INFORMATION TECHNOLOGY AND SECURITY POLICY

Department of Information Technology

Latest Revision Release Date: 08/06/2025 | **Initial Release Date:** 08/12/2025

Table of Contents

Purpose

The Information Security and Technology Policy ("Policy") is dedicated to the following purposes. First, the Policy is to convey the highest directive of cybersecurity posture of the City of Mission ("City") which stems to a subset of administrative, operational, and technical controls. Second, the Policy is developed, reviewed, updated, and implemented to mitigate imminent and potential cybersecurity risks to employees and affiliated third parties on data, network and information system owned by the City. Third, the Policy guides how the City complies with applicable industry standards and regulations including the Health Information Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, the Freedom of Information Act (FOIA), the Texas Public Information Act (TPIA), the Texas State Breach Disclosure Laws, the Payment Card Industry Data Security Standards (PCI-DSS), Criminal Justice Information System (CJIS), and American Water Works Association (AWWA).

Policies, Standards, Guidelines and Procedures Defined

- A Policy consists of high-level statements relating to the protection of information across the organization and should be produced and ratified by senior management. A documented policy is frequently a requirement to satisfy regulations or laws, such as those relating to privacy and finance. It is an organizational mandate.
- Standards consist of specific low level mandatory controls that help enforce and support the information security policy. Standards help to ensure security consistency across the business and usually contain security controls relating to the implementation of specific technology, hardware, or software.
- Guidelines consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place. Guidelines should be viewed as best practices that are not usually requirements but are strongly recommended. They could consist of additional recommended controls that support a standard or help fill in the gaps where no specific standard applies.
- Procedures consist of step-by-step instructions to assist workers in implementing the various policies, standards, and guidelines. While the policies, standards and guidelines consist of the controls that should be in place, a procedure gets down to specifics, explaining how to implement these controls in a step-by-step fashion.

Policy Set Structure

To ensure that best practices are woven into the City's technology infrastructure, the policy set is built off industry standard framework: National Institute of Standards and Technology (NIST).

Furthermore, to satisfy multiple external legal and industry requirements, such as Payment Card Industry Data Security Standard (PCI-DSS), the Federal Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Systems (CJIS), SWIFT, and Transportation Security administration (TSA) Standards specific requirements have been included.

Each Policy Standard has been noted with the specific framework requirements to enable rapid cross reference of City Policy against compliance requirements.

Each document consists of four levels of hierarchical statements: Policy Number (Chapter, Numeric) – Article (Numeric) – Clause (Numeric) – Item (Alphabetic).

Applicability

The policies apply to all City of Mission information technology systems and networks, those entrusted to third-parties, City employees and others including but not limited to contractors, vendors, and consultants.

Not all departments in the City have the same technological implementations. While the policies reflect current technology and security advances, implemented technologies in some departments may not be of immediate compliance with the policy. The use of such technologies must be reviewed by the IT Department and approved by the IT Director through a policy exception process.

These policies do not foresee any exceptional situations like new legal or regulatory obligations, best practices, or emergencies that require actions that might conflict with policy statements. Should that occur, it is the responsibility of the individual who has identified such a situation to report to the IT Director.

Policy 1		Policy Owner
Policy Responsibilities & Oversight		Department of Information Technology
Effective	**08-12-2025**	
Last Revision		

1. Policy Responsibilities & Oversight

I. Purpose

The purpose of the Information Security Policy is to formalize the Security and Internal Control standards that the City of Mission ("City") has adopted to mitigate security risks to employee and constituent data. The requirements and standards within this policy comply with applicable external controls and regulations, including the Health Information Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, the Payment Card Industry's Data Security Standards (PCI-DSS), and the Freedom of Information Act (FOIA).

In addition, this policy defines the requirements for how computing and communication assets, systems and resources should be accessed, configured, used, and protected. These requirements, along with monitoring activities of City personnel's internet use help maintain the security of the City's technology environment.

This document is published under the authority of the IT Director, and provides a framework for safeguarding data, including personally identifiable information (PII), protected health information (PHI) and payment cardholder data (CHD), throughout the information lifecycle within the City of Mission.

All City Departments are subject to the provisions within. Exceptions to any provision can only be granted by the IT Director, or delegate.

II. Policy Statements

1.1. Roles and Responsibilities

City of Mission employees, contractors and agents should support the information security program detailed herein.

1.1.1. Management Commitment to Information Security & Sponsorship

Management should approve and be committed to all Information Security initiatives set forth in this Information Security Policy. As such, management shall identify a sponsor to drive assessment, compliance, and enforcement activities.

a. Ultimately, the IT Director should be responsible for the establishment of the Information Security Policy. The IT Department should be responsible for driving day-to-day activities and enforcement.

b. The IT Department is the internal group responsible for managing and directing a city-wide information protection program. Specific responsibilities include:

- Developing, or coordinating the development of information security policies, standards, and guidelines.
- Managing a data and asset classification program, which includes the identification of information and application owners.
- Identifying information protection goals and objectives within the scope of a strategic plan.

- Identifying key information security program elements.
- Identifying key corporate information security initiatives and standards.
- Developing information security guidelines for personnel.
- Developing and managing an information security program budget.
- Ensuring the timely publication of approved information security related policies and procedures.
- Coordinating information security awareness activities across the City of Mission.
- Taking appropriate action on security violations..

1.1.2. Allocation of Information Security Responsibilities

Roles and responsibilities for ensuring support of the Information Technology and Security Policy should be assigned.

a. The IT Director is responsible for the security of information assets and technology in the City. The IT Director may delegate specific responsibilities related to information security to others within the City based on their job function. Specific responsibilities are assigned as follows:
    - The responsibility to establish, document, and distribute security policies and standards is assigned to the IT Director. Should the IT Director position become vacant, this responsibility will be assigned to a knowledgeable member of management by the IT Manager.
    - The responsibility to monitor and analyze security alerts and information and distribute to appropriate personnel is assigned to the IT Director. Should the IT Director position become vacant, this responsibility will be assigned to a knowledgeable member of management by the IT Department.
    - The responsibility to establish, document, and distribute information security incident response and escalation procedures to ensure timely and effective handling of all situations is assigned to the IT Director. Should the IT Director position become vacant, this responsibility will be assigned to a knowledgeable member of management by the IT Manager.
    - Overall responsibility for administering user accounts, including additions, deletions, and modifications, is assigned to the IT Manager. Should that position become vacant, this responsibility will be assigned to a knowledgeable member of management by the IT Department. Wherever additional user accounts may be required for a specific software application or Program, the responsibility for administering user accounts, including additions, deletions, and modifications, is assigned to the Program Manager responsible for that Program.
    - The responsibility to monitor and control access to data is assigned to the Cybersecurity Analyst for file, print, email, and network access. Should that position become vacant, this responsibility will be assigned to a knowledgeable member of management by the IT Director. For data that is created, maintained and/or managed in conjunction with a specific software application or program, the responsibility to monitor and control access to data is assigned to the Information Owner responsible for that program or their delegate.

b. The IT Department is responsible for coordinating the review of risks and security implications associated with the use of technologies within the City's operating environment.

c. An Information User is any City employee, vendor, contractor, or other authorized person who uses City information in the course of their daily work. Information User responsibilities include:
    - maintaining the confidentiality of their user credentials.
    - reporting suspected security violations to the IT Department.
    - adhering to corporate information security policies, standards, and technical controls; and
    - using City information resources responsibly and for authorized purposes only.

d. An Information Owner is a manager responsible for the City's information assets. Individual Information Owners reside within Business Units or Departments, not the Department of Technology. Information Owner responsibilities include:

- Assigning initial information classification levels.
- Periodic reviews to ensure current information classification meets the current business need and level of perceived risk.
- Verifying that employee and third-party access rights are current.
- Determining security access criteria; and,
- Determining availability and backup requirements for the information they own.

e. An Information Custodian is any City employee, vendor, contractor, or other authorized person who has the responsibility for maintaining and/or supporting information. Information Owners have the right to delegate data maintenance and ownership responsibilities to Information Custodians. The Information Owner may designate one or more Information Custodians based on the level of delegated responsibilities. The Information Custodian must provide the following:
   - Assistance to the Information Owners in determining appropriate levels of data; and
   - Operationally provide assurance for the confidentiality, integrity, and availability of information.

f. System Administrators are required to maintain, operate, and implement technology solutions for the City in accordance with the security policy. Access to servers is restricted to authorized System Administrators who are responsible for deploying, implementing, and monitoring security controls on an operational basis. Guidance for the specific controls should be provided by IT Department. Responsibilities include system security patch applications; System documentation; System performance; Security monitoring; Application of necessary technical security controls; and Communication to IT Department on security related incidents and issues.

g. The IT Department is responsible for monitoring compliance with the standards and guidelines outlined by the security policy.

h. The IT Department is responsible for the day-to-day data center operations. This includes the management of the Uninterruptible Power Supply (UPS) and other environmental controls, in addition to racking new devices, pulling cabling, and operating network jacks. This team is also responsible for understanding, maintaining, and operating the data center fire suppression systems. Additional responsibilities include:
   - Configuring and maintaining the City network.
   - Network segmentation.
   - Providing network access control.

1.1.3. Review of Information Security

A review of the City environment must be conducted by either the IT Department, a designated Internal Audit team, or an independent third party. The goal of the review should be to ensure proper security controls are in place throughout the organization.

The City's security policy, standards and security environment should be reviewed annually. Any recommendations from this review must be resolved and considered for incorporation into the security policy and implemented as applicable. Determining the level of assurance is the responsibility of the IT Department.

1.2. Information Technology and Security Policy Maintenance

The City of Mission Information Security Policy is approved, maintained, and annually reviewed to ensure its effectiveness.

1.2.1. Security Policy Approval

The Information Security Policy is approved by management. Based on the review being conducted, approvals follow the pre-defined, documented information security policy approval process.

a. The IT Department is responsible for creating, reviewing, and coordinating the approval and implementation of security practices, policies, and standards. Responsible for ensuring that the security practices and standards are reviewed and approved on an annual basis.

1.2.2. Additions and Changes to Policy

Any additions or changes to the Information Security Policy are managed and approved. All additions to the information security policy follow the pre-defined, documented information security policy change process.

a. Any business unit, group or department may initiate practice or standards development with the IT Department. The IT Department will analyze requests and address each at their discretion based upon this analysis.

b. The IT Department is responsible for ensuring that new information security policies and standards follow the existing practice structure and format of the information security policy or as deemed appropriate by the IT Director. At a minimum, the following tasks must be conducted for new or changed information security policies:

- A communication plan must be developed, at a minimum including notification of new practices, integration into security awareness materials, and special training for technical users/personnel (if deemed necessary).
- An impact analysis may be conducted or coordinated by the IT Department prior to information security policy changes to measure the risk and security implications driving the requested change and potential implementation requirements for full implementation of the changed policy.

1.2.3. Review of the Information Security Policy

An annual review of the Information Security Policy is conducted to ensure relevance and identify any gaps in the policy.

a. The IT Department is responsible for initiating an annual review of the information security policy.

b. The IT Department reviews to ensure standards remain in sync with business requirements, vendor, and industry-recommended practices, current technology, and regulatory requirements.

c. The annual review must include a review of any impacting legal changes to ensure practice compliance with applicable municipal, state, and federal laws.

d. The annual review results must be presented to the City's Executive Department.

III. Exceptions

Any exception to the policy must be submitted through a "Policy Exception form" for review and approval by the IT Department in advance.

IV. Revision History

Date	Version	Description	Author

Policy 2		Policy Owner
Awareness and Training Policy		Department of Information Technology
Effective	**08-12-2025**	
Last Revision		

2. Awareness and Training Policy

I. Purpose

To ensure that the appropriate level of information security awareness training is provided to all Information Technology (IT) users.

II. References and Standards

National Institute of Standards and Technology (NIST) Special Publications: NIST SP 800-53 – Awareness and Training (AT), NIST SP 800-12, NIST SP 800-16, NIST SP 800-50, NIST SP 800-100; Electronic Code of Federal Regulations (CFR): 5 CFR 930.301

III. Policy Statements

2.1 Security Awareness Training

The City of Mission shall:

a. Schedule security awareness training as part of initial training for new users.

b. Schedule security awareness training when required by information system changes and then annually thereafter.

The IT Department shall:

c. determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content shall:

   i. Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.

   ii. Address awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

2.2 Security Awareness | Insider Threat

IT Department shall:

a. Include security awareness training on recognizing and reporting potential indicators of insider threat.

2.3 Role-Based Security Training

IT Department shall:

a. Provide role-based security training to personnel with assigned security roles and responsibilities:

   i. Before authorizing access to the information system or performing assigned duties.

   ii. When required by information system changes and yearly thereafter.

2.4 Physical Security Control

IT Department shall:

a. Provide initial and ongoing training in the employment and operation of physical security controls; physical security controls include, for example, physical access control devices, physical intrusion alarms, and monitoring/surveillance equipment.

b. Identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training.

2.5 Practical Exercises

IT Department shall:

a. Provide practical exercises in security training that reinforce training objectives; practical exercises may include, for example, security training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives. These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes.

2.6 Suspicious Communications and Anomalous System Behavior

IT Department shall:

a. Provide training to its specified staff on how to recognize suspicious communications and anomalous behavior in organizational information systems.

2.7 Security Training Records

The City of Mission shall:

a. Designate personnel to document and monitor individual information system security training activities including basic security awareness training and specific information system security training.
b. Retain individual training records for a minimum of two years.

IV. Exceptions

Any exception to the policy must be submitted through a “Policy Exception form” for review and approval by the IT Department in advance.

V. Revision History

Date	Version	Description	Author

CITY OF MISSION

Policy 3		Policy Owner
Access Control Policy		
Effective	**08-12-2025**	Department of Information Technology
Last Revision		

3. Access Control Policy

I. Purpose

To ensure that access controls are implemented and in compliance with IT security policies, standards, and procedures.

II. References and Standards

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Access Control (AC), NIST SP 800-12, NIST 800-46, NIST SP 800-48, NIST SP 800-77, NIST SP 800-94, NIST SP 800-97, NIST SP 800-100, NIST SP 800-113, NIST SP 800-114, NIST SP 800-121, NIST SP 800-124, NIST SP 800-164; NIST Federal Information Processing Standards (FIPS) 199

III. Policy Statements

3.1. Account Management

IT Department shall:

a. Identify and select the following types of information system accounts to support organizational missions and business functions: individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.

b. Assign account managers for information system accounts.

c. Establish conditions for group and role membership.

d. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.

e. Require approvals by system owners for requests to create information system accounts.

f. Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures.

g. Monitor the use of information system accounts.

h. Notify account managers and system/network administrators within one (1) day when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes.

i. Authorize access to the information system based on valid access authorization or intended system usage.

j. Review accounts for compliance with account management requirements at least annually.

k. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

l. Employ automated mechanisms to support the management of information system accounts.

m. Ensure that the information system automatically disables temporary and emergency accounts after usage.

n. Ensure that the information system automatically disables inactive accounts within (1) week

o. Ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate IT personnel.

3.2. Access Enforcement

IT Department shall:

a. Ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

3.3. Information Flow Enforcement

IT Department shall:

a. Ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy.

3.4. Separation of Duties

IT Department shall:

a. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.

b. Document the separation of duties of individuals.

c. Define information system access authorizations to support separation of duties

3.5. Least Privileged

IT Department shall:

a. Employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

b. Authorize explicitly access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.

c. Require that users of information system accounts, or roles, with access to privileged security functions or security-relevant information (e.g., audit logs), use non-privileged accounts or roles, when accessing non-security functions.

d. Restrict privileged accounts on the information system to privileged users.

e. Ensure that the information system audits the execution of privileged functions.

f. Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

3.6. Unsuccessful Logon Attempts

IT Department shall ensure that the information system:

a. Enforces a limit of consecutive invalid logon attempts by a user during five (5) unsuccessful login attempts by a user during a 15- minute time period.

b. Locks the account/node automatically until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

3.7. System Use Notification

IT Department shall ensure that the information system:

a. Displays to users an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance and states informing that:

   i. Users are accessing a restricted City of Mission information system.

   ii. Information system usage may be monitored, recorded, and subject to audit.

   iii. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.

   iv. Use of the information system indicates consent to monitoring and recording.

   v. There are no rights to privacy.

b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

c. For publicly accessible systems, the IT Department shall ensure that the information system:

   i. Display system use information consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines before granting further access.

   ii. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

   iii. Includes a description of the authorized uses of the system.

3.8. Session Lock

IT Department shall ensure that the information system:

a. Prevent further access to the system by initiating a session lock after 30 minutes of inactivity or upon receiving a request from a user.

b. Retain the session lock until the user re-establishes access using established identification and authentication procedures.

c. Conceal, via the session lock, information previously visible on the display with a publicly viewable image.

3.9. Session Termination

IT Department shall:

a. Ensure that the information system automatically terminates a user session after a user has been logged out.

3.10. Permitted Actions Without Identification or Authentication

IT Department shall:

a. Identify user actions that can be performed on the information system without identification or authentication consistent with organizational missions and business functions.

b. Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

3.11. Remote Access

IT Department shall:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

b. Authorize remote access to the information system prior to allowing such connections.

c. Ensure that the information system monitors and controls remote access methods.

d. Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

e. Ensure that the information system routes all remote accesses through managed network access control points to reduce attack surface.

f. Authorize the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.

g. Document the rationale for such access in the security plan for the information system.

3.12. Wireless Access

IT Department shall:

a. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.

b. Authorize wireless access to the information system prior to allowing such connections.

c. Ensure that the information system protects wireless access to the system using authentication of users and devices and encryption.

3.13. Access Control for Mobile Devices

IT Department shall:

a. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

b. Authorize the connection of mobile devices to organizational information systems.

c. Employ full-device encryption or container encryption to protect the confidentiality and integrity of information on approved devices.

3.14. Use of External Information Systems

IT Department shall:

a. Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

   i. Access the information system from external information systems.

   ii. Process, store, or transmit organization-controlled information using external information systems.

b. Permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

   i. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.

   ii. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

3.15. Information Sharing

IT Department shall:

a. Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information as defined on agreement or contract.

b. Employ attribute-based access control or manual processes ad defined in the agreement or contract to assist users in making information sharing/collaboration decisions.

3.16. Publicly Accessible Content

IT Department shall:

a. Designate individuals authorized to post information onto a publicly accessible information system.

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.

c. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.

d. Review the content on the publicly accessible information system for nonpublic information quarterly and removes such information, if discovered.

IV. Exceptions

Any exception to the policy must be submitted through a "Policy Exception form" for review and approval by the Information Security Office in advance.

V. Revision History

Date	Version	Description	Author

	Policy 4		Policy Owner
	Incident Response Policy		
CITY OF MISSION	Effective	**08-12-2025**	Department of Information Technology
	Last Revision		

4. Incident Response

I. Purpose

To ensure that Information Technology (IT) properly identifies, contains, investigates, remedies, reports, and responds to computer security incidents.

II. Reference and Standards

National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-53a – Incident Response (IR), NIST SP 800-16, NIST SP 800-50, NIST SP 800-61, NIST SP 800-84, NIST SP 800-115

III. Policy Statements

4.1. Incident Response Training

The City of Misson shall:

a. Provide incident response training to information system users consistent with assigned roles and responsibilities:

   i. Prior to assuming an incident response role or responsibility.

   ii. When required by information system changes, and annually thereafter.

b. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.

c. Employ automated mechanisms to provide a more thorough and realistic incident response training environment.

4.2. Incident Response Testing

The City of Mission shall:

a. Test the incident response capability for the information systems annually using tabletop or walk-through exercises; simulations; or other agency-appropriate tests to determine the incident response effectiveness and document the results.

b. Coordinate incident response testing with City of Mission contacts responsible for related plans such as Emergency Operation Plans.

4.3. Incident Handling

The City of Mission shall:

a. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

b. Coordinate incident handling activities with contingency planning activities.

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

4.4. Incident Monitoring

The City of Mission shall:

a. Employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

4.5. Incident Reporting

The City of Mission shall:

a. Require personnel to report suspected security incidents to the incident response capability immediately but not to exceed one (1) hour after discovery.

b. Report security incident information to IT Department.

4.6. Incident Response Assistance

The City of Mission shall:

a. Provide an incident response support resource, integral to the incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents

4.7. Incident Response Plan

The City of Mission shall:

a. Develop an incident response plan that:

   i. Provides the City of Mission with a roadmap for implementing its incident response capability.

   ii. Describes the structure of the incident response capability.

   iii. Provides a high-level approach for how the incident response capability fits into the overall City of Mission.

   iv. Meets the unique requirements of the City of Mission, which relate to mission, size, structure, and functions.

   v. Defines reportable incidents.

   vi. Provides metrics for measuring the incident response capability within the City of Mission.

   vii. Defines the resources and management support needed to effectively maintain and mature an incident response capability.

   viii. Is reviewed and approved by executive leadership annually.

b. Distribute copies of the incident response plan to personnel with incident handling responsibilities.

c. Update the incident response plan to address system changes or problems encountered during plan implementation, execution, or testing.

d. Communicate incident response plan changes to personnel with incident handling responsibilities.

e. Protect the incident response plan from unauthorized disclosure and modification.

IV. Exceptions

Any exception to the policy must be submitted through a “Policy Exception form” for review and approval by the Information Security Office in advance.

V. Revision History

Date	Version	Description	Author

Policy 5		Policy Owner
Personnel Security Policy		Department of Information Technology
Effective	**08-12-2025**	
Last Revision		

5. Personnel Security Policy

I. Purpose

To ensure that personnel security safeguards are applied to the access and use of information technology resources and data.

II. Reference and Standards

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Personnel Security (PS), NIST SP 800-12, NIST SP 800-60, NIST SP 800-73, NIST SP 800-78, NIST SP 800 -100; Electronic Code of Federal Regulations (CFR): 5 CFR 731.106; Federal Information Processing Standards (FIPS) 199 and 201;Intelligence Community Directive (ICD) 704 Personnel Security Standards

III. Policy Statements

5.1. Position Risk Designation

IT Department shall:

a. Assign a risk designation to all positions.

b. Establish screening criteria for individuals filling those positions.

c. Review and update position risk designations annually.

5.2. Personnel Screening

IT, HR and department system and application owners shall:

a. Screen individuals prior to authorizing access to the information systems.

b. Rescreen individuals according to as needed.

c. Ensure personnel screening and rescreening activities reflect applicable state and federal laws, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions.

5.3. Personnel Terminations

Departments shall, upon termination of individual employment:

a. Disable information system access within (24 hours).

b. Terminate/revoke any authenticators/credentials associated with the individual.

c. Retrieve all security-related information system-related property.

d. Retain access to information and information systems formerly controlled by terminated individual.

e. Notify HR immediately.

Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes.

The City of Mission shall:

f. Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of information.

g. Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the termination process as directed by Counsel and Human Resources (HR).

h. Employ automated mechanisms to notify IT Department upon termination of an individual.

The HR Department shall:

i. Notify IT Department immediately upon learning of employee separation from City of Misson.

5.4. Personnel Transfer

Departments shall:

a. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions.

b. Initiate appropriate actions such as closing and establishing accounts and changing system access authorizations within twenty-four (24) hours.

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.

HR Department shall:

d. Notify IT Department prior to personnel transfer.

This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted.

5.5. Access Agreements

Departments shall:

a. Develop and document access agreements for information systems.

b. Review and update the access agreements at least annually.

c. Ensure that individuals requiring access to information and information systems:

i. Sign appropriate access agreements prior to being granted access.

ii. Re-sign access agreements to maintain access to information systems when access agreements have been updated or when signatories change.

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.

5.6. Third-Party Personnel Security

IT Department shall:

a. Establish and document personnel security requirements including security roles and responsibilities for third-party providers.

b. Require third-party providers to comply with personnel security policies and procedures established by the entity.

c. Require third-party providers to notify IT Department of any personnel transfers or terminations of third-party personnel who possess credentials and/or badges, or who have information system privileges within within twenty-four (24) hours.

d. Monitor provider compliance.

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management.

5.7. Personnel Sanctions

IT and HR shall:

a. Employ a formal sanction process for individuals failing to comply with established information security policies and procedures

b. Notify IT Department within twenty-four (24) hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Sanction processes reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for those organizations.

IV. Exceptions

Any exception to the policy must be submitted through a “Policy Exception form” for review and approval by the Information Security Office in advance.

V. Revision History

Date	Version	Description	Author