INFORMATION TECHNOLOGY POLICY

City of Brighton

Revision History

Version	Date	Author	Description of Change
V3	03/01/07	Margaret Brocklander	
V4	01/06/12	Margaret Brocklander	PCI
V5	02/02/15	Jeromy King	PCI, CJIS

Table of Contents

Security

1.1 Maintain an Information Security Policy

1.1.1 Purpose

Without strong security policies and procedures many of the layers of security controls become ineffective at preventing data breech. Unless consistent policy and practices are adopted and followed at all times, security controls break down due to inattention and poor maintenance. The following documentation policies address maintaining the City of Brighton security policies described above.

A strong security policy sets the security tone for City of Brighton and informs employees and vendors what is expected of them. All employees and vendors should be aware of the sensitivity of data and their responsibilities for protecting it.

Note: "Employees" refers to all individuals, temporary employees and personnel, and contractors and consultants.

1.1.1.1 Publish the Information Security Policy

- City of Brighton requires that the most recent version of the information security policy be published and disseminated to all relevant system users (including vendors, contractors, and business partners).
- The City of Brighton Information Technology policy must be reviewed at least annually to keep it up to date to be in compliance with policy changes such as PCI (Payment Card Industry), CJIS (Criminal Justice Information Systems) security policy, etc… and with any changes in the network environment.

1.1.1.2 Employee Facing Technologies

- City of Brighton must develop usage policies for all critical employee-facing technologies (e.g., remote-access technologies, wireless technologies, removable electronic media, laptops, mobile devices, e-mail usage and Internet usage).

1.1.1.3 Assign Information Security Responsibilities & Train Employees

- The City of Brighton's Information Technology policy and procedures must clearly define the information security responsibilities of both employees and contractors.
- Responsibilities of information security at City of Brighton must be formally assigned to a specific individual(s), position, or team.
- Specifically the following responsibilities must be assigned:
  - Responsibility of distributing the City of Brighton information security policies and procedures must be formally assigned to a specific individual(s), position, or team.
  - Responsibilities to monitor, analyze, and distribute security alerts and information.

- Generate detailed documentation security incident response and escalation procedures and formally assign the responsibility of creating and distributing these procedures to a specific individual(s), position, or team.
- Responsibility to administer users in the data network. Includes all additions, deletions and modifications to user access.
- Responsibility to monitor and control all access to sensitive cardholder data.

- A formal security awareness program must exist and participation is required for all employees working within the cardholder data environment.

1.2 Access to Information Resources

1.2.1 Purpose

City of Brighton facilitates legitimate access to information and information technology resources to facilitate normal business activities for all users of ***City of Brighton*** systems while at the same time reducing exposure to unauthorized access of both employees and non-employees.

1.2.2 Policy

It is the policy of the City that information resources will be used by the elected officials, officers, employees, staff and other Users of the City respect for the public trust through which they have been provided and in accordance with policy and regulations established from time to time by the City.

Access to the information resource infrastructure within the City, sharing of information, and security of such information, all require that each and every user accept responsibility to protect the rights of the City. Any User who, without authorization, accesses, uses, destroys, alters, dismantles or disfigures the City information technologies, properties or facilities, including those owned by third parties, thereby threatens the atmosphere of increased access and sharing of information, threatens the security within which Users may create and maintain records, and in light of this policy, has engaged in unethical and unacceptable conduct. Access to the networks and to the information technology environment of the City is a privilege and must be treated as such by all users of these systems.

1.2.2.1 Standard Practices, Generally

As more fully set forth herein, the following material outlines the City's position regarding several general issues in this area. The appropriate use of the City's Information Technologies is the responsibility of its Users who must all guard against abuses which disrupt and/or threaten the long-term viability of the information technology systems of the City. The City requires that all Users act in accordance with these responsibilities, this policy, relevant laws and contractual obligations, and the highest standard of ethics. The following, by way of illustration and not

limitation, are unethical and unacceptable, and just cause for taking disciplinary action up to and including revocation of a User's rights of access, denial of access, discharge, dismissal, and/or legal action, any activity through which an individual:

1. Violates any terms, provisions and conditions of these policies;
2. Assumes another person's identity or role through deception or without proper authorization;
3. Communicates or acts under the guise, name, identification, email address, signature, or indicia of another person without proper authorization, or communicates in the name of the City, its departments, other related entities or another person without the authority to do so;
4. Violates such matters as City license agreements and contracts or third party copyright or patent protection and authorizations;
5. Interferes with the intended use of the information technologies and resources;
6. Seeks to gain or gains unauthorized access to information resources;
7. Destroys, alters, dismantles, disfigures, prevents rightful access to or otherwise interferes with the integrity of computer-based information and/or information resources without authorization; or
8. Invades the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources without authorization.

This policy is applicable to all Users, whether at the City or elsewhere, and refers to all information technologies and resources whether individually controlled, or shared, stand alone or networked. Individual departments of the City may define "conditions of use" for facilities under their control. These statements must be consistent with this overall policy but may provide additional detail, guidelines and/or restrictions. Where use of external networks is involved, policies governing such use also are applicable and must be adhered to.

Information technology or resources referred to in this document are meant to include any information in electronic or audio-visual format or any hardware or software that make possible the storage and use of such information.

1.2.3 Basis

Many of ***City of Brighton*** employees rely on information and information technology to perform their job functions. Access to information resources should be reasonably simple, have integrity and maintain confidentiality. While security measures can sometimes complicate legitimate access, the consequences of security problems that result from unauthorized access can be severe and include:

- Time, effort and monetary resources to correct security problems
- Damage, deletion and compromise of critical data and information
- Damage to ***City of Brighton****'s* reputation

1.2.4 Data and Application Implications

- Department Directors are responsible for determining when the user accounts of ex-employees can be removed from the system and destroyed. Department Directors are also responsible for notifying the IT Department to carry out such actions.
- Employees should exercise precautions when sending or receiving information over the Internet to prevent viruses, worms, Trojan horses and other potentially damaging software.
- All computer files, including email, are City assets. Employees should be aware that computer files are not private and can be accessed or quarantined at any time by the ***City of Brighton***.
- ***The City of Brighton*** respects and adheres to all copyrights and licensing agreements.
- Department Directors are responsible for enforcing the terms of software agreements and preventing illicit software copying.
- Information Technology Department is responsible for testing and applying security patches and updates within one month of release.

1.2.5 Infrastructure Security Implications

- Access from remote locations and systems will be monitored and passwords changed on a periodic basis.
- Connections between computers on the ***City of Brighton*** network and computers outside the ***City of Brighton*** network must adhere to ***City of Brighton***'s firewall design.
- Access to the network from outside the firewall will only be allowed to those who require access to meet our business needs.
- Access to City of Brighton's information technologies, resources, computers and network, shall terminate upon the termination of service or employment of any official, or employee of the City. The City Manager or Department Director shall promptly inform the Information Technology Department of the termination and access will be removed. A Department Director may limit access for employees who are on leave of absence.
- Systems that connect to outside networks must be architecturally-compatible and secured.
- Information Technology Department will test and apply firmware and security updates within one month of release on all network devices.

1.2.6 Computer Security Implications

- Password security has been implemented and enforced.
- Department Directors are responsible for seeing that passwords for ex-employee accounts are changed or disabled promptly by sending an email to the Information Technology Department.
- User accounts will be disabled after 4 weeks of inactivity

- Account, file, and device access privileges, including file sharing on desktop computers, will not be turned on by default.
- Varying levels of access privileges will be applied to all systems.
- Remote access by vendors must be enabled only during the time period needed.

1.2.7 Physical Security Implications

- Restricted key or keyless entry access is enforced for all data center rooms and network access points.
- ***City of Brighton*** has the right to remove any computer from the network to ensure the integrity of the computer files.
- Sensitive and/or confidential records, including copies of, disks, tapes, or other portable media shall be kept in locked cabinets or rooms.
- When no longer needed, confidential and/or sensitive hard copy output must be shredded, not recycled.

1.2.8 Break-ins, Viruses, Worms, and Trojan Horse Implications

- ***City of Brighton***'s network and computers are routinely monitored for potential break-ins and security breaches.
- Information Technology Department reviews logs of all security problems daily.
- IT staff with use good judgment in publicizing security problems. Information will only be disseminated on a need-to-know basis.
- If a break-in is detected or a virus, worm, or Trojan horse infects ***City of Brighton***'s resources, IT staff is adequately prepared to take appropriate actions.
- All computers run current anti-virus software.

1.3 Information Technology Department Participation

All users of ***City of Brighton*** information technology systems must participate in Information security.

1.3.1 Basis

- Everyone must handle all information and information technology resources in a manner that doesn't compromise ***City of Brighton***'s Information Technology Department.
- ***City of Brighton*** owns all information produced by its employees in the conduct of the normal business and activities of the City.
- All files stored on a ***City of Brighton*** computer belong to ***City of Brighton***.

1.3.2 Employee Implications

- All employees are responsible for exercising sound business sense to maintain, protect, and share information and data except when doing so is for any reason necessary to conduct the normal business of the City.
- Employees should not share ***City of Brighton***'s information and data with people outside the City except when doing so helps achieve our business goals.
- Department Directors are responsible for their staff's appropriate use of ***City of Brighton***'s computers and related services.
- Failure to comply with ***City of Brighton***'s computer security is grounds for disciplinary action, including termination of employment.
- Employees will be permitted to use ***City of Brighton*** computers and services for personal use when such use does not interfere with the conduct of the normal business of the City; for-profit activities, activities in violation of these policies and unlawful or illegal activities.
- Storing City of Brighton data and information on personally-owned computers is not permitted. However, in the event unauthorized City data, information or software is installed or stored on a personally owned computer, the owner shall advise the City thereof and permit the Information Technology Department to remove the unauthorized data, information or software. If the City Manager or a Department Director has authorized the installation of City software or storing of City data or information on a personally owned computer, the owner of the computer shall permit a reasonable request by the City Information Technology Department for access to the computer, the City software, data and information thereon.
- Employees are responsible for protecting and destroying any ***City of Brighton*** data and information copied to any portable device, printed on faxes, and printed on printers.

1.3.3 Data and Software Implications

- IT Department is responsible for insuring that My Documents data on desktop computers is backed up regularly.
- ***City of Brighton*** has developed and implemented a comprehensive, tested backup procedure that includes making backups, storing backup material, and recovering data.
- Computer files, including email, created on ***City of Brighton***'s computer systems are ***City of Brighton*** property. They should not be considered private and may be searched at any time as needed.
- Posting to public bulletin boards or sending email to large distribution lists from ***City of Brighton*** computers may constitute publication.
- ***City of Brighton*** information, data, and software are not permitted on personally-owned computers. City of Brighton does require that information, data, and software stored on personally-owned computers be destroyed.
- Software may not be installed or downloaded. If new software is required contact the IT Help Desk for assistance.

1.4 Benefits, Risks and Costs

The cost of Information Technology Department measures are balanced against the risks and benefits involved.

1.4.1 Basis

- Security measures cost money, require personnel time, and inconvenience users and administrators of the services.
- The protection of the information technologies, data, information and systems of the City is necessary in the reasonable conduct of the business and activities of the City.
- Good judgment is necessary when balancing security concerns and business needs.

1.4.2 Implications

Costs may include:

- Extra hardware (Routers, Firewalls, Servers, etc…) with better filtering capabilities.
- Expansion of Infrastructure security.
- Operational costs to set up and run the equipment.
- Costs in convenience, productivity, and staff morale.
- Benefits may include protection of data critically important to ***City of Brighton***.

1.4.3 Identity Theft

1.4.3.1 Identity Theft on the Internet

Identity theft is on the rise. As defined by the Federal Trade Commission, identity theft occurs "when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes."

Victims of identity theft can spend a great deal of time and money cleaning up the mess made by thieves.

Identity thieves can obtain your personal information in lots of ways, including: from the trash, by hacking into computer systems where this data is stored, or from people with legitimate access.

Frequently, identity theft occurs on the internet via email or the web. A newer strategy employed by identity thieves, and seen frequently by ***City of Brighton*** employees, is called phishing (pronounced "fishing"). Phishing, as defined by anti-phishing.org, is:

Phishing attacks involve the mass distribution of 'spoofed' email messages with return addresses, links, and branding which appear to come from banks, insurance agencies, retailers or credit card companies. *These fraudulent messages are designed to fool the recipients into divulging personal authentication data* such as account usernames and passwords, credit card

numbers, social security numbers, etc. Because these emails look "official", up to 20% of recipients may respond to them, resulting in financial losses, identity theft, and other fraudulent activity.
You should always be wary of emails requesting personal information. Here are some steps you can take to help protect yourself from identity theft:

- Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves may pose as representatives of banks, Internet service providers (ISPs) and even government agencies to get you to reveal your SSN, mother's maiden name, account numbers, and other identifying information.
- Before you share any personal information, confirm that you are dealing with a legitimate Company. You can check the Company's Web site as many companies post scam alerts when their name is used improperly. Also, contact the Company through an address or telephone number you know to be genuine -- use the customer support number listed on your account statement or in the telephone book.
- If you receive an unexpected email saying your account will be shut down unless you confirm your billing information, do not reply or click any links in the email body.
- Before submitting financial information through a Web site, look for the "lock" icon on the browser's status bar. It means your information is secure during transmission.

For additional information on ID theft you can have a look at the Federal Trade Commission's web site:
http://www.consumer.gov/idtheft/

The anti-phishing site has information on the latest scams: http://www.antiphishing.org

1.5 Install and Maintain a Firewall Configuration

Firewalls are computer devices that control computer traffic allowed between City of Brighton's network (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within a company's internal trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet City of Brighton's specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connections such as business to business connections, via wireless networks, from less secure to more secure network segments on an internal City's network, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

1.5.1 Firewall/Router Configuration Documentation

City of Brighton will have documented Firewall/Router configuration standards that include the following:

A firewall must be present between each "public" network segment and the City's network. Public network segments would include the Internet.

- Firewall configuration documentation must contain the groups and/or individuals responsible for logical management of the firewalls/routers.
- Firewall configuration documentation must contain a detailed list of inbound and outbound services, protocols, and ports required for daily business. This list must contain a description and justification for use of the required services, protocols, and ports on all firewall interfaces.

1.5.2 Restrict Connections between Untrusted Network Segments and the City's network

City of Brighton will restrict connections from untrusted network segments to system components within the City's network environment.

Note: An "untrusted network" is any network that is external to the networks belonging to City of Brighton under review, and/or which are out City of Brighton's ability to control or manage (e.g., the Internet, connected vendor networks, public wireless networks).

- Firewall rules must limit all inbound and outbound traffic to/from the City's network to only that which is necessary for business.
- When wireless networking is used, require a firewall and/or strong ACL's (Access Control Lists) between any insecure wireless network and the City's network.

1.5.3 Prohibit Direct Public Access between the Internet and the sensitive networked Environment

City of Brighton will prohibit direct public access between the Internet and any system component in the sensitive networked environment by doing the following:

- Create a DMZ (using appropriate firewall configuration) to limit inbound and outbound traffic to only protocols that are necessary for the sensitive networked environment.
- Limit all inbound traffic to from the Internet to addresses within a DMZ.
- Direct network routes are prohibited (inbound or outbound) between the Internet and the segment of the sensitive network where sensitive data is persisted.
- Do not allow internal IP addresses (e.g., RFC 1918 address ranges) to pass from the Internet into the City's network.
- Outbound traffic from any sensitive networked environment zone must be explicitly authorized.
- Use firewall hardware that implements stateful inspection, also known as dynamic packet filtering.

- Hide the structure of your internal network from the Internet using technologies such as NAT (Network Address Translation), PAT (Port Address Translation), RFC 1918 address space, etc.

1.5.4 Personal Firewall Required on Mobile Computers

- Personal firewalls must be installed and active on all mobile and/or computers with direct connectivity to the Internet (for example, laptops used by employees)
- Personal firewall software is to be configured by City of Brighton to specific standards and is not alterable by computer users.

1.6 Change Vendor-supplied Defaults

System components used in sensitive networks often will come with default vendor settings (usernames, passwords, configuration settings, etc.). City of Brighton's general policy is to always change vendor-supplied defaults for system passwords or other security parameters before systems are installed in the secure network environment.

Individuals with malicious intent (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

1.6.1 Change Vendor-supplied Defaults

- All vendor-supplied defaults must be changed on all system components before being installed (Examples include: passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts, etc.)
- All default settings for wireless environments (equipment) connected to the City's network data must be changed before enabling the wireless system for production use.
- Require that all authorized City owned wireless devices be configured to support strong encryption technologies (i.e. WPA2/WPA2-Enterprise) for both authentication to the network and transmission of data on the corporate network.

1.6.2 Remove Unnecessary Functionality

- All unnecessary functionality or software is to be removed from system components.

1.6.3 Use Secure Protocols for Non-Console Access

- Strong cryptography must be used for any non-console and/or web-based management interface used for administration of systems and/or system components. (Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.)

1.7 Implement Strong Access Control Measures

Access to system components and software within the network environment must be controlled and restricted to those with a business need for that access. This is achieved through the use of active access control systems, strong controls on user and password management or dual factor authentication and restricting physical access to critical or sensitive components and software to individuals with a "need to know".

1.7.1 Assign a Unique ID to Access System Components

It is critical to assign a unique identification (ID) to each person with access to critical systems or software. This ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

1.7.1.1 Require Unique User IDs

- Unique IDs will be used for all users that access the City of Brighton network

1.7.1.2 Vendor Management Accounts

- Vendor accounts for remote or on-site maintenance are only created/enabled during the time period needed by the vendor and monitored by City of Brighton employee while being used, unless the vendor has read and signed the IT policy

1.7.1.3 System and Service accounts

- System and service accounts may be created for the purpose of what they are intended to do.

1.7.1.4 Restrict Access to Sensitive Data

Systems and processes must be in place to limit access to critical data and systems based on an individuals need to know and according to job responsibilities. Some sensitive may require stronger authentication methods.

"Need to know" is when access rights are granted to the least amount of data and privileges needed to perform a job.

1.7.1.5 Restrict Access to City of Brighton Systems

- Access to sensitive data and systems handling sensitive data must be restricted by business need to know.
- Role based access control systems must be in place on all systems in the cardholder data network. User ID's must limit users rights to only those necessary for their job classification and function.

- It will be the Department director responsibility to notify IT of a User role change so the proper access rights can be assigned necessary for their job classification or function.

1.8 Passwords

1.8.1 Policy

This policy applies to all ***City of Brighton "***Users". The term "users" applies to any person in ***City of Brighton***, third party contractors, guests, temporaries, licensees, as well as those who represent themselves as being connected – in one way or another – to ***City of Brighton*** who uses, possesses or has access to ***City of Brighton*** communications systems.

1.8.2 General

- All user-level passwords (e.g., email, desktop computer, local/domain, etc.) must be changed at least every 90 days.
- Passwords must not be inserted into email messages or other forms of electronic communication without using approved encryption software.
- All user-level and system-level passwords must conform to the guidelines described below.
- All local accounts (to the system) must conform to the guidelines described below.
- All application passwords must be generated randomly if not managed within the password management database. A standard, default password is not to be granted for all users or groups of users.

1.8.3 Guidelines

Some of the more common uses of passwords include: user level accounts, web accounts, email accounts, screen saver protection, and voicemail password.

Password construction;

- All passwords must contain at least nine (9) characters.
- Passwords must contain characters from three of the following four categories:
    - Uppercase characters
    - Lowercase characters
    - Base 10 digits (0 through 9)
    - Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Cannot reuse the last four passwords.

Weak passwords have the following characteristics:

- The password is a word found in any language (English, non-English, slang, jargon, proper nouns, etc.)
- The password is a common usage word such as:
    - Names of family members, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - Birthdays and other personal information such as addresses and phone numbers.

- Word or number patterns like aabbccdd, qwerty, zyxwvuts, 12344321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- Any of the above with some letters substituted (like passw0rd)
- Strong passwords have the following characteristics:
- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Contain numbers (0-9).
- Contain at least six characters.
- Is not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase.
- Password should never be shared with anyone for any reason. If an issue or situation arises that requires you to share your password, immediately change it at the first opportunity.

1.8.4 Password Management

Do not share ***City of Brighton*** passwords with anyone. All passwords are to be treated as sensitive, confidential information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't reveal a password to co-workers while on vacation
- In summation, don't talk about a password at all

If someone demands a password, refer them to this document or have them call the Information Technology Department.

Do not use the "Remember Password" feature of applications (e.g., Microsoft Internet Explorer, Microsoft Outlook, Mozilla Firefox, Chrome, Safari, etc.).

If you suspect an account or password has been compromised, report the incident and change all passwords.

Information Technology may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it. Password cracking and guessing are not to be performed by anyone outside of Information Technology Department or an approved 3rd party auditor.

1.8.5 Account Lockout

After five (5) consecutive failed login attempts, the account is locked for thirty (30) minutes or unlocked by an IT Technician

1.8.6 Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

- Support authentication of individual users, not groups.
- Must be encrypted on the screen.
- Should not cache the password in a cookie or any other local media format on the client system.
- Provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Should provide security capabilities for all sensitive data

1.8.7 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action which could include termination of employment.

1.9 Maintain a Vulnerability Management Program

System components within the City of Brighton networked environment must be part of an active vulnerability maintenance program. This program will control the existence of malicious software (e.g., anti-virus software) and provide policies covering development efforts and system or software updates/upgrades such that security is maintained.

The following policies ensure system components are protected from malicious software and vulnerabilities that result from software bugs and improperly patched applications and operating systems.

1.9.1 Anti-Malware Software

1.9.1.1 Purpose

Malicious software, commonly referred to as “malware”—including viruses, worms, and Trojans—enters a sensitive network segment during many business approved activities including but not limited to employees’ e-mail and use of the Internet, mobile computers, public

file sharing programs and storage devices, resulting in the exploitation of system vulnerabilities. Anti-malware (anti-virus) software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

1.9.1.2 Policy

This policy outlines how various viruses can infect the City's infrastructure, how the City of Brighton's IT department tries to prevent and/or minimize infections, and how the City's network users should respond to a virus if they suspect one has infected the City's network.

1.9.1.3 IT Responsibilities

City of Brighton's IT department fights viruses in several ways:

- Scanning Internet traffic—All Internet traffic coming to and going from our network must pass through City servers and other network devices. Only specific types of network traffic are allowed beyond the organization's exterior firewalls.
- For example, an email message that originates outside of the network must pass through the antivirus protection scanner before it is allowed to enter the email server. This device routes suspicious email and attachments to an isolated storage device, defeating the purpose of a virus.
- All anti-virus software and its associated definition files are to be kept up-to-date at all times.
- All anti-virus software must be actively running, and capable of generating audit logs.
- Anti-virus software audit logs must be retained for one year.
- Anti-virus software must be deployed on all systems on the City of Brighton's network that are commonly affected by malicious software. This includes personal computers, servers, etc. that are attached to the City's network segment.
- Anti-virus programs must capable of detecting, removing, and protecting against all known types of malicious software (adware, spyware, etc.).
- Running server and workstation antivirus software—all vulnerable servers run antivirus scanning software. This software scans our file-sharing data stores, looking for suspicious code.
- The antivirus protection software is also installed on all organization workstations. This software scans all data written to or read from a workstation's hard drive. If it finds something suspicious, it deletes the dubious file on the computer.
- Even though all Internet traffic is scanned for viruses and all files on the company's servers are scanned, the possibility still exists that a new or well-hidden virus could find its way to an employee's workstation, and if not properly handled, it could infect the City's network.
- The IT staff will attempt to notify all users of credible virus threats via email or telephone messages. Because this notification will automatically go to everyone in the organization, employees should not forward virus-warning messages. On occasion, well-meaning people will distribute virus warnings that are actually virus hoaxes. These warnings are typically harmless; however, forwarding such messages unnecessarily increases network traffic.

1.9.1.4 User Responsibilities

- As stated, it is the responsibility of all City network users to take reasonable steps to prevent virus outbreaks. Use the guidelines below to do your part:
- Do not open unexpected email attachments, or click on links inside emails even from coworkers or any other unsolicited email.
- Never open an email or instant messaging attachment from an unknown or suspicious source.
- Never download freeware or shareware from the Internet without express permission of the IT department.
- If a file you receive contains macros that you are unsure about, disable the macros.
- Notify the Information Technology Help Desk of suspicious files
- If you receive a suspicious file or email attachment, do not open it. Call the Information Technology Help Desk at extension 2057 and inform them that you have received a suspicious file.
- If the potentially infected file is on a disk that you have inserted into your computer, the antivirus software on your machine will ask you if you wish to scan the disk, format the disk, or eject the disk. Eject the disk and contact the Information Technology Help Desk at extension 2057.
- If the file is an infected spreadsheet or document that is of critical importance to the City, the Information Technology Department will attempt to scan and clean the file. The Information Technology Department, however, makes no guarantees as to whether an infected file can be totally cleaned and will not allow the infected file to be used on City's computers.

1.9.2 Develop and Maintain Secure Systems and Applications

Individuals with malicious intent use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities can be fixed by applying vendor-provided security patches. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of sensitive data by individuals with malicious intent and the use of malicious software.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, the introduction of vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

1.9.2.1 Regularly Update Systems and Software

- All system components and software must have the latest vendor-supplied system security patches installed.
- All critical system and software patches must be installed within 30 days of vendor release.

- All installed software must be within two versions of the latest released vendor software.

1.9.3 System Administrator Duties

Tier 3 administrators are to subscribe to outside sources for security vulnerability information and system configuration standards are to be reviewed and updated as new vulnerability information might dictate. Outside sources might include: SecurityFocus, A/V companies, SANS, CIS, Secunia, MS-ISAC, Microsoft, etc.

1.9.4 Protect Exposed Web Applications

All publicly exposed web applications used to store, process, or transmit sensitive data must be protected by a web application firewall that actively filters malicious traffic to prevent web-based attacks.

1.9.5 Regularly Monitor/Test Sensitive Data Networks

Important components of overall system security are the regular testing of networks for exposed vulnerabilities and the continuous monitoring of security indicators (logs, system events, etc.). The following policies address system monitoring and vulnerability testing.

1.9.5.1 Track and Monitor Access to Network Resources/Data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

1.9.5.2 Monitor System Components Within the sensitive Network

- Enable audit trails (active system tracking logs) on all system components within the sensitive network (e.g., server event logs, web server logs, firewall logs, payment application logs, etc.).
- Retain audit trail logs for 12 months.

1.9.6 Regularly Test Security Systems and Processes

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software must be tested frequently to ensure security controls continue to reflect a changing environment.

1.9.6.1 Rogue Wireless Network Detection

A wireless analyzer must be used at least quarterly to detect unauthorized wireless networks/devices within the network environment.

1.9.6.2 Vulnerability Assessment Scans

- Internal vulnerability assessment scans must be performed at least quarterly and after any significant change in the City's data network (e.g., changes in firewall rules, or upgrades to products within the environment, etc.).
- External vulnerability scans are to be performed at least quarterly and after any significant change in the City's data network (e.g., changes in firewall rules, or upgrades to products within the environment, etc.). An Approved Scanning Vendor (ASV) must conduct all scans. Scans must be run on all external IP addresses that could be used to gain access to the cardholder data environment.
- Systems failing a vulnerability assessment scan (either internal or external) are to be remediated and retested until a passing scan is achieved.
- Results of each quarter's internal and external vulnerability assessments are to be documented and retained for review.

Software Installation Policy

2.1 Introduction

Controlling software installed on enterprise end-user devices is not only a best practice for cost control, but also a potential issue of legal or regulatory compliance. Installation of unauthorized computer programs and software, including files downloaded and accessed on the Internet, can easily and quickly introduce serious, fast-spreading security vulnerabilities. Unauthorized software programs, even those seemingly provided by reputable vendors and trusted companies, can introduce viruses and Trojan programs that aid hackers' attempts to illegally obtain sensitive, proprietary, and confidential data. Protecting the City's computers, systems, data, and communications from unauthorized access and guarding against data loss is of paramount importance; adherence to the following Software Installation Policy serves a critical role in the process.

2.2 Purpose

The goal of the IT Department is to provide stable technology solutions that both perform well and appropriately address business needs. A lack of standards regarding what software titles can be installed on company end-user devices, including desktop and laptop machines, can hinder provision of excellent service to all end users and departments.

The purpose of this Software Installation Policy is to address all relevant issues pertaining to appropriate software installation and deployment on the City of Brighton's end-user computing devices.

2.3 Policy

Employees may not install software on the City’s computing devices that is owned and operated by the City of Brighton.

2.3.1 The IT Department expressly forbids installation of the following software

- Privately owned software.
- Non-Approved Internet downloads.
- Pirated copies of any software titles.
- Any title not approved by the IT Department

2.3.2 Software Requests

All new software requests must be submitted through an IT work order ticket. It is the responsibility of the IT Department to ensure the new software does not duplicate other licensed software and the City is in compliance with licensing agreements and fees. Once approved by the IT Department, IT will gain approval by the appropriate Department Director. The IT Department reserves the right to reject any software installation request for any reason.

2.3.3 Software Installation

Software titles are to be installed on City owned equipment by the IT Department. All Software installed on the City's systems (Including all commercial and shareware products) must be used in compliance with all applicable licenses, contracts, notices and agreements.

The IT Department reserves the right to uninstall any unapproved software from a city-owned machine.

2.4 Software Audits

The IT Department reserves the right to monitor software installation and usage on the City's end-user computing devices. The IT Department will conduct periodic audits to ensure compliance with this Software Installation Policy. Unannounced, random spot audits may be conducted as well. During such audits, scanning and elimination of computer viruses may also be performed. Other unsanctioned software may also be uninstalled at this time.

Photo Identification Cards

3.1 Purpose

The City of Brighton identification card identifies you as a current employee and/or contractor of the City of Brighton. Depending on the business, your ID card can also be used as an electronic door key and to access a variety of functions and facilities based on a "Need to know" access.

3.2 Scope

This policy applies to all individuals including but not limited to, City employees, officials, volunteers, contractual workers, visitors, vendors, etc.

3.3 Policy

The City issued Photo Identification Card shall contain the employee's picture, name, department and title. This Identification card shall remain the property of the City of Brighton and is non-transferable.

All on-duty City employees are required to wear their City issued Photo Identification Card. This Photo Identification will be worn face forward in full view, on or over the outermost garment, at or above the waist, at all times. City employees who are off-duty, but who are entering into an area within a City building or facility in which the public doesn't normally have access must wear their City issued Photo Identification Card in accordance with this policy.

Each department will be responsible for ensuring that Photo Identification Cards are worn as required. Upon approval by the Department Director or his/her designee, individual departments may exempt their employees from wearing their Photo Identification out in the field if those employees are required to wear a uniform that clearly identifies them as a City employee. These employees; however, are required to carry their Photo Identification Card while in the field in order to provide further identification.

Under no circumstances should an employee permit others to use his or her Photo Identification Card. Nor should any employee use the Photo Identification Card of another person.

When entering a secured area in a group of two or more, each employee must display his or her Photo Identification Card. Non-employee visitors must wear a visitors badge and must be accompanied by an employee wearing a Photo Identification Card when entering secure areas or during non-business hours.

No attachments such as: pins, stick-on emblems, or awards will be allowed on the Photo Identification Card, as this interferes with the access card readers and may obstruct clear identification.

Noncompliance of this policy may result in disciplinary action up to and including termination.

3.4 Procedure to obtain a Photo Identification Card

3.4.1 New Employee

New employees will be photographed and issued an Employee Photo Identification Card at the Police Department immediately following their benefits orientation, on their first day at work. The hiring supervisor will complete the Photo Identification Card section on the New Employee Request form with the type of access and submit to the IT helpdesk.

3.4.2 Current Employee

Current employees who have not been photographed for an Employee Photo Identification Card should contact the Police Department Operations Administrative Assistant x2309 to schedule an appointment to be photographed.

3.4.3 Volunteers, Contractors, etc. (Non-employees)

Contractors, volunteers, etc. working on-site are required to obtain a Photo Identification/Access Card. The supervisor will complete the Photo Identification Card section on the New Employee Request form and submit to the IT helpdesk for the non-employee to be photographed and issued a Photo Identification Card. The non-employee must have a picture ID (such as a driver's license or student ID card) with them to obtain their City Photo Identification Card.

3.4.4 Terminated Employee

Upon termination of employment, leave of absence, or change from active employee status, the Photo Identification Card must be surrendered to the employee's supervisor. The supervisor shall immediately notify the IT helpdesk, HR and if appropriate, the Police Department, to deactivate the Photo Identification Card. The Photo Identification Card must be returned to IT helpdesk.

3.5 Procedure to request a replacement photo identification card.

Accountability for issued Photo Identification Cards rests with the individual to whom it is assigned. Employees should protect the security of their Photo Identification Card, like they would with their personal house keys, driver's license, etc., knowing they are protecting City property and personnel.

3.6 Procedure to request key card access

The Department Director or it designee will need to complete the New Employee/Change request form to either grant access or change access based on their "need to know" and submit it to the IT Help Desk.

3.7 Lost or Stolen Photo Identification Cards

Report your missing Photo Identification Card immediately to the IT helpdesk and your Department Director.

Security Incident Policy

4.1 Purpose

The purpose of this policy is to establish a standard for escalating, reporting and resolving Information incidents. The Information Technology Department will escalate potentially sensitive information incidents and issues to the City Manager's Office.

4.2 Scope

This policy applies to all **City of Brighton** "Users." The term "users" applies to any person (City of Brighton, third party contractors, temporaries, guests, licensees or invitees, as well as those who represent themselves as being connected – in one way or another – to **City of Brighton**) who uses, possesses or has access to communications systems and equipment.

4.3 Policy

It is a violation of this policy for a User to access or monitor or attempt to access or monitor any City data, records or record systems for which he or she has not been granted access. It is also a violation of the policy if the User has been granted access to specified data and records and the User has accessed or attempted to access the data, records or record systems for purposes other than the purposes for which the User was granted access.

4.4 *Incident Reporting*

All users shall promptly report to the Information Technology Department a serious information security incident which may include (but not limited to):

a. Attempted or successful unauthorized access, use, disclosure, modification or destruction of information;
b. Interference with information technology operations;
c. Unauthorized use of systems or data;
d. Unauthorized change to computer or software;
e. Loss or theft of equipment used to store public, confidential or potentially sensitive information;
f. Interference with the intended use of information technology resources;
g. Compromised user account;
h. Potential unauthorized disclosure of personally identifiable information such as personnel records, birth dates, social security number, credit card numbers, and any other information designated as sensitive by the City and the Information Technology Department;

i. Violations of the City of Brighton Code of Ethics;
j. Misuse, misappropriation or loss of the City's computing assets;
k. An incident that may pose a threat to City records, resources and Information
l. Technology processes and resources;
m. May cause severe disruption to critical City and Information Technology services; and

Is a violation of explicit or implied acceptable usage standards and policies.

4.5 Resolution

Information Technology Department will confer on the referred matter as soon as possible to identify the potential risks/exposure and potential responses. **City of Brighton** Information Technology Department will engage City Manager's Office and other internal departments, as appropriate, in determining the appropriate course of action.

4.6 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5 Internet Usage and Mail Services Policy

5.1 Purpose

To communicate Management objectives for the acceptable use of City-provided electronic mail and Internet/Intranet services by all employees and agents ("Users") of **City of Brighton**.

5.1.1 Policy

5.1.1.1 City Business

City-provided electronic mail and Internet/Intranet services are valuable business tools that enhance productivity and communication, but these tools cannot be abused. While incidental and occasional personal use of City-provided electronic mail and Internet/Intranet services are permitted, they are valuable City resources and must not be used for personal solicitation of non-City business, advancement of individual views, or illegal activity. All use and product of such use, including emails, is the City's not the individual's.

5.1.1.2 *Confidentiality*

Electronic information on the City-provided electronic mail and Internet/Intranet services is an asset of **City of Brighton**, not the individual User. The City has the right at all times to monitor all electronic activity and information on the City-provided electronic mail and Internet/Intranet services. This Policy serves as notice to each User that the City may monitor activity on City-provided electronic mail and Internet/Intranet services without any advance notification to or consent by the User. The City reserves the right to disclose any information or communication transmitted or received using the City-provided electronic mail and Internet/Intranet services as may be appropriate, including disclosure to City Manager's Office and law enforcement.

5.1.1.3 *Controlled and Prohibited Activities*

All information posted on the Internet representing **City of Brighton** must be approved by the appropriate City Department Director, Public Information Office and consistent with the City's policy for communicating information to the public. Only specifically authorized management may send broadcast messages to all email Users i.e. Dist: Everyone.

5.1.1.4 *Prohibitions:*

- Creation of Web pages or information sites without appropriate written approval.

- Posting statements representing or purporting to represent the City on the Internet or Intranet.
- The generation or circulation of any form of "chain letter" or other nonprofessional communication.
- Use of the City-provided electronic mail and Internet/Intranet services to transmit information on behalf of any City or entity other than **City of Brighton**.
- Use of pseudonyms to disguise the identity of a sender.
- Postings to “message boards” about business or individuals within **City of Brighton** or any opinions about **City of Brighton** or individuals within **City of Brighton**.
- Communications on the City-provided electronic mail and Internet/Intranet services should be professional and should not contain any pictures, materials, comments, language, links or anything else that might be considered inappropriate or offensive.
- Communications on the City-provided electronic mail and Internet/Intranet services should be professional and may not contain any pictures, materials, comments, language, links or anything else that is threatening, obscene, unlawful, or which may be considered inappropriate or offensive.
- Use of proxies or services that by-pass the City controls for Internet content and message filtering.

5.1.1.5 ***Illegal Activities***

Illegal activities, such as harassing other users, accessing or distributing threatening or obscene material, the intentional spread of computer viruses or other destructive information, malicious service disruption, unauthorized attempts to break into any computer system or use resources or access or destroy data belonging to the City or any other City or individual, or unauthorized use or retrieval or distribution of copyrighted material are strictly prohibited. Any illegal use of City-provided electronic mail and Internet/Intranet services will subject the user to prosecution to the full extent of the law. Users can also be held personal liable for any and all damages caused by such activities and may be subject to immediate discharge.

5.1.1.6 ***Security***

Access to the City-provided electronic mail and Internet/Intranet services must be approved. Only City-approved software may be used when connecting to the Internet through the City's network. Before access to the City-provided electronic mail and Internet/Intranet services will be granted, the User is required to acknowledge receipt and understanding of this policy by accepting the user acceptance every time they log into City owned equipment. Account Ids and passwords for the Services are strictly for the use of the registered User and should not be shared or made accessible to others. Under circumstances in which passwords must be provided to others to gain access to the computer, such as system maintenance or repair, a new password should be created and used after the completion of that process. Computers capable of live access to the City-provided electronic mail and Internet/Intranet services should not be

left unattended. Sensitive City information must be protected while being transmitted over the Services.

5.1.1.7 ***Misaddressed Messages***

Recipients of messages or information inadvertently sent or misaddressed to them should not copy, retain or disclose the contents of such messages. It is the policy of the City that such messages should be deleted and the sender should be notified, if possible, that the message was misaddressed or misdirected.

Email is considered by the City to be a non-permanent form of communication and messages should be promptly deleted after use. Email messages stored in folders or archived should be maintained only so long as they remain in use and should thereafter be deleted unless otherwise directed by the City.

5.1.1.8 ***Accountability***

Every employee at each level is strictly accountable for the enforcement of this policy. Users and their Department Directors are strictly accountable for the accuracy and appropriateness of links and information available from the User's Internet sites.

5.1.1.9 ***Policy Owner/Contact***

This Brighton Information Technology Policy shall be monitored by the City's Director of Information Technology. Violations of the Policy shall be reported to the appropriate Department Director and if necessary to the City Manager. Questions regarding this policy should be directed to the Director of Information Technology.

5.2 Internet Usage

5.2.1 Internet Use Policy

- Any harmful executable software downloaded from non-City of Brighton sources via the Internet is not permitted.
- Not to place City of Brighton material (software, internal memos, etc.) in any location, on machines connected to City of Brighton internal networks or on the Internet, unless the persons who have access to that location have a legitimate need-to-know;
- Be aware that all publicly writable directories on City of Brighton Internet-connected computers can be reviewed and cleared each evening;
- Be aware that all internet traffic is recorded;
- Not to use the Internet for commercial purposes such as advertising, marketing, or business transactions without approval of City of Brighton management;

- Not to create, modify, execute, or distribute any computer program or instructions intended to obscure the true identity of the sender of electronic mail or electronic messages;
- Not to probe security measures at either City of Brighton or other Internet sites unless you have first obtained permission from City of Brighton;
- Not to send or disclose City of Brighton secret, proprietary, or confidential information over the Internet;
- Not to sell or transfer any City software, documentation or any other internal information to any non-City of Brighton party for any purposes other than business purposes expressly authorized by management;
- Not to participate in pirated software, music exchanges, or other non-business related newsgroups, chat rooms (including but not limited to: USENET, web forums, blogs, etc.), and FTP sites; and
- Not to participate in peer-to-peer applications (including but not limited to: WinMX, Kazaa, Bearshare, Morpheus, eDonkey, etc.).

City of Brighton Web Site

6.1 Policy

The City of Brighton web site is an effective tool in making City information and services easily and conveniently available to a variety of publics, primarily for the residents, businesses and other taxpayers of the City of Brighton. This policy delineates the processes and procedures related to establishing and maintaining site content. It also provides guidelines for the review of material prior to its posting on the web site.

Each department page shall have a clearly defined purpose that supports the mission of the City of Brighton and the department. Non-copyrighted material, text, clip art, hypertext links or images may be used only if they directly relate to the mission. Information requiring additional protection, information not approved for public release or information of questionable value to the public should not be placed on the site. For the purpose of preventing duplication of content on the site, the site should be limited only to information for which the establishing department is responsible.

6.2 Objectives

The City of Brighton web site shall:

- Provide information and services that meet the needs of the external publics it serves.
- Offer functional and visual design consistency.
- Offer levels of security consistent with its function.
- Offer up-to-date information.
- Enhance the delivery of information and services provided by the City.
- Offer a level of quality consistent with levels of quality of the City departments/divisions/offices it represents.
- Reflect positively on city government operations, city officials and staff

6.3 Responsibilities

6.3.1 Domain

The City domain shall be the sole source of Internet representation for all departments, divisions, offices, services of the City of Brighton. The site will be located under the domain address of www.brightonco.gov.

6.3.2 Responsibility

The City Manager and the Public information Office will be responsible for the overall supervision of the web site, including creating and managing user accounts. It is the responsibility of the web authors, appointed by Department Directors, to oversee the individual pages, content posted and maintain up-to-date information posted by

department representatives. If a web author assignment changes, the department director should notify the Public Information Office. All training on the content management software should be coordinated through the Public Information Office.

6.4 Content

Material posted to the web site shall be representative of the professionalism, ethics and level of service of the City of Brighton. Material shall be posted to the web site to inform, educate and/or better serve the citizens of Brighton. Material posted to the web site, whether prepared internally or by outside contractors, shall conform to the provisions of this policy.

Individual departments, divisions, offices, services shall be responsible for posting and maintaining the general content of their respective areas of the site. These same persons shall be responsible for periodic review of their material on the web site and be responsible for updating out-of-date material. Material that is inaccurate, out-of-date or incomplete shall be corrected, updated or removed in a timely manner along with all related links. Persons responsible for posting content shall not in any way access or modify any areas of the web site outside their area of responsibility.

The Public Information Office will closely monitor content and may contact department web authors to correct or update information posted on their department pages. All content should adhere to the City of Brighton website guidelines.

6.5 External Organizations

External organizations shall not be represented on the City of Brighton site except as they relate directly to the objectives stated herein or to the operation of City of Brighton government and/or the web site itself.

7 Instant Messaging Policy

7.1 Guidelines for Instant Messaging Use

- Employees are permitted use of Instant Messaging (IM) for business related work only.
- Accessing, contributing and downloading of pirated software such as application, music, games, movies, etc. is prohibited.
- File transfers are not supported.
- Use of offensive language and/or derogatory comments to any individual or group is prohibited.

8 General Computer Usage

8.1 Purpose

A computer is defined as any system, server or workstation, that runs an operating system, including imbedded, that is but not limited to Microsoft Windows, Linux, UNIX and Macintosh. Information on computers should be protected from disclosure to, modification of or theft by unauthorized persons, and controls should be in place to minimize loss or damage.

8.2 Guidelines

- Where appropriate, paper and computer media should be stored in suitable locked cabinets when not in use, especially outside working hours.
- Users should not store confidential information on City issued computers. File servers should be used to store confidential information since appropriate access restriction can be applied for such confidential data. Availability of information is also ensured by regular backup at the server level.
- Users should not download, install or store games on their computers.
- Sensitive or classified information, when printed, should be cleared from printers immediately.
- The following control measures should be undertaken by the users to secure City issued computers from unauthorized access:
    - The City computers are configured to lock after 15 minutes of idle time. However, users should terminate or lock their logon session if they are leaving the desktops unattended.
    - Remote access sessions will be disconnected after 15 minutes of inactivity.
    - Hard disk(s) of the personal computer cannot be shared. In the event sharing is required, then the hard disk will be shared by an access control list with no open shares.
- The usage of personally owned PCs or laptops in the office is not permitted.
- The use of non-approved Wireless Access Points (WAP) or non-approved wireless network adaptors for the purpose of communicating with other computers or networked devices is prohibited and not supported.
- Information Technology Department will scan for non-approved wireless and network technologies. Any non-approved wireless and network technologies will be confiscated immediately upon discovery. Violation shall be reported to the appropriate Department Director and the City Manager.

This policy defines the minimum training for users on the network to make them aware of basic computer threats to protect both themselves and the network. This policy is designed to protect the City's resources on the network and increase employee efficiency by establishing a policy for user training. When users are trained about computer use and security threats, they work more efficiently and are better able to protect organizational resources from unauthorized intrusion or data compromise. This policy will help prevent the loss of data and organizational assets.

8.3 Training Categories

Training categories will include but not be limited to the following areas:
Computer Basics
Excel
Outlook
PowerPoint
Project
Windows
Word
Access

Training categories as listed above are provided internally by the City and include on line training and instructor led training.

8.4 Requirements

All organizational staff shall make measurable and continuous progress in the training areas listed above. Each Department Director shall be responsible for ensuring that employees under their supervision make progress in the required training areas. Each employee must retain knowledge about training in areas listed above within the first year of employment.

8.5 New employee orientation

When new employees join the City of Brighton they are required to meet with an IT Staff member before receiving a user name and password to the City's systems. It is the responsibility of the Department Directors to contact the IT Department's Help Desk to schedule an orientation prior to the employee's first day.

New employee IT orientation will include:

- Overview of IT products and services
- How do I contact IT
- Copy of the IT organization chart
- Overview of using the phones
- Phone documentation
- User ID & passwords to systems
- Available Training overview
- Overview of email provided
- Review IT Policies

- Acceptable Use Acknowledgement Statement Form

Change Management

9.1 Purpose

The Change Management Process is designed to provide an orderly method in which changes to the IT environment are requested and approved prior to the installation or implementation. The purpose is not to question the rationale of a change, but to ensure that all elements are in place, all parties are notified in advance, and the schedule for implementation is coordinated with all other activities within the organization.

9.2 Scope

Change Management provides a process to apply changes, upgrades, or modifications to the IT environment. This covers any and all changes to the hardware, software or applications. This process also includes modifications, additions or changes to the LAN/WAN, Network or Server hardware and software, and any other environmental shutdowns. The process is for any change that might affect one or all of the environments that the users rely on to conduct normal business operations.

Changes to the IT environment arise from many circumstances, such as:
Periodic maintenance,
User requests,
Hardware and/or software upgrades,
Acquisition of new hardware and/or software,
Changes or modifications to the infrastructure,
Environmental changes,
Operations schedule changes,
Changes in hours of availability, and unforeseen events.

9.3 Change Management Process

IT Staff is responsible for pro-active planning in managing the environments. Change Requests should be submitted as soon as all planning has been completed, but no later than the 48 hours prior to the scheduled change. Hardware, software, applications, LAN/WAN, network or server hardware and software modifications, additions or changes requires IT Director approval.

The Change Request must include enough detail so that all areas know the relative impact of the change and how it may affect other areas.

9.4 Definitions

Emergency change exists only as a result of:
a customer is completely out of service,
there is a severe degradation of service needing immediate action,
a system/application/component is inoperable and the failure causes a negative impact,
a response to a natural disaster, or a response to an emergency business need.

All emergencies are handled on an as-required basis with the approval of the IT Director and the change notification shall include at a minimum, the following information:
Will the change cause an interruption in service?
What additional customers will be affected and who needs to be notified by the Help Desk?
What is the possible work around until the problem is resolved?
What is the approximate length of the outage?
Notify all users affected when resolution has been reached.
Completion of an IT work order to accurately describe the outage.

Emergencies after normal business hours, on the weekend or holidays, will be resolved immediately after reporting to the IT Director and Help Desk. A IT work order ticket will be generated and Help Desk will notify affected customers, as applicable. A completed Change Request Form must be submitted through the regular reporting process on the first work day immediately following when the change was made.

The IT Director will review all emergency submissions to ensure the change met the criteria for an "emergency change" and to prevent the process from becoming normal practice to circumvent the Change Management Process.

9.5 Change Requester

It is the primary responsibility of the requestor to evaluate the change prior to submission. The Change Requester's responsibilities include the following tasks:
Perform risk benefits/risk analysis.
Verify that all equipment, software, hardware, and updates are available.
Research the requirements to achieve a successful change (required patches and stability of upgrade).
Evaluate the impact to the system/network and to the customers.
Document and coordinate a fallback plan. This should explain the steps that must be taken to restore access in the event that the change has a negative impact.
Develop a plan of action to reduce the risk to an acceptable level.
Develop a plan of action to lessen the effects on the customer if the change should cause an outage.

Once the request is approved:
Ensure that the customer is aware of any possible impact.
Coordinate proper on-site or on-call support as needed to resolve any problems or answer any questions that may occur during installation, or immediately subsequent to installation. Contact names and numbers should be available to support staff to obtain additional or outside support.
Report unplanned outages or problems immediately to the IT Director.

9.6 Unplanned outages

All unplanned outages shall be reported to the IT Director immediately and updated with an IT work order ticket. For any major outages, an Outage Review report will be available within 36 hours of the resolved outage. The Outage Review will include such

information as the type of outage, down time, customers affected, and resolution. Provide accurate details of the problem and resolution in the IT work order ticket to facilitate the reporting process.

9.6.1 A Guideline for an Internal Checklist

- Risk benefits/risk analysis has been completed.
- All equipment, software, hardware, and updates are available.
- Requirements to achieve a successful change (required patches and stability of upgrade) have been researched.
- The impact to the system/network and to the customers has been evaluated.
- Fallback plan is documented. This plan explains the steps that must be taken to restore access in the event that the change has a negative impact.
- Plan of action to reduce the risk to an acceptable level has been completed.
- Plan of action to lessen the effects on the customer if the change should cause an outage is completed.
- Change Request Form is complete, concise, includes a detail description, and is submitted on time.
- If approved, customer has been notified of any possible impact.
- On-site or on-call support as needed to resolve any problems or answer any questions that may occur during installation, or immediately subsequent to installation has been coordinated. Contact names and numbers have been made available to obtain additional or outside support.

9.6.2 Types of Changes:

Following are examples of candidates for Change Management.

- Computing Systems Hardware: Hardware changes, additions, deletions, re-configurations, re-locations, preventive, or emergency maintenance.
- Computing Systems Software: Product releases, versions, I/O monitors, traps, or changes to priority mechanisms, job classes, and print classes.
- Environmental: UPS systems, air conditioning.
- Network Systems: Additions, modifications, lines, modems, routers, network access, controllers, servers, protocol converters. Software components either distributed or centralized, router software, printing routines, servers.
- Applications: Implementation of new applications, new systems, new releases, or modifications.
- Workstations: Changes in hours of availability, hardware configurations, operating systems, utilities, applications including release levels or versions, installations or de-installations of systems, servers.

10 Backups

10.1 Overview

This policy defines the backup policy for computers within the organization which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, app server, mail server, and the web server.

10.2 Purpose

This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

10.3 Definitions

- Backup - The saving of files for the purpose of preventing loss of data in the event of equipment failure or destruction.
- Restore - The process of bringing off line data back from the offline media and putting it on an online storage system such as a file server.

10.4 Disk Storage

The City of Brighton will store six (6) weeks of backups.

10.5 Disk Storage Locations

Original backups are stored locally and a duplicate copy is stored offsite.

11 Confidential Information Protection

11.1 Purpose

The protection of confidential information is critical to any business in defining and maintaining success. These information assets include:

Employee Information

- Personnel data (privacy data)
- Payroll and financial data
- Human Resources actions
- Performance review data
- Benefits and health plan data and actions
- Manager-employee personnel correspondence and actions

Sensitive and Proprietary Information

- City business strategies and plans until released to the public
- Security or Operational Vulnerability Assessments
- Safeguards and Security Controls
- Customers lists and customer information
- Security Investigations related information
- Passwords, security control codes, access codes, security mechanisms for systems, networks and applications
- Physical and Logical protection processes and procedures
- Financial information which has not been officially submitted for public release
- CJI (Criminal Justice Information)
- Cardholder Card Data
- Any other information that has value, and is not generally public

Confidential information can be presented or stored in many forms, including but not limited to: paper documents, information on electronic storage media, information passed by voice, charts and graphic presentations, audio and video tapes, and email. In any form, it must be protected.

11.2 Scope

This policy applies to all employees, contractors, temporary workers, and business partners of City of Brighton and its subsidiaries, worldwide. It applies to proprietary and confidential information in all forms and expressions, developed, owned, and maintained by and for City of Brighton.

11.3 Definition

Confidential information is defined as any data, whether it be technical, financial, operational, or strategic, that if improperly used or disclosed to unauthorized parties, could adversely affect City of Brighton, or be otherwise damaging to City of Brighton.

11.4 Responsibilities

Department Director Personnel are responsible for implementing information protection policy and procedures for secured courier and delivery and monitoring compliance within their respective departments.

The Director of Information Technology is responsible for establishing and implementing City-wide information systems and network security policies, standards, and procedures.

Employees, contractors, and temporary workers are responsible for protecting City of Brighton confidential information by following this policy and the related protection procedures and for protecting the confidential information of others that has been entrusted to City of Brighton.

The Originator of a document or other expression containing confidential information is responsible for classifying the information as "confidential" and labeling it properly with handling instructions as appropriate.

11.5 Classifying and Labeling Confidential Information

It is the responsibility of the originator of confidential information to identify it as confidential and label it properly. Information that needs safeguarding -- including emails and presentations -- should be visibly labeled "City of Brighton Confidential" at the top or the bottom of each page.

The originator of confidential information may specify distribution and handling instructions by including them in the label. Typical handling instructions include:

Internal Use Only, which specifies that the information is only for City of Brighton (who have signed confidentiality agreements).

Do Not Copy or Distribute, which stipulates that the receiver of this information may not distribute it further, forward it, or otherwise disclose it to others, without the agreement of the originator. The label should read, City of Brighton: Do Not Copy or Distribute.

In certain situations, documents will contain headings and labels established by the City Attorney to maintain attorney-client privilege or as "registered and restricted" as determined by management.
Once the City releases confidential information to the public or other circumstances undo the need for confidentiality, we should discontinue using these labels.

11.6 Information Protection Procedures

- Access rights for users are restricted to least privileges necessary to perform job responsibilities.
- Employees must be careful when discussing confidential information so those without authorization and a need-to-know do not overhear these conversations.

- When traveling, do not put confidential information in your checked baggage. Keep it with you and protect it at all times. Use the hotel room safe or safe deposit box to store it if you need to leave it at the hotel. Keep electronic versions of confidential information separate from your computer. Use password protection.
- Third parties, including contractors, and vendors who are privy to City of Brighton confidential information should sign confidentiality or non-disclosure agreements.
- Employees must lock their workstations (using a password screen saver, or other security feature) to prevent access when away from their desks
- Employees must protect their workstations and City networks from computer viruses by using City of Brighton resident virus scanning applications. Do not disable or modify this software.
- Documents and media containing confidential information must be stored out of view, inside the access controlled areas of our buildings, whenever possible. Confidential information should be stored in locked file cabinets or secure file rooms.
- The data should be stored on secured servers when feasible in order to protect against loss, theft, unauthorized access and unauthorized disclosure.
- For City employees that work with sensitive data, protecting that data is one of your most important responsibilities. If information must be stored on, hard drives and other electronic storage media temporarily, it must be protected by properly constructed passwords and promptly deleted when the task is complete. Employees must not divulge, or let others use, their passwords.
- Do not download or copy confidential or sensitive data to your home computer.
- Do not store confidential or sensitive data on a portable device.
- Do not store confidential or sensitive data on a publicly accessed file share.
- While visitor procedures may vary among City of Brighton locations, all guests are to identify themselves with, the receptionist or their host before entering City of Brighton facilities.
- Employees, contractors and partners must not make unauthorized copies of City of Brighton or others licensed software or products.
- When no longer needed, documents and media containing confidential information should be shredded or otherwise destroyed.
- Faxing Confidential Information. If you must fax a confidential document, take these precautions:
    - Telephone the recipient and have them wait at their fax machine.
    - Carefully dial the number, double check it, send the fax, and wait for it to complete.
    - Telephone the recipient a few moments later and make certain they received all pages.
    - Confidential faxes should contain a paragraph instructing the recipient that the fax is confidential, and, if they receive it inadvertently, they are to notify City of Brighton and not divulge the information. Our standard heading for this purpose is:

This fax contains confidential information intended only for the addressee. Do not read, copy or disseminate it unless you are the addressee. If you have received this fax in error, please call me immediately at **[phone number]**. Thank you.

- When photocopying confidential information, be careful to remove the original from the machine and take all the copies when you finish.

11.7Protecting Laptops

When a laptop computer is stolen two kinds of loss is suffered: the computer, and, perhaps far more serious, information stored in the computer. Take these precautions:

- Do not leave your laptop unsecured in a City of Brighton office. Lock it in its docking station, secure it with a cable lock, or lock it up in a cabinet or your desk when it is not being used.
- Do not leave your laptop unattended in open view in your hotel room. Utilize the room safe if possible.
- Lock the laptop away out of sight when you are not using it, preferably in a filing cabinet or safe.
- Do not leave your laptop unattended and in open view in your automobile. If you must leave it in your car, lock it in the trunk and in a laptop travel security case but it is much safer to take it with you. A secure laptop travel safe offers effective travel theft protection security for your laptop computer in the car, hotel & anywhere you travel.
- Never place your laptop in checked baggage and keep it securely with you in hotel lobbies, airports, restaurants, and other public places.
- Remember, the carrying case offers no protection from theft; what is inside is easily recognizable. Use a non-descript carrying case. Use a form fitting sleeve to protect the laptop and carry it in your briefcase, backpack or tote. If using something with a zipper, consider adding a small lock to the zipper to keep hands from easily reaching in to the bag.

Be careful using your laptop on airplanes and in public areas. Make certain those around you cannot read your screen if you are working with confidential presentations or other material. Keep it off the floor. No matter where you are in public—at a conference, a coffee shop, or a registration desk—avoid putting your laptop on the floor. If you must put it down, place it between your feet or at least up against your leg, so that you're aware of it. Keep a note of the make, model, and serial number but do not keep this information with the laptop. If it is lost or stolen, notify the Police immediately and inform the IT Help Desk as soon as practicable (within hours not days).

12 Revoking Privileges after Termination

12.1 Objective

The objective of this policy is to ensure availability, integrity and confidentiality of systems and information of **City of Brighton** by revoking the user accounts/accesses of those who are no longer employed by **City of Brighton**.

12.2 Scope

This Policy describes guidelines and procedures to revoke access for any **City of Brighton** "User" who is no longer employed by **City of Brighton**. The term "user" applies to any person (**City of Brighton** employees, third party contractors, temporaries, guests, licensees of **City of Brighton**, as well as those who represent themselves as being connected – in one way or another – to **City of Brighton**) who uses, possesses or has access to **City of Brighton** communications systems and equipment.

12.3 Policy

- IT Help Desk is responsible for revoking employee's access to City of Brighton information system in the event of Employee's termination.
- It is the responsibility of the Employee's Director and the Human Resources department to notify the IT Help Desk about an employee's termination and begin the process to revoke access.
- Upon receiving such notification to revoke access either via email or helpdesk work order, the IT Help Desk will initiate the process of revoking employee's access to information systems. This will prevent further access to any systems.

Computer Data and Media Disposal

13.1 Purpose

Digital storage devices which contain licensed software programs and/or confidential data must be reliably erased and/or destroyed before the device is transferred out of the City's control or erased before being transferred from one department or individual to another.

13.2 Scope

All computers and digital storage devices owned or leased including, but not limited to desktop workstation, laptop, server, notebook, and handheld computer, hard drives; external hard drives; and all external data storage devices such as disks, SANs, optical media (e.g., DVD, CD), magnetic media (e.g., tapes, diskettes), and non-volatile electronic media (e.g., memory sticks), are covered under the provisions of this policy.

13.3 Policy

The loss, theft or transfer of all computer equipment shall be promptly reported to the Department Director and the Director of Information Technology.

Before any computer equipment is surplused, transferred, reassigned within the City, traded-in, disposed of, or the hard drive(s) is replaced, all sensitive and/or confidential program or data files on any storage media shall be completely erased or otherwise made unreadable in accordance with this Policy unless there is specific intent to transfer the particular software or data to the recipient.

Whenever licensed software is resident on any computer media being surplused, transferred, traded-in, disposed of, or the hard drive(s) is replaced, the terms of the license agreement shall be followed.

Physical destruction shall be accomplished to an extent that precludes any possible further use of the hard drive.

13.4 Responsibilities

It is the responsibility of the Information Technology Department to oversee the removal of all such information.

Social Media policies will be updated and maintained by the Public Information Office.

Policies For Sharing Data With Service Providers

If confidential or sensitive data is shared with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), the following policies and procedures must be followed:

- City of Brighton must maintain a documented list of any service provider that is given confidential or sensitive data, provided direct access to the network, or can affect the security of the network.
- Any written agreement with a service provider that is given confidential or sensitive data, provided direct access to the network, or can affect the security of the network, must include an acknowledgement of the service provider's responsibility for securing all confidential or sensitive data they receive from City of Brighton.
- Prior to engaging with a service provider that is given confidential or sensitive data, provided direct access to the network, or can affect the security of the network, City of Brighton will conduct due diligence and follow an established process to ensure that the security of confidential or sensitive data within the service provider's network has been addressed.
- City of Brighton will have an ongoing program to monitor the compliance status (PCI, CJIS, etc..) of any service provider that is given confidential or sensitive data, provided direct access to the network, or can affect the security of the network.

Acceptable Use Acknowledgement.

Use of City provided Email, Internet or Intranet services constitutes acceptance of the IT policies, and consent to monitoring while using the services. I understand that I am personally liable for my misuse of Email, Internet or Intranet services provided by **City of Brighton**. I also understand failure to adhere to this policy may result in disciplinary action up to and including discharge.