

# Information Security Policies and Standards

City of Belen

[www.belen-nm.gov](http://www.belen-nm.gov)





# City of Belen

## Information Security Policies and Standards

---

Consistent City Information Security Policies and Standards (ISPS) 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. Policies and Standards specifically addressed in the Overview are labeled.

#### 5. Policy and Standards

IS PS001 Information Security Responsibility	
IS PS002 Business Continuity and Disaster Recovery	
IS PS003 Intellectual Property	(Overview)
IS PS004 Policy Exception Management Process	
IS PS005 Sanction Policy	(Overview)
IS PS006 Security Incidents	(Overview)
IS PS007 User Accounts and Acceptable Use	(Overview)
IS PS008 Passwords	(Overview)
IS PS009 Data Facility Security	
IS PS010 Network Service	(Overview)
IS PS011 Web Site Guidelines	(Overview)
IS PS012 Workstation and Computing Devices	(Overview)
IS PS013 Server Computing Devices	
IS PS014 Protection from Malicious Software	(Overview)
IS PS015 Backup of Data	
IS PS016 Inventory and Tracking of Computing Devices	
IS PS017 Enterprise Firewalls	
IS PS018 Cellular/Smart Phone Use	(Overview)
IS PS019 Telephone	(Overview)
IS PS020 New and Remodeled Infrastructure Review	
IS PS021 Internet Use	(Overview)
IS PS022 City Email Services	(Overview)
IS PS023 Acquisition of Technology	(Overview)

# 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

---

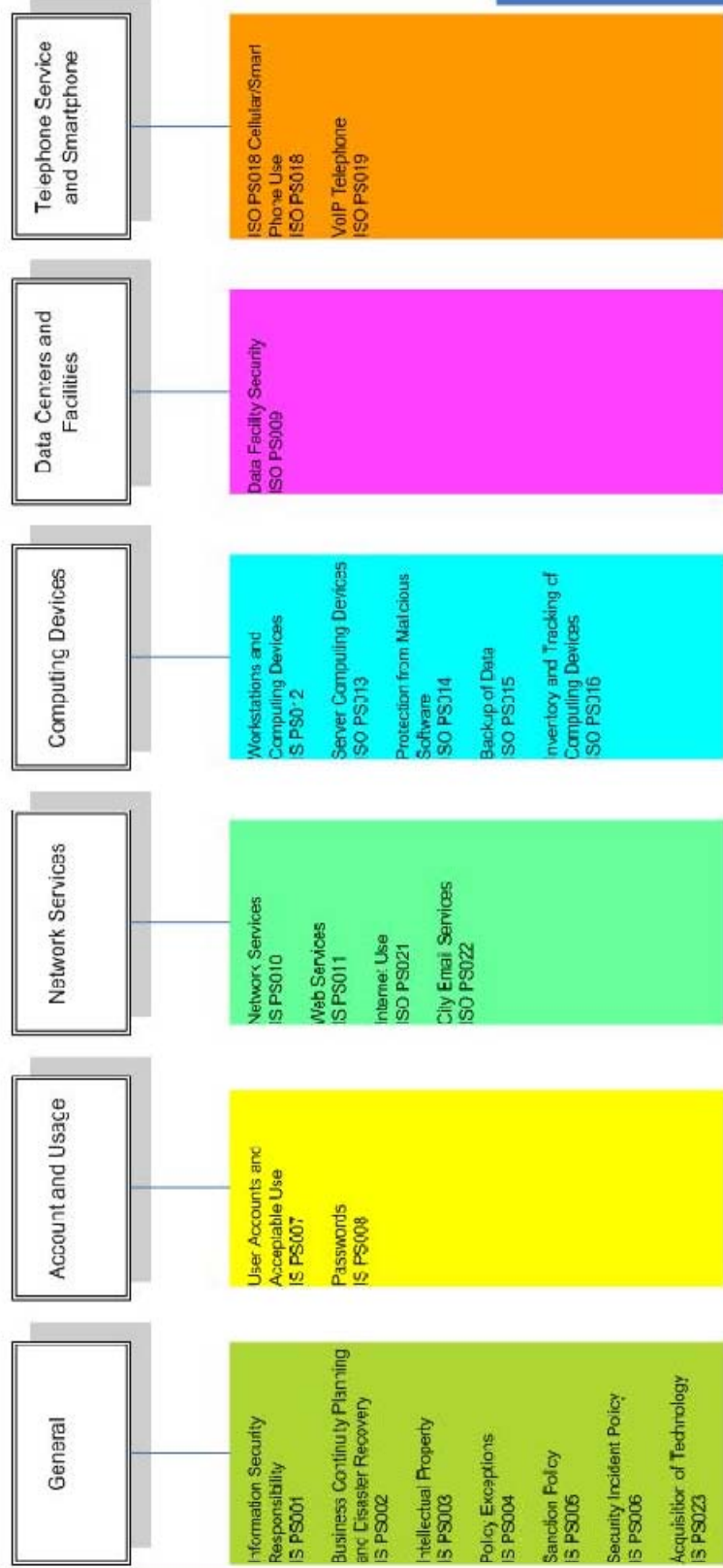
The policies and standards were divided into a framework of six basic areas:

- 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 ISPS 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

On initial implementation of these policies, two distinct documents will be presented to the employees of the City of Belen. The first document will be an Overview Summary of the ISPS and the second document is the Comprehensive ISPS.

# 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. Also referred to in the ISPS Document as the *IT Office*.

## 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 = Time of Crash to Time the system is operational (Tup - Tcrash)
- RPO = Time since the last backup of complete transactions representing data that must be re-acquired / (entered). (Tcrash - Tbackup)
- Lost business Time = (Tup - Tcrash - Tbackup)

**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 is 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]

# INFORMATION SECURITY POLICIES AND STANDARDS

## Overview

---

The following document is a overview of the Information Security Policies and Standards. Sections pertinent to the everyday use of Information Technology has been condensed and compiled into this IS PS overview. Refer to the main document, *Policies and Standards: Information Security Polices and Standards* for complete details on these and all 23 policies presented and approved in resolution 2010-19, August 16, 2010, Belen City Council Meeting.

### **INTELLECTUAL PROPERTY: IS PS003**

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.

### **SANCTIONS: IS PS005**

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.

#### **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 city 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 any 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.

## **SECURITY INCIDENTS: IS PS006**

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.

## **USER ACCOUNTS AND ACCEPTABLE USE: IS PS007**

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.

## **PASSWORDS: IS PS008**

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.

- Passwords to city accounts and devices must be kept confidential.
- Passwords will expire every 90 to 180 days.
- Domain and application passwords should 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 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.

## **NETWORK SERVICES: IS PS010**

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.

### ***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.

*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.

#### **WEB SITE GUIDELINES: IS PS011**

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.

- 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.

#### **WORKSTATIONS AND OTHER COMPUTING DEVICES: IS PS012**

All workstations and other computing devices shall:

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

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

## PROTECTION FROM MALICIOUS SOFTWARE: IS PS014

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.

- 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 *IS 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.
- 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.
- 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, anti-spyware and firewall 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.

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 *IS 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.

#### CELLULAR/SMART PHONE USE: IS PS018

The city provides a cellular phone and smart phones to the City Manager and Department Supervisors. Phones are also provided to staff within each department as the Department Supervisor deems necessary. The City of Belen contracts with cellular phone providers that have been approved by the State of New Mexico General Services Division.

- 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 Manager, 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. 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.

### **TELEPHONE: IS PS019**

The city provides phone service to all facilities. All voice communications are Voice over IP across the city wide network. 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. The phone system also allows for in-house control over add, changes and deletions of telephone hardware and users. The system also allows for integrated paging, hands free and desktop dialing.

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.

### **INTERNET USE: IS PS021**

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.

### *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.

### *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 shall 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 Office 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.

## **CITY EMAIL SERVICES: IS PS022**

The email system is intended for official city business. 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.

### *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*

An instructional video is available on the public share: \\Wdsharespace\public\Shared Instructions & Manuals\Email in the Workplace\89-223673 - Email in the Workplace.wmv

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.

### **ACQUISITION OF TECHNOLOGY: IS PS023**

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.