copyright Act.

Only software obtained through the City's acquisition process will be used on City computers. City owned software shall not be loaded on external systems.

SYSTEM SECURITY

Overview

Electronic information is a significant asset of the City. The goal of system security is to protect from unauthorized or inappropriate access or modification.

Control of Security

Users shall not add additional security to their workstations or files. Users who believe they have security needs beyond current settings should contact the Administrative Services Director.

User Access Controls

All users shall identify themselves to the system by signing on with their assigned login ID.

Employees must use a password when logging in to the system. Passwords shall not be shared, apart from the user's department head and/or the Administrative Services Director. Users must notify their department head of any new passwords or revisions of passwords of any type.

Users who will be away from their computer for a long period of time should logout of the system.

Access to Data

The user's ability to view, add or modify information in network files is based on access rights configured by Metro-INET. Employees must contact the Administrative Services Director to request changes to user access rights.

Virus Protection

Users are responsible for having ALL disks, jump/flash drives or other media storage devices scanned for viruses prior to their use. This includes but is not limited to; disks brought from home, downloaded files, disks or files received from outside agencies or people, and diagnostic disks brought in by technicians. Users needing to scan a disk should contact Metro-INET.

Users of portable equipment need to virus scan the hard drive of such equipment prior to connecting it to the City's local area network.

Users are responsible for any e-mail received. As some e-mail messages may contain viruses, users are not to open an e-mail message or click on any links and/or attachments if the origin of the message is unknown.

INTERNET POLICY

The City's Internet access has been installed to facilitate communications and information gathering for City business. Internet access is the property of the City and is intended to assist City employees in the performance of their jobs. The following policy describes the proper use of the Internet and the rights of City management to access information obtained through this system.

DEFINITIONS

Internet: A global computer network which joins government, educational institutions and private computers together over high-performance communication lines. The Internet is a rich source of information, electronic commerce and personal electronic communications.

Downloading: The transfer of computer files from one computer storage device to a different computer's storage device.

Browser: A computer program used to access the Internet with the ability to search the Internet for information. This program resides on the individual's workstation.

GENERAL INFORMATION

1. All information taken off the Internet should be considered suspect until confirmed by another source. There is not a quality control process of the Internet. Information obtained has the potential to be inaccurate or outdated.

2. The Internet will not provide private or confidential electronic communications. Users should understand that ALL communications created, received or backed up on City systems may be construed to be public documents and thus may be subject to legal requests for public disclosure.

3. Management reserves the right to examine e-mails, files & directories, internet usage, and any hardware containing City property. This examination ensures compliance with all legal requirements, internal policies and assists with the management of the City's information system.

4. Users should consider their internet activities as being periodically monitored and should act accordingly.

INTERNET USAGE

1. **Permitted Uses**

a. The primary purpose of City Internet access is City business.

b. Limited, occasional use of the Internet for personal purposes will be permitted only under the following conditions:

    1. Personal use is only allowed during non-work hours.

    2. Personal use does not interfere with another employee's business use of the Internet. (e.g., Too many employees are browsing during their lunch break that the response time slows down and employees working on City business are adversely affected.);

    3. Employee is currently performing at a ranking of satisfactory or higher; and

    4. Use complies with all parts of this policy and the Metro-INET Acceptable Use policy.

c. Only City employees, council members, contractors, and verified visitors are allowed to use the City's Internet access. Any exceptions to this rule must have the prior approval of the City Administrator.

d. Employees with a browser are responsible for compliance with this policy. It is required that employees with browsers have access to their workstation protected by password.

    Users should be aware that as the number of browsers and amount of time spent on the Internet by users increases, the response time of Internet functions will decrease.

e. Users are required to respect the legal protection provided to programs and data by copyright, license and privacy laws.

f. Users must conduct themselves in a manner that is consistent with City goals and policies.

2. PROHIBITED USE OF COMPUTER EQUIPMENT AND INTERNET ACCESS

The following is a list of those activities which, if conducted, may result in disciplinary action, up to and including termination of City employment and potential civil and/or criminal charges. City computer equipment and/or Internet access shall not under any circumstances be used for:

a. political purposes, religious reasons, harassment activities, obscene activities, racial or ethnic discrimination or any illegal activity;

b. gambling, fundraising, operating/conducting a private business, or for private gain or advantage;

c. presenting personal opinions or misinformation about the City, its programs, policies or personnel; and

d. activities that interfere with or disrupt network users, services or equipment.

e. Users shall not seek to breach system security, nor assist others in doing so.

3. INTERNET MONITORING AND BLOCKING

a. The City does monitor its internet access.

b. The City does block inappropriate websites. If users find a site blocked while performing your job duties inform your Department Director.

VIOLATIONS OF POLICY

Violation of these policies may result in the cancellation of the violator's access to City computer equipment and/or Internet browsing and Internet e-mail accounts and may be grounds for disciplinary action up to and including termination of employment with the City.

Metro-INET Acceptable Use Policy

VERSION 3.0

Table of Contents

Audience

This policy applies to any person using Metro-INET information systems and Metro-INET affiliate (hereon referred to as “agency”) equipment. Including, and not limited to, all employees, appointed and elected officials, contractors, and volunteers.

Overview

This policy serves to protect the security and integrity of Metro-INET’s electronic information systems by educating employees about appropriate and safe use of available technology resources. This policy is meant to provide a minimum-security baseline and supersedes any less restrictive policy.

Metro-INET reserves the right to inspect, without notice, all data, emails, files, settings, or any other aspect of an agency computer or related system, including personal information created or maintained by an employee as determined by the Metro-INET Information Security Manager or agency designated representative.

Beyond this policy, Metro-INET may distribute information regarding precautions and actions needed to protect Metro-INET systems; all employees are responsible for reading and following the guidance and directives in these communications.

Requests for exceptions to this policy can be submitted to Metro-INET and by completing the Metro-INET Risk and Treatment Acceptance form.

Identities

Account owners are responsible for the accounts assigned to them and for the actions taken with those accounts.

Accounts must not be shared without prior authorization from Metro-INET, except for calendars and related calendaring functions.

Accounts require a Metro-INET Acceptable Use Policy review and acknowledgement and must meet the Metro-INET Access and Identity standard. Accounts may automatically expire after specific timeframes at the discretion of the Metro-INET Information Security Manager.

Passwords

Passwords shall never be shared. If it is necessary to access an employee’s computer or files, contact your supervisor to review or request assistance from Metro-INET.

Metro-INET will not provide access to accounts without the approval of the Metro-INET Information Security Manager.

Passwords shall not be stored in any location on or near the computer or stored electronically such as in a cell phone or other mobile device other than an encrypted password manager solution. (Example: Microsoft Authenticator App)

Employees are responsible for maintaining computer/network passwords and must adhere to the Metro-INET Identity and Access Standards. Metro-INET Identity and Access Standards may be updated at the discretion of the Metro-INET Information Security Manager.

Advanced Authentication (example: Multi-Factor Authentication) is required when available for access to Metro-INET network resources.

Network access

Equipment not owned by a Metro-INET agency used in an agency building should only use the guest connection to the Internet unless approved by Metro-INET.

Metro-INET will review the Metro-INET network and connected devices for vulnerabilities and implement appropriate mitigation or remediation measures.

Metro-INET will not remotely access an active session without the logged-in account owner's permission to ensure integrity of access logs.

Reasonable availability is expected of both Metro-INET and those requesting support.

Remote Access

Examples of remote access include and are not limited to: Microsoft 365 / cloud services, virtual private network (VPN), Windows Remote Desktop, and Windows Terminal Server connections.

All aspects of the Metro-INET Acceptable Use Policy apply while connected to Metro-INET resources remotely.

Remote access to the Metro-INET network requires a request from a supervisor and approval from the Metro-INET agency designee.

All remote access connections to Metro-INET networks shall be made through approved remote access methods employing encryption and advanced authentication.

Remote access from a device not supported by a Metro-INET requires current Operating System, applications, and anti-virus software. It is the owner's responsibility to ensure all critical and security updates are installed prior to connecting. For additional information review the Metro-INET Computer Security Checklist.

Remote access privileges may be revoked at any time by an employee's supervisor or Metro-INET Information Security Manager.

Recreational use of remote connections to the Metro-INET network is strictly forbidden.

Private or confidential data should not be transmitted over an unsecured (public) wireless connection.

Clear Screen

Applications or network services shall be logged out or disconnected when they are no longer needed.

Workstations and laptops shall be logged out or locked when unattended.

Metro-INET may configure Metro-INET supported devices to automatically lock after a set duration of inactivity.

Data

Metro-INET cannot guarantee the privacy of any data stored on, transmitted, or accessed from an agency computer, device, or network. Employees should not assume any expectation of privacy.

Use of approved encrypted solutions is required when sending sensitive information outside of Metro-INET networks.

Information must be appropriately shared, handled, transferred, saved, and destroyed, based on the information sensitivity and the individual agency data practices policies and record retention schedule if applicable.

Disclosure of Public Information must not violate any pre-existing, signed non-disclosure agreements.

At the discretion of Metro-INET Information Security Manager, data may be reviewed by authorized staff without notice to the employee.

Management must be notified in a timely manner if sensitive information has been or is suspected of being lost or disclosed to unauthorized parties.

Communications

Metro-INET provides access to email and instant messaging services for work-related use. Incidental personal use of the communication systems by employees is allowed, provided it does not interfere with an employee's work and is consistent with all applicable policies.

All communications may be considered public data for both e-discovery and information requests and may not be protected by privacy laws.

Automatic forwarding of electronic messages outside the Metro-INET network is prohibited, except for members of governing bodies who have auto-forward enabled as of the effective date of this policy.

Communications, attachments, and links from an unknown sender should be reviewed with caution. Report suspected malicious communications to Metro-INET. Do not respond to suspicious senders.

Electronic communications shall not misrepresent the originator, agency, or Metro-INET.

Any use of Metro-INET communication methods should not:

- Involve solicitation
- Be associated with any political or religious entity
- Have the potential to harm the reputation of Metro-INET or agency
- Propagate chain emails
- Contain or promote anti-social or unethical behavior

- Violate local, state, federal, or international laws or regulations
- Result in unauthorized disclosure of Metro-INET or agency confidential information
- Or otherwise violate any other policies that have been approved and adopted

Internet

Information found on the Internet and used for agency work must be verified to be accurate and factually correct.

Reasonable personal use of the Internet is permitted. Employees may not at any time access inappropriate sites. Some examples of inappropriate sites include but are not limited to adult entertainment, sexually explicit material, or material advocating intolerance of other people, races, or religions.

Internet use found to compromise the integrity of the Metro-INET network will result in restricted access. Metro-INET will notify the account owner's manager and/or agency Human Resources to rectify the situation.

Metro-INET may monitor or restrict any use of the Internet without prior notice, as deemed appropriate by the agency Human Resources or Metro-INET Information Security Manager.

File Storage and Transfer

Metro-INET does not backup data stored locally on computers and holds no responsibility for data recovery on local computers. All agency-related electronic files should be stored in identified network locations.

Electronic files, including emails and business-related materials created on an employee's personal computer for agency business, must be stored in designated locations. Agency-related files should not be stored on an employee's personal computer, unless otherwise defined in policy.

Electronic sensitive information shall be stored in a location on the Metro-INET network that is properly secured.

Electronic sensitive information shall be encrypted if transferred outside of the Metro-INET network.

Removable Media

The use of removable media for storage of agency information must be supported by a reasonable business case.

All removable storage media (e.g., CD-ROM, flash or USB drive, or other storage media) must be verified to be virus-free prior to being connected to Metro-INET supported equipment.

Only agency owned removable media is permitted for storage of agency information.

All removable media must be stored in a safe and secure environment.

The loss or theft of a removable media device that may have contained agency information must be reported to your supervisor immediately.

Metro-INET can assist in the encryption of media.

Hardware

In general, Metro-INET or the agency will provide the hardware required for an employee to perform their job duties. Requests for new or different hardware should be made to your supervisor, who will forward the request to Metro-INET for review to ensure appropriate standards are satisfied.

Only agency staff may use agency computer equipment. Use of agency equipment by family members, friends, or others is strictly prohibited.

Employees are responsible for the proper use and care of agency computer equipment. Computer equipment must be secured while off premises. Computer equipment should not be exposed to extreme temperature or humidity.

Metro-INET may encrypt the storage of Metro-INET supported hardware to prevent data loss due to misplaced agency equipment.

Software

In general, Metro-INET or the agency will provide the software required for an employee to perform their job duties. Requests for new or different software should be made to your supervisor, who will forward the request to Metro-INET for review to ensure appropriate standards are satisfied.

Only agency staff may use agency software. Use of agency software by family members, friends, or others is strictly prohibited.

Software shall not be downloaded or installed on Metro-INET supported computers without the prior approval of Metro-INET. Exceptions to this include updates to software approved by Metro-INET such as Microsoft updates, or other productivity software updates.

Metro-INET may, without notice, remove any unauthorized programs or software, equipment, downloads, or other resources.

Software is to be in a current and supported state and have security related and critical updates applied within the timeframe set by the Metro-INET Information Security Manager.

Incidental Use

Incidental personal use of agency owned resources and related equipment is accepted.

Reasonable, incidental personal use of agency computers and software should never preempt or interfere with work. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

Personal files are not to be stored on Metro-INET supported computer equipment.

Metro-INET may delete personal files if found on the network, computers, or other Metro-INET supported equipment.

Metro-INET supported equipment or technology shall not be used for personal business interests, for-profit ventures, political or religious activities, or other uses deemed to be inconsistent with agency activities. Questions about whether a use is appropriate should be sent to your supervisor for determination.

Personal Devices

Employees may choose to use their own equipment to read or compose email or other agency data as governed in this policy. Employees understand that by connecting their personal equipment to the Metro-INET resources, their personal devices could be searched during an e-discovery or other court-ordered scenarios and agree to grant access to their personal devices should such a situation arise.

Mobile devices that have been configured to bypass manufacturer configurations (jailbroken / rooted) are not to be used to access Metro-INET resources.

Metro-INET may require Mobile Device Management or Mobile Application Management solution(s) to protect agency data.

Security Training and Awareness

All employees shall complete assigned security awareness training within 30 days of being granted access to any Metro-INET resources.

All account holders must be provided with and acknowledge they have received and agree to adhere to the Metro-INET Information Security Policies before they are granted access to Metro-INET Information Resources.

Enforcement

Employees found to have violated this policy may be subject to disciplinary action, up to and including revocation of system privileges, termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Policy Acknowledgement

I have received and read the above policy and have had an opportunity to ask questions. I understand that my failure to follow this policy may result in disciplinary action, including revocation of system privileges or termination of employment, and related civil or criminal penalties.

_____ (Print Account Owner Name)

_____ (Signature of Account Owner)

_____ (Print Agency Name)

_____ (Date)

Artificial Intelligence (AI) chatbot Usage

With the increasing popularity of generative AI chatbots such as OpenAI's ChatGPT, Google's Bard, and Microsoft 365's Copilot, it has become necessary to outline the proper use of such tools while working at the City of Lake Elmo. While we remain committed to adopting new technologies to aid our mission, when possible, we also understand the risks and limitations of generative AI chatbots and want to ensure responsible use. Our goal is to protect employees, clients, suppliers, constituents, and the city from harm.

OVERVIEW

While AI chatbots can be used to perform a variety of functions, this policy addresses only the use of a web-based interface to ask or "prompt" the chatbot in a conversational manner to find answers to questions or to create or edit written content.

There are, however, risks in using this technology, including uncertainty about who owns the AI-created content and security/privacy concerns with inputting proprietary city information or sensitive information about an employee, client, customer, etc., when interacting with the chatbot. Additionally, the accuracy of the content created by these technologies cannot be relied upon, as the information may be outdated, misleading or—in some cases—fabricated.

When you submit data to an AI-enhanced service, it leaves a copy of the submitted data with the service. This may pose security and privacy risks. These risks are magnified if the AI-enhanced service automatically incorporates submitted data into responses shared with other users as part of the data they are trained to use.

ELIGIBILITY

This policy applies to all employees of the City and to all work associated with the City that those employees perform, whether on or off company premises.

POLICY

Limited use of generative AI chatbots will be allowed while performing work for the City with the approval of your supervisor. City email addresses, credentials or phone numbers cannot be used to create an account with these technologies. No city data of any kind may be submitted (copied, typed, etc.) into these platforms.

All AI-generated content must be reviewed for accuracy before relying on it for work purposes. If a reliable source cannot be found to verify factual information generated by the chatbot, that information cannot be used for work purposes. Please refer to the AI flowchart to help determine whether it's appropriate for you to use AI on your work project.

Acceptable uses include:

- For general-knowledge questions meant to enhance your understanding on a work-related topic.
- Summarizing long documents that only contain information as defined by Minnesota Statutes Chapter 13 as "public" and is intended to be available to the public.
- To brainstorm ideas related to projects you are working on.
- Researching public topics where the resulting content can be verified by a subject matter expert (SME).
- To create formulas for Excel spreadsheets or similar programs.

Unacceptable uses include:

- Using any text created by an AI chatbot in final work products of any kind.
- Copying and pasting, typing, or in any way submitting city content or data of any kind into the AI chatbot.
- Failing to properly cite an AI chatbot when used as a resource.

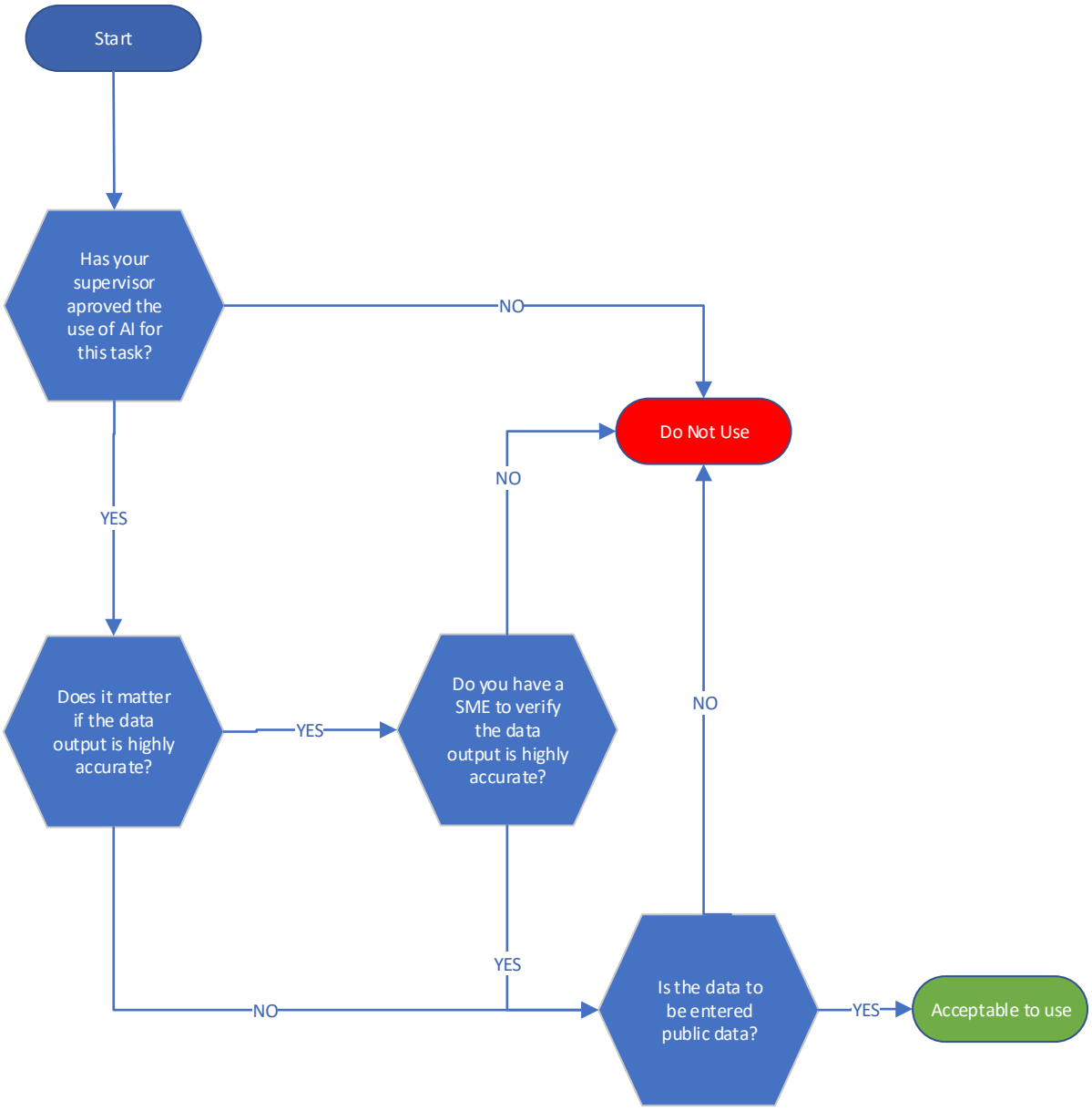
Any violation of this policy will result in disciplinary action, up to and including termination.

ETHICAL USE

Employees must use generative AI chatbots in accordance with the City's respectful workplace policies. These technologies must not be used to create content that is inappropriate, discriminatory or otherwise harmful to others or the company. Such use will result in disciplinary action, up to and including termination.

MONITORING

The City's Computer and Internet Use Policy and relevant monitoring policies still apply when using generative AI chatbots with company equipment.


Start
Has your supervisor aproved the use of AI for this task?
NO
Do Not Use
YES
NO
Does it matter if the data output is highly accurate?
YES
Do you have a SME to verify the data output is highly accurate?
NO
YES
NO
Is the data to be entered public data?
YES
Acceptable to use