Enterprise IT Security Policy Manual

Requirements and Guidance to Protect the Confidentiality, Integrity, and Availability of Information Systems and Data Across the City of Tulsa.

March 2025 • Version 2024.5

CITY OF TULSA

Information Technology

Purpose

The purpose of this Manual is to provide clear and actionable policies to guide authorized users in protecting the City's information systems, services, business processes, and data. These policies establish the responsibilities and expected behaviors for all users, ensuring compliance with security best practices, regulatory requirements, and organizational objectives. This manual aims to foster a culture of security awareness and reduce risks associated with human factors in cybersecurity.

Scope

This Manual applies to all users who access, manage, or interact with the City's information systems, including employees, contractors, temporary staff, and third-party partners. It covers the use of organizational devices, networks, applications, and data, whether accessed on-premises, through remote connections, or via cloud-based platforms. The scope includes user responsibilities related to data protection, account management, acceptable use, and incident reporting, ensuring alignment with organizational security policies and regulatory obligations.

Maintenance and Roles

Overall responsibility and authority for this manual belongs to the Chief Information Officer (CIO). Production of recommended guidelines is the responsibility of the Information Technology Security Manager. Governance is the responsibility of the Technology Security Committee as authorized by the Technology Governance Board. This Manual will undergo an audit and update on an annual basis, as counted from the last approval. Changes may be recommended by the CIO, the IT Security Manager, or any member of the Technology Security Committee, but must be approved by the Technology Security Committee and Technology Governance Board. Changes outside of the normal annual cycle may be undertaken at need and establish a new anniversary date.

1. Network Host Policy (Previously PPM 817)

The network access systems are owned and provided by the City to assist employees and other users in conducting City business. Violation of the provisions of this policy may result in disciplinary action up to and including termination of an employee and/or other appropriate legal action as concerns both employees and other users.

1.1. Information accessed and transmitted using City-managed or -controlled systems may be subject to disclosure under provisions of the Open Records Act. There is no guarantee of privacy, nor should there be any expectation of privacy with regard to any transaction or site. Any Internet or Intranet information accessed or transmitted is considered a business record of the City and accordingly may be used in administrative, judicial or other proceedings to the extent allowed by law.

1.2. City of Tulsa managed or controlled systems may not be used to solicit, communicate or proselytize for outside commercial ventures, religious or political causes, organizations not connected to City business, or other non-job-related solicitations.

1.3. City of Tulsa managed or controlled systems are not to be used to access, view or transmit any offensive or disruptive messages, or contents that violate other City or internal departmental policies. All messages will conform to the City of Tulsa HR Non-Discrimination Policy (§ 829.1 and .2).

1.4. City of Tulsa managed or controlled systems shall not be used to knowingly send (upload) or retrieve (download) unauthorized copyrighted materials, trade secrets, proprietary financial information, chain letters, malicious code, social engineering content, or similar materials. Exceptions may be made in select cases with authorization from a department head and/or the City Attorney as appropriate.

1.5. The City reserves and may exercise the right to review, audit, intercept, access, disclose, delete, and purge all messages or contents created, received or sent over City of Tulsa managed or controlled systems for any purpose. An employee's or other user's use of City of Tulsa managed or controlled systems grants management permission to review any and all transactions or sites.

1.6. City of Tulsa managed or controlled systems may be used for personal communications or transactions provided that such use does not interfere with the conduct of City business, cause system cost increases, unreasonably interfere with the employee's duties or work time, create reputational or financial damage to the City or its citizens, or violate any provision of the Personnel Policies and Procedures Manual or established policies and procedures within individual departments.

1.7. Any employee who discovers a violation of this policy shall notify his or her immediate supervisor as soon as reasonably possible.

2. Electronic Communication Tool Policy (Previously PPM 818)

Access to Electronic Communication Tools, such as email and enterprise chat (Teams or others) are provided by the City to assist employees and other users in conducting City business. Violation of the provisions of this policy may result in disciplinary action up to and including termination of an employee and/or other appropriate legal action as concerns both employees and other users.

2.1. Communications and material on these systems may be subject to disclosure under provisions of the Open Records Act. There is no guarantee of privacy nor should there be any expectation of privacy with regard to any message. Messages carried by these systems are business records of the City; accordingly, they may be used in administrative, judicial or other proceedings to the extent allowed by law.

2.2. All messages composed, sent, or received are and remain the property of the City. They are not the private property of any user.

2.3. It is understood that occasional and limited use of these systems for personal messages to other individuals will occur. Any user's personal use shall be subject to review for inappropriate or excessive use. The systems may not be used to solicit, communicate or proselytize for outside commercial ventures, religious or political causes, organizations not connected to City business, or other non-job-related solicitations.

2.4. These communication systems shall not be used to knowingly send (upload) or retrieve (download) copy-righted materials, trade secrets, proprietary financial information, chain letters, or similar materials without prior authorization from a department head and/or the City Attorney as appropriate.

2.5. The City reserves and may exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over a City-owned or -provided system. Any user's use of City communication systems grants management permission to review any and all messages. Therefore, the confidentiality of any message should not be assumed due to possible audit or Open Records process. Even when a message is deleted, it may be possible to retrieve and read that message from City server archives. However, only those personal messages which are in violation of this policy, constitute or disclose a City work rule violation, or that could negatively impact City work processes shall normally be disclosed or acted upon by management absent an Open Records request.

2.6. While management reserves the right to retrieve and read messages transmitted or stored on City electronic communication systems, such messages should be treated as confidential by other users and accessed only by the intended recipient or other authorized individual. Users are not authorized to retrieve or read any messages that are not sent to them. Any exception to this provision must receive prior approval from a department head and/or the City Attorney as appropriate.

2.7. While SMS and other mobile communications are not normally City-provided services, they are occasionally used for emergency or other communications by City employees. City employees are warned that SMS and cellphone voice are not a secure modes of communication, and per FBI and CISA alerts, may be compromised and monitored by foreign threat actors. No sensitive information should be transmitted using these or other unsecured methods.

2.8. Any employee who discovers a violation of this policy shall notify his or her immediate supervisor as soon as reasonably possible.

3. Endpoint Device Usage Policy (Previously PPM 819)

The City owns and provides computers, mobile phones, and other devices to assist employees in conducting City business. The City may also allow for the use of personally owned devices. Personally owned devices used for City business upon approval must meet the relevant standards set forth in policy.

The following procedures have been established as the City's endpoint device policy. Violation of this policy may result in disciplinary action up to and including termination of an employee and/or other appropriate legal action as concerns both employees and other users.

The City owns, provides, or allows endpoint devices to assist users in conducting City business. Violation of this policy may result in disciplinary action up to and including termination of an employee and/or other appropriate legal action as concerns both employees and other users. At the City's discretion, Endpoints or Users that violate this policy or otherwise represent a risk to the City of Tulsa may be disconnected or disabled.

Limited Personal Use of City-Provided Endpoint Devices

3.1. Supervisors may permit the occasional, limited, appropriate personal use of a City endpoint if the use does not: (a) interfere with the users' work performance, (b) interfere with any other employee's work performance, (c) have undue impact on the network or operation of any City system or the business of the City, or (d) violate any other provision of this policy or any other policy, guideline, or standard of the City of Tulsa.

3.2. The City does not guarantee the safekeeping of personal data stored on a system. Users who choose to use a City endpoint to store personal data assume all the risk of losing such data regardless of the cause.

Expectation of Privacy

3.3. Users expressly waive any right of privacy in anything they create, store, send, or receive on a City device, or on a City-provided application or service on an authorized personally owned device. By utilizing City systems or services, users consent to allow personnel of the City to access and review all materials users create, store, send, or receive.

3.4. The City has the right, but not the duty, to monitor any and all aspects of its systems, including, but not limited to, monitoring sites visited by users on the Internet, including chat messages and discussion groups, reviewing material downloaded or uploaded by users to the Internet, and reviewing messages sent and received by users.

Software or Hardware

3.5. Users may not add software or hardware (including peripherals) to any computer system owned or operated by the City. All software and hardware integrations and installations must be reviewed and approved by the IT Security Committee and/or the Data Governance Committee and must be installed by information Technology Department personnel or systems.

3.6. Exceptions. Given unique and inherent technical competence and system requirements, specialized systems that do not have a direct network connection, shared authentication, or shared data with the larger City network will use departmental software and hardware selection and change processes. A summary of changes will be submitted to the IT Security Committee in session by the departmental representative within 90 days of the change. Further exceptions may be made using IT Standards Exception Request.

Moving or Relocating Endpoints

3.7. With certain authorized exceptions, users may not move or relocate endpoint systems to new locations on the City network or to unregistered locations, including but not limited to connected computers, laptops, and tablets owned or operated by the City of Tulsa. Authorized exceptions are mobile computers covered by a work from home agreement; mobile computers used away from City facilities for authorized work purposes; endpoints moved by departmental IT or system Subject Matter Experts; relocations, either temporary or permanent, authorized by department heads in their role as Data Owners. As an accurate inventory is necessary for IT operations and security, all permanent computer moves or relocations must be submitted to the Information Technology Department via the IT Department service management system for either approval or tracking.

Copyright Production

3.8. Users may not illegally copy, request to copy, or allow others to copy material protected under copyright law. Users who are uncertain as to whether any material is copyrighted should seek guidance from their department head or designee.

Prohibited Activities

3.9. All information stored, displayed, or sent from endpoint devices owned or managed by the City of Tulsa, or personally owned devices while in performance of City of Tulsa duties, will conform to City of Tulsa Work Rules (HR policy 411.4).

Security Standards

3.10. All endpoints that are used for City of Tulsa business are expected to adhere to the standards in the Endpoint Protection Standards. This includes personally owned devices that are authorized under Bring-Your-Own-Device (BYOD) agreements.

4. Telephone and Cellular Telephone Policy (Previously PPM 820)

The City owns and provides telephones and cellular telephones (cell phones) to assist employees in conducting City business. Users of City of Tulsa provided phones have no reasonable expectation of privacy in their communications over these systems or in the contents of cell phones so provided. Misuse or illegal use of City telephone equipment or violations of the provisions of this policy may result in disciplinary action up to and including termination and/or other appropriate legal action.

General Policy

4.1. Incoming and outgoing personal calls should be limited in terms of number and duration so as to not interfere with City business and overall employee performance.

4.2. Only applications that have been explicitly authorized by the City of Tulsa IT Department will be installed on City-provided cell phones. Only applications that have been made available via City-managed Mobile Device Management and are visible in the Apple App store or Google Play store (or equivalent) will be installed on the Work profile of personally owned cell phones that are participating in the Bring-Your-Own-Device program.

4.3. City telephone systems may not be used to solicit, communicate or proselytize for outside commercial ventures, personal profit, religious or political causes, organizations not connected to City business, or other non-job-related solicitations.

4.4. The City reserves the right to review City telephone usage. Additionally, supervisors may review telephone bills or records for purposes of detecting misuse or monitoring customer service quality. Periodically, broader system audits will also be performed to determine if any abuse has occurred.

4.5. Any City manager who may be implementing telephone monitoring or recording systems shall contact the Human Resources Director to ensure appropriate legal considerations are addressed.

4.6. Telephone activity and cell phone use records may be a matter of public record under the Open Records Act and may be requested and/or published by the media.

4.7. Collect calls should not be accepted on City telephones except in emergency conditions or when necessary to the operation of the department.

4.8. The Information Technology Department is the sole contact with telecommunication companies. The Solution Center at 918-596-7070 will assist in any telephone requirements.

Cell Phone Usage

4.9. The general use of cell phones shall not be in lieu of more cost effective, practical, and available means of communication. The assignment and purchase of cell phones and subsequent rate plans shall be approved by the department head or designee and shall be based on the employee's job requirements.

4.10. There is no guarantee of privacy nor should there be any expectation of privacy with regard to the use of City-provided cell phones.

4.11. Cell phones are the property of the City of Tulsa and must be turned in immediately upon termination of employment.

4.12. Employees should recognize that cellular transmissions, including SMS ("texting") are not secure; consequently, discretion should be used during cell phone calls especially as involves confidential or sensitive information.

5. Information Systems Security Policy (Previously PPM 821)

The City owns and provides information systems and network services to assist employees and other authorized users in conducting City business.

Violation of this policy may result in disciplinary action up to and including termination of an employee, and/or contract termination with any contractors, subcontractors, consultants, or vendors, and/or other appropriate legal action as it concerns both employees and other authorized users.

5.1. Authorization

The City of Tulsa is subject to various regulations (i.e. CJIS, PCI, HIPPA, etc.), frameworks, and guidelines for Information Technology Security. Data Owners and System Owners ensure intended recipients of information have the right and need to know the information before granting access (i.e., the minimum access required to perform their job functions). The right-to-know principle equates to a justifiable business case. If the request for access to information fulfills a verifiable business need, then the user is given access pending approval from the information owner or manager. When an appropriate Data or System owner grants a user access to data, such authorization is documented and tracked via the IT Service Management System.

5.1.1. When making a determination regarding access to data, or when auditing such access, Data Owners or System Owners will be guided by recognized Information Technology Security principles. Data Owners or System Owners should work with IT to ensure effective configurations.

5.1.1.1. Confidentiality, Integrity, Availability: All protected data will be restricted to authorized users, protected from accidental deletion or corruption, monitored for service availability, and regular audits will be performed to ensure appropriate scope of access.

5.1.1.2. Non-repudiation: No shared accounts will be used without an exception ticket approved through the standard workflow. No credentials will be shared, and a user cannot be forced to share personal credentials. All permissions or configuration changes will be made under an authorized user account associated with a known person or persons that are accountable.

5.1.1.3. Separation of Duties: Where practicable, impactful changes to authorized access to protected data or related services will require at least two individuals to make the change enforced by technical controls. Where not practicable, at least two individuals with an official relationship to the protected data must be aware of the change and consent to it. Impactful changes to authorization are new roles, significant changes in the rights of existing roles, or changes in Owner, Steward, or Custodian role membership.

5.1.1.4. Least Privilege: No rights beyond those necessary for the performance of official duties will be granted.

5.1.1.5. Security by Design: IT Security Services will be engaged as soon as reasonable for new vendor or role access to streamline secure implementation and avoid undesirable rollbacks. New authorizations in a current role do not require a review.

5.1.1.6. Accountability: Role changes will be documented by Data Owners or System Owners, or their designees.

5.1.2. Access to information that is not inherent to official duties must be approved by managers of the requesting party and the Data Owners or System Owners of the information being accessed. This approval is retained electronically by the IT Solution Center System for historical purposes; it is also retained to prove that authorization was given to a specific employee(s) and/or non-employee(s) for user access.

5.1.3. Data and information should not be used, accessed, or operated upon except by authorized employees and/or authorized non-employees for their assigned responsibilities based on a need-to-know, need-to-see, or need-to-use basis.

5.1.4. Authorized Users are required to comply with the provisions of this policy, the Oklahoma Computer Crimes Act (OCCA), (21 O.S. § 1951 et. seq. as in effect at any given time), any City of Tulsa Information Technology Department published policies, and any internal departmental security procedures.

5.1.5. Anyone with unsupervised access to areas containing CJIS equipment or data, whether an authorized user or not, must have a fingerprint-based records check conducted within 30 days of employment, appointment, or assignment. In addition, no unescorted access will be given without a completed CJIS-compliant Security Awareness Training that aligns with their level of access and responsibilities, authorization by the CJIS Security Officer (CSO) or another authorized representative, and no disqualifying Criminal History. Employees will also be required to have fingerprints reprinted in accordance with The Oklahoma Law Enforcement Telecommunications System (OLETS) and Criminal Justice Information Service (CJIS) requirements.

5.2. Authentication

Users are required to maintain a unique identification as a front-line defense for the protection of the City's information. This unique identification serves to authenticate and log all transactions initiated by the user.

5.2.1. Authentication is a control established for each information system and typically consists of verification of: (a) username (identification) of a person requesting use and/or being permitted use of the system, and (b) validation of that person's identity such as a password, magnetic card, biometric device, or by some other trusted means.

5.2.2. Authorized Users shall use the username (identification) and validation (password) assigned to them and not divulge it to others or leave it unprotected. Using or attempting to use any other method of authentication or identification is prohibited, and for employees is a violation of policy which could lead to disciplinary action up to and including termination.

5.3. Multifactor authentication must be used for access to the City of Tulsa's information. Authorized exceptions include specialized systems that do not have a direct network connection, shared authentication, or shared data with the larger City. Other exceptions may be with an IT Standards Exception Request and attendant security review.

USER RESPONSIBILITIES

5.3.1. Users are responsible for, and in some cases can be held liable for, the misuse of their accounts.

5.3.2. Users must protect their accounts and passwords.

5.3.3. Users are the owners of their passwords.

5.3.4. Users will not share passwords or reveal passwords to anyone, regardless of the circumstances unless directed in writing by the Director of Human Resources and/or Chief Information Officer.

5.3.5. Users will not use a User ID or password that belongs to another employee unless they have express permission in writing from the Director of Human Resources and/or Chief Information Officer.

5.3.6. The combination of a City User ID and password will not be used for authentication on external Internet sites, unless such authentication is part of an authorized Single Sign On (SSO) or similar approved access.

5.3.7. City passwords must be unique. Passwords will not used on any outside system since passwords on external systems can still be tied back to the City employee and used to gain unauthorized access to City systems.

5.3.8. Users will choose passwords that are difficult to compromise. Passwords will follow the guidance published in NIST SP 800-63-3. To summarize:

5.3.8.1. Passwords will be at least the minimum defined by a system, but in no case less than 8 characters. Current City of Tulsa network access accounts require 15 characters. The IT Department may modify this standard as new security risks are identified.

5.3.8.2. Complexity rules will be followed, including numbers, capital letters, symbols, and non-standard characters. Non-standard characters are not available directly on a standard keyboard and may not be applicable to a particular system.

5.3.8.3. Where possible, passphrases will be used. Passphrases are sentences or clauses with complexity rules applied in such a way that they are easily remembered by humans, but difficult to decode by a computer. (e.g. "1_like2-READ_about %00s")

5.3.9. Passwords should not be written down or stored in any unsecured repository. Of special concern are online repositories, and passwords should only be stored in online "secure" sites, if they are approved by the Information Technology Department. Built-in browser-based storage is never authorized.

5.3.10. Passwords will not be inserted into email messages or other forms of unsecured electronic communication. Email is an insecure protocol and should never be used for password transmission.

5.3.11. Users are required to promptly change any password that is either suspected or known to have been disclosed to unauthorized parties.

5.3.12. Users are responsible for all activity performed with their User IDs.

5.3.13. Users are responsible for timely reporting possible security violations involving their User IDs.

5.4. Elevated Access

Elevated Access allows the user/client to possess additional access to a computer above "basic" user privileges. This right may include the ability to install hardware or software, edit the registry, manage the default-access accounts, change file-level permissions, or other higher-risk changes.

Elevated user privileges are only allowed when a special exception has been granted. Exceptions may be requested by documenting a business justification through an IT Standards Exception Request, which requires the approval of the department-head and the Chief Information Officer. The IT Standards Exception Form request is accessible through the current IT Solution Center management software.

ELEVATED USER RESPONSIBILITIES

Every employee and non-employee is responsible and obligated to ensure that all City information, assets, computing, and communication resources are used only for approved and intended business purposes. The following rules apply to all users who use elevated privileges:

5.4.1. Users should never log on to their computers using their administrator account to perform common tasks as this can make the computer vulnerable to malicious software and other security risks. Malicious software will

run with the same privileges as the logged-on user and can utilize elevated privileges to exploit administrative-level functions.

5.4.2. When administrative tasks must be performed on a local computer, users should use the "Run As" command to start the program with administrative credentials, where feasible.

5.4.3. Users may not install or uninstall any application, operating system, or peripheral provided without IT Department involvement. Authorized exceptions include specialized systems that do not have a direct network connection, shared authentication, or shared data with the larger City. Other exceptions may be with an IT Standards Exception Request and attendant security review.

5.4.4. Users are not permitted to access applications that are likely to cause a dangerous increase in bandwidth utilization or cause network congestion without authorization by the CIO. These applications can be potential risks to the City's network environment.

5.4.5. Users will not disable or change security software or configurations installed on systems. Authorized exceptions include specialized systems that do not have a direct network connection, shared authentication, or shared data with the larger City. Other exceptions may be with an IT Standards Exception Request and attendant security review.

5.4.6. Users with elevated access are strictly prohibited from providing other user accounts with elevated access. The IT Security section of IT is solely responsible for determining which accounts receive elevated access.

5.4.7. Employees/non-employees may also be required to demonstrate knowledge of how to properly use elevated access.

5.5. Remote Computing

Remote Computing is the ability of users to use a computer or other electronic device to connect through the Internet to a City information system either through the use of a Virtual Private Network (VPN) or other secure connection method. Unsecured remote computing is not authorized.

5.5.1. Authorized Users using remote access must comply with all provisions of this policy.

5.5.2. In addition to department head authorization to access the City's network, separate authorization by the IT Department is required for remote access. Authorized Users requiring such access must contact the IT Solution Center to receive such authorization.

5.5.3. Excepting authorized solutions provided by IT, programs which emulate a City-networked PC from a remote location are not allowed.

5.5.4. VPN (Virtual Private Network) access shall be granted to users that are exempt employees and only to a limited number of non-exempt employees who have been granted approval by their Department Head and the Personnel Director or his/her designee.

5.5.4.1. If an employee transfers to another position (either within the same department or in another department), it is the responsibility of the department submitting the original request to terminate the employee's VPN access. A separate request for VPN access in the new position should then be completed.

5.5.4.2. All employees who access the City network through VPN from a personally owned computers are responsible for ensuring their personally owned computers are secure, have appropriate and current virus protection and other necessary security software to minimize risk to the City of Tulsa network. Users are required to abide by all security and confidentiality policies and procedures when accessing the City network using VPN.

5.6. Protection of Information, Detection and Reporting Violations

5.6.1. The Technology Governance Board (TGB) is responsible for establishing security policies for information systems. However, TGB authority will not supersede regulatory or legal requirements.

5.6.2. An employee shall be responsible to promptly notify their supervisor of any suspected violations of this policy. Supervisors shall notify the department head as soon as possible concerning any such alleged violation.

5.6.3. As per state and federal requirements, it is the responsibility of the City of Tulsa Information Security Manager to report suspected computer incidents, and/or breach of personally identifiable information, as quickly as possible. The ultimate goals, regardless of incident, are the protection of assets, containment of damage, and restoration of service.

5.6.4. The reported cyber incident will be coordinated by the Oklahoma Cyber Command with the Oklahoma Office of Homeland Security, Information Analysis/Infrastructure Protection Division (OHS IA/IPD) and the Oklahoma State Bureau of Investigation (OSBI).

5.6.5. In the event of an actual or imminent breach, the City of Tulsa Information Security Manager must complete and submit the "Breach of Personally Identifiable Information (PII) Report" to the District Attorney's Council (DAC) and if applicable an OJP Program Manager no later than 12 hours after an occurrence of an actual breach is known, or the detection of an imminent breach.

5.7. Security Awareness Training

Due to the current cyber threat landscape, Information Technology Security awareness, precautions, and comprehensive training are all essential and are the responsibility of all parties including the authorized user, management, and the IT Department. Each time a user accesses the network and/or uses a City device, there should be a focus on security and precaution that cannot be compromised.

Failure to follow the directives outlined below may lead to disciplinary action up to an including termination of employment and/or user access.

5.8. IT Department Responsibilities

SYSTEM ACCESS

5.8.1. The IT Department (IT) will be responsible for regular system updates to ensure security measures are in place at all times.

Exceptions. Given unique and inherent technical competence and system requirements, specialized systems that do not have a direct network connection, shared authentication, or shared data with the larger City network will use update processes. Security incidents resulting from departmental updates will be reported to the Technology Security Committee by the departmental representative in session.

5.8.2. IT may restrict access to sites it deems unsecure, unstable, and/or threatening.

TRAINING

5.8.3. IT will make available initial, periodic refresher, and remedial security training as needed to enable authorized users to understand and practice security awareness.

5.8.4. In order to secure the network, IT may periodically test users for the effectiveness of Security Awareness Training. If an authorized user is determined to act contrary to best practices outlined in Security Awareness training and/or policy, IT will categorize the user as needing remedial training. The user will then have thirty (30) days to complete remedial security training.

5.8.5. Anyone who demonstrate a disregard for security awareness as defined above and/or during training must successfully complete Security Awareness refresher training within the timeframe specified in this policy section.

5.8.6. IT may restrict and/or suspend access to information systems and/or deny the creation or assignment of additional access to an authorized user if the user fails to successfully complete Security Awareness training as assigned, whether initial, periodic refresher, or remedial.

USER RESPONSIBILITIES

5.8.7. All users will be required to complete initial Security Awareness training within 30 days of being granted access to City information systems.

5.8.8. Failure to meet the requirements of Security Awareness training as outlined in policy may result in disciplinary action up to and including termination and/or suspension of the employee's or authorized user's access.

MANAGEMENT RESPONSIBILITIES

5.8.9. The employee's/authorized user's department is responsible for ensuring all users comply with Security Awareness Training. IT will notify management of any outstanding training needs of its employees.

5.8.10. Failure to meet the requirements of the Security Awareness training as outlined in this policy may result in disciplinary action up to and including termination and/or the IT department placing the user into an unauthorized status, disabling system access as applicable, and/or restricting use of City devices.

6. Change Management Policy

This policy defines the process for enacting changes to Information Technology (IT) production environments (e.g., firewalls, routers, servers, telephony, applications, and source code) that can affect programs, systems software, hardware, or any other aspect of the information-processing environment.

This policy applies to all employees and non-employees associated with the City of Tulsa who are involved in the request, authorization, approval, programming, testing, and/or implementation of software or hardware changes and have connectivity to and from the City's data, video, or voice network.

Exceptions: Given unique and inherent technical competence and system requirements, specialized systems that do not have a direct network connection, shared authentication, or shared data with the larger City network will use departmental change processes. A summary of changes will be submitted to the IT Security Committee in session by the departmental representative within 90 days of the change.

Change Management

The Change Advisory Board (CAB) has the responsibility to ensure that appropriate documentation, testing, notification (posting announcements), training (customers and associates), and recovery procedures are in place for each change requested. The CAB will be comprised of IT Department management selected by the CIO and delegates from the various departments.

The primary objective of Change Management is to ensure that infrastructure changes are applied in a controlled manner so that the stability and security of systems and information are not compromised. Changes to systems and applications must be implemented based on formal Change Requests that are authorized by management. This helps ensure proper segregation of duties and environments which further ensures the continued compatibility of all software and hardware components.

All changes to shared hardware, systems software, application software, or procedural processes that could impact the production environment and services during and/or after the change, must be presented to the CAB before implementation. The Change Management process ensures that all elements are in place, all parties are notified and trained, and the implementation schedule is coordinated with all other activities in the City.

6.1. Change Management Examples

This policy defines the process for enacting changes that can affect applications, programs, systems software, hardware, or any other aspect of the information-processing environment. The Change Management Process includes changes or modifications to any items in the following categories:

- **Technological:** e.g. Network, servers, firewall, phone systems, internet access.
- **Environmental:** e.g. Power, UPS systems, generators, air conditioning, electrical work, facility maintenance, security systems, fire control systems, and alarms.
- **Procedural:** e.g. Changes in equipment downtime schedules, planned system outages, changes in delivering services, or changes to service levels.
- **Applications:** e.g. Product release or version upgrades, patch updates, table changes, tuning, alterations to libraries or programming.

6.2. Violation of Policy

Violations of this policy will be reviewed and may result in termination of privileges and/or disciplinary action, up to and including termination.

7. Incident Response Policy

The City's IT Security Incident Response Policy exists to protect the integrity, availability, and confidentiality of proprietary or confidential information, including Financial Data (FI) (PCI DSS, GLBA, SOX), Health Data (PHI) (HIPAA, HITECH), Trade Secrets (IP) and the information specified in the State of Oklahoma Security Breach Notification Act, to prevent loss of service, and to comply with legal requirements. This policy establishes the coordination of the City's response to incidents involving computerized and electronic communications systems. It also enables expeditious reporting, investigation, and remediation of security-related events that fall within the scope of this document.

7.1. Requirements

IDENTIFICATION OF INCIDENTS

- Any individual, whether a City employee or not, must refer an activity or concern regarding an IT Security Incident to the IT Solution Center which will immediately escalate the incident to the IT Security Manager.
- The IT Security Manager may also identify an incident through proactive monitoring of the City's network and information system activities.
- The IT Security Manager will maintain an Incident Response Plan, on file with the Solution Center in both electronic and physical copies.
- The IT Security Manager will use standard internal procedures to log and track incidents, and working with others as appropriate, take steps to investigate, escalate, remediate, refer to others, or otherwise address the incident as outlined in this policy.

RESPONSE TO INCIDENTS

The IT Operations Security Manager is responsible for incident interdiction and remediation of computer and electronic communications-based resources affected by these incidents. As such, the IT Security Manager will coordinate the City's response by

1. investigating the validity of the incident by consulting members of the IT Department, and/or administrators in affected offices or City Departments, public safety and public health officials, and other entities as warranted.
2. reporting the incident to the proper authorities, City Departments, and other affected agencies.

3. appropriately logging and tracking the incident from report to closure (archival).
4. establishing an internal risk assessment classification matrix to focus the response to each incident, and to establish the appropriate team participants to respond. This classification matrix will correspond to an "escalation" of contacts across the City indicating which City authorities should be involved and which procedure would be applicable for each class of incident.
5. identifying any IT Security Incidents involving PHI to implement the relevant HIPAA Security procedures. Incident reporting will be provided by the IT Security Manager to the Director of IT Operations & Support and/or Chief Information Officer.
6. maintaining standard subordinate procedures for the response and investigation of each incident, as well as securing the custody of any evidence obtained in the investigation. The application of these procedures will be governed by the custody of evidence of a criminal case. The procedures will specify the location and method of custody for each incident if custody of evidence is required
7. working with the IT Security Incident Response Team to communicate the incident to appropriate personnel and maintain contact for updates and instructions for the duration of the incident.

ROLE OF CITY PERSONNEL, TRAINING

All employees seeking access to managed IT systems are required to attend CJIS, HIPAA, PCI, or other sensitive data training as required before gaining access to those managed IT systems.

RELATIONSHIP TO STATE AND FEDERAL AGENCIES

A response or remediation plan defined by this policy may be preempted as required or at the City's discretion by the intervention of federal and state executive officials.

INCIDENT PREVENTION

When possible, the City will endeavor to prevent incidents by monitoring and scanning City networks for anomalies and developing clear procedures for the configuration and protection of its IT resources.

SPECIAL SITUATIONS/EXCEPTIONS

Any personally owned devices, such as tablets, phones, laptops, or other wireless devices that have been used to store City information or protected data that are determined to contribute to an incident, may be subject to seizure and retention by the City until the incident has been remediated. By using these devices within the City network for business purposes, individuals are subject to the City's policies governing their use and accountably subject to the Oklahoma Open Records Act.

7.2. Manager and Supervisor Responsibilities

Managers and Supervisors are responsible for reporting violations of this policy to the Information Technology.

Managers and Supervisors are responsible for working with IT to establish any new services needed on mobile devices that are not already approved.

8. Software Purchasing and Installation

All software installed on City computers/peripherals must be properly licensed and installed by Information Technology (IT). This includes software that is user-installable, such as "Click-Once" applications, licensed Web-based applications, or standalone executables. All software (including hosted or web-based solutions) purchases will be made through IT to ensure proper licensing and tracking of installed or accessed software and adhere to the Finance Purchasing Policies.

8.1. Regardless of purchase or license requirements, no unvalidated software, whether installable, standalone, Web-based or open source, will be used on the City network. Validation is the process whereby software is reviewed by IT Security, IT Operations, and IT Architecture for suitability and safety. If the software will be used in a completely isolated fashion from the larger City network, it may be validated by the appropriate Data Owner for their department. In this instance, the department will maintain records of such approvals and is responsible for ensuring that the software has no negative effect on the City at large.

8.2. Manager / Supervisor Responsibilities: All requests for adding software that is not pre-approved and listed on the "Authorized Software" list MUST be submitted to and approved by IT. Requests must be submitted through a completed IT Standards Exception Form request in the IT Solution Center management software. If approved, IT personnel will be tasked with installing the software. Software Purchases should not be made using a purchasing card, except as directed by the City's Chief Information Officer or designee.

While IT provides training classes for end users on the recommended use of some installed software, it is ultimately the responsibility of each department to ensure that its end users receive proper training on the use of software. Departments may contact the Solution Center for recommendations on software training classes.

8.3. Exceptions: Given unique and inherent technical competence and system requirements, specialized systems that do not have a direct network connection, shared authentication, or shared data with the larger City network will use departmental software selection and change processes.

9. Computer Equipment Purchasing

The following policy defines the methods and procedures for purchasing computer equipment at the City of Tulsa. Standardized configurations are a critical factor in an effective IT security program.

Requirements

- Standard configurations are established by the IT Department and are included in bid specifications for annual computer purchases.
- Computer equipment for all City departments is purchased following configurations outlined in the IT Computer Equipment Specifications document. Where no standard has been defined, the purchase is processed as an exception and requires an approved IT Standards Exception Form request in the IT Solution Center management software.
- Authorized spending for standard configurations is consistent with the information detailed within the IT Computer Equipment Specifications document.
- All computer equipment purchase requests must be submitted to the IT IT Solution Center
- IT Administration Services is responsible for ensuring that requested computer equipment complies with standard configurations, meets business requirements, and is purchased from an approved vendor.

- Computer purchases, including parts that may be purchased to assemble a computer, should not be made using a purchasing card, except as directed by the City's Chief Information Officer or designee.
- If an exception to a standard configuration is being requested, the requestor must complete the IT Standards Exception Form request in the IT IT Solution Center management software. The Chief Information Officer or designee is responsible for final approval of all computer exceptions.
- Department heads are responsible for approving requisitions and exceptions in their respective departments.
- All requested configurations must be authorized by the appropriate department head.

Exceptions: Given unique and inherent technical competence and system requirements, specialized systems that do not have a direct network connection, shared authentication, or shared data with the larger City network will use departmental hardware selection and change processes. A summary of changes that may create a connection or potential connection to the greater City network will be submitted to the IT Security Committee in session by the departmental representative within 30 days of the change.

10. Auditing and Accountability

All systems, services, and data under City of Tulsa control will conform to system auditing, data governance, and security standards. All systems, services, and data under City of Tulsa control will have assigned City staff responsible for compliance. Unless delegated, the responsible person is the Data Owner or System Owner.

10.1. Data Owners and System Owners, in cooperation with IT, will perform periodic reviews at least annually of City systems and data to ensure adherence to all City Enterprise IT Security Policies.

10.2. Identified issues without a documented exception will be immediately remediated and brought into compliance when possible. Issues than cannot be brought into compliance will be brought before Technology Security Committee for recommended action to the Technology Governance Board. For systems that have compliance requirements that limit access and remediations to externally licensed or certified individuals, auditing or accountability issues will be managed at the departmental level.

10.3. Any data generated as part of a security policy audit is classified as protected data.

10.4. Data will be retained in accordance with the current City Record Retention Schedule.

10.5. Data will be securely disposed of in compliance with the current City Record Destruction Policy.

10.6. Access to this data will be recorded and will be limited to individuals with a specific need for access to the records. Access to the data will be limited to the specific sets of data appropriate for the business need.

10.7. Audit summary reports will be created for each system security audit conducted, and the reports will be provided to the IT Security Manager for archival and consolidated reporting.

10.8. Every security audit deficiency must be accompanied with a recommendation.

Policy Exceptions

Departments requesting exceptions to this policy shall provide such requests in writing via the IT Service Management system to the IT Security Manager. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein. The IT Security Manager will provide this information along with a recommendation to the Chief Information Officer (CIO) and the Technology Security Committee (TSC).

11. Vendor and Partner Management Policy

This policy ensures that vendors and partners adhere to our security, compliance, and operational standards. The policy outlines the requirements for evaluating, onboarding, managing, and offboarding vendors to mitigate risks related to vendor relationships.

This policy applies to all vendors or partners providing products or services that interact with the City of Tulsa ("City") systems, data, or operations. Partners are organizations that provide a product or service, or reciprocal product or service, but have no commercial relationship with the City.

- **11.1.** Evaluation.
  - **11.1.1.** All vendors or partners must undergo a risk-based evaluation prior to engagement.
  - **11.1.2.** This evaluation will include an assessment of financial stability, reputation, security practices, compliance with regulatory requirements, and alignment with the City's business needs.
- **11.2.** Tiered Risk Assessment.
  - **11.2.1.** Vendors or partners will be categorized into risk tiers based on the nature of their services, access to sensitive data, and potential impact on operations.
  - **11.2.2.** Higher-risk vendors will be subject to more stringent due diligence and monitoring.
- **11.3.** Contractual Obligations.
  - **11.3.1.** City of Tulsa agreements must include clauses covering data protection, confidentiality, security controls, incident reporting, and compliance with relevant regulations.
- **11.4.** Ongoing Monitoring.
  - **11.4.1.** Vendors or partners will be monitored regularly based on their risk tier.
  - **11.4.2.** This includes ad-hoc performance reviews, security audits, and compliance checks to ensure continued alignment with our policies and standards.
  - **11.4.3.** Vendors or partners in good standing with the City may submit an attestation of security posture, subject to the approval of the CIO with the advice of his IT Security team.
- **11.5.** Incident Management.
  - **11.5.1.** Vendors or partners must promptly report any incidents or breaches that may impact our data or operations.
  - **11.5.2.** Response procedures and communication channels will be defined in advance, as part of the initial due diligence process.
- **11.6.** Offboarding.
  - **11.6.1.** Upon termination of services, vendors must follow established procedures to securely return or destroy any City of Tulsa data.
  - **11.6.2.** Access to systems must be revoked immediately.
- **11.7.** Procedures.
  - **11.7.1.** Detailed procedures for vendor evaluation, onboarding, risk assessment, and monitoring are documented separately.
- **11.8.** Maintenance.
  - **11.8.1.** This standard will be reviewed annually or as needed to adapt to evolving risks, regulatory changes, or business needs.

Appendix A: Definitions

Authorized User or User – An individual, process, or entity that interacts with an information system to perform authorized activities, access data, or utilize resources. At the City of Tulsa, this includes all employees, including interns, temporary, emergency, and special qualification personnel employed or under contract for temporary periods, and any temporary situations or assignments, and all contractors, subcontractors, consultants, and vendors who are permitted to use the City's information systems for any reason.

IT Change Management – The collaborative process that protects Information Technology Systems, hardware and software, supporting systems such as environmental controls, services, business processes, and users from changes that are potentially disruptive or have unacceptable risks associated with them. It is the ongoing process of communicating, coordinating, monitoring, approving, and scheduling changes to an environment. In the context of this definition, change makes a difference, alters, or modifies any production process or configuration.

Change Owner – Department designee responsible for overseeing change

Change Technician – Person making the actual change to the system. Also responsible for developing the change procedure, rollback, and testing plans.

Change Request – A request initiated by a ticket in the IT ticketing system, authorized by the Department Head or designated department liaison

Change Advisory Board (CAB) – IT staff and managers which meet with affected departmental liaisons to review and approve changes.

Change Management Quality Assurance – Internal IT review of proposed change request before official CAB meeting

Change Management/CAB Meeting – A meeting of CAB for the purpose of communicating, coordinating, monitoring, approving, and scheduling changes to an environment.

City Device – Any City-owned computing device such as a desktop or laptop computer, smart phones or tablet.

CJIS – Criminal Justice Information Systems, a category of protected systems under the guidelines established in CJIS policy by the FBI.

Computer Equipment – Any device used to access the City of Tulsa data or networks, including desktop and laptop computers, tablets, kiosks, smartphones, printers, or streaming media devices.

EPHI / PHI – Electronic Protected Health Information means individually identifiable health information that is maintained or transmitted using electronic media. This includes information about the past, present, or future physical or mental health or condition, or provision of health care. This includes descriptive data that can identify an individual but excludes data maintained by an employer in its role as an employer.

Exception – Approval of a request for anything non-standard, approved by the Requestor's department and IT, to include management, IT Security, and the Architects as appropriate.

HIPAA – The Health Insurance Portability and Accountability Act provides federal protection for the privacy of personal health information.

Information System – Any software, network, peripheral device, computer, or media used to store, transfer, manipulate, or otherwise use information electronically. This also includes any documents in any form, including electronic or printed, used to prepare, support, manage or use an information system.

ITD – Information Technology Department

IT Management – Chief Information Officer, IT Directors, IT Managers, or their designees

IT Operations Security Manager – The City of Tulsa IT Operations Security Manager is responsible for day-to-day security operations, oversight of the IT security committee, advancing technology used for security incident detection, and leadership of the IT Security Incident Response Team during crisis.

Information Security Manager – The city of Tulsa Information Security Manager is responsible for developing, maintaining, improving and implementing the IT Security program and the overall security posture of the city. This may include advisory and enforcement actions related to compliance with relevant regulations and laws such as HIPAA security regulations and the State of Oklahoma Security Breach Notification Act.

IT Security Incident Response Team – A team that can include key representatives of the Information Technology Department, administrators in affected offices, the City of Tulsa Cybercrime Unit, Disaster Recovery, Legal Department, Communications, Internal Audit, and other units as warranted to establish an IT Security Incident Response Team appropriate to respond to a specific Incident.

Initial Security Awareness Training – Security system training required for users within thirty (30) days of having been granted access to City Information Systems and/or devices which is made available by the IT Department. Failure to complete this required training may result in a temporary suspension of access until completion.

IT Security Incident – An IT Security Incident (incident) is any activity that harms or represents a serious threat to the whole or part of the City's computer, telephone, and network-based resources such that there is an absence of service or inhibition of functioning systems. This includes unauthorized changes to hardware, firmware, software, or data. This also includes unauthorized exposure, change, or deletion of EPHI, a crime, or a natural disaster that destroys access to or control of these resources. Routine detection and remediation of a "virus," "malware," or similar issue that has little impact on the day-to-day business of the City is not considered an Incident under this policy.

Management – The department management staff responsible for the employee and/or authorized user.

Multifactor Authentication (MFA) – A security process in which a user is granted access to a system or application only after successfully presenting two or more pieces of evidence to verify their identity. The two or more pieces of evidence are known as factors.

The most common factors used in MFA are:

- Something you know: This is typically a password or PIN.
- Something you have: This is typically a physical device, such as a security token or smartphone.
- Something you are: This is typically a biometric identifier, such as a fingerprint or facial scan.

Periodic Security Awareness Refresher Training – Security system training required for users at periodic intervals as determined by the IT Department.

PCI – Payment Card Industry related to information contained in credit card transactions on online payments.

Remedial Security Awareness Training – Security awareness training required for users after having demonstrated an inability or unwillingness to follow IT security-related policies, guidelines, and good security practices, and thus placing the City at greater than necessary risk. Remedial training addresses learning gaps by reteaching skills and responsibilities with a focus on weak areas. Failure to complete this required training would result in a temporary suspension of access until completion.

Security Awareness – Security awareness is the knowledge and attitude members of an organization possess regarding the protection of its information systems assets and resources whether physical or virtual, (online, email, software, internet, etc.) Security awareness training is a strategy used by IT and security professionals to prevent and mitigate user risk. These programs are designed to help users and employees understand the role they play in helping to combat information security breaches.

Security Breach Notification Act – This is an act specific to the State of Oklahoma that relates to identity theft. It involves creating a short title, defining terms, and requiring disclosure of security breaches to certain persons without unreasonable delay. It also requires providing guidelines for notice requirements and providing enforcement authority to the Attorney General or district attorney, et al.

System Owner – Information Technology or Operational Technology staff responsible for the technical functioning of a system or service.

Data Owner – Senior leader with overall responsibility and authority for the business use of the data related to a system or service. Typically a Department head.

Data Custodian – Information Technology or Operational Technology staff responsible for the data security of a system or service as defined by the Data Owner.

Version History

Version	Editor	Description	Date	Comments
2024.1	Michael Dellinger	2024 Policy Consolidation	04/25/2024	Moved PPM policies to this policy document – 817 – 821 should be removed from PPM upon approval.
2024.2	Darren Fritz	Technology Security Committee Update		
2024.3	Tesker LeMoine	Technology Security Committee Update + Addition of New Policies	11/20/2024	Resolved some comments in session, in preparation for TGB.
2024.4	Tesker LeMoine	Technology Security Committee Update	12/03/2024 – 12/12/2024	Team edits in preparation for submission
2024.5	Jake Brown	IT Management Review	12/17/2024	