

**CITY OF SANTA FE
ADMINISTRATION MANUAL**

Originating Business Unit: Information Technology and Telecommunications

SUBJECT

Information Security and Privacy Policy	Policy Number	# Pages 08
	Effective Date	Revision Date 00-00-0000

Policy Owner: City Manager, City of Santa Fe

Version .02

1. PURPOSE:

1.1 The City of Santa Fe seeks to identify and manage security, privacy risks and select cost-effective measures to reduce risks to levels that comply with legal requirements or that represent a mitigation risk approach. This policy provides the necessary framework guidance for identifying and managing information security and privacy risks to a reasonable and acceptable level. The security and privacy of the information that the City of Santa Fe creates or that is entrusted to the City by the public or internal personnel resources is the responsibility of every City of Santa Fe employee and contractor. The overall goals for information security at the City of Santa Fe are the following:

- 1.1.1 Compliance with current laws, regulations and guidelines.
- 1.1.2 Comply with methods from international standards for information security, e.g. National Institute of Standards and Technology 800-53, 800-171, 800-37.
- 1.1.3 Achieve an acceptable level for confidentiality, integrity and availability.
- 1.1.4 Establish controls for protecting the City of Santa Fe's information and information systems against theft, abuse and other forms of harm and loss.
- 1.1.5 Maintain the responsibility for, ownership of and knowledge about information security, in order to minimize the risk of security incidents.
- 1.1.6 Continuation of City services even if major security incidents occur.
- 1.1.7 Protection of personal data.
- 1.1.8 Availability and reliability of the network infrastructure and the services supplied and operated.

2 APPLICABLE TO:

2.1 All City of Santa Fe employees and City of Santa Fe contractors who utilize Information Technology and Telecommunication (ITT) resources or otherwise have access to City information in the performance of said responsibilities.

3 DEFINITIONS:

- 3.1 **Authentication.** A process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access.
- 3.2 **Authorization.** The function of specifying access rights to resources related to information security and computer security in general and to access control in particular. More formally, "to authorize" is to define an access policy.
- 3.3 **Availability.** Maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts.
- 3.4 **Compromise.** An incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.
- 3.5 **Confidentiality.** Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it: Access must be restricted to those authorized to view the data in question. It is common, as well, for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories.
- 3.6 **Continuous Monitoring.** A risk management approach to cybersecurity that maintains an accurate picture of an agency's security risk posture, provides visibility into assets, and leverages use of automated data feeds to quantify risk, ensure effectiveness of security controls, and implement prioritized remedies.
- 3.7 **Information Security.** The practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).
- 3.8 **Integrity.** Maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to

ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality).

- 3.9 **Incident.** The act of violating an explicit or implied security policy, attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.
- 3.10 **Risk.** Is any event that could result in the compromise of organizational assets i.e. the unauthorized use, loss, damage, disclosure or modification of organizational assets for the profit, personal interest or political interests of individuals, groups or other entities.
- 3.11 **Risk Management Framework.** Categorized in to 6 steps that address, *Categorizing* the information system, *Selecting* the proper security controls, *Implementing* the security controls, *Assessing* the how the security controls are properly implemented, *Authorizing* the information system for deployment by determining risk to organizational operations and assets and individuals, and *Monitoring* the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.
- 3.12 **Security Control.** Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.
- 3.13 **System Development Life Cycle.** A term used in systems engineering, information systems and software engineering to describe a process for planning, creating, testing, and deploying an information system.
- 3.14 **Vulnerability.** A weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

4 REQUIREMENTS:

4.1 ITT Information Security and Privacy Program. The City of Santa Fe information and information systems security and privacy program is based upon the information security compliance regulations of PCI-DSS and HIPAA.

4.2 Communications and Operations Management. ITT Security is responsible for ensuring the confidentiality, integrity, and availability of information assets. This includes the protection of the information processing networks and communication facilities, while minimizing the risk of systems failures and compromises, in order to sustain effective and efficient communications and operations management.

4.3 Risk Assessment and Standards. ITT Security sets the City's Risk Management Framework for managing operational risk. ITT Security is responsible for assessing, monitoring, and reporting information security risk and for establishing and publishing standards to manage the security of City of Santa Fe information assets and information systems.

Security Assessment and Authorization. ITT Security will develop and implement a security assessment plan that describes industry best practices and the information security control standardization for the City of Santa Fe. This standardization will enhance effective security procedures that will continuously assess environment, information asset, vendor relationships, and enforcement of security policies, plan of action and milestones to remediate weaknesses or deficiencies to reduce or eliminate known vulnerabilities in the system.

4.4 ITT Security Continuous Monitoring. ITT Security will provide continuous monitoring which will be implemented as part of a holistic approach to risk management and (defense-in-depth) information security strategy. Monitoring will be integrated into enterprise ITT architectures and system development life cycles. This approach will enable executive management to take into consideration the necessary risk-based decisions.

4.5 Information Security Education and Training. ITT Security will deliver information security training to all City of Santa Fe employees concerning City policies and procedures, Security Controls and current industry information security trends and challenges.

4.6 Privacy Program Guidelines. The City of Santa Fe will comply with applicable privacy laws as it collects, uses, discloses, stores, and transfers personally identifiable information (PII) on behalf of the City of Santa Fe, its employees or its customers. These include HIPAA, The Privacy Act of 1974 and other applicable state, e.g. IPRA, and Federal laws.

4.7 Acceptable Use Agreement. Employees and contractors who have a need to access to the City of Santa Fe Information Technology resources must sign and comply with

the City of Santa Fe Acceptable Use and User Access Agreement Guidelines for the ITT managed computing equipment. Failure to comply with such guidelines will result in revocation and/or disciplinary action up to and including termination.

- 4.8 **Access Control.** ITT Security will implement appropriate access controls that address the purpose, scope, roles, responsibilities, management commitment and coordination among department entities to ensure that proper controls have been established for all City employees to accomplish their respective duties safe and securely by only accessing information that is based on job duties and functions.

- 4.9 **Asset Management.** ITT Security will maintain the appropriate inventory of Information Technology (IT) assets which consist of but not limited to, physical and logical IT assets: hardware, software, network devices, applications, licensing. Inventories of assets will assist in ensuring that effective asset protection takes place and are key to the Risk Assessment process.

- 4.10 **Physical Security.** Departments will enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information asset resides (excluding those areas within the facility officially designated as publicly accessible). This includes:
 - 4.10.1 Validate individual access authorizations before granting access to the facility. Control entry to the facility containing the information asset using physical access devices and/or guards.
 - 4.10.2 Control access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk.
 - 4.10.3 Secure keys, combinations, and other physical access devices.
 - 4.10.4 Change combinations and keys at least annually, when keys are lost, combinations are compromised, or individuals are transferred or terminated.

- 4.11 **Security in Supplier Relationship.** All suppliers that access, process, store, or provide various IT components must be in agreement with the City of Santa Fe's security requirements around suppliers' relationships with the assets. Types of information access should be defined that different types of suppliers will be allowed, as well as monitoring and controlling the access. This includes details on addressing risks surrounding the
 - 4.11.1 Handling, processing, and communicating of assets or services.
 - 4.11.2 Business processes involving external parties shall be identified and appropriate controls implemented before granting access.
 - 4.11.3 Legal and regulatory requirements, including data protection, intellectual property rights, and copyright, etc. should be clearly identified and addressed.

- 4.12 **Configuration Management.** ITT Security will maintain a baseline capable of ensuring standardization, integrity interoperability to all system(s) hardware and software configurations, baselines, application software, systems architecture and

infrastructure throughout the Systems Development Life Cycle. This will include maintaining a high standard to address ongoing security assessments and authorization of systems to deploy within the City of Santa Fe ITT architecture.

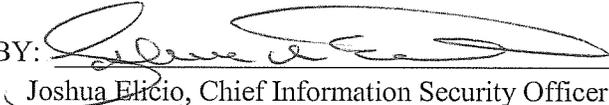
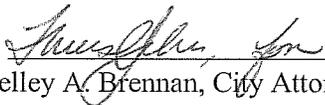
- 4.13 **Contingency Planning.** ITT Security will institute contingency plans designed to mitigate risks of system and service unavailability by focusing on effective and efficient recovery solutions. These risks to the availability of the ITT infrastructure will be mitigated through technical, administrative, and operational solutions. These plans will focus on recovery objectives, restoration priorities, and metrics; the contingency plans will also address contingency roles and responsibilities that are assigned individuals with contact information all while maintaining essential missions and business functions despite an information system disruption, compromise, or failure.
- 4.14 **Identification and Authorization.** ITT Business Applications will document and implement business system requirements that address authentication measures uniquely identifying employees through the use of passwords, tokens, biometrics, multi-factor authentication or some combination thereof prior to the establishment of a connection to the ITT system. This will include, specific measures to safeguard authenticators, verification of initial authenticator distribution, the identity of the individual and/or device receiving the authenticator defined by the role of the individual, managing lost/compromised or damaged authenticators, and for revoking authenticators as appropriate.
- 4.15 **Data Classification and Protection.** City Departments and ITT Security will develop, adapt and adhere to a formal, documented data protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among departmental entities, and compliance. This will include media protection procedures, accesses, marking, storage, transportation, and sanitization.
- 4.16 **Incident Reporting and Response.** Employees and contractors must comply with City of Santa Fe incident reporting requirements and procedures for security, privacy and other incidents related to City of Santa Fe-owned computing equipment, ITT systems and information. The ITT Help Desk (#4357) is chartered with providing computer network defense Tier I support and incident response for the City of Santa Fe.
- 4.17 **Coordinated Approach.** The Chief Information Security Officer (CISO), under the direction of the ITT Director is primarily responsible for creating and maintaining the Information Security Program. CISO is responsible for assessing the security and privacy controls applied to the City of Santa Fe's information systems where data is received, used, disclosed, stored, developed and implemented. The CISO will coordinate, as appropriate, the implementation and maintenance of this policy via the City of Santa Fe ITT Security Governance Sub-Committee.

5 ENFORCEMENT:

5.1 This policy must be adhered to by all City of Santa Fe employees and contractors. Individual departments may develop more detailed policy and procedures to handle department-specific cases, provided they adhere to and support this policy.

5.2 Violators of these policies may be subject to employee disciplinary actions up to and including termination.

6 REVIEW AND APPROVALS:

- 6.1 PREPARED BY:  9-7-16
Joshua Elcío, Chief Information Security Officer DATE
- 6.2 REVIEWED BY:  9-21-16
Lynette Trujillo, Human Resources Department Director DATE
- 6.3 REVIEWED BY:  9-8-16
Renee J. Martinez, Department Director ITT DATE
- 6.4 REVIEWED BY:  8-29-16
Kelley A. Brennan, City Attorney DATE
- 6.5 APPROVED BY:  09/23/2016
Brian K. Snyder, City Manager DATE

VERSION CONTROL HISTORY

Version	Date	Comment	Responsible
Final Version 1.0	8-29-2016	CISO review	Director ITT

REFERENCES:

National Institutes of Standards and Technology 800-53 – Revision 4 – Security and Privacy Controls for Federal Information Systems and Organizations. Retrieved from <https://web.nvd.nist.gov/view/800-53/Rev4/home>

National Institute of Standards and Technology 800-37 – Revision 1 – Guide for Applying the Risk Management Framework to Federal Information Systems. Retrieved from <http://web.nvd.nist.gov/view/ncp/repository>

PCI DSS v3-1 Data Security Standards. Framework for a robust payment card data security process. Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework. Retrieved from <http://www.hhs.gov/sites/default/files/NIST%20CSF%20to%20HIPAA%20Security%20Rule%20Crosswalk%2002-22-2016%20Final.pdf>