CITY OF STAR

TECHNOLOGY SYSTEMS POLICY

Approved by xxx
Insert date

TABLE OF CONTENTS

I. SCOPE

This Policy applies to all users of the City of Star's technology systems, herein referred to as "Technology Systems". Use of the City of Star's Technology Systems, even when carried out on privately owned computers or other devices that are not owned, managed or maintained by the city, is governed by this Policy.

II. PURPOSE

The purpose of this Policy is to ensure a technology infrastructure that promotes the basic missions of the City of Star. This Policy aims to promote the following goals:

A. Ensure the integrity, reliability, availability, and superior performance of Technology Systems;

B. Ensure that use of Technology Systems is consistent with the principles and values that govern the use of other city facilities and services;

C. Ensure that Technology Systems are used for their intended purposes; and

D. Establish processes for addressing policy violations and sanctions for violators.

III. DEFINITIONS

A. *TECHNOLOGY SYSTEMS*

Servers, any kind of personal computing devices, applications, printers, networks (virtual, wired and wireless), online and offline storage media and related equipment, software, and data files that are owned, managed, connected to or maintained by the City of Star.

B. *USER*

Any person, whether authorized or not, who makes any use of any Technology System from any location.

IV. APPROPRIATE USE

A. All Technology Systems are City of Star property and anything you create or load on the Technology Systems becomes city property.

B. Technology Systems are in place to facilitate your ability to efficiently and productively do your job. To that end, these Technology Systems are solely for business purposes. Only incidental personal use that does not interfere with work

or consume Technology Systems resources will be allowed. Personal use may be permitted on an occasional, limited basis within the guidelines established by this policy provided that such use does not result in a cost to the City of Star or interferes with city business operations or the employee's job performance.

C. The City of Star reserves the right to intercept, monitor, copy, review and download any communications or files you create or maintain on the Technology Systems, at any time, without prior notice to you. Be advised that regular monitoring will occur.

D. The City of Star purchases and licenses the use of various computer software programs for business purposes. City of Star does not own the copyright to this software or its related documentation. Unless authorized by the software developer, the City of Star does not have the right to reproduce such software for use on more than one computer. Users may only use software on Technology Systems or according to the software license agreement. Illegal duplication of software and its related documentation for personal use is prohibited.

E. Each user is prohibited from sharing their network password with anyone. The City's Information Technology (IT) Director has the right and capability to change any user's network password at any time when required to gain access to information from any individual user's network profile. The user will be notified of this password change wherein the user must change their network password after such activity for confidentiality.

F. Stealing or coercion to obtain another user's code or password as well as using or disclosing a user's code or password is strictly prohibited. Also, attempting to break into any City of Star Technology Systems is strictly prohibited.

G. E-mail and Internet access is provided by the City of Star to enhance communications and provide access to work related information and technology. Consequently, users should always ensure the business information contained in Internet E-mail messages and other transmissions is legal, accurate, appropriate and ethical. The following are examples of prohibited uses of E-mail and Internet systems:

    1. Sending or posting discriminatory, harassing, or threatening messages or images;

    2. Using city time and resources for personal gain;

    3. Unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material;

    4. Engaging in unauthorized transactions that may incur cost to the City of Star

or initiate unwanted Internet or e-mail services and transmissions;

5. Sending or posting messages or material that could damage the city's image or reputation;

6. Participating in the viewing or exchange of pornography or obscene materials, that are not work related;

7. Sending or posting messages that defame or slander other individuals;

8. Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities;

9. Using the Internet for political causes or activities, religious activities, or any sort of gambling;

10. Jeopardizing the security of the organization's electronic communications systems;

11. Passing off personal views as representing those of the City of Star;

12. Sending anonymous e-mail messages;

13. Engaging in any other illegal activities while using city Technology Systems.

V. EXTERNAL DEVICES

This section provides standards and rules of behavior for the use of personally owned smart phones, tablets, or external storage devices by users to interface with the City of Star's Technology Systems. Access to and continued use of Technology Systems is granted on condition that each user follows the city's policies concerning the use of these devices and services.

A. *CURRENT DEVICES APPROVED FOR USE*

1. Android Smart Phones and Tablets

2. Apple iPhones and iPads

PROHIBITED DEVICES

1. No personally owned storage devices may be used to transfer or download any city-related files or documents, this includes but is not limited to: External Hard

Drives, USB Thumb Drives, Memory Cards or any other type of storage media.

B. *EXPECTATIONS*

1. Privacy. The City of Star will respect the privacy of your personal device and will only request access to the device to implement security controls, as outlined below, or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings. This differs from policy for the city's provided equipment/services, where users do not have the right, nor should they have the expectation, of privacy while using city equipment or services. While access to the personal device itself is restricted, City of Star's Technology Systems Policy regarding the use and access of city e-mail and other Technology Systems remains in effect.

2. Only upon written authorization from the City of Star IT Director or his/her designees will connection to external devices be granted. Connection to our Technology Systems may be disabled by the City of Star at any time.

3. The City of Star is not responsible for any loss or theft of, damage to, or failure in the device that may result from use of third-party software and/or use of the device in this program.

4. Contacting vendors for troubleshooting and support of third-party software is the user's responsibility, with limited configuration support and advice provided by city staff.

5. Business use may result in increases to the user's personal monthly service plan costs. The city will not reimburse any business-related data/voice plan usage of user's personal device without prior approval.

6. If the user chooses to discontinue connection of the external device, the user will allow the city to remove and disable any city provided third-party software and services from the personal device.

C. *REQUIREMENTS FOR ACCESSING THE CITY OF STAR'S TECHNOLOGY SYSTEMS*

1. User will not download or transfer sensitive business data to their personal devices. Sensitive business data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual (personally identifiable information), the outcome of a claim, proprietary information, or agency financial operations;

2. User will protect the mobile device with a four-digit numeric PIN/Password;

3. User agrees to maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer. The user will not install software that allows the user to bypass standard built-in security features and controls (Jail Break) the device;

4. User agrees the device will not be shared with other individuals or family members, due to the business use of the device;

5. User agrees to delete any sensitive business files that may be inadvertently downloaded and stored on the device through the process of viewing e-mail attachments.

6. If the device is lost or stolen, the user must notify the IT Director or their department manager within eight hours. The City of Star will lock the device, and a full erase of the device's data and programs will be completed. Failure to report the lost or stolen device may result disciplinary action, up to and including termination.

VI. REMOTE SYSTEMS WORK AND ACCESS

The purpose of this section is to address the requirements and expectations for employees desiring to work outside of the city's home office located in Star, Idaho. This practice is herein referred to as "remote". The work needs of the City of Star and the security of Technology Systems are the first considerations in granting remote work and remote access. Working remotely requires employees to be focused and disciplined to avoid personal distractions that may not be present in an office environment. Remote work also requires trust from management that employees are productive and professional in their work. Remote work and the technology supporting it are evolving rapidly. Hence, this policy serves only as a basic outline of requirements and expectations. It does not serve as the absolute position of the City of Star on remote work and access practices.

A. *REMOTE WORK APPROVAL*

1. Granting authority for remote work opportunity and remote access to the City of Star Technology Systems resides with the Executive Director, who may delegate this authority to department managers. Only upon written authorization from the Executive Director or his/her designees will remote work or remote access be granted.

B. *REQUIREMENTS FOR REMOTE WORK*

1. Submission of a work plan outlining work to be completed during scheduled remote work time must be submitted to employee's manager.

2. Maintenance of a professional work environment in which communications and concentration are not disrupted by noise or distractions.

3. Technical knowledge required to access the city systems necessary to complete assignments in a remote work setting

C. *REQUIREMENTS FOR REMOTE ACCESS*

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. At no time should any user provide their login or email password to anyone, not even family members.

2. Users of hardware that connects to the city's network using a virtual private network (VPN) connection must ensure they are not connected to any other network using a VPN connection at the same time. This excludes the local network (i.e., Home, Hotel, Public Wireless), the remote user my use to connect to the internet.

3. Users with remote access privileges to the city's corporate network must not use non-city email accounts (i.e., Hotmail, Gmail, Yahoo), or other external resources to conduct city business, thereby ensuring that official business is never confused with personal business.

4. All hosts that connect to the city internal network must meet the following minimum-security baseline:

   a. Anti-Virus software must be installed and kept up-to-date. This software is required to be always operating on the computer in real time protection mode. The anti-virus library definitions shall be updated at least once per day. Anti-virus scans shall be done a minimum of once per week. If your anti- virus software does not already provide separate spyware/malware protection, you must install separate applications to prevent these items.

   b. A software firewall must be installed and enabled. If not using an operating system that has a built-in firewall, a separate firewall program must be installed and kept up-to-date.

   c. The operating system of the device must be kept up to date with the most current available security patches, service packs and updates at all times.

VII. ENFORCEMENT

Your consent to and compliance with all the above items is a term and condition of your employment. Failure to abide by these rules may be grounds for disciplinary action, up to and including termination.

VIII. ACKNOWLEDGMENT

ACKNOWLEDGMENT OF RECEIPT OF CITY OF STAR TECHNOLOGY SYSTEMS POLICY.

I,_____acknowledge receipt of the City of Star Technology Systems Policy, amended [insert date last amended]. Please initial each statement below if it is true.

I understand that it is my responsibility to read and understand the contents of this Policy.

I understand that I am obligated to perform my duties of employment in conformance with the provisions of this Policy and any additional rules, regulations, policies or procedures imposed by the department in which I work whether or not I choose to read the Policy.

I understand that this Policy may be modified without prior notice to me.

DATED this_____day of _____, 20_____.

_____
(Employee Signature)