Technology Security

All Employees

Effective: March 28, 2025

Signature:

Authorization: Nuria Rivera-Vandermyde, City Manager

Topic: Guidance for maintaining a secure technology environment

Policy and Scope

It is the city's policy that technology security is the responsibility of all employees throughout the organization. Employees must maintain a culture of responsible behavior and vigilance related to technology security. City employees must not circumvent the policies, procedures, and safeguards in place to protect the city's technology assets, information, and data. In the event of technology related security incidents or concerns, employees must immediately report to the Innovation and Technology (IT) Department.

This policy applies while using city-owned devices, accounts (including email and Internet accounts), or other technology to engage in city business and/or use of personal devices used to access city technology.

Definitions

City Data: Information which belongs to the City of Boulder or for which the City of Boulder is responsible. Data include, but are not limited to, written or printed documents; passwords; certificates; digital signatures; encryption keys; intellectual property; source code; geographic information; digital information stored in technology devices; and other data archived in any medium and stored within the premises of city facilities.

Technology: Devices, software, website accounts, knowledge, resources, techniques, and access which are used to conduct city business.

Encryption: The process of converting data into a code.

Multi-Factor Authentication: A login procedure requiring a username, password, and one (1) or more additional elements.

Devices: Equipment which contains one (1) or more of the following elements: a computer; wired or wireless network interface, digital data storage including cloud services or virtualization.

Technology Related Security Incident: Any situation which harms or has the potential to harm citizens, property, city employees, or the city which is specifically related to city technology or city data.

Responsibilities

Employees

Any password loss or exposure must be promptly reported to the IT Department. Employees must not reveal the passwords for their city account under any circumstances, including supervisors. IT Department staff are prohibited from asking anyone for their password.

Employees are responsible for exercising good judgement regarding personal use of city technology and devices. Employees are encouraged to enable Multi-Factor Authentication, when available, in creating website accounts for city business.

Personal use of city data is prohibited.

Employees are required to lock the screens, or otherwise secure, of city-owned devices when not in use.

Untrusted or unknown portable electronic storage devices such as thumb drives and hard disk enclosures must not be connected to city-owned technology.

City employees must use caution when connecting city-owned devices, or personal devices used to access city technology, to untrusted or public wireless networks.

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.

Innovation and Technology (IT) Department
The Innovation and Technology Department will centrally manage hardware and software settings to detect unauthorized access, malware infection, theft, and other security threats to include security updates to city-owned devices, installation of antivirus software, and firewalls.

The IT Department is responsible for investigation and resolution of data security incidents and/or breaches.

The IT Department, or in some cases department designated administrators, is/are responsible for access control to types and sources of data.

The IT Department is responsible for monitoring compliance of this policy.

Interpretations

This policy supersedes all previous policies covering the same or similar topics. Employees with questions concerning the interpretation or application of this policy should contact the Innovation & Technology Department. Any exception to this policy may be granted only by the Chief Innovation & Technology Officer or the City Manager. This policy may be reviewed and changed at any time. This policy is not intended to be or to create an employment contract.

Connected Policies

City of Boulder
Electronic Communications and Retention
Use of City Property