Information Security Policy

1.0 Common Policy Elements

1.1 Purpose and Scope

Information is a valuable asset that must be protected from unauthorized disclosure, modification, use or destruction. Prudent steps must be taken to ensure that its confidentiality, integrity and availability are not compromised.

This document provides a uniform set of information security policies for using the City of Pensacola's (hereafter referred to as "the City" or "City") technology resources.

In addition to defining roles and responsibilities, information security policies increase users' awareness of the potential risks associated with access to and use of technology resources. Employee awareness through dissemination of these polices helps accelerate the development of new application systems and ensure the consistent implementation of controls for information systems.

City information security policies are based upon the internationally accepted ISO 27002.2005 information security standard framework. The standards are designed to comply with applicable laws and regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The standards will be considered minimum requirements for providing a secure environment for developing, implementing and supporting information technology and systems.

1.2 Enforcement

These policies must be adhered to by all City departments, divisions and enterprises (hereafter referred to as "departments") unless specifically granted an exception. Individual departments may develop more detailed procedures to handle department-specific cases, provided they adhere to the policies that they support.

This policy will guide annual security reviews by Technology Resources, as well as audits by a designated third party as requested by City Administration. Violators of these policies may be subject to employee disciplinary procedures as described in the City's Human Resources Policies. Departments and divisions may impose sanctions upon their employees, within accepted City guidelines, for violations of these standards.

1.3 Exceptions

Exceptions to this policy must be approved by the Technology Resource Administrator with a review by the City Administrator. In each case, the department or vendor must include such items as the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organization requesting the exception, and the management approval. If approved, exceptions will be documented and added to this Security Policy as an addendum.

2.0 Information Security

2.1 Policy

2.1.1 Information Security Commitment Statement

2.1.1.1 Information is a valuable City asset and must be protected from unauthorized disclosure, modification, or destruction. Prudent information security policies and procedures must be implemented to ensure that the integrity, confidentiality and availability of City information are not compromised.

2.1.2 Security Responsibility, Review and Evaluation

2.1.2.1 Technology Resources is responsible for establishing and managing the security of all systems. Technology Resources will as needed but at a minimum on an annual basis review the most current best practices regarding the use of technology and will amend and/or issue new policies, procedures, and/or controls to reflect the most appropriate solution for security of City information.

2.1.3 User Responsibility

2.1.3.1 City technology resources are provided to authorized users to facilitate the efficient and effective performance of their duties in a secure electronic environment. The use of such resources imposes certain responsibilities and obligations on users and is subject to all applicable City policies. It is the responsibility of every user to ensure that such resources are not misused and to adhere to all City security policies and procedures, which are located in the Technology Resources section of the City's Intranet website.

3.0 Risk Assessment and Treatment

3.1 Assessing Security Risks

3.1.1 Risk Assessments

3.1.1.1 Risk assessments will be performed annually to address changes in the security requirements and in the risk situation, e.g. in the assets, threats, vulnerabilities, impacts, the risk evaluation, and when significant changes occur.

3.1.1.2 Risk assessments will be undertaken in a methodical manner capable of producing comparable and reproducible results.

3.1.1.3 Risk assessments will have a clearly defined scope in order to be effective.

3.1.1.4 The outcome of a risk assessment will be a report defining and prioritizing risks, based on vulnerabilities and impact to City information.

4.0 Organizational Security

4.1 Information Security Infrastructure

4.1.1 Management Commitment to Information Security

4.1.1.1 City management is fully committed to actively supporting security within the organization through clear direction, demonstrated commitment, explicit assignment, acknowledgment of information security responsibilities, and the support of a Technology Governance Committee developed to provide Governance for all Information Technology policies and procedures.

4.1.1.2 The Technology Governance Committee will be comprised of appointed City leaders and will meet, at a minimum, on a quarterly basis. The committee will:

- review and approve information security policy;
- provide clear direction and visible management support for security initiatives;
- approve the resources needed for information security;
- approve assignment of specific roles and responsibilities for information security across the City;
- approve plans and programs to maintain information security awareness; and
- ensure that the implementation of information security controls is co-coordinated across the City.

4.1.2 Information Security Co-ordination / Allocation of Information Security Responsibilities

4.1.2.1 The Technology Resources Administrator will be the focal point for all technology security related matters.

4.1.2.2 When required, departments will designate a security liaison to serve as the primary point of contact to the Technology Resources Administrator.

4.1.2.3 Departments will implement additional procedures as necessary to meet City security requirements.

4.1.3 Independent Review of Information Security

4.1.3.1 The City's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) will be reviewed on an annual basis.

4.1.3.2 Such a review will be carried out both internally and by individuals independent of the area under review such as a third party organization specializing in such reviews. Individuals carrying out these reviews must have the appropriate skills and experience and be approved by the Technology Governance Committee.

4.1.3.3 The results of the independent review will be recorded and reported to the Technology Governance Committee. If the independent review identifies that the organization's approach and implementation to managing information security is inadequate or not compliant with the direction for information security stated in this document, corrective actions will be defined and implemented.

4.2 Security of Third Party Access

4.2.1 Identification of Risks from Third-Party Access

4.2.1.1 All prospective third-party agents will be provided with a copy of the City's Information Security Policies, must verify in writing acceptance of said polices, and will be required at all times to comply with said policies.

4.2.1.2 When third-party agents have access to City-owned technology resources, they must observe the same standards as City employees and agree to abide by and sign both the Vendor Security Management Policy and the City's Acceptable Use Policy.

4.2.1.3 When third-party agents are working in a City environment without being directly supervised, City employees must be vigilant about logging off sessions, logging out or securing PC access, and keeping paper information properly discreet.

4.2.1.4 Stringent controls must be applied to user accounts using remote login access. Where the third-party access will involve a network-to-network connection, the use of a firewall, access logging and systems monitoring is mandated.

4.2.1.5 Network connection ports will be constantly monitored for unknown devices and unauthorized connections.

4.2.1.6 Technology Resources will, on an annual basis, review all required third-party agreements and audit external systems.

5.0 Asset Classification and Control

5.1 Accountability for Assets

5.1.1 Ownership of Assets

5.1.1.1 All information and assets associated with information processing will be owned by a designated City staff member. The asset owner will be responsible for:

- ensuring that information and assets associated with information processing facilities are appropriately classified; and
- defining, providing, and annually reviewing access restrictions and classifications, taking into account applicable access control policies.

5.1.1.2 Routine tasks may be delegated, e.g., to a custodian looking after the asset on a daily basis, but the ultimate responsibility remains with the owner.

5.1.1.3 Technology Resources will maintain a knowledge base of information assets information and perform annual reviews of all access privileges.

5.1.2 Acceptable Use of Assets

5.1.2.1 City information technology resources are provided to authorized users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations on users and is subject to City policies. It is the responsibility of each user to understand and abide by the City's Technology Acceptable Use Policy and to ensure that such resources are not misused.

5.1.2.2 Departments may establish more stringent procedures consistent with this document. However, all additional policies or procedures must be approved by the Technology Resource Administrator and the Technology Governance Committee.

5.1.2.3 The City reserves the right to retrieve and read any data composed, transmitted or received through online connections and/or stored on City equipment.

5.2 Data Classification

5.2.1 Data Classification Guidelines

5.2.1.1 All City information and information entrusted to the City from outside agencies falls into one of three sensitivity classifications:

- **CONFIDENTIAL** – This category includes protected health information (PHI) as defined by HIPAA, and similar information. Access to confidential information must be tightly controlled based on need to know. Except as specifically allowed by HIPAA and other federal and state laws, disclosure to other parties is not allowed, and may result in significant civil and criminal penalties.
- **RESTRICTED** – This is the default classification for any information not specifically designated. Disclosure of restricted information could cause harm to the general health, safety and welfare of affected parties. This information will be disclosed to third parties only if reviewed by the appropriate body and, if approved for disclosure, a confidentiality or non-disclosure agreement has been signed.
- **PUBLIC** – Examples include any data deemed applicable under the Florida Sunshine Laws. This information has been explicitly approved by the City as suitable for public dissemination.

5.2.1.2 The ownership and classification of data will be determined by the applicable department director or administrator in conjunction with the Technology Resources Administrator.

6.0 Human Resources Security

6.1 Prior to Employment

6.1.1 Screening / Terms of Employment

6.1.1.1 Background checks will be conducted on all City employees, contractors, and vendors when access to sensitive information dictates.

6.2 During Employment

6.2.1 Management Responsibilities

6.2.1.1 All managers must attend annual security policy and review training.

6.2.1.2 Management will require employees and third party users to apply security in accordance with the City's Information Security Policies and Procedures.

6.2.1.3 Management responsibilities will include ensuring that employees and third party users:

- Are properly briefed on their information security responsibilities prior to being granted access to sensitive information or systems;
- Are required to fulfill the security policies of the City;
- Achieve a level of awareness on security relevant to their roles and responsibilities within the City;
- Provide necessary proof of security compliance and sign appropriate verifications;
- Comply with the terms and conditions of employment, which includes the City's information security policy and acceptable use policy

6.2.2 Information Security Education and Training

6.2.2.1 All employees will be required to complete annual training on information security awareness and concepts.

6.2.2.2 All employees will practice security awareness and remain vigilant against fraudulent activities.

6.2.2.3 All employees will immediately report incidents involving any City accounts to their direct supervisor or the Technology Resource Administrator.

6.2.2.4 All employees are required to report any incidents, concerns, or suspicious activities to their direct supervisor, Human Resources, or the Technology Resource Administrator.

6.2.2.5 Users will note and report observed or suspected security weaknesses to systems and services directly to the Technology Resource Administrator. Users will not try to emulate the security breach or attempt to prove the threat as a test. Vendors and contractors who provide services to the City must agree to follow the applicable information security procedures of the department for which they work.

6.2.3 Disciplinary Process

6.2.3.1 A formal disciplinary process, as defined in the City's HR Manual, will be followed to deter and discipline employees or third party agents who violate the City Information Security Policies and Standards.

6.3 Termination or Change of Employment

6.3.1 Termination Responsibilities

6.3.1.1 Responsibilities for performing employment termination or change of employment are defined in the City's HR Manual.

6.3.1.2 Human Resources is responsible for the overall termination process and will coordinate with the manager of the person terminating and Technology Resources to manage the security aspects of the relevant procedures.

6.3.2 Return of Assets

6.3.2.1 All employees, contractors, and third party users must return all of the City's assets in their possession upon termination of their employment, contract, or agreement.

6.3.2.2 In cases where an employee or third party user has knowledge that is important to ongoing operations, that information will be documented and transferred to the City.

6.3.3 Removal of Access Rights

6.3.3.1 The access rights of all employees and third party users to information and information processing facilities must be removed upon termination of their employment, contract, or agreement, or adjusted as necessary upon any change in employment.

7.0 Physical and Environmental Security

7.1 Secure Areas

7.1.1 Physical Security Perimeter

7.1.1.1 A security assessment of all key information processing facilities will be performed annually to assess their physical security and a report submitted to the Technology Governance Committee.

7.1.2 Physical Entry Controls

7.1.2.1 Access to any City data center, network operations center, or telecommunications or other similar information processing facility will be restricted and physically controlled.

7.1.2.2 Access to any office, computer room, or work area that contains confidential information will be physically restricted.

7.2 Equipment Security

7.2.1 Equipment Location and Protection

7.2.1.1 Production systems, including, but not limited to servers, network equipment, and telephony systems will be located within a physically-secured area.

7.2.1.2 Appropriate precautions including removing or encrypting sensitive or confidential data will be taken when sending equipment offsite for maintenance.

7.2.2 Secure Disposal or Re-use of Equipment

7.2.2.1 Prior to approved disposal, media (floppy disks, CD's, DVD's, tapes, etc.) containing confidential information must be destroyed to render the information unrecoverable.

7.2.2.2 All hardcopy materials that contain confidential information must be shredded.

7.2.3 Removal of Property

7.2.3.1 The use of any City-owned equipment outside of the City premises must be authorized by department management.

8.0 Communications and Operations Management

8.1 Media Handling

8.1.1 Management of Removable Media

8.1.1.1 If no longer required and not under public records requirements, the contents of any re-usable media that are to be removed from the organization will be made unrecoverable.

8.1.1.2 Where necessary authorization will be required for media removed from the City and a record of such removals will be kept in order to maintain an audit trail.

8.1.1.3 All media will be stored in a safe, secure environment, in accordance with manufacturers' specifications.

8.1.2 Disposal of Media

8.1.2.1 When media is worn, damaged or otherwise no longer required, it will be disposed of in a secure manner. To prevent the compromise of confidential information through careless or inadequate disposal of computer media, formal procedures will be established for secure media disposal.

8.2 Access to Systems

8.2.1 Publicly-Accessible Systems

8.2.1.1 The dissemination methods for City information classified as public will have, at a minimum, protection from unauthorized modification and denial of service attacks.

8.2.1.2 Consideration of security controls that will be applied to publicly-available systems will include the following:

- Information to be disseminated is classified in compliance with data protection legislation
- Confidential information must be protected during the collection process and when stored
- Access to the public system does not allow unauthorized access to networks to which it is connected.
- City information classified as other than public will not reside on systems where public information is being served.
- Information to be made available to restricted groups, such as employees, will be protected by appropriate security mechanisms.

9.0 Access Control

9.1 Business Requirement for Access Control

9.1.1 Access Control Policy

9.1.1.1 All confidential information will be protected via access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

9.1.1.2 Access control procedures will control access based on the need to know.

9.1.1.3 A supervisor and/or manager will initiate the access approval process, and the privileges granted will remain in effect only until the employee's job function changes or the employee leaves the employment of the City.

9.1.1.4 All production information possessed by or used by a particular City unit will have a designated owner who is responsible for determining appropriate sensitivity classifications and criticality ratings, making decisions about who can access the information, and ensuring that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.

9.1.1.5 The authority to grant access to City information will be provided in writing, only by the owner of the information or their designate.

9.1.1.6 Default access privileges will be set to "deny-all" prior to any specific permissions being granted.

9.1.1.7 Unless it has specifically been classified as public, all City information will be protected from disclosure. If non-public information is compromised or suspected of being compromised, the information owner and the appropriate security administration will be notified immediately.

9.2 User Access Management

9.2.1 Access Authorization

9.2.1.1 User IDs may be granted to specific users only when approved in advance by the user's management.

9.2.1.2 Prior to being granted to users, application system privileges will be approved by the involved application system owner.

9.2.1.3 Without specific written approval from the user's management, administrators will not grant system privileges to any user.

9.2.2 Clear Desk and Screen Policy

9.2.2.1 Departments that process confidential information will consider adopting a clear desk policy for paper and removal storage media and a clear screen policy, in order to minimize the risks of unauthorized access to and loss of such information, both during and after normal working hours.

9.2.2.2 PCs that access or use confidential data will be protected by password-protected screensavers when unattended.

9.2.2.3 Sensitive or confidential information will be removed from printers and facsimile machines immediately upon printing.

9.2.2.4 The use of power-on passwords will be required where the PC or any device that contains confidential information.

10.0 Information Security Incident Management

10.1 Reporting Information Security Events and Weaknesses

10.1.1 Reporting Security Incidents

10.1.1.1 Any suspected or observed breaches of confidential or restricted information must be reported to the Technology Resource Administrator, appropriate supervisor, or Human Resources immediately.

10.2 Management of Information Security Incidents and Improvements

10.2.1 Responsibilities and Processes

10.2.1.1 It is the responsibility of all management staff to be familiar with the Technology Resource incident management process.

10.2.2 Collection of Evidence / Learning from Incidents

10.2.2.1 All collection and presentation of evidence will be in compliance with the Technology Resource incident management process.

10.2.2.2 The information gained from the evaluation of information security incidents will be used to identify recurring or high impact incidents.

11.0 Compliance

11.1 Compliance with Legal Requirements

11.1.1 Identification of Compliance Areas

11.1.1.1 Technology Resources has been assigned responsibility for the establishment of city-wide information security policies. However, each department is responsible for developing its own specific procedures necessary to ensure operational compliance with City, state and federal requirements, such as HIPAA.

11.1.1.2 The information processing resources of the City are provided for the business purposes of the City.

11.1.1.3 Compliance with data protection legislation (e.g., HIPAA Privacy and Security Rules) requires appropriate management control. The owner of such data is responsible for ensuring awareness of the data protection requirements defined in the relevant legislation.

11.2 Compliance with Security Policies and Standards, and Technical Compliance

11.2.1 Identification of Compliance Areas

11.2.1.1 City information systems will submit to regular reviews of technical security audits. These reviews will be performed annually to measure compliance with existing security implementation standards. Technical compliance evaluations are based on performing various types of tests and examining configurations.

11.2.1.2 Compliance testing will identify weaknesses subject to exploitation, and qualify results as to the nature of criticality. Technical evaluations will be done in cooperation with operations personnel to avoid impact on productions environments.

11.2.1.3 The handling of results and data obtained in such evaluations will be handled as confidential information.

12.0 Revision History

Standard Number	Author	Revision Date	Revision Content