

# **Policies and Standards**

## **Information Security Policies and Standards**

---

Consistent City Information Security policies and supporting standards provide a common approach to compliance, regulatory and operational requirements and support the City of Belen in its missions.

### **Policies and Standards Contents**

- 1. A common foundation**
- 2. Policies and Standards**
  - A common foundation
  - What is a policy?
  - Overview
- 3. Related Information Security Office Services**
  - Consulting, education, training and awareness programs
- 4. Information Security Glossary**
  - Definitions and glossary of terms used in this policy
- 5. Policy and Standards**
  - ISO PS001 Information Security Responsibility
  - ISO PS002 Business Continuity and Disaster Recovery
  - ISO PS003 Intellectual Property
  - ISO PS004 Policy Exception Management Process
  - ISO PS005 Sanction Policy
  - ISO PS006 Security Incidents
  - ISO PS007 User Accounts and Acceptable Use
  - ISO PS008 Passwords
  - ISO PS009 Data Facility Security
  - ISO PS010 Network Service
  - ISO PS011 Web Page Guidelines Rev
  - ISO PS012 Workstation and Computing Devices
  - ISO PS013 Server Computing Devices
  - ISO PS014 Protection from Malicious Software
  - ISO PS015 Backup of Data
  - ISO PS016 Inventory and Tracking of Computing Devices
  - ISO PS017 Enterprise Firewalls
  - ISO PS018 Cellular/Smart Phone Use
  - ISO PS019 Telephone
  - ISO PS020 New and Remodeled Infrastructure Review
  - ISO PS021 Internet Use
  - ISO PS022 City Email Services
  - ISO PS023 Acquisition of Technology

## Policies and Standards A Common Foundation

---

The City of Belen's Information Security Policies and Standards were developed as a *common foundation* for information security outlook, approach and practice. Primary consideration was given to the following objectives:

1. Help the city to focus on its core missions of serving the citizens of Belen lowering the risk of security incidents which could distract from these missions.
2. Define a compliance posture relative to information security statutes, regulations, contracts and good practice without duplication of effort. (One set of policies and standards designed to address all information security compliance objectives instead of one for HIPAA, one for PERA, etc.)
3. An approach that is, where possible, technology neutral that allows for some variation given legitimate requirements so long as the risk is explicitly defined and accepted by a level of directly responsible management appropriate to the risk being assumed.
4. An approach that accounts for the dynamic environment we are in today, an environment of changing statutory and regulatory expectations and changing technology where awareness is an integral part of everyone's job

### What is a Policy

The definitions of what is a policy, what is a standard and what is a procedure also had to be understood. Without this understanding of related but distinct terms, policies tend to become too detailed and take on the characteristics of standards or procedures.

For the purposes of the City's Information Security Policies and Standards (as well as related procedures), the following definitions are used:

- **Policy** - High level requirement statement or paragraph about a type of technology or behavior in the IT environment.
- **Standard** - A required approach for conducting an activity or using technology and/or descriptive requirements for a behavior based policy.
- **Procedures** - Clear steps to follow to accomplish specific tasks or behave in certain ways. Procedures should support organization, contractual, regulatory and/or statutory obligations and requirements.
- **Policy Review** – The frequency at which a policy is reviewed and determination is made whether to make changes to the policy.
- **Compliance** – Any policy is only as good if it's enforced. There are sanctions listed for each of the policies.
- **Revision History** – Each section of this policy stands on its own. When a particular policy needs revising, only the effected policy needs to be changed and not the entire policy. The revision table indicates the version of the policy and the revision date and type.

## Overview

---

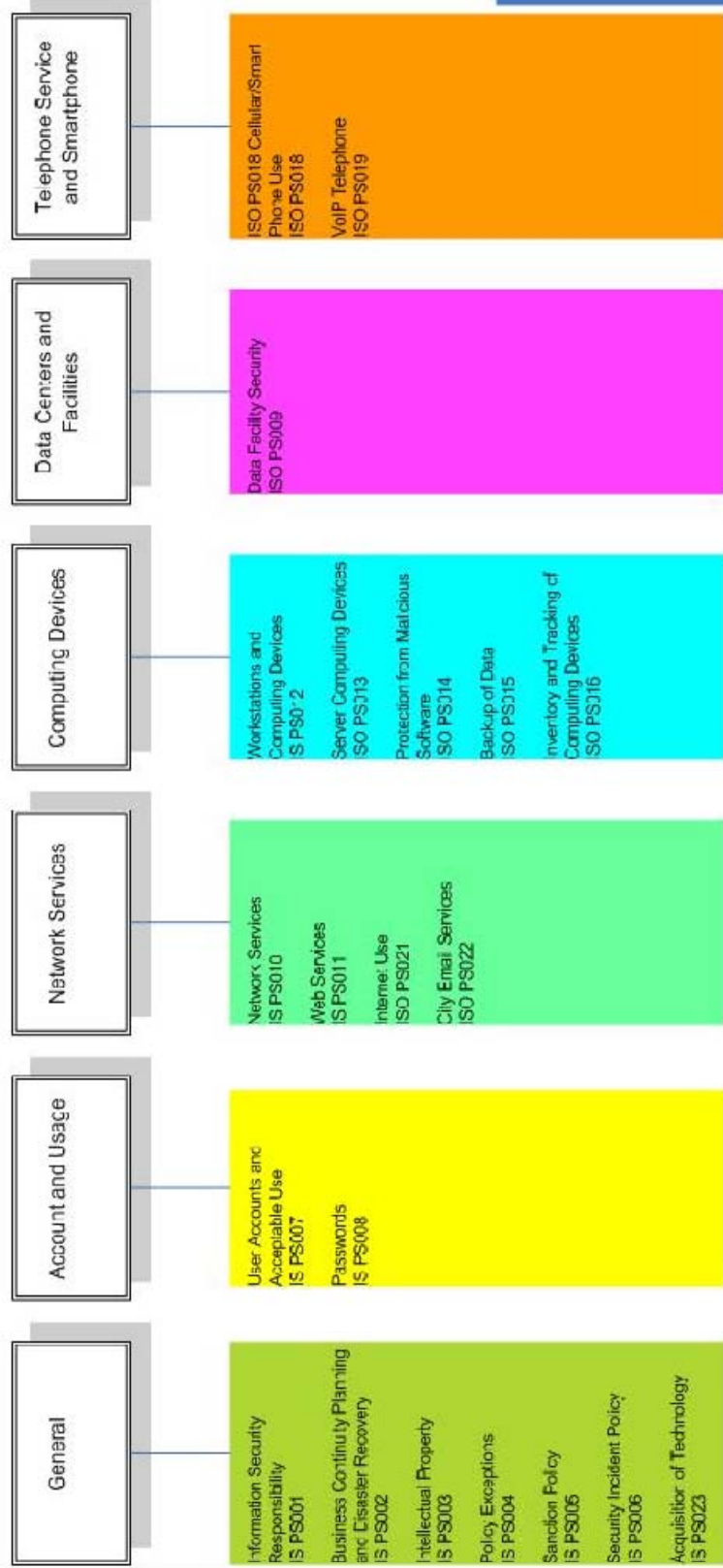
The policies and standards were divided into a framework of six basic areas:

- 1. General**  
Basic responsibilities, business continuity and disaster recovery, intellectual property, exceptions, sanctions and incidents.
- 2. Accounts and Usage**  
User accounts, acceptable use and passwords.
- 3. Network Services**  
Network service and web sites.
- 4. Computing Devices**  
Workstations, servers and other computing devices, protection from malicious software, backup and retention of data as well as inventory, tracking, redeployment and discarding of computing devices or media.
- 5. Data Centers and Facilities**  
Data facility security.
- 6. Telephone Service and Smartphone's**  
Voice or IP network phones and Smartphone integration.

The charts below illustrate the framework at both the policy level and the standards level. Policy Map:

# City of Belen Information Security and Technology Policy

Monday, August 16, 2010



## **Policies and Standards**

### **Consulting, education, training and awareness programs**

---

Consulting, education, training and awareness programs are important and required parts of any compliance program. The ISO will be developing programs in these areas outlined as follows:

#### **Educate and Encourage Use**

- Training
- Awareness
- Consulting

#### **Improve Compliance using**

- Consulting
- Auditing and Monitoring
- Assessment,
- Adjustment
- Enforcement

#### **Maintain Policy Relevance using**

- Self Assessment/audit
- Feedback
- Adjustment

## Information Security Glossary

---

### Administrators

Individuals with administrative responsibility for City Wide Computer and Network Services.

### Assess alternate continuity/recovery strategies. Select continuity/recovery strategy.

1. Develop continuity/recovery strategy plans.
2. Disaster Recovery Plans as part of a broader Business Continuity Plan should include:
  - 2.1. Classification of critical systems and records.
  - 2.2. Mitigation strategies and safeguards to avoid disasters.
  - 2.3. Necessary electronic files back-up and off site storage strategy (see IS PS015 Back-up of Data).
3. Define organizational responsibilities for implementing plans and implement.
4. Off-site storage for the planning documents. Training and testing of plans.
5. Annual review and revision of the plans.
6. Coordination with central IT disaster recovery strategy, if applicable.

### Business Continuity Plan (BCP) Typically includes:

1. Perform Gap Analysis
2. Conduct Risk Assessment
3. Perform Business Impact Analysis
4. Determine Continuity/Recovery Strategy
5. Implement Continuity/Recovery Strategy
6. Establish BCP and Disaster Recovery Maintenance and Awareness Program

### BCP and Disaster Recovery Maintenance and Awareness Program Typically includes:

1. Conduct education and awareness training with personnel.
2. Perform periodic BCP plan walkthrough and testing.

### Business Impact Analysis

In business continuity planning, a risk assessment will typically include:

1. Identification of critical business processes at departmental/unit level.
2. Quantification of impact of an event.
3. Identification of points of failure and process interdependencies.
4. Development of recovery time objective (RTO) and recovery point objective (RPO). See definitions of these terms in this document.
5. Prioritization of processes for recovery.

### Computing Devices

Includes but is not limited to workstations, desktop computers, notebook computers, tablet computers, network enabled printers, scanners and multi-function devices, PDAs, email/messaging devices and cell phones, all hereafter referred to as "computing devices".

### Computing Operation Centers

Specially designated areas or secured rooms that house Server Computing Devices or network infrastructure.

### Continuity/Recovery Strategy

In disaster recovery or business continuity planning, a continuity and recovery strategy will typically include these steps:

## Electronic Media

Includes all electronic data storage devices funded as under Computing Devices above or other electronic data storage devices used to store City of Belen related data. Media includes but is not limited to removable and non-removable storage such as hard drives, CDs, DVDs, magnetic tape, removable disks (floppy, zip, cartridge systems, etc.) and flash memory devices.

## Gap Analysis

A process where the current state vs. the desired state for a process, system or organization is prepared. The differences between the current state and the desired state are called gaps. These gaps then become the basis for prioritization, planning and basis for action to move to the desired state.

## ISO Information Security Officer

In regard to the City of Belen the ISO is the Information Technology Specialist or department comprised of IT professionals. It is the responsibility of the IT department to maintain and enforce the ISP.

## Least Required Access

Only the access needed to perform required functions is assigned to an account. For example, an Oracle database administrator's (DBA) operating system account on the Oracle host system would not allow the DBA to configure or affect underlying operating system functions except as required within the DBA role.

## Providers

Individuals who design, manage, and operate campus electronic information resources, e.g. project programmers, or system administrators.

## Recovery Point Objective (RPO)

Describes the point in time to which data must be restored in order to successfully resume processing. This is often thought of as time between last backup and when outage occurred and indicates the amount of data lost.

**Note:** The Recovery Point Objective definition is copied from the definition on "The Free Dictionary by Farlex" (<http://encyclopedia.thefreedictionary.com/>). This definition is distributed under the terms of "GNU Free Documentation License" (<http://www.gnu.org/copyleft/fdl.html>).

## Recovery Time Objective (RTO)

Determined based on the acceptable down time in case of a disruption of operations. It indicates the latest point in time at which the business operations must resume after disaster.

- RTO must be considered in conjunction with Recovery Point Objective (RPO) to get a total picture of the total time that a business may lose due to a disaster. The two of them together are very important requirements when designing a disaster recovery solution.
- $RTO = \text{Time of Crash to Time the system is operational} (T_{up} - T_{crash})$
- $RPO = \text{Time since the last backup of complete transactions representing data that must be re-acquired / (entered). } (T_{crash} - T_{backup})$
- $\text{Lost business Time} = (T_{up} - T_{crash} - T_{backup})$

**Note:** The Recovery Time Objective definition is copied from the definition on "The Free Dictionary by Farlex" (<http://encyclopedia.thefreedictionary.com/>). This definition is distributed under the terms of "GNU Free Documentation License" (<http://www.gnu.org/copyleft/fdl.html>).

## Risk Assessment

In disaster recovery or business continuity planning, a risk assessment will typically include:

1. Identification and classification of primary risks and exposures including external and environmental risks as well as inherent business risks;
2. Probability of occurrence;
3. Cost of occurrence;
4. Senior management risk tolerance and level of acceptance of identified risks vs. cost of various mitigation plans.

**SCADA (Supervisory Control and Data Acquisition System)**

SCADA refers to an industrial control system: a computer system monitoring and controlling a process. The process can be industrial, infrastructure or facility-based.

**Sensitive Information**

Sensitive information is information of a confidential or proprietary nature as well as other information that would not be routinely published for unrestricted public access or where disclosure is prohibited by laws, regulations, contractual agreements or city policy. Sensitive information includes but is not limited to information such as medical and health records, and other employee information, credit card, bank account and other financial information, social security numbers, personal addresses, phone numbers, etc.

**Note:** Sensitive information does not include personal information of a particular individual which that individual elects to reveal (such as via opt-in or opt-out mechanisms).

**Server Computing Devices**

For the purposes of this policy, server computing devices are those whose primary purpose is to store, contain or transmit information from within the City network (or hosted outside the City network if used to host utility or citation related information and funded by the City of Belen) to users within or outside of the city network. Computing devices that are not servers, for the purposes of this policy, are covered under the IS PS011 Workstation and Computing Devices policy.

**Spoofing**

The use of software or other techniques to appear on the network as something other than reality (masquerading as something you are not). **Example:** The hacker tricked the system into allowing him onto the trusted network by spoofing the identity of a trusted server

**Staff**

The staff shall consist of all employees of the City of Belen

**User**

Includes public computer users, staff, administrators, and other employees of the City of Belen and its affiliated entities and any other individual having a computer account, email address or utilizing the computer, network or other information technology services of the City of Belen.

**Valuable Information**

Information that that has significant value to the City's mission and/or result in possible harm to the City, its staff, and clients if lost. This information may or may not be sensitive information (see definition above).

## Information Security Standards and Equipment Policy Acknowledgment

My signature on this form indicates that I have read the City's Information Security Standards Policy, and I agree to abide by their terms. I understand that any communications I send or receive using City equipment, including but not limited to email, instant messages, and text messages, are not private, and that the City may access, monitor, read, and/or copy those messages at any time, for any reason. I also understand that the City of Belen reserves the right to monitor my use of the Internet, and that such monitoring may occur at any time, for any reason.

I understand that all electronic equipment issued to me by the City of Belen, including but not limited to *Computers, Cell phones, Laptops and Smartphone*, belonging to the City of Belen, and that I must return such equipment upon the City's request. I also understand that the City reserves the right to monitor my use of this equipment, and that such monitoring may occur at any time, for any reason.

---

Employee Signature

---

Date

---

Employee Name (Print)

[Intentionally left blank]

**POLICY:**

All employees of the City of Belen are responsible for the security and protection of electronic information resources over which he or she has control. Resources to be protected include networks, computers, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Activities outsourced to off-city entities must comply with the same security requirements as in-house activities

**STANDARDS:**

**General roles and responsibilities:**

Responsibilities range in scope from administration of security controls for a large system such as Caselle, TLC, Justice Systems and Sleuth to the protection of one's own access password. A particular individual often has more than one role.

*Administrators*, their designees or individuals with functional ownership of data must:

- identify the electronic information resources within areas under their control;
- define the purpose and function of the resources and ensure that requisite education and documentation are provided as needed;
- establish acceptable levels of security risk for resources by assessing factors such as:
  - if the data is sensitive information,
  - the level of criticality or overall importance to the continuing operation of the city as a whole, individual departments, research projects, or other essential activities;
  - how negatively the operations of one or more units would be affected by unavailability or reduced availability of the resources,
  - how likely it is that a resource could be used as a platform for inappropriate acts towards other entities,
  - limits of available technology, programmatic needs, cost, and staff support;
- ensure compliance with the city's general Information Security policies and standards;
- ensure that requisite security measures are implemented for the resources;

*Providers* must:

1. become knowledgeable regarding relevant security requirements and guidelines;
2. analyze potential threats and the feasibility of various security measures in order to provide recommendations to Administrative Officials;
3. implement security measures that mitigate threats, consistent with the level of acceptable risk established by administrative officials;
4. establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements;

5. ensure compliance with the city's general Information Security policies and standards and establish procedures for their resource area in support of these policies and standards;
6. communicate the purpose and appropriate use for resources under their control.

*Users* - Individuals who access and use city electronic information resources must:

1. become knowledgeable about relevant security requirements and guidelines;
2. protect the resources under their control, such as access passwords, computers, and data they download.

#### **Responsibility for Privacy and Confidentiality:**

Applications must be designed and computers must be used to protect the privacy and confidentiality of the various types of electronic data they process, in accordance with applicable laws and policies. Users who are authorized to obtain data must ensure that it is protected to the extent required by law or policy after they obtain it. For example, when sensitive data is transferred from a well-secured system such as *Justice Systems FullCourt* to a User's location, adequate security measures must be in place at the destination computer to protect this data.

#### **Responsibility for Compliance with Law and Policy:**

City departments, units, or groups, for specific systems and activities under their purview, must comply with this and other City Information Security Policies and standards as well as applicable laws and regulations. These groups should, as appropriate and relevant to their area, establish security guidelines, standards, or procedures that support and refine the provisions of the city information security policies and standards for specific activities under their purview.

#### **SCOPE/APPLICABILITY:**

All persons while conducting/performing work, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

#### **POLICY AUTHORITY / ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City's Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**



**POLICY:**

Effective business continuity and disaster recovery plans are required in all areas of the city. Each Department and Administrative Division must develop plans that will allow it to perform its core required operations in an alternative fashion as well as an appropriate disaster recovery policy for their working environment.

**STANDARDS:**

Also see *IS PS015 Backup of Data*.

An effective Business Continuity Plan (BCP) contains the steps outlined below. Each Department, Administrative Division or other city entity's BCP is expected to contain these steps, as appropriate, completed in a proficient and well documented manner.

**Note:** The Information Technology Operations Center is available to consult on the BCP process.

**Administrative Standards:**

- Perform Gap Analysis
- Conduct Risk Assessment
- Perform Business Impact Analysis
- Determine Continuity/Recovery Strategy
- Implement Continuity/Recovery Strategy
- Establish BCP and Disaster Recovery Maintenance and Awareness Program

**SCOPE/APPLICABILITY**

All persons while conducting/performing work, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY / ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City's Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city's direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

<b>Version</b>	<b>Revision Date</b>	<b>Description</b>
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**

---

**POLICY:**

The City of Belen respects the intellectual property rights of others and expects Users to respect the intellectual property rights of others. Users must abide by applicable intellectual property laws and/or regulations, including but not exclusive to those pertaining to text, graphics, art, photographs, music, software, movies and games. Users must refrain from actions or access which would violate the terms of licensing and nondisclosure agreements.

**STANDARDS:**

**Administrative Standards:**

1. Users must understand copyright and intellectual property regulations as they pertain to city resources.
  - As a General Rule; the creator or inventor owns, EXCEPT if an employee working within the scope of employment, then the employer (City of Belen) owns the work; or
  - the work is specially commissioned in one of 9 enumerated categories, and identified as a work for hire in writing (i.e. instructional text); or
  - the work is assigned by the inventor or author.
2. Users must conform to U.S. Intellectual Property laws and regulations including the **Digital Millennium Copyright Act of 1998 (DMCA)**, which strengthened copyright laws pertaining to digital media. Users need to understand how the DMCA applies to the activities they perform while using a city supported network or device and act in a manner that is compliant with the DMCA when engaging in such activities. Relevant aspects of the DMCA include:
  - Criminalizes circumvention of anti-piracy measures in most commercial software.
  - Makes the manufacture, sale, or distribution of code-cracking software or devices illegal when used to illegally copy software.
  - Provides specified exemptions from anti-circumvention provisions for nonprofit
  - Libraries, archives, and educational institutions under certain circumstances.
  - Creates the expectation that service providers remove material from users' web sites if
  - It appears to constitute copyright infringement.
  - Requires that "webcasters" pay licensing fees to record companies.
  - There are numerous other provisions within the act, this link provides relevant information: <http://www.copyright.gov/legislation/dmca.pdf>
3. Downloading or sharing of any electronic information that violates the DMCA or any other copyright or intellectual property law or regulation must not be done.
4. Use of Peer-to-Peer (P2P) software "file sharing" applications to infringe copyright and/or intellectual rights of others is not permissible. Configuration of such programs for legitimate use must be in compliance with the city's information security policies and standards.

**SCOPE / APPLICABILITY:**

All persons while conducting/performing work, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY / ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**

---

**POLICY:**

Information security concerns such as regulatory, compliance, confidentiality, integrity and availability requirements are most easily met when city constituents employ centrally supported or recommended technologies. The City of Belen understands that centrally supported or recommended technologies are not always the preferred choice of a specific departments, division or other city sub-division. Deviation from centrally supported or recommended technologies is discouraged.

However, it may be considered provided that the alternative presents a reasonable, justifiable business and/or research case for an information security policy exception; resources are sufficient to properly implement and maintain the alternative technology; the process outlined in this and other related documents is followed and other City Policies and Standards are upheld.

**Note:** The purpose of this policy is to allow city entities the ability to do what is needed to further their area's mission while, at the same time, have reasonable assurance that solutions adopted are in compliance with applicable laws, regulations and city requirements.

**STANDARDS:**

**Administrative Standards:**

The Department, Division or other entity desiring a policy or standard exception will be, except for minor approved exception request, guided through an assessment methodology that clarifies direct and indirect costs associated with the alternative technology; including technical, physical and administrative requirements consistent with laws, regulations, city policy, risk being assumed and the regulatory climate at large by using the "Policy Exception Management Template" (see below).

1. Preliminary:

- Prior to completion of the Policy Exception Management Template the basic request should be sent via email to [lawrence.kaneshiro@belen-nm.gov](mailto:lawrence.kaneshiro@belen-nm.gov). **Note:** Minor exceptions due to isolated circumstances may be able to be adequately accounted for by this form and the Policy Exception Management Template will not be required.
- After the basic information is received via the form it will be reviewed. The submitter will then be notified of the next step.

2. If instructed to do so, the Policy Exception Management Template must be fully completed, including:

- Approval signature of appropriate level of City Management for the level of potential risk being assumed (this may be a Department Manager, or the City Manager).
- Business and/or research case section which contains:
  - Description of technology and its application.
  - Information on why IT supported or recommended technology does not meet requirements including IT discussion.
  - Suggestions on what a viable central IT supported solution would look like.
  - Implementation and maintenance costs including both initial and on-going costs for required licenses, hardware, software, infrastructure, training and procedural documentation, administrative and support personnel, temporary consultants, disaster recovery, back-up, business continuity, and identified funding to support the technology during the technology's projected life cycle.

- Data Sensitivity Assessment:
    - Data definition.
    - Expected users of the data (staff, research, public, etc.).
    - Data access restriction requirements due to laws/regulations (HIPAA, FERPA, PCI, NIH requirements, other laws or regulations, etc.), general privacy or proprietary/intellectual property concerns, city policy and/or prudent practice (this may be completed in conjunction with the Information Security Office).
    - Security methodology for managing this data and access to include logical security via the operating system, database, application and other means, as applicable, as well as physical security of hardware and other related infrastructure.
  - Implementation Plan
    - Project implementation plan and resources, timeline devoted to implementation.
  - Maintenance Plan
    - Plan and resources devoted to on-going maintenance, administration, user training and contingencies.
  - Risk Acceptance Document
    - The Committee will complete a Risk Acceptance Document for the responsible entity. These documents will overview the risks being assumed by the entity. This form will also document, based on the committee's assessment of the entity's documentation (as described above) if the proposal is approved for implementation.
    - The Risk Acceptance Document must be accepted, approved and signed-off by the appropriate City Manager or Finance Director. This approval documents that the entity management is aware of the risks inherent in the project and system, accepts them and will use entity resources to maintain the system and mitigate any risk events that may arise.
  - Barring exceptional circumstances and given a proposal that is thorough and complete, the review committee will review and assess the proposal within 30 days of receipt.
  - If approved, entity proceeds with implementation. Subject Matter Expert (SME) from IT will monitor implementation for adherence to plan or appropriate changes. If implementation proceeds as planned, technology is allowed to go into production. Note: The SME is not the project manager.
  - If implementation can not proceed according to plan, entity can correct any deficiencies or seek alternative solutions.
3. Future review or audit
- Audit Services, IT Office or City Management may at future date review technology for continued adherence to plan, security, etc.

#### **COPE / APPLICABILITY:**

All persons while conducting/performing work, teaching, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY / ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city's direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**



---

**POLICY:**

The City of Belen requires that users of city computing infrastructure, devices or data comply with all applicable laws, regulations, statutes and city policies relating to information security and information technology.

The city must be prepared to respond fairly and appropriately (1) to violations of law, regulation or City Policy relating to information security, (2) when questionable or unacceptable computing practices occur, or (3) where there is non-compliance with information security policy requirements or with reasonable requests for action or cooperation necessary to implement the city's information security policies. Lack of compliance will result in sanctions or other appropriate action.

**STANDARDS:**

**Background and definition:**

Sanctions are a requirement of many information security laws and regulations. Sanctions also encourage following the policies, standards and procedures promulgated to help the city maintain the confidentiality, integrity and availability of the city's information and computing infrastructure. The *Personnel and Safety Policies and Procedures* of the City of Belen (<http://www.belen-nm.gov>) is the basic governance document of the city and supports staff or administration disciplinary action.

**Organizational Responsibilities:**

- **City of Belen, Staff and other Users**

Knowledge of violations of or non-compliance with information security policies should be immediately reported to the City of Belen IT Office as well as the appropriate administrator for the department or unit in which the violation occurred.

The IT Office will work with the reporter to determine the administrative level at which the initial advisory should occur. IT Office can be reached at [lawrence.kaneshiro@belen-nm.gov](mailto:lawrence.kaneshiro@belen-nm.gov) or, if the violation has potentially serious consequences and requires immediate attention, the violation should be reported to the IT Office at 505-966-2755 with Priority One status requested.

The IT Office will assess the reported violation and/or incident using an established procedural framework. This framework has been established to apply a consistent methodology to all assessments. Goals of the framework include:

- documentation of the reported violation or incident;
- preservation of evidence;
- impartial assessment of the accuracy of the reported violation or incident, including hearing the particulars from the personnel apparently responsible for the violation;
- possible escalation of the violation or incident to Human Resources, City Manager's Office, Department of Public Safety, outside authorities or others;
- containment and mitigation of the violation or incident;
- remediation of the violation or incident; and
- imposition or recommendation of sanctions if and as appropriate.

Corrective actions and sanctions applied pursuant to this policy shall not supersede or impede any regulatory authority conferred upon other compliance oversight offices at the City of Belen to apply sanctions or take other corrective actions appropriate to their authority. Corrective actions and sanctions applied pursuant to this policy do not supersede any sanctions imposed by external regulatory bodies.

**Corrective Actions and Sanctions Available:**

Corrective actions and sanctions available to the city in those circumstances where a violation or non-compliance of information security or technology policy has occurred include, but are not limited to:

- Imposition of a requirement to obtain additional appropriate training;
- Temporary suspension or permanent revocation of computing accounts or computing access rights at the city;
- Requirement to bring self, unit, department or school managed computing resources up to specified and on-going standards or place these resources under the management of the Information Technology Office;
- Imposition of a mandate and timetable for corrective or remediating action;
- Letter of Reprimand placed in personnel file;
- Loss of improperly collected data;
- Requirement to make financial restitution;
- Suspension of some or all activities at the city;
- Any action that may be required by applicable law, regulation or contract;
- Any other disciplinary actions available as corrective action in a case of inappropriate behavior by a student, faculty member, staff, administrator or other employee up to and including termination;
- When appropriate and warranted, a department or unit may be held accountable for fees, charges, fines, or expenses incurred or resulting from or related to any such violation or non-compliance where the unit or department is deemed in whole or part responsible.

**COPE / APPLICABILITY:**

All persons while conducting/performing work, teaching, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY / ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**



---

**POLICY:**

The policy of the City of Belen is to minimize both the frequency and the severity of information security incidents within the city environment. All users are responsible for and must maintain their city computing devices and data in as safe a manner as is reasonably possible. In the event of an incident, the standards outlined in this document as well as the related procedures must be followed.

**STANDARDS:**

**Background and definition:**

Compromises in security can potentially occur at every level of computing from an individual's desktop computer to the largest and best-protected systems in the city. Incidents can be accidental incursions or deliberate attempts to break into systems and can be benign to malicious in purpose or consequence. Regardless, each incident requires careful response at a level commensurate with its potential impact to the security of individuals, sensitive information and the City of Belen as a whole.

The accelerated pace of technological change and concurrent reliance on electronic information systems has greatly increased both the potential exposure of sensitive information to the world at large via electronic means and the motivation of some to exploit computing devices, computing infrastructure and software either for gain or to cause organizational difficulties. Governmental authorities, regulatory bodies and standards organizations have recognized this new reality and responded with laws, regulations and other measures to motivate organizations to take the steps necessary to minimize or prevent security incidents before they occur.

*This environment means that all persons within the City of Belen have an active role in preventing security incidents or in minimizing them when and if they occur.*

For the purposes of this policy a "Security Incident" is any accidental or malicious act with the potential to

- result in misappropriation or disclosure of sensitive information,
- affect the functionality of the information technology infrastructure of the city,
- provide for unauthorized access to city resources or information,
- allow city information technology resources to be used to launch attacks against either other internal resources or the resources and information of other individuals or organizations.

The city has established procedures and identified the IT Office as its authority in developing response plans to serious security incidents. As described below, reports of security incidents will be forwarded to the IT Office. Depending on the nature of the incident, the IT Office will frequently work with department heads or staff and administrators. Incidents may be escalated to City Manger, Human Resources or other city officers as well as to law enforcement or outside authorities.

This document outlines the standards and process individuals should follow to report potentially serious security incidents. City staff members whose duties include managing computing and communications systems have even greater responsibilities. This document outlines their responsibilities in securing systems, monitoring and reporting IT security incidents, and assisting individuals, administrators, and other IT staff to resolve security problems.

### **Administrative standards:**

#### **Dealing with Viruses, Worms and other common “Malicious” Software**

- Individuals and information technology support professionals are not required to report IT security incidents involving viruses, worms, and other common malicious software if self contained and completely removed by anti-virus, anti-spyware or other software. If, in the judgment of the Tier 1 or other authorized technical support personnel, the software could pose a risk to city data and was not successfully removed the incident must be reported. Please follow the standards in the next section, “Reporting and Responding to IT Security Incidents”
- Because malicious software can reduce the functionality or otherwise affect the city computing and communication environment, individuals and information technology support professionals are expected to:
  - prevent computer equipment under their control from being infected with malicious software by the use of preventive software and monitoring (see *ISO PS014 Protection from Malicious Software policy and standards*), and
  - take immediate action to prevent the spread of any acquired infections from any computers under their control.
- Assistance is available from your Tier 1 or other local information technology support and from the Enterprise Network Security Team in IT See next section for contact information.

#### **Reporting and Responding to IT Security Incidents**

- Individuals
  - Should attempt to stop any further damage from an IT security incident by powering-down the computer and disconnecting it from the city network.
  - Report IT security incidents to the IT Office at [lawrence.kaneshiro@belen-nm.gov](mailto:lawrence.kaneshiro@belen-nm.gov). IT staff will help you assess the problem and determine how to proceed.
  - If the incident has potentially serious consequences and requires immediate attention, individuals should report the incident to the IT Office at -505-966-2755 and request Priority One status.
- Following the report, individuals should comply with directions provided by IT support staff to repair the system, restore service, and preserve evidence of the incident.
- No retaliatory action should be taken against a system or person believed to have been involved in the IT security incident. All response actions should be guided by the IT Security policy and all other applicable City Policies.

- **IT Support Professionals**

Information Technology support professionals have additional responsibilities for IT security incident handling and reporting for both the systems they manage personally for their units and the systems of users within their units. In the case of an IT security incident, IT support staff should:

- Respond quickly to reports from individuals.
- Take immediate action to stop the incident from continuing or recurring.
- If the incident has potentially serious consequences and requires immediate attention, individuals should report the incident to the IT Office at 505-966-2755 and request Priority One status.
- Notify the appropriate department that an incident has occurred and that the IT Office has been contacted.
- Refrain from discussing the incident with others until a response plan has been formulated.
- Follow Security Incident Policy guidance to repair the system, restore service, and preserve evidence of the incident.

**SCOPE/APPLICABILITY:**

All persons while conducting/performing work, teaching, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY/ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**

**POLICY:**

City computer user accounts and computing facilities are provided for persons who legitimately need access to city computing resources. Other persons may qualify for a computer user account and access to computing facilities on a case by case basis.

**STANDARD:**

**Acceptable Use**

Persons using city resources (users) are responsible for lawful and appropriate use of computing facilities and devices.

Computing resources are for all users. Users must respect the usage rights of others that use city resources.

Computing accounts and facilities must not be used in any manner which could be disruptive, degrade the performance of or cause damage to city computing infrastructure, resources or data and/or other users. Personal use of computing devices should be kept to a minimum and in no case should a city account be used for non-city business purposes.

**Confidentiality of Data**

- Sensitive Information must not be accessed, copied or disseminated except to the extent necessary to fulfill assigned responsibilities, and then only to the extent that the individual is authorized.
- The confidentiality, security and integrity of the city data and computing infrastructure must be maintained at all times by city personnel. This obligation continues beyond the termination of the individual's relationship with the city.

**Misuse of Computing Accounts or Computing Infrastructure**

- Misuse of city computing accounts or computing infrastructure is not tolerated. Generally, behavior considered unacceptable if done without a computer in is also unacceptable if done using a computer. Examples of misuse include, but should not be construed as being limited to: Harassment, unauthorized hacking of computing systems, denial of service attacks, spoofing of identity, chain letter distribution, solicitation of non-city business and obscene language.

**Expectation of Privacy and Disclosure**

- Privacy of computing activities while using city resources is neither guaranteed nor should it be expected:
  - User access, security, audit and other logs are maintained to facilitate compliance with laws and regulations as well as to facilitate activity reviews when necessary.
  - Access may be given to persons outside of the city on a case-by case basis or under certain conditions when warranted. Disclosure of this information may not be given to the individual(s) involved.
  - The City of Belen does not guarantee the confidentiality or privacy of electronic data or voice mail messages. This should be kept in mind when using these services.
  - Third party vendors are involved with both internet and voice mail data. All users of electronic data and voice mail should familiarize themselves with policies set forth by these vendors.

**Administrative Standards:**

**General**

- Access to additional required resources not provided upon account creation can be requested by completing the appropriate form (see <http://www.belen-nm.gov>).
- Access to a city business application or data may be denied, if the appropriately completed authorization does not accompany the request. Access to information is granted based on position requirements and job duties.
- All account holders must agree to comply with the computer account usage agreement (<http://www.belen-nm.gov>).

**Naming Convention**

- Account names will consist of the user's first name a dot and the last name. The purpose of this is to easily identify all city employees making the User ID unique to city staff. For consistency throughout all applications, the User's ID should be used with all applications, but the password can be different.

**Employee Account Requests**

- Accounts are automatically generated upon notification from the Human Resources Department. HR must notify Information Technology of the new user's *name, title, department, and supervisor*.
- Depending on the job position, Email services are assigned upon request of the department supervisor. The User ID and Password are given to the supervisor and will be the responsibility of the user to change the password.

**Sponsored Account Requests**

- Sponsored accounts may be granted to individuals external to the City of Belen under the following conditions:
- A specific relationship exists with a city unit or individual in support of a city mission, function, project or business.
- A city unit or individual is willing to sponsor the individual's computer account.
- Sponsored accounts will be reviewed annually as a group to determine whether renewal is necessary.
- Sponsored accounts can only be requested by full-time faculty, staff or administrators.

**Service Account Requests**

- Service accounts are granted to city units and departments under the following conditions:
  - The purpose is directly related to a city Mission, function, project or business;
  - A need exists to share access to an account;
  - A need exists to centrally manage and store electronic communications or data;
  - All individuals who will use the service account must have their own individual computer account.
- A service account is the only exception to the computer account naming standard. A service account can have any descriptive name, indicating its purpose, within eight characters. For example, the webmaster has a service account available for the community to send questions, comments and problems called [webmaster@belen-nm.gov](mailto:webmaster@belen-nm.gov).

### **Termination of an Account**

Termination of computer accounts will occur under the following circumstances:

- The account holder does not agree to the Computer Account Usage Agreement.
- The account holder requests the computer account be closed.
- The account holder is no longer affiliated with the City of Belen.
- The account holder misuses computing facilities or resources.
- The department or sponsor requests that the computer account be closed.
- Accounts will be closed upon termination of employment and all contents from the account will be archived or deleted in accordance with the Local Government Records Retention and Disposition Schedule, 1.19.8 NMAC.
- Retired personnel may retain their email accounts, however if at any time no activity has occurred for one month the account will be closed, and its contents deleted one month later.
- The HR department or the department supervisor must notify IT of any pending termination or separation of employment of any user from the City of Belen, whether it is permanent or temporary. Depending on the cause of separation, notification can range from within minutes to 24 hours of the employee leaving the premises

Once a computer account has been closed, access to the account or the data contained within it may be granted to City of Belen individuals to facilitate the transfer of responsibilities or the retrieval of data.

### **SCOPE/APPLICABILITY:**

All persons while conducting/performing work, teaching, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the city or affiliates.

### **POLICY AUTHORITY/ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

### **POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**

---

**Passwords**

---

**POLICY:**

All computer accounts must be password protected to help maintain the confidentiality and integrity of electronic data as well as to help protect the city's computing resources and infrastructure. This policy establishes a minimum standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

**STANDARDS:****Administrative Standards:****General**

- Passwords to city accounts and devices must be kept confidential.

**City of Belen Network and/or Enterprise Software Accounts**

(In addition to the general standard above, these standards apply to city network and Enterprise Software accounts)

- Account holders should set up their challenge questions to facilitate self-service password resets.
- Notification of password expiration will be provided to account holders in advance of the password expiration.

**Technical Standards:****General**

- Passwords will expire every 90 to 180 days.
- Passwords to systems containing sensitive information, including *Caselle*, *TLC*, *Sleuth* and *FullCourt* must expire no less often than every 180 days.
- Domain passwords should be at least 8 positions in length.
- Passwords to systems containing sensitive information, including *Caselle*, *TLC*, *Sleuth* or *FullCourt* must be at least 8 positions in length.
- Strong passwords should be used. A strong password should include a combination of:
  - Alphabetic, including both upper and lower case: "A to Z" and "a to z".
  - Numeric: 0 to 9.
  - Special Characters such as: ~!@#\$%^&\*()+= [ ] { } ? < >, etc.
- Passwords to systems containing sensitive information, including *Caselle*, *TLC*, *Sleuth*, and *FullCourt*, must require at least two of the three criteria specified immediately above.
- Passwords should not consist solely of personal information or words found in a dictionary (any language). Ideally, this information should not be used. If used, the use of at least two of the three types of strong password characters noted above as part of the password is required.

**City of Belen Network and/or Enterprise Software Accounts**

(In addition to the general standards above, these standards apply to city network and Enterprise Software accounts)

- Passwords expire every 180 days and meet the sensitive information complexity requirements.

**SCOPE / APPLICABILITY:**

All persons while conducting/performing work, teaching, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY / ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**

---

**POLICY:**

Data Facilities are controlled facilities devoted to housing servers, networking equipment, Wi-Fi devices, phone equipment and other computing devices. Access to any data facilities must be controlled and restricted to appropriate personnel as required by their position and responsibilities.

**STANDARDS:**

**Administrative Standards**

**General:**

- Access control procedures must be in place to reasonably ensure that only authorized personnel have access to a data facility.
- Visitor, contractor or other appropriate but non-routine access to a data facility must be granted and logged through designated personnel.
- Either a visitor or service badge must be assigned or the person must be escorted while in the data facility.
- Access control devices and their related maintenance records must be well maintained.
- Procedures must be in place for contingency operations. *IS PS002 Business Continuity and Disaster Recovery.*

**Information Technology Division Computing Data Facilities**

- If access to the data facility is required on a regular basis, a key, a card key or Personal Identification Number (PIN) shall be issued.
- All authorized personnel entering the data facility must wear their City of Belen identification or the visitor/service badge assigned.

**Technical standards:**

**General:**

- Adequate conditioned power, uninterruptible power supplies, fire suppression devices, climate control and other environment maintenance equipment must be used if an assessment of the criticality and sensitivity of systems housed within the computing operational center deems it appropriate.
- **Information Technology Data Facilities**
  - Access Control – key card and personal identification number and/or city card with proximity chip must be used for authentication and access control.
  - Data facilities shall only be used to house servers, network, Wi-Fi, phone or video equipment. There shall be no access to the public at such facilities.

**SCOPE/APPLICABILITY:**

All persons while conducting/performing work, teaching, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY/ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**

Note: The need for and depth of these types of services within the data facility is information developed within a Business Continuity and Disaster Recovery Plan (see ISO PS002 Business Continuity and Disaster Recovery).

---

**POLICY:**

The city will provide the required infrastructure for enterprise-wide local area network services, (including wireless) and connections to the internet, public internet and other external networks to further the mission of the city.

The Information Technology office is responsible for the provision and management of enterprise-wide local area network services, including wireless networks. All connections to the network must be via city approved mechanisms. Only authorized Information Technology staff may install, manage or change the network infrastructure including but not limited to enterprise servers, routers, switches, security and telecommunications equipment as well as access to these devices.

**STANDARDS:**

**Administrative Standards:**

**Network Configuration Authority:**

**To help maintain the integrity, security, availability and necessary resources of the city network:**

- Information Technology provides all network address assignments.
- Unauthorized city network installations or modifications will not receive IP addresses for computing devices on the unauthorized network. Such devices will be physically disconnected from the city network and the device's IP and/or MAC addresses will be blocked from city network access. **Note:** This includes wireless networks not connected to the city's enterprise network and/or private network devices operating within city facilities.

**Connecting to city and affiliated computing resources from outside the city network:**

All connections to these resources (servers, personal computing devices, networking equipment, etc.) must, except as noted, follow these standards:

- Be via a secure and/or encrypted connection such as a VPN, secure HTTPS, secure FTP, SSH or other secure and/or encrypted method.
- Be configured so that a user account and password is required and be compliant with the policies and standards described in *IS PS007 User Accounts and Acceptable Use* and *IS PS008 Passwords*.
- Connection interface (a VPN or dial-in vendor service line, for example) used for occasional connections should be disabled except during the periods when the connection capability is expected to be used.

**Exception:** If the connection does not allow access to sensitive information then a properly configured and administered connection method is acceptable and no log-on is required.

**Example:** A web site providing information intended for public availability could use standard http or https access.

### **Network Use**

- Staff with city LAN accounts usually receives secure drive space accessed via the LAN for individual use (commonly called “*Public on wdsharespace*”). This space is commonly used by all departments and staff for the purpose of sharing information.
- The city enterprise network drives also include the “I” drive and the “S” drive. Space on these drives, are used by their respective applications at City Hall and Police Department. Account holders have read/write access to subdirectories as appropriate.

### **Monitoring/Altering Network Traffic**

- Users are expected to use end user applications such as network drive access, email and similar programs, as they are intended to be used on the city network. Scanning of the network, “packet sniffing”, packet interception/copying/decryption and any other means of reading, altering, spoofing or otherwise monitoring and/or changing network communications is forbidden without specific approval in writing from the Information Technology Office.
- The city reserves the right to analyze network traffic at any time deemed necessary by either manual or automated means. For example, the city may specifically monitor network traffic if instructed by legal authorities or for the purpose of assessing system integrity, performance, management or possible policy violations.

### **Guest/Temporary Network Use**

- Guest access to the wired network requires staff or administrator account sponsorship. See *IS PS007 User Accounts and Acceptable Use* for more details.
- Guest access to the wireless network is available to the Public at City Hall, Municipal Court, Recreation Center, Community Center at Eagle Park and Library for Internet use ONLY. The Private wireless network is available at the above locations as well as the Police and Fire Departments. Access to the private network must be requested from the Information Technology Office.

## **Technical Standards:**

### **General**

- All enterprise level authentication requirements external to an application must be configured to use the city’s enterprise Active Directory Services. (**Note:** This also allows easier configuration of single sign-on abilities).

### **Wireless**

- Full authenticated network access requires a secure wireless connection to use the Private side of the wireless network.
- A Wireless adapter card that fully supports 802.1x is required to access the network

### **Voice**

- The city’s Voice Networking (Voice over Internet Protocol – VoIP) provided by Information Technology is based on FCC standards and specifications. This consists of the telecommunications services, dial tones, telecommunications equipment, FAX service and specialized circuitry. All VoIP connections are maintained and provisioned by the IT Office.

**SCOPE / APPLICABILITY:**

All persons while conducting/performing work, teaching, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY / ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with the City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**



---

**POLICY:**

The web presence of the City of Belen is to securely provide information, allow for interactive functions and promote a positive image of the City of Belen to other municipalities, accrediting agencies, funding agencies, the media, constituents, prospective families wanting to relocate to the area, and the public.

**STANDARDS:**

**Administrative Standards:**

**General (all web sites)**

- Intellectual Property must be respected. See *IS PS003 Intellectual Property*.
- The City of Belen owns the belen-nm.gov domain and must renew the domain name yearly. Only official city business can be conducted using this domain.
- Privacy laws, regulations and standards of the city must be followed. All sensitive information must be managed appropriately so that unauthorized access to sensitive information is prevented to the extent possible. If you are unable to assure that sensitive information is adequately controlled via a website or other network accessible method, the information should not be placed on or collected via the website.
- The city reserves the right to disable and/or remove the web page links and publishing capability on city managed servers (or internet accessibility to such by city supplied network components) of anyone who uses these resources to violate city contractual obligations; to perpetrate, aid or abet criminal acts or intellectual property/copyright violations to make accessible materials that are obscene or consume (or result in the consumption of) excessive amounts of computing or network resources.
- Security of these pages on the City of Belen web site are the responsibility of the IT Office who produces and maintains these pages and must comply with security guidelines outlined in this document as well as other applicable city guidelines.
- Secondary web sites should conform to the city's graphic identity standards when directly linked to the belen-nm.gov domain.

**Individual Web Sites**

- To preserve continuity, individual websites with the City of Belen branding is not allowed. Any official information concerning the City of Belen can be disseminated through the belen-nm.gov website. Any information released through individual web sites must reference the official belen-nm.gov website.

## Web Sites

**Technical standards:**

- All enhanced capabilities configured on web pages must be deployed with security in mind. The web site creator must use appropriate settings for any enhanced capabilities deployed to prevent or minimize opportunity to misuse or exploit the enhanced capability.

**Example:** Use of a form to generate an email to the web page owner: Care must be taken to ensure that settings for the form mail are such that the form mail can not be used to generate SPAM.

- The standards outlined in *IS PS010 Network Service* must be followed. Pay special attention to the “Connecting to city affiliated computing resources from outside the city network” section.

**Software Standards:**

The City of Belen website is hosted by a third party vendor on an Apache Web Server. Microsoft Expression Web is used to manage the website.

**SCOPE/APPLICABILITY:**

All persons while conducting/performing work, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY/ENFORCEMENT:**

The city’s Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**

**POLICY:**

All workstations and other computing devices shall:

- be maintained in an environment and manner so that access is reasonably restricted to authorized users only;
- be used in a prudent manner so that data, system and network integrity is maintained to the highest degree reasonably possible; and
- have operating systems and other software maintained in the most up-to-date and secure manner reasonably possible.

**Note 1:** All workstations and other computing devices used within the city that contain or transmit sensitive information or that attach to the city network are covered by this policy.

**Note 2:** If the standard is not technically possible for the specific computing device then mitigating controls should be employed where possible.

**STANDARDS:**

**Administrative standards:**

**Implementation**

- The department head is responsible for implementation of these security policies and standards, including methods to:
  - Educate the staff on computing device security practices.
  - Observing suspicious behavior or activity.
  - Following through with education practices when provided.

**Documentation**

- Procedures for complying with these policies and standards, as well as any additional department policies, standards and procedures will be developed and maintained by the department head or his designee for each division or other subsidiary unit.
- All department or division policies, standards and procedures for computing devices must be well documented, up-to-date and meet the minimum requirements established in this policy and accompanying standards.

After review and approval by the City Manager or designee, documentation of procedures (as well as any additional policies or standards) are to be forwarded, in electronic format, to the Information Security Office or IT Office for review. All major updates to the documentation and their effective dates should be forwarded to the IT Office.

## Workstations and Other Computing Devices

---

### **Compliance**

- Each department or division is expected to ensure compliance with these policies and standards as well as their own policies, standards and procedures.
- The Information Security Officer will work with Audit Services, IT and others to schedule periodic audits of computing devices to further ensure compliance with the policies and standards.

### **Use of Computing Devices**

- Computing devices and access to the network and internet are provided to perform city functions.

### **Use of Personal Computing Devices**

- No personal computing device shall directly be attached to the wired network without the direction or supervision of the IT Staff.
- No personal computing device shall be joined to the city domain.
- The city is not responsible for the security of data on a personal computing device if attached to the wired network.
- Personal computing devices must follow the same provisions, as any city owned computing device in regards to virus and malware protection see *ISO PS014 Protection from Malicious Software*.
- It is acceptable for personal computing devices to attach to the Public Wi-Fi.

### **Licensing**

- Licensing documentation must be maintained for any commercial software loaded on city owned computing devices.

### **Technical and physical standards:**

#### **System Maintenance:**

- All computing device operating systems and other software should be kept up-to-date by reviewing security updates, patches and tools on a regular schedule but not less often than every 90 days. Automated update capabilities must be turned on.

#### **Physical System Access:**

- Reasonable efforts should be made to limit and/or monitor physical access to computing devices to only authorized personnel. The computing device display screen should be positioned to minimize the chance for viewing by unauthorized individuals, where appropriate and feasible.

**Logical System Access and Security:**

- **Passwords**

All computing devices should require entry of a user ID and complex password. See *IS PS007 User Accounts and Acceptable Use* and *IS PS008 Passwords*.

- **Administrator or Administrative Accounts**

The Tier 1 support staff for the Department or Division should be used for installation of any software or performance of administrative functions on computing devices.

- Individuals with administrative access to computing devices must be familiar with and abide by the City's Acceptable Use Policy (see *ISO PS007 User Accounts and Acceptable Use*), as well as all technology standards, policies and procedures in using these rights.

In addition, as the city transitions to new operating systems that require changes in practice:

- The Administrator or its equivalent account should not be the active user account;
- User accounts should not have administrative privileges unless such access is required based on the user's routine city business activity; and
- Administrator account or accounts with administrator rights should only be used when necessary and should have a secure password (see *ISO PS008 Passwords*).

- **System Time-Out**

All computing devices connected to the city's networks or used to store, process or transmit information of a proprietary or sensitive nature must be configured to lock or "time-out" after a short period of inactivity and require a user ID and password or other authentication mechanism to unlock the machine. Thirty minutes is the recommended period before time-out. Departments and Divisions should establish appropriate time-outs based on the business use of the device.

- **System Maintenance and Updates**

Computing devices connected to the city's network update automatically from the Windows Update Server. For updates to be applied, workstations need to be left on. IT staff will remote to computing devices after hours to do routine maintenance on user's workstations. The only exception to this will be holidays or long weekends.

- **Security of data**

No secured data should be kept on any portable computing device. All portable computing devices and computing devices not demonstrably located in a secure area used to store, process or transmit sensitive information must maintain information of this nature in a secure fashion.

Encryption of proprietary or sensitive data fields, files or storage partitions or encryption of the entire system storage area is the recommended method to secure data residing on system storage devices. If this data is transmitted over any network other than the city's internal network, the data or the transmission protocol should be encrypted. (See backup standard below – it is important that all proprietary or sensitive information be backed up to prevent loss in the event of equipment loss or hardware failure).

---

**Workstations and Other Computing Devices**

---

- **Systems used to store, transmit or access other sensitive information:**

Computing devices in this category must use encryption as described above unless the device is maintained and used only in a highly secure, access controlled environment.

**Note:** Personal devices must not be used for sensitive city information unless you are personally able to configure your device to comply with these standards. Your City Tier support is able to configure the device and train you in operating the device in the necessary secure fashion.

- **Wireless Network Access**

Access to the city network via wireless technology must be appropriately configured to access the city's secure wireless network. See *IS PS010 Network Service*.

- **Protection from Malicious Software**

All computing devices connected to the city's network adhere to this policy and standards. See *IS PS014 Protection from Malicious Software*.

- **Data Backup and Recovery**

- Files containing valuable information must be backed up (note that the city network drives may be suitable for many back-ups).
- It is the responsibility of the user to establish a Backup and Recovery process that will best suit the user and to perform this process on their computing device.
- Back-ups will be performed on a regular basis.
- Back-ups will be maintained in a secure environment removed from the physical location of the computing device whenever possible.
- Back-ups should be encrypted and must be encrypted if custody of the back-ups is entrusted to a third party (non-City of Belen personnel).
- Ability to successfully recover back-up files may be tested by the IT Staff periodically.

See *IS PS015 Backup of Data*, *IS PS002 Business Continuity and Disaster Recovery*.

**SCOPE / APPLICABILITY:**

All persons while conducting/performing work, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY/ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REIVEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVIEW HISTORY:**

<b>Version</b>	<b>Revision Date</b>	<b>Description</b>
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**



---

**POLICY:**

The city maintains enterprise class secured data centers for the housing of city servers. All servers used to store, process or transmit sensitive information must be registered with the Information Technology Office.

All server computing devices must:

- be maintained in an environment and manner designed to physically and logically restrict access to unauthorized users;
- be used in a manner designed to maintain data, system and network integrity; and
- have operating systems and other software maintained in the most up-to-date and secure manner reasonably possible.

**STANDARDS:**

**Note:** These standards apply for servers fully managed by IT as well as those partially or fully managed by other city entities.

**Administrative standards:**

**Implementation**

- The Information Technology Office is responsible for server devices administratively within the City of Belen Domain for ensuring the implementation of the Server Computing Device security policies, standards, and procedures including implementing methods to:
  - Educate the department or division heads on Server Computing Device security practices.
  - Configure and maintain all servers to meet the Server Computing Device and other applicable standards.

**Documentation**

- Procedures for complying with these policies and standards, as well as any additional city policies and standards will be developed and maintained by the IT Office.
- All city policies, standards and procedures for servers must be well documented, up-to-date and meet or exceed the minimum requirements established in this policy.
- After review and approval by the City Manager or designee, documentation of procedures for the department or division is to be forwarded, in electronic format, to the Information Security Office for review. All major updates to the documentation and their effective dates should be forwarded to the Information Security Office.

**Compliance**

- Each department or division is expected to ensure compliance with these policies and standards as well as their own policies, standards and procedures.
- The Information Systems Security Officer will work with Audit Services, IT and others to schedule periodic audits of servers to further ensure compliance with the policies and standards.

### **Use of Computing Devices**

- Computing devices and access to the network and Internet are provided to perform city functions.

### **Licensing**

- Licensing documentation must be maintained for software loaded on any servers attached to the city network or otherwise hosted by the city.

### **Technical and physical standards:**

#### **System Maintenance:**

- All server operating systems and other software should be kept up-to-date by reviewing and installing appropriate security updates, patches and tools on a regular schedule but not less than every thirty days.

#### **Physical System Access:**

- All servers must be kept in a secured access controlled environment. Reasonable efforts shall be made to limit and/or monitor physical access to servers to authorized personnel. See *IS PS009 Data Facility Security*.

#### **Software:**

- Server class operating systems and software must be used for city servers.
- Non-City IT Division servers must be:
  - approved for the specified use by Information Technology management,
  - currently supported for security updates, and be
  - in full compliance with all applicable Information Security policies.

#### **Logical System Access and Security:**

##### **• Passwords**

All servers must require entry of a user ID and complex password. See *IS PS008 Passwords*.

##### **• Administrator Account, other Privileged Accounts and User Accounts**

###### **Administrator and Privileged Accounts**

- Individuals with server administrative rights must be familiar with and abide by *IS PS007 User Accounts and Acceptable Use* as well as all technology standards, policies and procedures in using these rights.
- The Administrator or other equivalent accounts must not be used as active user accounts. All accounts with administrative rights should only be used when necessary and must have a complex password.

###### **User Accounts**

- Any operating system or enterprise/back office software requiring accounts to be set-up for users must use the least required access approach for configuring user access to these accounts.

**Activity and Transaction Auditing, Logging and Monitoring**

- User activity within the system should be monitored. Audit and/or transaction logs should be maintained, monitored and/or audited as appropriate for the system. Appropriate auditing, logging and monitoring activity must be defined in the context of applicable laws and regulations as well as reasonable practice to ensure the integrity and security of the system.
- All servers processing sensitive information should log any transactions or other events that cause the creation, updating/modification or deletion of this type of information.
- This logging should be done at the server operating system, database and/or application levels, as appropriate, to ensure that these activities are captured.
- Logs should include as much of the following information as is technically and reasonably possible: date, time, user ID, transaction/activity type, event type (write, update/modify, delete, read), data changed (data before and after change or data after change) and other information necessary to analyze and/or reconstruct transactions, activity or events.

● **System Time-Out**

All server authentications or server software accessed by end-users must be configured to lock after a short period of inactivity (10 minutes is the recommended time unless system requirements necessitate a longer time) and require a user ID and password or other authentication mechanism to unlock or reactivate. Automated programs and services should also be configured with an authentication time-out unless this prevents proper functioning of the program or service.

● **Wireless Network Access**

All servers must use a hardwired network connection.

● **Protection from Malicious Software:**

All servers must -

- Run real time virus protection if such software is available for the computing device;
- Utilize a hardware (preferred) and/or software firewall either for the server or for a dedicated network server subnet;
- Use spyware protection and detection programs, if available;
- Have all operating system and software services not required for the proper functioning of the server be disabled or set to manually start if occasionally used.

See *IS PS014 Protection from Malicious Software*.

- **Data Backup and Recovery**

- Files containing valuable information must be backed up (note that the city network drives may be suitable for many back-ups).
- Back-ups will be performed on a regular basis.
- Back-ups will be maintained in a secure environment removed from the physical location of the server.
- Ability to successfully recover back-up files will be tested periodically (at least every 180 days) and at the time of any significant hardware or software updates or changes to the system.

See *IS PS015 Backup and Retention of Data*, *IS PS002 Business Continuity and Disaster Recovery*.

**E-Mail, Calendar and Personnel/Group Scheduling Servers - Additional technical standards:**

**Interoperability:**

- Systems designed to perform email, calendaring or scheduling must automatically interoperate with the City of Belen furnished enterprise solution for these tasks. This includes all city departments, divisions, and other affiliated entities.
  - E-mail must flow in a timely fashion between the systems and remain within the city network while doing so.
  - Calendar and personnel/group scheduling functions must work in both directions so that personnel using the enterprise system or personnel using other city entity solution are able to transparently review personnel availability, schedule meetings, and related expected functions.

**SCOPE/APPLICATION:**

All persons while conducting/performing work, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY/ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

---

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**



**POLICY:**

Malicious software (viruses, worms, Trojans, root kits, hostile Active X controls, etc.) must be actively guarded against within the city network. All computing devices must be configured with appropriate safeguards against malicious software.

**STANDARDS:**

Anti-virus, anti-spyware and firewall software must be deployed on all Windows® based workstations, portable computers, servers and other computing devices that attach to the city networks. Non-Windows computing devices should use equivalent products, if available. Servers behind a properly configured hardware firewall and meeting other enterprise class configuration, administration and maintenance requirements may be exempted from some of these requirements. All exemptions must follow *IS PS004 Policy Exception Management Process*.

**Administrative Standards:**

- Antivirus software is available from IT for workstations and servers. Exceptions to the recommended tools such as firewalls, antivirus, and anti-spyware should be approved by the IT Office.
- Intrusion detection, network monitoring, incident logging, and response coordination necessary for the detection, elimination, and recovery from various forms of attack on city resources is managed by the IT Office (See *ISO PS006 Security Incidents*.)
- Systems found to be infected will be removed from the network until such time as the infection is removed or the system is reformatted.
- The Department Head is responsible for the implementation of these security policies and standards so that all computing devices in their areas of responsibility have implemented the appropriate virus protection, antispyware and firewall controls as outlined in this document and that all such tools are kept current with the most recent updates installed.

Proper preparation of all systems (desktops, laptops, servers, printers and handheld devices) must be conducted. Tier Support must install virus protection, anti-spyware and firewall software on all applicable computing devices and should ensure that unnecessary services are disabled before distribution to the user community.

- System Administrators must ensure that the appropriate virus protection, anti-spyware and firewall programs are installed on all servers and ensure that unnecessary services are disabled before installation in the production environment.
- Use of Peer-to-Peer (P2P) software “file sharing” applications is not permissible for any file sharing activities to facilitate abuse of copyright and intellectual property laws.
- Instant messaging programs must not be used for file sharing.
- Non-city web based e-mail will not be allowed through the city network. Only client based e-mail can be scanned for malicious intent.
- The IT Office will work with Audit Services and others to schedule periodic audits of servers, workstations, laptops and other computing devices to ensure compliance with the established virus protection, antispyware and firewall standards.

**Technical standards:**

- All computing devices must be appropriately configured for automatic virus detection and spyware blocking.
- Virus and anti-spyware definitions must be updated at least every four hours at the server. An automatic definition update option should be enabled if supported by the virus or anti-spyware protection tool. Virus and anti-spyware definitions on the workstations must be updated at least once a day.

**Note:** Information Technology will centrally provide updates to the virus definition files.

- All software, regardless of origin, should be scanned for viruses and spyware before installation on any city system.

**Note:** Software obtained directly from IT has already gone through this process. Software from approved and/or major vendors has low risk (but it has happened) of virus or spyware contamination. Software downloaded from freeware/shareware or other non-major vendor web sites has the highest risk of spyware or virus contamination, this software should always be scanned before installation. Downloads from these type of sites are strictly forbidden, unless under the supervision of the IT Office.

- Workstation virus scanning software should be configured to automatically scan all e-mail attachments upon receipt with auto-protect/real time protection enabled.
- All computing devices not running approved anti-virus and anti-spyware software must be scanned for malicious software prior to connection to the city network. The IT Office has CD based software for this purpose.

Home computer systems connecting, as privileged users, to the city networks must meet the same anti-virus, anti-spyware and firewall standards as systems on city premises. **Note:** This does not mean browsing web pages but does mean other activities including but not limited to “I” and “S” drive connections, via SSH Secure Shell, etc.

- All virus and spyware occurrences that are not fully removed by the anti-virus or antispyware software must be reported to IT for cleansing of the computer (See *ISO PS006 Security Incidents*.)
- Anti-virus, anti-spyware or firewall protection programs must not be disabled while connected to the city network. **Note:** If installation of software requires the temporary termination of these programs, the computing device must be disconnected from the network while the software is being installed. The protection programs must be restarted before the computing device is reconnected to the network.
- Memory sticks, flash drives, CDs, and other removable media from unknown or un-trusted sources must be scanned for viruses and spyware. Auto-start mechanisms must be bypassed when first using removable media that has not been scanned for viruses and spyware.

**Software Standards:**

The following software has been tested and is recommended by the IT Office for Windows™ anti-virus, anti-spyware and firewall protection:

- AVG Anti-Virus Small Business Edition (provided by the City of Belen for all staff, and affiliated entities).
- Microsoft Defender (legacy).
- Microsoft® Windows™ Firewall.
- Other tools maybe made available when they have been tested and released as necessary.

**SCOPE/APPLICABILITY:**

All persons while conducting/performing work, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY / ENFORCEMENT:**

The city’s Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**



**POLICY:**

Regular back-ups are required for all city related data not hosted on city enterprise systems if the data is sensitive, proprietary or needed during the course of normal operations. Back-ups of data must be retained in accordance with City, State or Federal retention guidelines as appropriate for the data being backed-up.

**Note:** Information Technology conducts regular backs-up of all data stored on enterprise servers and shares, but not on individual PCs or mobile devices. It is the user's responsibility to backup their data to the network shares. Data stored on any other removable media is also the responsibility of the user.

**STANDARDS:**

**Administrative Standards**

**General:**

Back-ups are an important part of disaster recovery and business continuity planning. Also see *IS PS002 Business Continuity Planning and Disaster Recovery*.

- Files containing sensitive information must be backed up (note that the city network drives may be utilized for this purpose).  
**Note:** city network drive back-ups are maintained for 8 days. Departments or users with longer retention needs are encouraged to contact the IT Office to arrange special requirement back-ups.
- Back-ups must be performed at regular intervals not less than weekly for all city wide valuable information. Smaller city entities and individuals must back-up valuable information at regular intervals not to exceed monthly (more often if the information changes frequently).
- Back-ups must be maintained in a secure environment removed from the physical location of the data facility.
- Back-ups should be encrypted and password protected if custody of the back-ups is entrusted to a third party.
- Ability to successfully recover back-up files must will be tested periodically, but not less than annually and at the time of any significant hardware or software updates or changes in the system in question.
- Back-ups must be retained in accordance with retention guidelines to help the city meet all relevant regulatory or institutional requirements.

**Computing Operations Centers**

- Incremental back-ups of enterprise systems must be done daily
- Full back-ups of enterprise systems must be done weekly.
- Copies of back-ups must be rotated offsite daily for disaster recovery purposes.
- Back-ups will be retained for a minimum of 10 days.
- Back-ups must be created for enterprise disaster recovery purposes.
- Back-ups should not be relied upon for recovery of accidentally deleted files as a matter of routine.

**SCOPE/APPLICABILITY:**

All persons while conducting/performing work, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY/ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**

---

**Inventory, Tracking, Discarding and Redeployment of Computing Devices or Media**

---

**POLICY:**

All computing devices and electronic media being redeployed, surplused, discarded or otherwise removed from service or changing service facilities must, regardless of the value of the computing device or media, have all sensitive information permanently deleted.

**STANDARDS:**

**Important Note:** See related Purchasing Department Policies and Procedures for inventory and surplus of equipment. These policies and standards apply to all computing device or associated electronic media, regardless of expendable classification per purchasing department policies and procedures.

**Administrative Standards:****Computing Device or Media Redeployment**

- Any computing device being moved from one department or other city entity to another (or between personnel with different access and need to know privileges if in the same unit) must have all sensitive information eradicated (see Technical Standards section for eradication guidelines).
- Any electronic media being moved from one department, or other city entity to another (or between personnel with different access and need to know privileges if in the same unit) must have all sensitive information eradicated (see Technical Standards section for eradication guidelines).

**Computing Device or Electronic Media Disposal or Surplus**

- Any computing device being discarded, donated, sent to surplus or otherwise being removed from service must have all sensitive information eradicated (see Technical Standards section for eradication guidelines).
- Any electronic media being discarded, donated, sent to surplus or otherwise being removed from service must have all sensitive information eradicated. Physical destruction of the media is the best method of media disposal (see Technical Standards section for data eradication and destruction guidelines).

**Technical Standards:**

Proper tools are required to eradicate sensitive information. The IT Office will obtain the necessary tools to accomplish this task.

**Eradication of Data**

- Total eradication of data on the computing device or electronic media is the preferred way to provide a reasonable assurance that sensitive information has been eliminated if the device or media is not to be destroyed (see physical media destruction below).

A total eradication tool must be used if the device or media is being removed from service within the city. Selective eradication of data may be used for computing devices or electronic media being redeployed (not disposed or surplused) provided sensitive data was not housed on the computing device or electronic media.

---

**Inventory, Tracking, Discarding and Redeployment of Computing Devices or Media**

---

**Note:** computing devices or electronic media which contain or contained police or municipal court data must have the media cleansed using a total eradication method.

- **Tier One or other qualified support staff** who understand how to use the tools outlined above must perform this procedure. This is to both maximize assurance of data eradication and to minimize the chance of accidental inappropriate data deletion.
- **Certification of Data Eradication** – “Computing Devices Surplus Certification” labels are provided by the Purchasing Department to affix to the device and signify that the device or electronic media has had its data eradicated. It is extremely important that the procedures for this are followed.

**Physical Media Destruction**

- Physical destruction of electronic media is the preferred way to provide a high level of assurance that sensitive information has been eliminated if the electronic media is being disposed and not redeployed. Physical destruction is considered complete only if the media has been disposed of with a shredder or other equipment designed for destroying electronic media. “Casual destruction” (bending, cutting with scissors, breaking and similar activities) is not an adequate way to physically destroy electronic media.

**Note:** If proper physical destruction tools are not available for media being disposed, properly performed total eradication of data, as described above, is acceptable.

**PROCEDURES:**

- See related procedures at the Purchasing Department web site <http://www.belen-nm.gov/departments/administration/purchasing.htm>

**SCOPE/APPLICABILITY:**

All persons while conducting/performing work, research or study activity or otherwise using city resources. Scope/Applicability also includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY/ENFORCEMENT:**

The city’s Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

<b>Version</b>	<b>Revision Date</b>	<b>Description</b>
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**



**POLICY:**

The city provides a hardware firewall to protect the central city servers and host systems, and to protect the city network from the Internet.

**STANDARDS:**

**Administrative Standards:**

Any requests for modification to firewall configurations can be made. Emergency changes must be requested in writing and with approval from the IT Office. Justification must also be submitted as to why it is important to open specific ports in the firewall. Those changes will be monitored, and any anomalies will be sufficient cause to close the offending port without prior notice.

**Technical Standards:**

All outbound packets are allowed to travel outside, and inbound packets are allowed inside the firewall only if they can be determined to be responses to outbound requests.

The following type of network traffic should always be blocked:

- Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself.
- Inbound traffic with a source address indicating that the packet originated on a network behind the firewall.
- Inbound or Outbound traffic from a system using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks. For reference purposes, RFC 1918 reserves the following address ranges for private networks:
  - 10.0.0.0 to 10.255.255.255 (Class A)
  - 172.16.0.0 to 172.31.255.255 (Class B)
  - 192.168.0.0 to 192.168.255.255 (Class C)
- Inbound traffic from a non-authenticated source system containing SNMP (Simple Network Management Protocol) traffic. Inbound traffic containing IP Source Routing information.
- Inbound or Outbound network traffic containing a source or destination address of 127.0.0.1 (local host).
- Inbound or Outbound network traffic containing a source or destination address of 0.0.0.0. Inbound or Outbound traffic containing directed broadcast addresses.

The firewall should block all inbound traffic unless that traffic is explicitly needed for inbound server connections. The following services and applications should only be allowed in extreme circumstances:

Application	Port Numbers	Action
<b>Login Services</b>		
Telnet	23/tcp	always block
FTP	21/tcp	always block
NetBIOS	139/tcp	always block
Services	512/tcp - 514/tcp	always block
<b>RPC and NFS</b>		
Portmap/rpcbind	111/tcp/udp	always block
NFS	2049/tcp/udp	always block
Locked	4045/tcp/udp	always block
<b>NetBIOS in Windows NT</b>		
	135/tcp/udp	always Blocked
	137/udp	always blocked
	138/udp	always blocked
	139/tcp	always blocked
Windows 2000	445/tcp/udp	always blocked
XWindows	6000/tcp - 6255/tcp	always blocked
<b>Naming Service</b>		
DNS	53/udp	restricted to external DNS
Servers	DNS zone transfers - 53/udp	blocked unless External
LDAP	389/tcp/udp	always blocked
Mail	SMTP - 25/tcp	external mail
<b>Relays</b>		
POP	109/tcp	always blocked
	110/tcp	always blocked
IMAP	143/tcp	always blocked
<b>Miscellaneous</b>		
tftp	69/udp	always blocked
finger	79/tcp	always blocked
NNTP	119/tcp	always block
NTP	123/tcp	always block
LPD	515/tcp	always block
syslog	514/udp	always block
SNMP	161/tcp/udp, 162/tcp/udp	always block
BGP	179/tcp	always block
SOCKS	1080/tcp	always block

**SCOPE/APPLICABILITY:**

This policy applies to all city workforce, (including, but not limited to: staff, temps, trainees, volunteers, and other persons as deemed appropriate) while conducting/performing work, research or study activity using city resources and includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY/ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**



---

**POLICY:**

The city provides a cellular phone to the City Manager and all Department Supervisors and Managers. Also to staff within each department as the department head deems necessary. The City of Belen contracts with cellular phone providers that have been approved by the State of New Mexico General Services Division.

**STANDARDS:**

**Procedures**

- Cell phones issued by the City of Belen are city property. Employees should not have any expectation of privacy on any city-issued phone. Employees must comply with city requests to make their city-issued cell phones available for any reason, including upgrades, replacement, or inspection. Employees who leave the city for any reason must turn in their city-issued cell phones.
- Requests for all services (including adds, moves, and changes) may be obtained through the IT Office.
- The Department Head, City Manger, or Finance Manager, is responsible for monitoring the use of all cellular devices assigned to that department (i.e., cellular, long distance, base charges, etc.)
- Personal calls to or from a city owned cellular telephone should be kept to a minimum, and will be at the discretion or approval of the Department Head. Personal use that exceeds this standard will result in discipline, up to and including termination or loss of cell phone privileges. Employees are expected to reimburse the city for any costs or charges relating to personal use of their cell phones.
- All costs associated with cellular phone will be borne by the department ordering the equipment. Such costs include, but are not limited to, the following: equipment acquisition; service initiation; monthly fees for cellular service; per-minute cost of calls in excess of the calling plan allocation; maintenance and repair of equipment; and replacement of lost or stolen equipment.
- Cellular phones should not be issued to contract employees, part-time, temporary personnel, or others not having a compelling use for the technology unless specifically requested by the department head.
- Security of these phones is the responsibility of the department or the IT Office in the case of “smart phones” such as “Blackberry” which are centrally managed through city servers.
- From time to time, internal audits conducted by the Finance Office and/or the IT Office may review individual usage and suggest cellular plans to assure that the most appropriate rate plan is in use and to screen for possible abuse. This information will then be forwarded to the user’s department for administrative review.
- User departments will be responsible for coordinating repair and billing issues of cellular phones with the appropriate vendor. If issues are not resolvable to the department’s satisfaction, contact the IT Office for assistance and escalation procedures.

- Employees are responsible for the security of city-issued cell phones and the information stored on them. Always keep your cell phone with you when traveling; never leave it unattended in your car or hotel room. If your city-issued cell phone is lost or stolen, notify the IT Office immediately. Never store confidential city information on a cell phone.

#### **Personal Cell Phones at Work**

- Although the City of Belen allows employees to bring their personal cell phones to work, employees are expected to keep personal conversations and texting to a minimum. While occasional, brief personal phone calls are acceptable, frequent or lengthy personal calls and texting can affect productivity and disturb others. For this reason, we generally expect employees to make and receive personal phone calls during breaks only.
- Employees must turn off the ringers on their cell phones while away from their cell phones. If you share workspace with others, you must turn off the ringer on your phone while at work.
- Employees must turn off their cell phones or leave their phones elsewhere while in meetings, presentations, or trainings. Employees must also turn off their cell phones or leave their phones elsewhere while meeting with clients or serving customers.
- It is inappropriate to interrupt a face-to-face conversation with a coworker or client in order to take a personal phone call.
- Remember, others can hear your cell phone conversations. Try to talk quietly, and save intimate discussions for another time.
- Employees who violate this policy will be subject to discipline, up to and including termination.

#### **Don't Use a Cell Phone While Driving**

- Employees are prohibited from using cell phones for work-related matters while driving. The city is concerned for your safety and for the safety of other drivers and pedestrians, and using a cell phone while driving can lead to accidents.
- If you must make a work-related call while driving, you must wait until you can pull over safely and stop the car before placing your call or text message. If you receive a work-related call while driving, you must ask the caller to wait while you pull over safely and stop the car. If you are unable to pull over safely, **do not** pickup the call instead allow the call to go to voicemail and listen to your voicemail when it is safe to do so.

#### **Using Your Cell Phone for Business**

- The city's overtime rules apply to any type of work done after hours, including using a city-issued cell phone to make business calls. All overtime work -- including such work-related calls -- must be approved in writing, in advance. Working overtime without permission violates city policy and may result in disciplinary action.
- Employees may not use their own personal cell phones to make business calls. If you feel that you need a cell phone to perform your job, please ask your manager to get you a city-issued cell phone.

**SCOPE/APPLICABILITY:**

This policy applies to all city workforce, (including, but not limited to: staff, temps, trainees, volunteers, and other persons as deemed appropriate) while conducting/performing work, research or study activity using city resources and includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY/ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**



---

**POLICY:**

The city provides phone service to all facilities. All voice communications are Voice over IP across the city wide network. There are two voice entry points servicing the City of Belen for redundancy and failover. The Primary entry point is at city Hall and the secondary entry point is at the Public Library. Should connectivity be lost at an entry point, calls can be routed to the other, providing an almost “zero” lost of communications to the city’s main core which consists of City Hall, Police Department, Fire Department, Municipal Court, and Library. Voice communications at the external sites such as Airport, RSVP, Community Center, Recreation Center and Waste Water will be maintained as “best can” dependent on which entry point is affected.

This phone system offers a lot of functions and flexibility. One of the functionality that this system offers is integration with Microsoft Outlook Client for voice mail and fax services and integration with “Smart phones” such as the Blackberry. Complete control over add changes and deletions of telephone hardware and user administration. The system also allows for integrated paging, hands free and desktop dialing and telephone device administration.

**STANDARDS:****Administrative Standards**

Instruction for use of the telephone devices can be found in the \\wdsharespace\public\Shared Instructions & Manuals\Shortel. All instruction material is in PDF format.

- Access may be given to persons outside of the city on a case-by-case basis or under certain conditions when warranted. Disclosure of this information may not be given to the individual(s) involved.
- The use of electronic data and voice mail is provided for city staff for the purpose of conducting business on behalf of the City of Belen. The city staff should limit their use for these purposes.
- Usage of electronic data and voice mail should adhere to other city policies.
- The City of Belen can not guarantee the confidentiality or privacy of electronic data or voice mail messages. This should be kept in mind when using these services.
- Third party vendors are involved with both internet and voice mail data.
- All users of electronic data and voice mail should familiarize themselves with policies set forth by these vendors.
- In-coming and out-going calls for City Hall, Police, Fire, and Municipal Court are recorded.
- The city administration or IT Office does not monitor electronic communications on a routine basis; however, it does reserve the right to do so if instructed by legal authorities or for the purpose of system integrity or policy violations.
- On voice mail systems, please record a professional outgoing message identifying name, title, department (if applicable) and any instructions.
- Messages left in voice mail systems must be addressed in a timely manner, those calls will be returned within 24 hours of returning to work. Calls will be deleted from the system upon completion by the user.
- If an employee will be gone from his or her office for an extended period of time, (more than two work days) arrangements must be made for those calls to be forwarded or taken by another colleague within the department.
- Upon severing employment with the City of Belen, the employee must forward those messages to another colleague within the department. He shall also relinquish passwords or pass codes to the IT Office or his immediate supervisor so that call forwarding can be set.

---

**Privacy and use of speaker**

- Except when duly notified, callers to the City of Belen have a right to expect some privacy during their phone conversation with staff. It is unacceptable to place any call on speaker phone in an open office.
- When it is necessary for a call to be placed on speaker, the caller must be notified of such activity.
- Calls placed on speaker should only take place in private offices and not in open areas where there is public foot traffic.
- Phone conversations should not be shared amongst other staff or persons nearby.

**FAX Services**

All Direct Dial extensions on the phone system is also the fax number where a user can receive or send a fax. When a fax is received by the system, it is automatically sent to the FAX server where the fax is processed and then sent to the user via email.

- Users shall use the FAX service whenever possible.
- FAX services are private to the extent that they appear only in the users e-mail account.
- Outgoing faxes are as easy as printing if the document is user created. Otherwise if the user is not the originator of the document then the document must be digitally scanned and then faxed.
- Outgoing faxes are created by using a proprietary print driver that a document or image is printed to. The driver then converts the document to a fax image which is sent via the Outlook client.

**Technical Standards**

- The telephone devices use Power over Ethernet or (PoE).
- Telephone devices shall not be unplugged from the wall jack for any extended amount of time.
- The telephone device is powered by the network, and therefore shall be the first device or the only device plugged into the wall jack. Other devices such as computers can subsequently be plugged into the back of the phone.

**SCOPE/APPLICABILITY:**

This policy applies to all city workforce, (including, but not limited to: staff, temps, trainees, volunteers, and other persons as deemed appropriate) while conducting/performing work, research or study activity using city resources and includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY/ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

---

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**



**POLICY:**

Technology is becoming ever more embedded into everything we do these days. Whether we are contemplating a brand new building or remodeling an old one, the use of technology is somehow going to impact the facility. Even if there will be nothing more than a telephone at a site, the IT Office needs to review the plan to see how a facility will impact future plans for IT needs.

**STANDARDS:**

**Administrative Standards**

- During the preliminary planning for any city project whether it be street, building, new or old; the IT Office needs to be involved.
- The IT Office needs to be advised of any planned upgrades to any computing device, security device, software application, communications device, and energy device and infrastructure improvements.
- Because of the use of a VoIP phone system through out all city facilities, CAT5, CAT6 or network cabling is now considered the standard in all building projects.
- Wireless communications should now be considered where applicable.
- Video monitoring equipment should be standardized for digital transport across the city-wide network.
- City projects should take on a “whole” approach wherever possible when funding projects. When applying for grants to fund projects, include the city as a “whole” instead of limiting the scope of a project to just one department or entity. See also *ISO PS023 Acquisition of Technology*.
- Future proof City Projects by including the necessary equipment, material or utilities in projects so that the work is done now instead of discovering later that this should have been included.
- The same process holds true for the decommission of any city facility. The IT Office must make arrangements for the removal of network infrastructure in such facilities.

**SCOPE/APPLICABILITY:**

This policy applies to all city workforce, (including, but not limited to: staff, temps, trainees, volunteers, and other persons as deemed appropriate) while conducting/performing work, research or study activity using city resources and includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY/ENFORCEMENT:**

The city’s Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

Information Security Policy  
New and Remodeled Infrastructure Review

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**

**POLICY:**

Our network and Internet access are for official city business. Employees may access the Internet for personal use only outside of work hours and only in accordance with the other terms of this policy. An employee, who engages in excessive Internet use, even during nonworking hours, may be subject to discipline.

**STANDARDS:**

**Prohibited use of the Internet**

Employees may not, at any time, access the Internet using city equipment for any of the following purposes:

- To view websites that offer pornography, gambling, or violent imagery, or are otherwise inappropriate in the workplace.
- To operate an outside business, online auction, or other sales site; solicit money for personal purposes; or to otherwise act for personal financial gain or profit.
- To download or copy software, games, text, photos, or any other works in violation of copyright, trademark, or other laws.
- To stream, run, or download any non-city-licensed software program without the express consent of the IT department.
- To stream, run, or download music, video, games, mini-desktop applications (widgets), or any form of multimedia, from the Internet.
- To read, open, or download any file from the Internet without first screening that file for viruses using the city's virus detection software.

If you believe that your job may require you to do something that would otherwise be forbidden by this policy, ask your manager how to proceed.

To assure that employees comply with this policy, we use Content Filtering on our Firewall that will block your access to many prohibited sites. However, some inappropriate websites may escape detection by the Firewall: The fact that you can access a particular site does not necessarily mean that site is appropriate for workplace viewing.

**Administrative Standards**

- **No Personal Posts Using City Equipment**
  - Employees should not use the city's equipment to transmit their personal opinions by, for example, posting a comment to a blog or contributing to an online forum. Even if you don't identify yourself as a city employee, your opinion could be mistaken for the city's view.
- **Internet Use Is Not Private**
  - We reserve the right to monitor employee use of the Internet at any time. You should not expect that your use of the Internet -- including but not limited to the sites you visit, the amount of time you spend online, and the communications you have -- will be private.

- **Don't Use Personal Email Accounts for Work**
  - Employees may not use their own personal email accounts to transact city business. This includes storing work-related documents and email messages in your personal email account, sending work to your personal email account, engaging in work-related communications (with customers, clients, or coworkers, for example) using your personal email account, or "bouncing" messages from your city email to your personal email when you are out of the office.
  - Although employees may find these practices convenient, they can create significant security problems, expose confidential city information, and compromise the city's record-keeping obligations. If you work offsite (for example, at home or on business travel), please contact the IT department to find out how to safely transmit and protect city information.
- **No Access to Personal Email**
  - Accessing your personal email account from work creates security risks for the city's computer system and network. Therefore, employees may not use city equipment to access their personal email accounts.
  - The city's Firewall blocks access to many Web-based email sites. The fact that you can access a Web-based email site does not mean that you are free to check personal email using the city's equipment, however.

#### **SCOPE/APPLICABILITY:**

This policy applies to all city workforce, (including, but not limited to: staff, temps, trainees, volunteers, and other persons as deemed appropriate) while conducting/performing work, research or study activity using city resources and includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

#### **POLICY AUTHORITY/ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

#### **POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

#### **COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

---

**REVISION HISTORY:**

<b>Version</b>	<b>Revision Date</b>	<b>Description</b>
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**



---

**POLICY:**

The email system is intended for official city business. Although city employees may use the email system occasionally for personal messages, you may do so during nonworking hours only. If you send personal messages through the city's email system, you must exercise discretion as to the number and type of messages you send. City employees must also ensure that your personal use of the email system does not interfere in any way with your job duties or performance. Any employee who abuses this privilege may be subject to discipline.

**STANDARDS:**

**Email Is Not Private**

Email messages, including attachments, sent and received on city equipment are the property of the city. We reserve the right to access, monitor, read, and/or copy email messages at any time, for any reason. City employees should not expect privacy for any email you send using city equipment, including messages that you consider to be personal, or label with a designation such as "Personal" or "Private."

City employees shall not assume that any message contents or data are automatically subject to public inspection under the state *Inspection of Public Records Act*. There are numerous exclusions to this law, and such message contents or data may not be forwarded, uploaded, or otherwise transmitted to non-city entities without appropriate approvals.

**All Conduct Rules Apply to Email**

All of our policies and rules of conduct apply to employee use of the email system. This means, for example, that you may not use the email system to send harassing or discriminatory messages, including messages with explicit sexual content or pornographic images; to send threatening messages; or to reveal city secrets or confidential information.

**Check Email Regularly**

City employees will regularly check their city email accounts for correspondence no less than four times a day. A lot of important information from administration is disseminated through email communications regularly.

**Automatic Forwarding**

Sensitive information requires special precautions when emailing, especially outside the city network and must not be automatically forwarded.

**Complaints and Resource Management**

Complaints regarding misuse or misconduct will be investigated. **Note:** The intent of the communication along with the perspective of the recipient is considered during investigations. Electronic mail use is monitored for resource consumption and storage management.

### **It's All About the Branding**

City employees shall use only city branded e-mail accounts to send and receive e-mail messages in the conduct of official city business. Users shall not automatically forward e-mail messages received at a users account to any personal or non-city e-mail account or address.

“Email for life” users and other email users must not use their City of Belen email address to misrepresent their affiliation with the city.

### **No Solicitation by Email**

City employees may not use the email system to solicit others to patronize an outside business or to support an outside organization, a political candidate or cause, or a religious cause.

### **Professional Tone and Content**

We expect city employees to exercise discretion in using electronic communications equipment. When you send email using the city's equipment, you are representing the City of Belen. Make sure that your messages are professional and appropriate, in tone and content. Remember, although email may seem like a private conversation, email can be printed, saved, and forwarded to unintended recipients. You should not send any email that you wouldn't want your boss, or your mother to read.

### **Guidelines for Email Writing**

1. Always spell-check or proofread your email messages. Email is official city correspondence. spelling errors in email are all too common, and they look sloppy and unprofessional.
2. Use lowercase and capital letters in the same way that you would in a letter. Using all capital letters is the email equivalent of shouting at someone -- and it can be hard on the eyes. Failing to use capital letters at all (to begin a sentence or formal noun) can confuse readers and seem overly cute. Unless you are writing poetry, use standard capitalization.
3. Remember your audience. Although email encourages informal communication, that might not be the most appropriate style to use if you are addressing the CEO of an important customer. And, remember that your email can be forwarded to unintended recipients, some of whom may not appreciate joking comments or informalities.
4. Don't use email for confidential matters. Again, remember the unintended recipient. Your email might be forwarded to someone you didn't anticipate or might be sitting at a printer for all to see. If you need to have a confidential discussion, do it in person or over the phone.
5. Send messages sparingly. There is rarely a need to copy everyone in the city on an email. Carefully consider who really needs to see the message, and address it accordingly.
6. Always think before you send. Resist the urge to respond in anger, to "flame" your recipient, or to get emotional. Although email gives you the opportunity to respond immediately, you don't have to take it.
7. **Don't leave the subject line blank.** Always include a brief description, so readers will know what your email is about at a glance. This makes it easier for all of us to manage our email -- and makes it more likely that you will receive a response to your message.
8. Don't overuse the "urgent" tag. Mark a message as urgent only if it is truly important and must be answered right away.

---

## **Email Security**

To avoid email viruses and other threats, employees should not open email attachments from people and businesses they don't recognize, particularly if the email appears to have been forwarded multiple times or has a nonexistent or peculiar subject heading. Even if you know the sender, do not open an email attachment that has a strange name or is not referenced in the body of the email -- it may have been transmitted automatically, without the sender's knowledge.

If you believe your computer has been infected by a virus, worm, or other security threat to the city's system, you must inform the IT Office immediately.

Employees also may not share their email passwords with anyone, including coworkers or family members. Revealing passwords to the city's email system could allow an outsider to access the city's network.

## **Retaining and Deleting Email Messages**

Because email messages are electronic records, certain messages must be retained for compliance purposes. Please refer to our record -- keeping policy for guidance on which records must be kept, and for how long. If you have any questions about whether and how to retain a particular email message, please ask your manager.

Because of the large volume of emails our city sends and receives each day, we discourage employees from storing large numbers of email messages that are not subject to the retention rules explained above. Please make a regular practice of deleting email messages once you have read and/or responded to them. If you need to save a particular message, you may print out a paper copy, archive the email, or save it on your hard drive or disk by creating a PST file or letting Outlook Archive your messages. The Exchange Server will purge email messages that have not been archived after 90 days or as per the records retention policy.

The city may have occasion to suspend our usual rules about deleting email messages (for example, if the city is involved in a lawsuit requiring it to preserve evidence). If this happens, employees will be notified of the procedures to follow to save email messages. Failing to comply with such a notice could subject the city to serious legal consequences, and will result in discipline, up to and including termination.

### **SCOPE/APPLICABILITY:**

This policy applies to all city workforce, (including, but not limited to: staff, temps, trainees, volunteers, and other persons as deemed appropriate) while conducting/performing work, research or study activity using city resources and includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

### **POLICY AUTHORITY/ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

---

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**

**POLICY:**

The City of Belen is striving for a homogenous technology environment where computers, vehicles, valves, pumps, water meters, HVAC, lighting, security systems, and irrigation systems all over the city can communicate across the same network. The ultimate goal is a Supervisory Control and Data Acquisition system (SCADA) that will help manage city assets more efficiently and cost effectively. Technology purchases are costly investments. When a new piece of technology is introduced into this homogenous environment, it is important to know that the new technology will be compatible with existing technology and “fit” into the long term plans of the city. It makes no sense to purchase equipment that either duplicates efforts in another department or does not “fit into the big picture” or just plain will not work.

**STANDARDS:**

**Introduction of Technology**

When any department is contemplating purchasing technology of any kind, this information should be shared with the IT Office. The IT Staff will determine if said technology is compatible with existing technology or if it even needs to integrate with network services.

The IT Office will determine the best way to accommodate the needs for the new technology and make recommendations on how to best execute the installation of equipment.

**Computer Purchases**

Although each department is responsible for funding their purchases, it is the IT Office that will specify the type and brand of computer hardware the city will purchase. All PCs must meet an industry standard in configuration and warranty. The IT Office will publish a minimum standards list for PCs Laptops, Servers, PDAs, Network Equipment, and Printers. The IT Staff is best suited to make the determination of which equipment will best suit the city, since they are familiar with the network and software needs.

Department Supervisors or users will outline for IT Staff exactly what the PC needs to accomplish. Based on this evaluation the IT Staff will configure and purchase the PC.

**Other Technology Purchases**

To consolidate and streamline the city’s printing needs, work group printers will be used instead of desktop printers where feasible. Where Multifunction Printers (Printer, Scanner, Copier) devices are allowable, any device that is inkjet based will be strongly discouraged.

**SCOPE/APPLICABILITY:**

This policy applies to all city workforce, (including, but not limited to: staff, temps, trainees, volunteers, and other persons as deemed appropriate) while conducting/performing work, research or study activity using city resources and includes all facilities, property, data and equipment owned, leased and/or maintained by the City of Belen or affiliates.

**POLICY AUTHORITY/ENFORCEMENT:**

The city's Information Security Officer (ISO) is responsible for the development and oversight of these policies and standards. The ISO works in conjunction with City Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

**POLICY REVIEW:**

This policy will be reviewed annually to determine if the policy is in compliance with the applicable security regulations and city direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

**COMPLIANCE:**

Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the City of Belen and/or action in accordance with local ordinances, state or federal laws.

**REVISION HISTORY:**

Version	Revision Date	Description
1.0	August 16, 2010	Original Publication

**This policy is subject to change or termination by the City of Belen at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.**