

GREEN RIVER UTAH

RESOLUTION R08-2023

A RESOLUTION REGARDING COMPUTER SYSTEM USE AND SECURITY

WHEREAS; the City of Green River wants to improve its fraud risk assessment score; and

WHEREAS; the City of Green River wishes to be more prepared against cyber-attacks; and

WHEREAS; the City of Green River wants to protect its information and technology;

NOW THEREFORE, be it resolved that:

The following will become SECTION XX of the personnel policy.

The Current SECTION XX and the sections that follow it will be pushed back. (I.e., SECTION XX will become SECTION XXI, SECTION XXI will become SECTION XXII, etc.)

This policy will be formatted as needed to fit the personnel policy.

The personnel policy will have its formatting changed to accommodate this policy. (I.e., numbering may be changed, etc...)

SECTION XX: IT AND COMPUTER SECURITY POLICY

1. STATEMENT

- A. The City of Green River furnishes computers for employees' use in conducting City business. This includes access to e-mail and the Internet. The internet contains many useful features, including email to non-City resources, access to research materials, and information exchange.
- B. This policy establishes:
 - (1) Basic rules for employees' use of the City's computer systems
 - (2) How to properly configure the City's computer systems
 - (3) Actions to take to ensure safe use of the City's computer systems
 - (4) How employees are to handle cyber attacks

2. COMPUTER SYSTEM, INTERNET, AND E-MAIL USE POLICIES

- A. The Internet can be misused in a variety of ways, including but not limited to:
 - (1) Downloading files that contain viruses, thereby endangering City information services;
 - (2) Accessing objectionable material;

- (3) Wasting work time by performing unauthorized research or accessing non business related information and people or for computer games, or online games.

B. Individual Responsibilities:

- (1) Internet users are responsible for complying with this and all other City policies when using the City's resources for accessing the Internet. Violation of this policy is grounds for disciplinary action, up to and including termination.

C. General Policies for Use of the Entity's Computer System, Including the Internet:

- (1) An employee does not have a right to privacy when using the Internet via City resources and employees should not expect or assume any privacy regarding the content of email communications. The Entity reserves the express right to monitor and inspect the activities of the employee while accessing the internet at any time, and to read, use and disclose e-mail messages. In addition, all software, files, information, communications, and messages (including emails) downloaded or sent via the Internet using City resources are the City's records and property of the City; such records are subject to potential review and disclosure under the public disclosure law of the State of Utah. Even after an email message has been "deleted," it may still be possible to retrieve it.
- (2) The City Council, Mayor, and City Manager have the right to restrict or prohibit any employee from Internet access for violation of the policy. Violations may also result in disciplinary action, up to and including termination.
- (3) Offensive (E.g., pornographic), harassing, discriminatory, or illegal (i.e. gambling) activities are prohibited.
- (4) Personal Use of City Devices
 - i. Internet use via City resources is for City business. Except as outlined here, use of the City's computer, internet and email services are for City business only.
 - ii. Some limited personal use is permitted, so long as it does not result in cost to the City, does not interfere with the performance of duties, is brief in duration and frequency, does not distract from the conduct of City business and does not compromise the security or integrity of City information or software.
 - iii. Such limited use is permitted immediately before or after work hours, during an employee's breaks, and at such times as the Mayor or City Manager allow (E.g., during the weekend or after workday hours).
 - iv. Examples of allowable personal use include accessing a weather report or news item on the Internet, transmitting email to a family member to assure safe arrival at home, playing music, or making an online purchase.
 - v. Any personal use of City's computer, internet and email services must comply with all applicable laws and City policies, including anti-discrimination policies and Internet usage policies.

- vi. Costs associated with applications downloaded to City devices are the financial responsibility of the user assigned to the device. (Unless the application(s) is required or recommended by city management.) Downloaded applications should not be offensive, harassing, discriminatory or illegal (i.e. gambling) in content. Applications with security vulnerabilities should be uninstalled.
 - vii. Offensive (i.e. pornographic), harassing, discriminatory, or illegal (i.e. gambling) activities are prohibited.
- (5) Internet use must comply with applicable laws and City policies including but not limited to all federal and state laws, and City policies governing sexual harassment, discrimination, intellectual property protection, privacy, public disclosure, confidentiality, misuse of City resources, information and data security.
- (6) City's computer system permits employees to perform jobs, share files, and communicate internally and with selected outside individuals and entities in the performance and conduct of City business. Employees are prohibited from gaining unauthorized access to another employee's email messages, or sending messages using another employee's password.
- (7) In order to prevent potential City liability, it is the responsibility of all Internet users to clearly communicate to the recipient when the opinions expressed do not represent those of the City.
- (8) The City of Green River has the capability and reserves the right to access, review, copy, modify and delete any information transmitted through or stored in its computer system. The City may disclose all such information to any party (inside or outside the Entity) it deems appropriate and in accordance with applicable law. Accordingly, employees should not use the computer system to send, receive or store any information they wish to keep private. Employees should treat the computer system like a shared file system—with the expectation that files sent, received or stored anywhere in the system will be available for review by any authorized representative of the City for any purpose, as well as the public if a proper request is made for public records.
- (9) Good judgment should always be employed in using the City's email and Internet systems. Employee email messages may be read by someone other than the person(s) to whom they were sent. Email inconsistent with the City's policies must be avoided. For example, it is prohibited to make jokes or comments which could offend someone on the basis of gender, race, age, religion, national origin, disability or sexual orientation. These comments would be in direct conflict with the City's policies prohibiting discrimination and harassment. Accordingly, employees should create and send only courteous, professional and businesslike messages that do not contain objectionable, offensive, or potentially discriminatory material.

- (10) Caution should be taken in transmitting confidential information on the computer system. Employees should use due care in addressing email messages to assure messages are not inadvertently sent to the wrong person inside or outside the Entity. Email creates a written record subject to court rules of discovery and may be used as evidence in claims or legal proceedings. Once sent, email cannot be retracted. Even after deletion at a workstation, email can be retrieved and read.
- (11) The safety and security of the City's network and resources must be considered at all times when using the Internet. Any programs (other than additional programs available in a suite of programs used by the city) must not be downloaded or installed without prior permission from the City Manager and without being properly scanned for viruses.
- (12) There is a wide variety of information on the Internet. Some individuals may find information on the Internet offensive or otherwise objectionable. Individual users must be aware that the City has no control over available information on the Internet and cannot be responsible for the content of information.
- (13) Playing music on City devices during work time is allowed.
 - i. Music should not be loud/intrusive enough to disrupt the workflows of the City, or to make it hard for working with customers. (E.g., Too loud for a customer to hear an employee well, or too loud for the employee to hear the customer well.)
 - ii. Employees should not play music that is offensive to their co-workers.
 - iii. Listening to music with earphones is allowed. Unless the music disrupts the employee's workflow. If the music is quiet enough that coworkers cannot hear it, then the employee no longer needs to worry about what is offensive to their co-workers.

D. Prohibited uses of City devices and internet access:

The following is a non-exclusive list of prohibited uses of the Internet and email:

- (1) Personal for-profit business, religious, or political activities, or for personal financial benefit outside of employment is prohibited;
- (2) The sale of personal items or non-business items through advertising on the Internet is prohibited;
- (3) Copyright violations – the unlawful reproduction or distribution of copyrighted information, regardless of the source, is prohibited;
- (4) Discrimination / Harassment – the use of the Internet to send messages or other content which is harassing, derogatory or unlawfully discriminatory to employees, citizens, vendors or customers is prohibited;
- (5) Political – the use of the Internet for political purposes is prohibited;

- (6) Aliases / anonymous messages / misrepresentation – the use of aliases or transmission of anonymous messages is prohibited. Also, the misrepresentation of an employee's job title, job description, or position with the City is prohibited;
 - (7) Social networking sites – the accessing and/or creation of social networking sites, such as Facebook, Twitter, Instagram, Blogs and similar sites on city desktops and laptops is prohibited for non-entity business purposes during work time;
 - (8) Instant messaging for non-city business is prohibited during work time;
 - (9) Misinformation / Confidential Information – the release of untrue, distorted, or confidential information regarding City business is prohibited;
 - (10) Viewing or downloading from entertainment sites, pornographic sites, sexually explicit sites, chat rooms and bulletin boards is prohibited;
 - (11) Unauthorized attempts to access another's network or e-mail account is prohibited;
 - (12) Display or transmission of sensitive or proprietary information to unauthorized persons or organizations is prohibited;
 - (13) Spamming email accounts from the City's email services or City machines is prohibited;
 - (14) Personal use of software and applications which disrupts or distracts the conduct of City business due to volume, timing, or frequency is prohibited;
- E. Employees that were offered a device as a benefit before this policy went into effect are allowed to follow the personal use guidelines as agreed upon between the employee and management when the device was given.
- (1) All other policies besides personal use still apply to the device.
 - (2) A new employee in the position, or a new device void the above mentioned exemption.

3. COMPUTER, NETWORK, APPLICATION, ETC. CONFIGURATION POLICIES

- A. Every City device and user account may be required to have additional security software and settings installed/configured as chosen by the Mayor or the City Manager.
- B. Every Desktop/Laptop will have an administrator account and a standard user account.
 - (1) Employees will use the standard user account for their work.
 - (2) The administrator account will be for the use of management and IT personnel.
 - (3) The main reason for this requirement is to ensure that if a malicious actor gains access to any employee's account, they will not have administrator privileges.

- C. Desktops and laptops will be set to sleep and require a password after 5 minutes of inactivity.
- D. Employees are to keep their devices up to date by trying to ensure that software updates are installed on the day they become available. (Excluding weekends, after hours, and days off.)
- E. Ensure computer settings do not Allow Remote Assistance connections.
- F. All firewalls will have a default deny rule on inbound traffic.
 - (1) E.g., Inbound connections that don't match a rule are blocked.
- G. The City will have a guest network and an employee/officials network. Individuals/entities who are not part of the City are not allowed access to the employee network. (Other than policing agencies and those hired to perform IT work.)
- H. The network's encryption standard shall be at least WPA2 with AES, but WPA3 is preferred.
- I. Google Chrome is the city's preferred internet browser.
- J. Popup blocking will be enabled on all internet browsers used on City devices.
 - (1) Unless popups need to be allowed for specific City business.
 - (2) After the specific business is complete popup blocking will be re-enabled.

4. PASSWORD POLICIES

- A. Employees will not reuse the same password for multiple accounts.
- B. Passwords at Green River City will:
 - (1) Contain 8 or more characters
 - (2) Not use dictionary words (e.g., Green, River, City, dog, cat, etc.)
 - (3) Will not use 3 or more numbers in a sequence matching the city phone number
 - (4) Will not use the same character more than 2 times in a row
 - (5) The exception to these rules is the password to access the guest Wi-Fi network.
- C. Employees are not to share or reveal individual passwords to anyone.

5. AVOIDING PHISHING ATTACKS

- A. City of Green River employees are to follow these guidelines for recognizing phishing emails:
 - (1) Watch for poor spelling and/or grammar.
 - (2) Check sender email addresses for suspicious characteristics.

- (a) Unfamiliar website referenced in the email.
 - i. E.g. yehoo.com instead of yahoo.com
 - (b) Appears close to the same email address as a trusted source but is slightly different.
- (4) Watch for language that is meant to scare or rush you.
- (a) Could be pretending to be your supervisor, a cop, a doctor, etc...
- (5) ALWAYS be suspicious of links in emails.
- (a) Hover over the link and ensure the URL that appears matches what it should be.
 - i. Attackers will often have the hyperlink appear safe, but the true underlying link is malicious.
 - (b) Copy and paste the link into Google's URL checker.
<https://transparencyreport.google.com/safe-browsing/search>
 - i. Do not trust the site if Google doesn't.
- (6) To check if an attachment to an email is safe:
- (a) Right click the attachment.
 - (b) Click "copy link address".
 - (c) Paste into VIRUSTOTAL's URL checker.
<https://www.virustotal.com/gui/home/upload>
 - i. You do paste it into the URL option. The file option is only for files you have already downloaded.
- B. The guidelines in SECTION XX.5 are subject to be changed by the Mayor or City Manager based on the continual change in phishing attack styles and methods of mitigating phishing.

6. ENSURING FILES/PROGRAMS ARE SAFE

- A. WINDOWS DEVICES: City of Green River personnel are to follow these guidelines for handling files that are already downloaded, but seem suspicious.
- (1) Right click file/folder
 - (2) Click "Show more options"
 - (3) Click "Scan with Microsoft Defender"
 - (4) View results of scan in page that automatically comes up.

(a) “0 threat(s) found.” means you should be able to trust the file.

(b) If a threat is found, follow on screen promptings.

B. WINDOWS AND APPLE MAC DEVICES

(1) Go to the VIRUSTOTAL website. <https://www.virustotal.com/gui/home/upload>

(2) Click on “Choose file”.

(3) Upload suspicious file.

(4) Remove file if VIRUSTOTAL finds malicious software.

7. REMOVING PROGRAMS (APPLICATIONS)

C. To Remove a program (app) using CCleaner:

(1) Open CCleaner

(2) Click on “Tools”

(3) Click on “Uninstall”

(4) Select the program you wish to uninstall

(5) Click “Uninstall”

D. To Remove a program (app) using Windows Control Panel:

(1) Open Control Panel. (Type “Control Panel” into search bar.)

(2) Click on “Uninstall a program”. It will be under the word “Programs”.

(3) Select the program that you wish to uninstall.

(4) Click on “Uninstall”.

8. IF A CYBER ATTACK TAKES PLACE

A. If City personnel feel that they are or even possibly are being subjected to a cyber-attack they are to follow these steps:

(1) 1st Unplug the ethernet connection to the desktop. If it is a mobile device on Wi-Fi, then remove the device from Wi-Fi signal and/or turn on airplane mode.

(2) 2nd Run CCleaner and contact the City Manager and/or the Mayor. If CCleaner is not on device, then contact Mayor/City Manager and proceed to step 3.

(3) 3rd Run Microsoft Defender full scan or device’s equivalent virus protection software.

(4) 4th DO NOT SHUT OFF THE DEVICE.

(5) IT personnel will handle the recovery of the device.

9. POWER TO ADAPT AS NEEDED

- A. The Mayor and City Manager have the power to adapt any of the policies in 3. through 8. of SECTION XX due to the ever-changing landscape of cybersecurity.

Nothing in this chapter prohibits the use and access of the described systems for bona fide law enforcement and investigation purposes.

This resolution shall go into effect upon passage.

PASSED and ADOPTED by the City Council of the City of Green River Utah this 12th day of September 2023.

Mayor, Ren Hatt

Attest: _____
City Recorder, Julie Spadafora