CITY OF
TULSA
INFORMATION TECHNOLOGY

Policy Summary

COP 1200: Enterprise IT Security Policy Manual

About

The Enterprise IT Security Policy Manual establishes a framework for protecting the confidentiality, integrity, and availability of information systems and data across the City of Tulsa.

> The City of Tulsa is committed to protecting its information assets from all security threats. The goal is to create a strong security culture and reduce risks caused by human mistakes in cybersecurity.

Key Concepts

- **Information Security Management** – *Rules for keeping data and systems safe.*
- **Access Control** – *Guidelines on who can access what and how permissions are managed.*
- **Data Protection** – *Ensuring sensitive data is classified, encrypted, and stored securely.*
- **Network and System Security** – *Safeguards for servers, networks, and IT infrastructure.*
- **Incident Response and Management** – *Steps to detect, report, and respond to security issues.*
- **Change Management** – *Procedures for safely updating and modifying IT systems.*
- **Compliance and Audit** – *Regular checks to make sure security rules follow laws and regulations.*
- **User Responsibilities** – *Expectations for employees and third-party users regarding cybersecurity.*

For the full policy, including clear guidelines and expectations on the use of the City's network and devices on how to follow security best-practices, meet legal requirements, and to protect the City from cyber threats, click here.

Below is a summary for all employees and users.

Policy Summary

Q: **Who does this policy apply to?**
A: This policy applies to all users.

Q: **Who is considered a user?**
A: Anyone who accesses, manages, or interacts with the City's information systems, including complete work.

Whether in the office, working remotely, or using cloud-based tools, these guidelines of this policy apply to everyone who uses the City's computers, devices and systems, including:

- Employees
- Contractors
- Temporary Workers

- External partners

User Responsibilities

Q: Does everyone need to know and understand this policy?
A: Yes - this policy applies to all employees and authorized users. So it's critical to understand what's required.

Violations could lead to:

- Disciplinary action up to and including termination of employment
- Contract termination with any contractors, subcontractors, consultants, or vendor
- Appropriate legal action

Q: Does it matter where I work or what I do for my job?
A: Whether a security threat is internal or external, deliberate or accidental, all users are responsible for following the expectations of this policy.

All users, including ***all employees***, must:

- Protect data
- Responsibly manage and protect accounts and passwords
- Follow cyber security and legal best practices
- Immediately report all security issues and concerns

Maintenance and IT Department’s Responsibilities

Management and IT will ensure that the necessary resources, training, and support are provided to maintain a secure information environment.

The policy is reviewed every year to keep up with changes in technology and business needs. Urgent updates will also be made throughout the year as needed.

- The Chief Information Officer (CIO) is in charge of this manual.
- The IT Security Manager develops security guidelines.
- The Technology Security Committee, under the Technology Governance Board, oversees and approves changes.