# 1 - GENERAL INFORMATION

## 1.4 – Appropriate use of the City of Marshalltown's Computing, Network Resources and Equipment.

Revised: May 2022

This policy applies to all City officials and City employees while using the City's computing, network resources and equipment and shall apply to use of the Internet, World Wide Web, electronic mail (both in-house and Internet), or any similar forms of electronic communications including printing and file copying. City employees shall be required to comply with this policy and shall be required to sign the Statement of Compliance form **prior to** usage.

Use of the City's equipment and computer-based services shall be **only** for city business purposes. Any other use, whether during work hours or at any other time, shall be prohibited. All electronic messages stored in or transmitted by the City's computer equipment are the sole property of the City and the City may access and monitor officials' and employees' communications and files as appropriate.

Transfer of files, by any method, presents a serious opportunity for infection of local systems with computer viruses. Files shall only be downloaded to a machine equipped with an approved anti-virus program that is loaded into the machine's memory and that is running at the time of the download.

All city employees covered by this policy shall maintain the highest level of ethical standards. Appropriate conduct is expected and required. The following list of expected conduct is not all-inclusive and is provided as a general guideline:

- Avoid sexual harassment, voyeurism, and other sexual behavior.
- Avoid all harassment and discrimination based on race, creed, color, age, national origin, religion, sexual orientation, gender identity, marital status or disability.
- Protect all confidential city information, personal identifiable information and other sensitive or regulated information.
- Protect all city resources and assets.
- Protect hardware, software and mobile devices from theft by not allowing the use of such devices by anyone outside the organization unless specifically authorized.
- Handle all City devices, or personal devices with City systems on them, with extra precautions.
- Do not transport confidential city information, personal identifiable information or other sensitive or regulated information on unprotected devices such as, but not limited to, a flash drive or CD unless it is a part of a regular duty or task.
- Do not author, generate, or forward anything that might damage community relations or have a harmful effect on the City's image either within the community or elsewhere.
- Adhere to all software licensing agreements; copying, downloading, or uploading of software or information that is not consistent with the supplier's licensing agreement is forbidden. Do not duplicate copyrighted materials without permission.
- There are numerous unanswered legal questions as to use of electronic communication and state open meetings and open-records laws. City employees are advised that instant messaging and chat rooms may raise open meeting questions, so consultation with the City Attorney prior to use of this service is suggested.

**USER NAMES AND PASSWORDS**

- Default administrative and initial passwords for all computers/devices, systems, and applications shall be changed during initial setup/use.
- Personal identifiable information, such as, but not limited to, social security numbers shall not be used as a user ID or password.
- Passwords shall be:
    - Changed every 180 days. A system notification will prompt you to do so.
    - Include an uppercase, lower case, number AND special character.
    - Not contain any part of the username, first or last name.
    - At least 8 characters long.
- Passwords cannot ever be re-used.
- Usernames and password shall be assigned to single individual and not a group or entity.
- Authentication information, including but not limited to user names and passwords, shall not be shared with anyone.
- Authentication information, including but not limited to user names and passwords, shall not be openly displayed, and systems and applications shall be configured to mask passwords during entry.

**MULTI-FACTOR AUTHENTICATION (MFA)**

- MFA shall be used for remote network connections, including but not limited to, VPN or remote desktop.
- MFA shall be used for any device that an employee or official is accessing their City based email accounts.
- Employees and Officials will be given the option to use a City issued token or be able to choose to use an application on their personal device or City issued device.

**TRAINING**

Training will be provided on security awareness as necessary or requested.

**CITY ISSUED TOKENS FOR MFA**

- Employees and officials opting for a City issued token for purposes of MFA shall be stored in a secured area when not in use and not directly on the work station of the assigned user.
- Employees and officials will be responsible for the replacement cost of any lost or damaged tokens.
- Tokens that are lost shall be reported immediately to their supervisor or designee.

**PERSONAL DEVICES USE FOR MFA**

- Employees and Officials choosing to use their personal devices for MFA, will not receive any stipend for using their personal device.
- Nonexempt employees may not use their personal devices for MFA purposes outside of their normal work schedule, or while on leave, without authorization in advance from their supervisor or designee.

## STATEMENT OF COMPLIANCE

I have read and agree to comply with the requirements contained in this policy and in this statement of compliance. Additionally, I agree not to allow unauthorized use of my Internet access privileges, through either city-owned equipment or any equipment located elsewhere.

I am aware that transfer of files presents an opportunity for infection with computer viruses and I agree that files shall only be downloaded to a machine equipped with an approved anti-virus program that is loaded into the machine's memory and that is running at the time of the download.

I shall have no expectation of privacy while sending messages or documents using these computer-based services, whether in-house or via the Internet, and I understand that usage may be monitored for compliance with this policy.

I understand choosing to use my personal device to access my City based email accounts subjects my personal device to open records laws. I further understand that if I am choosing to use my personal device for purposes of MFA, I will not receive a stipend from the City.

I understand that if I choose to use a City issued token for purposes of MFA, I am fully responsible for maintaining this device in good working condition. I further understand that if the device is lost or damaged, I am responsible for the replacement cost of said device.

I understand that the City has the right to amend, change, or delete this policy at any time, and that additional policy statements may be issued pertaining to related issues, processes, and procedures.

I understand that violations of this policy may result in disciplinary action, which may include oral or written reprimands, loss of computer system privileges, suspensions, or termination of employment. Violations could also result in prosecution.

Signature: _____ Date: _____

# City of Marshalltown – Multi-Factor Authentication (MFA) Election Form

☐ **I am electing to use a CITY ISSUED TOKEN FOR MFA.**

**By signing below, I am acknowledging my understanding that:**

- This token shall be stored in a secured area when not in use and not directly on my work station.
- I will be responsible for the replacement cost if my token is lost or damaged. By signing below, I am authorizing that the replacement cost will be deducted from my next available paycheck. I further understand I will be given written notice that this is occurring in advance of that deduction.
- I will have the responsibility to immediately report to my supervisor, or designee, that my token has been lost or damaged.
- I will be responsible for returning my token in good working order upon resignation or termination.

☐ **I am electing to use my PERSONAL DEVICE FOR MFA.**

**By signing below, I am acknowledging my understanding that:**

- I will not receive any stipend from the City for using my personal device.
- I am voluntarily making this election and have been offered another option (a token) for purposes of MFA.
- I understand if I am a nonexempt employee that I may not use my personal device for MFA purposes outside of my normal work schedule, or while on leave, without authorization in advance from my supervisor or designee.

Signature: _____

Print Name: _____

Date: _____

Token #: _____