Information Technology
Use of Technology Resources

Adopted April 25, 2023 by Ordinance O-23-37

Purpose

The Use of Technology Resources Policy outlines appropriate use of technology resources within the city of Conway. This policy is in place to safeguard the security and integrity of our technology resources, prevent unauthorized access or misuse, and ensure compliance with all relevant laws and regulations.

Scope

This policy applies to all employees, contractors, and other authorized individuals who use the city of Conway's technology resources. The City's technology resources include, but are not limited to all equipment, software, and infrastructure used, owned, or controlled by the City, as well as any data stored or processed by these resources. This includes, but is not limited to, computers, websites, databases, mobile devices, and communication systems. The policy applies to the use of these resources both on and off the City's premises.

Privacy

Users have no expectation to privacy for what they create, store, send or receive on the City's computer or telecommunications systems. The City can inspect this information anytime and it may be subject to the provisions of the Freedom of Information Act, unless protected by law.

To protect privacy, employees are advised to use City-owned equipment and software when communicating for work, instead of personal devices which can expose personal information to public disclosure.

Acceptable Use

All uses of technology resources must comply with all City policies, standards, procedures, and guidelines, as well as any applicable license agreements and laws including federal, state, local, and intellectual property laws.

The acceptable use of technology resources involves a comprehensive understanding of the baseline information security controls necessary to maintain the confidentiality, integrity, and availability of information. This includes protecting organizational information and resources from unauthorized use or disclosure, and safeguarding personal, private, sensitive, or confidential information from unauthorized access. Additionally, users must observe authorized levels of access and use only approved technology resources. In the event of suspected information security incidents or weaknesses, users must immediately report the issue to the appropriate manager and the Information Security Officer (ISO) or designated security representative.

Prohibited Use

The following list is not exhaustive, but aims to provide a framework for activities that constitute unacceptable use of City technology resources. Users may be exempt from these restrictions during their authorized job responsibilities, with approval from City management and in consultation with City IT staff (e.g., storage of objectionable material for disciplinary purposes). Any unacceptable use of technology resources may be subject to disciplinary action, up to and including termination of employment or contract termination.

Unacceptable use of City technology resources includes, but is not limited to:

- Unauthorized use or disclosure of personal, private, sensitive, and/or confidential information;
- Unauthorized use or disclosure of City information and resources;
- Distributing, transmitting, posting, or storing any electronic communications, material, or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;
- Attempting to represent the City in matters unrelated to official authorized job duties or responsibilities;
- Connecting unapproved devices to the City's network or any technology resource;
- Connecting City technology resources to unauthorized networks;
- Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with City policies;
- Using City technology resources to circulate unauthorized solicitations or advertisements for non-City purposes, including religious, political, or not-for-profit entities;
- Providing unauthorized third parties, including family and friends, access to City technology information, resources, or facilities;
- Using City technology information or resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);
- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using City technology resources; and
- Tampering, disengaging, or otherwise circumventing City or third-party IT security controls.

Occasional and Incidental Personal Use

Occasional, incidental, and necessary personal use of City technology resources is permitted, provided it meets the following conditions: it aligns with this policy; it's limited in amount and duration; and does not negatively impact the ability of the individual or other users to fulfill their responsibilities and duties. Good judgment must be exercised regarding personal use. City management reserves the right to revoke or limit this privilege at any time.

Off-Site Transmission and Storage of Information

Users must not transmit restricted City, non-public, personal, private, sensitive, or confidential information through personal email accounts or use personal email accounts to conduct City business unless explicitly authorized by City management. They must also not store restricted City, non-public, personal, private, sensitive, or confidential information on a non-City issued device or with a third-party file storage service that has not been approved for such storage by the City.

User Responsibility for Technology Resources

Users are routinely assigned or given access to technology resources in connection with their official duties. The equipment belongs to the City and must be returned promptly upon request or upon separation from the City. Users may be held financially responsible for equipment assigned to them if it is not returned. In case of loss, theft, or damage of equipment, users must provide a written report and may face disciplinary action, including repayment of replacement value. The City reserves the right to withhold issuance or re-issuance of technology equipment to users who repeatedly lose or damage such equipment.

Security

City users and contractors must follow security policies and procedures, which include guidelines for protecting confidential information, secure password management, and data encryption. They must keep login credentials confidential and follow the Password Management Policy. Confidential data must be protected using encryption or appropriate measures. Any suspected security breaches must be reported immediately. Compliance with data privacy and intellectual property laws is also required. Personal devices accessing company data must follow the approved mobile device management solution and be configured according to security policies. Only secure software and applications may be installed on company devices, and employees and contractors must be cautious when using public Wi-Fi networks to protect City technology resources.

Incident Reporting

Users and contractors must report any suspected or actual security incidents or policy violations to the appropriate manager and the Information Security Officer or designated security representative. This includes unauthorized access, loss/theft, data breaches, policy violations, or any other incidents that pose a threat to the security or integrity of the City's technology resources. Failure to report incidents may result in disciplinary action. Confidentiality will be maintained during investigations, and employees and contractors are encouraged to report incidents in good faith, even if uncertain.

Mobile Device Management

All access to the City's technology resources from a mobile device must be through the approved Mobile Device Management (MDM) solution. Devices must be enrolled in the MDM and configured per the City's security policies, including setting password protection, enabling remote wipe, and installing necessary security updates and patches.

Users and contractors must ensure their personal devices are in compliance with this policy. Failure to do so may result in restricted access to City technology resources, including revocation of access privileges.

Use of Social Media

Users should exercise caution when posting on social media sites, as their actions reflect not only on themselves but also on their professional lives. Once information is shared on social media, it may be captured and used in ways not intended, as it can persist in copies, archives, backups, and cache. Users must respect the privacy of their colleagues and not post identifying information about them without permission (including but not limited to names, addresses, photos, videos, email addresses, and phone numbers). Users may be held accountable for comments posted on social media sites. If a personal

email, post, or electronic message could be perceived as official communication, it is strongly recommended to include a disclaimer such as, "The views and opinions expressed are those of the author and do not necessarily reflect those of the city." Using personal social media accounts for official city business is not allowed, unless explicitly authorized. To prevent unauthorized access to city resources, using the same passwords for personal and city devices and technology resources is strictly prohibited.

Training

All City users are required to complete annual training on information security and any additional relevant topics as directed by City management. This training ensures that all employees are up-to-date on the latest security practices and are able to effectively implement them in their daily work. Completing this training is a critical component of maintaining the City's secure technology environment and safeguarding confidential information. Failure to complete required training may result in restrictions on access to City technology resources.

Consequences of Non-Compliance

Violations of this Use of Technology Resources Policy may result in disciplinary action, up to and including termination of employment or contract termination. Legal action may also be taken if the violation constitutes a criminal offense. Additionally, the City reserves the right to revoke or limit use of or access to City technology resources at any time.