CITY OF BOULDER
***
POLICIES AND PROCEDURES

Technology Security Policy

Effective Date: **Dec 12, 2017**
Last Revised: **Dec 12, 2017**

Jane S Brautigam
Jane S. Brautigam, City Manager

I. PURPOSE

All city employees use technology to accomplish their duties, and every department has employees who administer City Data and City Technology. City employees also use technology to support themselves and their families.

The use of technology is critical to the advancement of the city's mission, but also exposes the city to financial loss, infrastructure damage, reputation damage, and legal risks. The use of technology also results in the city being responsible for compliance with Regulatory Requirements, audit findings, and the terms of the city's cyber security insurance policy.

The choices which will protect the city from these risks can no longer be treated primarily as a technical function carried out by IT experts who manage the city's technology infrastructure, but as an essential responsibility of all city employees.

This policy defines that responsibility and seeks to make technology security an established practice within city culture.

City employees are encouraged to employ the behaviors described in this policy at all times, not just at work, to protect themselves and their families.

II. POLICY

It is the City of Boulder's policy to maintain a culture of responsible behavior and vigilance in the area of technology security.

City employees must not circumvent the policies, procedures, and safeguards in place to protect the city.

City employees must promptly report Technology Related Security Incidents or concerns to the IT Department. Other types of Security Incident must be reported to law enforcement.

III. DEFINITIONS

A. Administrator

City employees whose duties include the procurement, setup, maintenance, or disposal of City Technology or the management of City Data. The role of Administrator is not limited to employees in the IT Department.

Software Administrator examples: City employees who administer software services such as web presence; customer relations; accounting; tax assessment; benefits enrollment; records management; geographic information (GIS); point of sale; or asset management.

Hardware Administrator examples: City employees who administer network connected hardware such as building energy systems; door card and gate access; ICS/SCADA systems; credit card readers; parking kiosks; environmental sensors; traffic signal systems; irrigation controllers; or cameras.

B. **City Data**

Information which belongs to the City of Boulder or for which the City of Boulder is responsible.

Examples: written or printed documents; passwords; certificates; digital signatures; encryption keys; intellectual property; source code; cryptocurrency; geographic information (GIS); digital information stored in Technology Devices; and other data archived in any medium and stored within the premises of city facilities.

C. **City Technology**

Technology Devices, software, website accounts, knowledge, resources, techniques, and access which are used to conduct City of Boulder business.

Examples: city accounts; security groups; door cards; email boxes; databases; storage; cloud storage; applications; cloud applications; computers; mobile devices; networks; and network hardware.

D. **Encryption**

The process of converting data into a code. Data converted in this way can be stored and moved more economically and is more resistant to unauthorized access.

E. **Multi-Factor Authentication**

A login procedure requiring a username, password, and one or more additional elements. Accounts with Multi-Factor Authentication enabled are more resistant to unauthorized access.

Examples of additional elements: biometric markers such as a fingerprint; access codes generated by a mobile application; or the presence of a trusted device.

F. **Regulatory Requirements**

Rules issued by a governing body, backed by penalties, that are intended to manage industry specific risks.

Examples: Critical Infrastructure Information Act of 2002 (PCII); Payment Card Industry Data Security Standard (PCI DSS); Personally Identifiable Information (PII); Health Insurance Portability and Accountability Act of 1996 (HIPAA); FBI Criminal Justice Information Services (CJIS); North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP).

G. **Technology Devices**

Equipment which contains one or more of the following elements: a computer; wired or wireless network interface; or digital data storage. This includes an emulation of such equipment provided through virtualization or cloud services.

Examples: servers; personal computers; laptops; tablets; mobile phones; VoIP desk phones; hard drives; thumb drives; printers; scanners; fax machines; digital cameras; modems; routers; switches; hubs; wireless access points; industrial control systems (ICS); supervisory control and data acquisition (SCADA) systems; smart appliances; smart sensors; and “internet of things” devices.

Emulation examples: virtual servers; application containers; cloud hosted services; software as a service; and infrastructure as a service.

H. **Technology Related Security Incident**

Any situation which harms or has the potential to harm citizens, property, city employees, or the City of Boulder which is specifically related to City Technology or City Data and which is not appropriate for referral to law enforcement.

Examples: unauthorized access, theft, or loss of City Technology or City Data; password exposure; fraudulent email, voice, or other electronic communication; evidence of malicious software or hardware; denial of service.

IV. SCOPE

This policy applies to all types of city employees, city council members, boards and commissions members, city advisory group members, and volunteers while using the internet or technology to engage in city business.

This policy applies to all types of city employees, city council members, boards and commissions members, city advisory group members, and volunteers while using City Technology or City Data for any purpose.

V. EMPLOYEE RESPONSIBILITIES

A. **Password Management**

1. City employees are required to select strong passwords. Strong passwords prioritize length over the use of complex characters, taking the form of a phrase. Phrases are easier to

remember and are more difficult to guess than short, complex passwords. Weak password example: “B0uld3r!”. Strong password example: “correct horse battery staple”.

2. The use of the same password for multiple accounts and services is prohibited. The damage of a lost or stolen password must be limited to a single account.

3. City employees must not reveal the passwords for their city account under any circumstances, even to their supervisors. IT staff are prohibited from asking anyone for their password.

4. Any password loss or exposure must be promptly reported to the IT Department. Accounts with lost or exposed passwords must be locked or have their passwords changed immediately.

5. City employees are encouraged to use an electronic password management application to generate and store their passwords.

6. City employees are encouraged to enable Multi-Factor Authentication when creating website accounts.

B. **Email and Electronic Communication**

1. City issued email addresses must be used for all city business. This includes creating accounts on websites for services that will be used by the city. Accounts created with non-city email addresses are difficult to recover.

2. City employees are required exercise caution in the use of email, attachments, shared documents, text messages, chat sessions, and other electronic communication. These communications must be screened for fraud. Examples: fake login prompts designed to harvest passwords; infected files or links to untrusted websites that could result in malware infection; and requests for information or actions that are not in the best interest of the city.

3. Any communication with the potential to harm the city must be promptly reported to the IT Department.

C. **Personal Devices**

1. The responsibilities in this policy apply when using personal devices to engage in city business.

2. City employees who use personal devices to access City Technology resources are required to install an IT provided management application. Personal devices without the management application will be denied access to City Technology resources. The management application will confirm that personal devices have secure settings and that City Data on those devices is protected.

D. **Secure Device Settings**

1. The default settings on computers and mobile devices are often not secure. The following settings will make City Technology and personal devices more resistant to

unauthorized access, malware infection, and theft. The IT Department will centrally manage these settings wherever possible.

2. Computers and mobile devices must be set up to screen lock automatically after a short period of inactivity.

3. Computers and mobile devices must be set up to require a password, PIN, or biometric reading to unlock the device.

4. Mobile devices must have encrypted storage enabled if possible.

5. Security updates must be promptly applied to mobile devices and mobile device applications.

6. Computers must have security software (antivirus and local firewall) installed.

7. Portable electronic storage devices such as thumb drives and hard disk enclosures must have encryption and password protection enabled.

E. Security Behavior

1. City employees are required to lock the screens of computers and mobile devices when not in use.

2. Untrusted or unknown portable electronic storage devices such as thumb drives and hard disk enclosures must not be connected to City Technology. Those devices pose a significant threat of infecting the city with malware.

3. City employees must use caution when connecting mobile devices to untrusted or public wireless networks. Communication on such networks is subject to eavesdropping.

4. The loss or theft of a personal device which is set up to access City Technology resources or a city issued computer or mobile device must be promptly reported to the IT Department.

5. Other nations may have laws and customs which allow them to demand passwords and access to mobile devices. City employees planning to travel internationally are encouraged to evaluate travel warnings to determine if bringing a personal device or City Technology will place the city at risk.

F. Acceptable Use

1. City employees are responsible for exercising good judgment regarding the reasonableness of personal use of City Technology.

2. Personal use of City Data is prohibited.

3. City employees have no expectation of privacy in their use of City Technology.

4. All cryptocurrency mined using City Technology remains the sole property of the City of Boulder.

5. Introduction of unauthorized wired or wireless networks, network hardware, or internet connections to City of Boulder facilities is prohibited.

6. Activity that is illegal under local, state, federal, or international law is prohibited.

7. Activity that violates the property rights of any person or company is prohibited. This includes software piracy and media piracy.

8. Activity that violates Regulatory Requirements which apply to the city is prohibited.

VI. ADMINISTRATOR RESPONSIBILITIES

Administrators are the city employees best positioned to inventory City Technology, manage security settings, and protect City Data. Because of this role, they have additional responsibilities.

A. Account Management

1. The IT Department is responsible for maintaining an account management system which provides employee accounts and enforces password requirements. Administrators must integrate the City Technology for which they are responsible with the account management system. This integration ensures that accounts are centrally managed and that employees do not have to maintain multiple user names.

2. Accounts must be set up to require Multi-Factor Authentication wherever possible. Exceptions will be made where multi-factor authentication is not compatible with the business purpose of the account.

3. Accounts must be set up to automatically log out after a period of inactivity.

4. Accounts must be assigned to an individual or service. Generic or multi-user accounts are prohibited. If a group of people need access to a system, an account must be created for each person in the group.

5. Administrators who manage accounts within an application must control the privileges associated with each account. Accounts with administrator privileges and other types of elevated permissions are to be provided only to meet a business need, revoked when no longer needed, and must be provided with an expiration date wherever possible.

6. Accounts with administrator privileges and other types of elevated permissions may only be used for the exact purpose for which those privileges were provided. Administrators must log out of accounts with administrator privileges before returning to non-Administrator duties such as web browsing or reading email.

B. Inventories and Secure Settings

1. Administrators are required to maintain an inventory of all hardware and software for which they are responsible. City Technology that is unknown cannot be protected.

2. City Technology must be set up to use encrypted storage and encrypted protocols.

3. Security logs must be enabled on City Technology wherever possible.

4. Administrators are required to manage the application of security updates to the City Technology for which they are responsible. The IT Department will centrally manage the application of security updates for city issued computers and mobile devices.

5. When decommissioning City Technology, storage media must be irreversibly erased prior to physical disposal.

6. City Technology which is externally accessible or subject to Regulatory Requirements is required to undergo a security audit before being put into production. Security audits are facilitated by the Chief Information Security Officer.

7. Systems which are unauthorized, unsupported, or outdated are a significant risk to the city. The IT Department may seek to remove or apply restrictive safeguards to such systems to protect the environment.

C. City Data

1. City Technology must be set up to control access to, retain, and dispose of City Data in accordance with the city's data policies and Regulatory Requirements relevant to that data.

VII. PROCEDURES

A. Policy Exceptions

Any exceptions to this policy must be documented in a Security Policy Exemption Form. Security Policy Exemption Forms can be obtained from the Chief Information Security Officer. The exemption request must include the names and signatures of the city staff making the request, the director of the department making the request, and the Chief Information Officer. When a completed Security Policy Exemption Form is submitted to and accepted by the city's Chief Information Security Officer, an exemption will be granted.

B. Remote Access

Any requests to provide remote access to the city's connected partners, volunteers, contractors, subcontractors, and consultants must be documented in a Remote Access Form. Remote Access Forms can be obtained from the Chief Information Security Officer. The form must include the initials and signature of the requesting party indicating that they have read and agree to abide by all relevant city policies including the Technology Security Policy and the Connected Partner Security Policy. When a completed Remote Access Form is submitted to and accepted by the city's Chief Information Security Officer, access will be provided.

C. Incident Management

Any city employee who detects a Technology Related Security Incident must promptly report the incident to the IT Department. The Chief Information Security Officer or their designee will be the incident commander for Technology Related Security Incidents. Incidents will be handled and documented according to the Technology Security Incident Handling Procedure. The procedure includes a mechanism for escalating the incident to local or federal law enforcement when necessary. The closeout of a Technology Related Security Incident must be documented in a Technology Security Incident Handling Form, including the name and signature of the Chief Information Officer.

VIII. POLICY COMPLIANCE

A. Compliance Measurement

The IT Department may monitor compliance with this policy through the use of software and network security tools; incident investigations; internal and external audits; intelligence reports from external agencies; and reports made to the IT Department.

B. Non-Compliance

Violation of this policy will be grounds for additional training; performance improvement action; or disciplinary action, up to and including termination of employment.

IX. INTERPRETATION AND APPLICATION

This policy supersedes previous policies covering the same or similar topics. This policy specifically supersedes the Administrator Guide and Information Security Policy, Computer User Security Policy, and Software Application Security Policy.

City employees who have questions concerning possible conflict between their interests and those of the City are encouraged to contact the Human Resources Department.

City employees who have questions concerning the interpretation and application of this policy are encouraged to contact the Chief Information Security Officer.