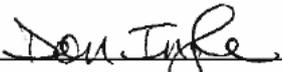


CITY OF BOULDER

POLICIES AND PROCEDURES

**ADMINISTRATOR GUIDE AND
INFORMATION SECURITY POLICY**

**EFFECTIVE DATE:
LAST REVISED: 09/22/2011**



DON INGLE, DIRECTOR OF INFORMATION TECHNOLOGY

Table of Contents

| | |
|--|----|
| I. <u>INTRODUCTION</u> | 5 |
| II. <u>POLICY</u> | 5 |
| A. Acceptable Use / Allowed Services Policy..... | 5 |
| A.1 Overview..... | 5 |
| A.2 Policy..... | 5 |
| B. Staff Awareness..... | 8 |
| B.1 Overview..... | 8 |
| B.2 Policy..... | 8 |
| B.3 Requirements..... | 8 |
| C. Account Administration..... | 8 |
| C.1 Overview..... | 8 |
| C.2 Policy..... | 8 |
| C.3 Requirements..... | 9 |
| D. Personnel Background Screening..... | 9 |
| D.1 Overview..... | 9 |
| D.2 Policy..... | 10 |
| D.3 Requirements..... | 10 |
| E. Physical Security..... | 10 |
| E.1 Overview..... | 10 |
| E.2 Policy..... | 10 |
| E.3 Requirements..... | 10 |
| F. Backups..... | 11 |
| F.1 Overview..... | 11 |
| F.2 Policy..... | 11 |
| F.3 Requirements..... | 11 |
| G. Remote Access..... | 12 |
| G.1 Overview..... | 12 |
| G.2 Policy..... | 12 |
| G.3 Requirements..... | 12 |
| H. Change Management..... | 13 |
| H.1 Overview..... | 13 |
| H.2 Policy..... | 13 |
| I. Authentication..... | 14 |
| I.1 Overview..... | 14 |
| I.2 Policy..... | 14 |
| I.3 Requirements..... | 14 |
| J. Elevated Privileges..... | 15 |
| J.1 Overview..... | 15 |
| J.2 Policy..... | 15 |
| K. Asset Management / Software Policy..... | 15 |
| K.1 Overview..... | 15 |
| K.2 Policy..... | 15 |
| L. Hardware Disposal..... | 17 |
| L.1 Overview..... | 17 |
| L.2 Requirements..... | 17 |
| M. Information Sensitivity..... | 17 |
| M.1 Overview..... | 17 |
| M.2 Policy..... | 18 |
| M.3 Requirements..... | 18 |
| N. Email Handling / Restrictions..... | 18 |
| N.1 Overview..... | 18 |

| | |
|---|-------------------------------------|
| N.2 Requirements | Error! Bookmark not defined. |
| O. Virus Protection | 19 |
| O.1 Overview..... | 19 |
| O.2 Policy | 19 |
| O.3 Requirements | 19 |
| P. Wireless Communication..... | 19 |
| P.1 Overview | 19 |
| P.2 Policy..... | 19 |
| P.3 Requirements | 21 |
| Q. Networking Device Security..... | 20 |
| Q.1 Overview..... | 20 |
| Q.2 Policy | 20 |
| R. Server Security..... | 21 |
| R.1 Overview | 21 |
| R.2 Policy | 21 |
| S. Encryption..... | 22 |
| S.1 Overview | 22 |
| S.2 Policy..... | 22 |
| S.3 Requirements..... | 22 |
| T. Database Administration..... | 22 |
| T.1 Overview | 22 |
| T.2 Policy | 22 |
| T.3 Requirements..... | 22 |
| U. Ongoing Vigilance..... | 23 |
| U.1 Overview..... | 23 |
| U.2 Policy | 23 |
| U.3 Requirements | 23 |
| V. Documentation..... | 24 |
| V.1 Overview..... | 24 |
| V.2 Policy | 24 |
| W. Managing Software Patches and Upgrades..... | 25 |
| W.1 Overview..... | 25 |
| W.2 Policy | 25 |
| W.3 Requirements | 25 |
| X. External Connections..... | 25 |
| X.1 Overview..... | 25 |
| X.2 Policy | 25 |
| X.3 Requirements | 25 |
| Y. Auditing | 26 |
| Y.1 Overview..... | 26 |
| Y.2 Policy | 26 |
| Y.3 Requirements | 26 |
| Z. Non-City-Owned Equipment | 27 |
| Z.1 Overview | 27 |
| Z.2 Policy | 27 |
| Z.3 Requirements..... | 27 |
| AA. Mobile Devices | 27 |
| AA.1 Overview..... | 27 |
| AA.2 Policy | 27 |
| AA.3 Requirements | 27 |
| BB. System / Application Certification Checklists | 27 |
| BB.1 Overview | 27 |
| BB.2 Policy..... | 28 |
| BB.3 Requirements..... | 28 |
| CC. Exception Reporting | 28 |
| CC.1 Overview | 28 |

| | |
|--|----|
| CC.2 Policy..... | 28 |
| CC.3 Requirements..... | 28 |
| III. <u>DISCIPLINARY ACTION</u> | 28 |
| IV. <u>CONSTRUCTION AND INTERPRETATION</u> | 29 |
| V. <u>EXCEPTIONS/CHANGE</u> | 29 |
| VI. <u>REVIEW AND REVISION</u> | 29 |

I. INTRODUCTION

The City of Boulder manages information technology security with an emphasis on confidentiality, integrity, and availability. Ensuring confidentiality means keeping all data private from unauthorized individuals or systems. Integrity is the assurance that only appropriate individuals can modify existing data. Finally, availability is achieved with infrastructure that provides reliable accessibility and performance. The City's holistic approach to security is focused on protecting each of these key security components.

The most effective control point for an organization's security is its network, system, and application administrators, who are not only responsible for implementation and operation of the technology but who also are in day-to-day contact with users and partners/affiliates. The watchful eye of the administrators can make the difference between an incident that goes undetected versus one that is addressed quickly and completely. Likewise, administrators should "lead by example" in their own security habits in hopes of garnering a large user following.

This document details the City of Boulder's policy on security awareness and compliance as it relates to network, system and application administrators. This policy applies to all resources that are owned, leased, or used by the City. This policy addresses specific staff responsibilities required in the Cardholder Data Environment (CDE) as defined by the PCI Security Standards Council and established and maintained by the city to be compliant with the PCI Security Council PCI DSS Requirements.

For the purposes of this policy, employees include contractors, part-time employees, temporary employees, and seasonal employees, as well as full-time staff.

This policy has been developed in an effort to support the City's business objectives and as a way to reduce losses associated with intentional or accidental information disclosure, modification, destruction, or denial of service. All administrators are responsible for knowing and complying with all components of this policy. The IT Security Team Charter further assigns security responsibilities to staff who are assigned specific roles and are members of specific committees. Questions about the policy should be directed to the IT Department Director.

II. POLICY

A. Acceptable Use / Allowed Services Policy

A.1 Overview

This policy component outlines acceptable use of City of Boulder computing resources, including resources that are owned, leased, or used by the City. Such resources are provided by the City to assist in the conduct of organizational business. Employees are responsible for ensuring that these computing resources are used in an effective, ethical, and legal manner and that any limited personal use does not negatively impact systems or job productivity. Inappropriate use exposes the City to risks including virus attacks, compromise of network systems and services, additional cost, and legal issues. These rules are in place to protect the City and its employees, as well as its residents, contractors, vendors, and agents.

A.2 Policy

A.2.1 General Use and Ownership

- **A.2.1.1:** All information technology resources, including but not limited to computer equipment, software, operating systems, storage media, and network accounts providing email, network browsing, and file transfer, are the property of the City of Boulder. These systems are to be used for business purposes in serving the interests of the City, and of the City's residents in the course of normal operations.
- **A.2.1.2:** Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Employees who have questions about what personal use might be considered

appropriate should contact their supervisors. It is the supervisor's responsibility to contact the IT Director to make an informed decision on any new issues.

- **A.2.1.3:** Supervisors have management authority and responsibility to ensure the appropriate use of employee work time and resources; limited personal use of City resources may be revoked or limited at any time at the discretion of the employee's supervisor.
- **A.2.1.4:** Employees who wish to express personal opinions not related to City business duties in Internet newsgroups, chat rooms, or other broadcast methods should use their own personal user accounts on non-City systems for this purpose.
- **A.2.1.5:** There should be no expectation of privacy when using the City's network. The City of Boulder reserves the right to access, retrieve, read and disclose any data, messages or files stored on City of Boulder-funded systems. The City of Boulder reserves the right to monitor use of these systems to prevent abuse, enforce other policies, and access information. Access may occur in, but is not limited to, situations indicating: (1) impropriety, (2) violation of City of Boulder policy, (3) legal requirements, (4) suspected criminal activities, (5) breach of system security, or (6) a need to locate substantive information or monitor employee conduct. The contents of these systems may be disclosed by City of Boulder Management within or outside of the City of Boulder without employee permission. Furthermore, all communications including text and images may be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. The City of Boulder has unlimited access to protect the security of these systems or the City of Boulder's property rights. The City reserves the right to access and monitor all messages and files on City computing resources, and such data may be reviewed at any time to determine whether an employee's usage complies with the intent of this policy.
- **A.2.1.6:** All messages created, sent, or retrieved using City of Boulder network computing resources, including email, are the property of the City and may be a public record under the Colorado public records law subject to public inspection under C.R.S 24-72-203.
- **A.2.1.7:** Recognizing that technology processes are constantly changing, for any current or future technology-related issues not explicitly covered by this policy, employees should act in the spirit of this policy. Any questions should be directed to the IT Director.
- **A.2.2 Acceptable Use**
- The following activities are examples of acceptable or encouraged uses of City of Boulder computing resources:
 - **A.2.2.1:** Computing, communications, and information exchanges directly relating to the mission, charter, and work tasks of the City of Boulder.
 - **A.2.2.2:** Announcements of City of Boulder procedures, meetings, policies, services, or activities.
 - **A.2.2.3:** Use for advisory, standards, research, analysis, and professional society or development activities related to the user's City of Boulder job duties.
 - **A.2.2.4:** Use in applying for or administering grants or contracts for the City of Boulder.
 - **A.2.2.5:** Personal use of computing resources limited to situations that would be analogous to receiving an occasional quick personal telephone call.

A.2.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a computer if that computer is disrupting production services, and law enforcement staff may need special access to facilitate crime investigation).

Under no circumstances is a City of Boulder employee authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing City of Boulder-owned resources.

The lists below are by no means exhaustive, but they attempt to provide a framework for activities that fall into the category of unacceptable use.

The following are examples of activities that are strictly prohibited:

- **A.2.3.1:** Engaging in any activity that interferes in any way with official City business.

- **A.2.3.2:** Engaging in any activity that incurs any incremental expense to the City for non-City business.
- **A.2.3.3:** Transmitting or accessing sexually-oriented, obscene, discriminatory, harassing, gambling-related, defamatory, false, inaccurate, abusive, profane, pornographic, threatening, racially offensive, or otherwise improperly biased upon the basis of discriminatory or illegal material.
- **A.2.3.4:** Engaging in any activity that degrades network performance or otherwise consumes City computer resources for non-City business.
- **A.2.3.5:** Using file sharing or peer-to-peer applications (e.g., Napster-like products, Gnutella, Morpheus, Kazaa, etc.).
- **A.2.3.6:** Using Internet-based file sharing or storage applications to store City data (e.g., Xdrive, Backpack, etc.).
- **A.2.3.7:** Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the copying, installation, use, or distribution of unlicensed software.
- **A.2.3.8:** Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws. Employees should consult their supervisor prior to exporting any material in question.
- **A.2.3.9:** Intentionally introducing malicious programs into the network or a server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- **A.2.3.10:** Installing or using software not approved by the IT department, or otherwise violating the City Software Policy.
- **A.2.3.11:** Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, intentionally accessing data of which the employee is not an intended recipient or logging in to a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forging routing information for malicious purposes.
- **A.2.3.12:** Engaging in any activity intended to be retaliatory toward another employee, management, a vendor, a resident, or any outside party.
- **A.2.3.13:** Port scanning or security scanning of City of Boulder systems, vendor systems, or of any third-party systems.
- **A.2.3.14:** Executing any form of network monitoring that will intercept data not intended for the employee’s computer.
- **A.2.3.15:** Using City of Boulder resources for business purposes not related to the City (e.g., home businesses, work for outside companies, etc.).
- **A.2.3.16:** Accessing a computer, computer network, or computer system or any part thereof without authorization or accessing such a system in a manner that exceeds authorization.
- **A.2.3.17:** Accessing a computer system in violation of Section 18-5.5-102 C.R.S. “Computer crime.”
- **A.2.3.18:** Accessing or providing access to a computer system within the CDE unless authorized to do so in order to support a business process or while performing support or administrative duties in support of the computer systems and/or networking devices within the CDE environment.
- **A.2.3.19:** Providing access to the Internet to any devices within the CDE is prohibited except when needed to perform specific credit card handling processes. In this case, Internet access to these sites is facilitated via a “White List” of sites identified and documented as required to facilitate credit card processing for the business unit.

B. Staff Awareness

B.1 Overview

Security awareness is necessary for employees and administrators to understand the importance of the City's IT security policies. City users must be educated on what security policies exist in the organization, why they exist, and how they are enforced.

B.2 Policy

City of Boulder employees and administrators must understand and be aware of the IT security risks to the organization from external and internal threats.

B.3 Requirements

- **B.3.1:** Users must review and sign the Internal User Policy.
- **B.3.2:** Administrators must review the City's security policy map as well as review the associated security policies.
- **B.3.3:** Users must be educated on new security policies and policy changes annually.
- **B.3.4:** Policies must be stored in a central location (e.g., the City's Intranet) and made available for users to review.

C. Account Administration

C.1 Overview

User accounts, which permit specific system and network access to specific individuals, are an important control point in the overall security model of an organization. If the number and owners of active accounts are not monitored closely, security risk to the organization greatly increases.

The key to effective, secure account administration is adherence to a strict set of policies that describe who is permitted to have accounts, who authorizes accounts, and when accounts expire.

C.2 Policy

Accounts at the City of Boulder shall be granted only to individuals meeting criteria and through the approval procedures detailed in the following table.

Table 1: City of Boulder Account Administration

| Classification | Approval procedures for granting account | Account Implementation | Account expiration |
|--|--|-------------------------------|---|
| City of Boulder Employee | City of Boulder Supervisor grants permission | City of Boulder IT Help Desk | Immediately upon termination of employment, instructions from supervisor, or change of role or employment status which no longer requires account |
| City of Boulder Vendor or Consultant | City of Boulder Sponsor or Project Manager grants permission | City of Boulder IT Help Desk | Termination of vendor agreement, instructions from project sponsor or project manager, or 120 days from start date or renewal |
| Contract/Temporary/Fixed-Term Employee | City of Boulder Supervisor grants permission | City of Boulder IT Help Desk | Termination of contract or instructions from supervisor |

C.3 Requirements

- **C.3.1:** Accounts may be granted only to individuals with a verified business need to access City of Boulder resources.
- **C.3.2:** Accounts must never be shared.
- **C.3.3:** Accounts must be granted with the minimum level of access and on the minimum number of systems required for the user to complete his required business tasks.
- **C.3.4:** Accounts must never be issued to a party whose identity and authorization cannot be positively verified.
- **C.3.5:** Accounts must only be issued when authorization for the accounts can be verified.
- **C.3.6:** Abuse of accounts or violation of this policy may result in immediate account termination.
- **C.3.7:** Accounts must be authorized and issued in a planned, thoughtful way to ensure procedural correctness. Accounts must never be authorized or issued under the pressure of time or outside of proper procedure.
- **C.3.8:** Accounts must adhere to the Passwords policy section of this document.
- **C.3.9:** Accounts determined to be idle or unused by otherwise active employees, vendors, contractors, or consultants for a period of six months must be disabled and the direct supervisor of the account holder notified.
- **C.3.10:** All non-console administrative account access must be encrypted for both internal and remote access.
- **C.3.11:** The Human Resources and Organizational Effectiveness Department is responsible for notifying the IT Department of terminations of all permanent, temporary, and seasonal City employees in a regular and timely manner so that their accounts can be disabled in accordance with this policy.

D. Personnel Background Screening

D.1 Overview

Personnel with administrator-level access to City of Boulder Police Department computer systems often have unlimited access to view and/or modify the information contained in those systems. As such, the criminal backgrounds of these personnel are relevant to any decision to grant them administrator-level system access.

D.2 Policy

All City of Boulder employees (permanent, contract, temporary, fixed-term, or otherwise), as well as vendors and consultants, must pass a fingerprint-based criminal background record check before being permitted access to any City of Boulder Police Department computer systems (whether servers, networking equipment, or client workstations) at an administrator-equivalent level. In cases where a criminal history is found, access will be permitted or denied by decision of the individual's supervisor or sponsor in consultation with the IT Department Director and representatives from the HROE Department, Police Department, or City Attorney's Office as appropriate.

D.3 Requirements

- **D.3.1:** Any employee, vendor, or consultant of the City of Boulder requiring administrator-level access to any City of Boulder Police Department computer system must be fingerprinted by the City of Boulder Police Department. Fingerprints and other necessary personal information from this individual must be analyzed by appropriate law enforcement agencies to assess the criminal background of the individual. Sufficient information on the results of this background check must be provided to the individual's supervisor or sponsor to allow an informed decision on appropriate computer system access.

E. Physical Security

E.1 Overview

There are several types of physical security risks inherent in the City of Boulder's environment. Direct, physical access to a server provides multiple opportunities for an attacker to circumvent system and network access controls. Unattended or unaudited physical network access presents a number of opportunities for unauthorized information access and exposure. Additionally, environmental concerns such as excessive heat and moisture can damage or destroy systems and data.

E.2 Policy

City of Boulder network and systems administrators are responsible for creating appropriate safeguards to limit physical access to all City of Boulder servers as a way to protect them from unauthorized use or theft. Administrators are also responsible for putting environmental controls in place to reduce the risk of damage or loss of data and resources.

E.3 Requirements

- **E.3.1:** A UPS (uninterruptible power supply) must be installed in case of power failure along with associated software that alerts the administrator via phone, pager, or email when the power in the UPS is almost depleted.
- **E.3.2:** An environmental control system must be set up to monitor temperature and humidity levels that could cause damage to equipment. This system must be configured to alert the administrator via phone, pager, or email.
- **E.3.3:** Facility additions or changes must be evaluated to verify they satisfy local building regulations, limiting physical access to resources as well as reducing the risk of damage or loss to City of Boulder resources.
- **E.3.4:** Sensitive areas and systems must be physically secured and access permitted only to authorized individuals. Access to sensitive areas must be logged.
- **E.3.5:** Access to sensitive areas and systems may be granted only to authorized personnel, all of whom must demonstrate they understand the City's security policies as they apply to physical resources. Access will be revoked upon inappropriate use, security breach, or employee termination.
- **E.3.6:** Unauthorized personnel are not allowed entry to City of Boulder offices, communications and utility facilities, data centers, etc. Non-City of Boulder parties performing maintenance on

facilities must be escorted and/or monitored by City of Boulder staff. Additionally, resources that are not exclusively owned or operated by the City of Boulder, such as shared telco entrance facilities, require escort and/or monitoring by City of Boulder staff. All non-City of Boulder parties must have a work plan approved by the IT Department prior to commencing work.

- **E.3.7:** Unused/inactive network connections in unsupervised areas will remain in a disabled state. Areas such as public conference rooms and community access areas should have network connections disabled when not in use. Activation of disabled ports must be approved and performed by the IT Department.
- **E.3.8:** Community access terminals, such as kiosks, will be isolated from the City of Boulder internal network. Network access granted to the terminals should only remain active during periods of supervision by City of Boulder staff, i.e., business hours.
- **E.3.9:** Regular auditing of public access terminals and connections will be performed to ensure connection integrity. All unauthorized system changes must be documented. Connectivity to the compromised environment will be deactivated until the environment can be restored to a known good state.
- **E.3.10:** In the event of a disaster, the City's Data Center Emergency Disaster Procedure must be followed.

F. Backups

F.1 Overview

Files are backed up to tape on a regular basis primarily so they can be restored in case of a disk failure, accidental deletion, or intentional deletion during a security incident. Users should not rely on the backup system to recover files after they are intentionally deleted (although in most cases the backup system should be able to recover them).

Because these backups provide a path to recovery in the event of a security incident, and a system baseline that can be used to determine the extent of a security incident, they are integral to organization security. One of the most important administrator tasks is ensuring that usable backups of all important data are occurring on a regular basis.

F.2 Policy

Backups must be vigilantly performed and tested by administrators according to the guidelines set forth below. If at any time an administrator responsible for backups according to the guidelines below cannot adequately perform his duties in this regard for any reason, he must notify the IT Director.

F.3 Requirements

- **F.3.1:** All critical data and operating system files on servers should be backed up (at least for incremental changes) on a daily basis.
- **F.3.2:** Full system backups should be performed at least every four weeks.
- **F.3.3:** Firewalls and stateful network equipment configurations should be backed up on a weekly basis and prior to and following major changes made to that equipment.
- **F.3.4:** Critical data should be backed up in such a manner that it can be restored in full up to 90 days following the day it was backed up. Critical operating system data should be backed up in such a manner that it can be restored in full up to 30 days following the day it was backed up.
- **F.3.5:** One-half of the full system backup tapes (usually every other month's worth of tapes) should be stored in a secure, off-site, climate-controlled tape storage facility.
- **F.3.6:** Tapes should be "checked-out" from either on-site or off-site storage facilities when they are needed, in a manner such that they are logged with who accessed them and what dates they were checked out and checked back in.
- **F.3.7:** On-site backup tapes must be stored in a physically secure, climate-controlled location.

- **F.3.8:** Only administrators and backup operators should physically handle on- or off-site backup tapes or have access to tapes that have been mounted in drives.
- **F.3.9:** Every backup tape must be labeled so as to identify its contents. If machine readable labeling is used, a tape manifest should be stored in a safe location at least monthly.
- **F.3.10:** Tapes and backup sets should be verified quarterly to verify restoration capability. Backup sets and tapes that fail restoration checks should have additional sets tested and verified.
- **F.3.11:** If a backup tape contains a credit card number, the tape must be encrypted if one of the following techniques is not used:
 - One-way hashes (hashed indexes), such as SHA-1
 - Truncation
 - Index tokens and PADs, with the PADs securely stored
 - Strong cryptography, such as Triple-DES 128-bit or AES 256-bit with associated key management processes and procedures
- **F.3.12:** Backup tapes that contain sensitive data should be transported by a secure courier.
- **F.3.13:** Deviations from these requirements may be allowed where the law or other City of Boulder policy requires that data not be backed up or archived as described above.

G. Remote Access

G.1 Overview

The purpose of this section of the policy is to define standards for connecting to the City of Boulder's network from remote locations. These standards are designed to minimize the potential exposure to the City from damages that may result from unauthorized use of City resources. Damages may include the loss of sensitive or City confidential data, damage to public image, or damage to critical City of Boulder internal systems.

Remote access implementations that are covered by this policy include, but are not limited to, Citrix, VPN, SSH, Remote Desktop, dial-in or cable modems, and other leased-line services.

G.2 Policy

Only individuals with specific business need may be granted remote access to the City of Boulder network. Requests for remote access by non-employees must be approved by the IT Department following completion and submission of a Remote Access Request Approval form.

It is the responsibility of City of Boulder employees, contractors, vendors, and agents with remote access privileges to the City network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the City network.

G.3 Requirements

- **G.3.1:** Citrix is the preferred connection type for remote access
- **G.3.2:** In cases where Citrix is not sufficient, an exception must be made and the requester must fill out the Remote Access Request Approval form.
- **G.3.3:** Secure remote access must be strictly controlled.
- **G.3.4:** At no time may remote login information be shared with anyone.
- **G.3.5:** All remote access achieved through public connections (such as cyber-cafes and public access terminals) must utilize encryption to protect all data during transmission. No unencrypted communication channels will be permitted across public networks.
- **G.3.6:** City of Boulder employees and contractors with remote access privileges must ensure that their City-owned or personal computer or workstation that is remotely connected to the City network is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

- **G.3.7:** Nonstandard remote access modes, hardware, or configurations must be approved by the City of Boulder IT Department.
- **G.3.8:** All computers, including personal computers, that are connected to City of Boulder networks via remote access channels must use antivirus software in accordance with the Virus Protection policy section of this document.
- **G.3.9:** All computers, including personal computers, that are connected to City of Boulder networks via remote access channels must be patched with the latest security patches and hotfixes in accordance with the Managing Software Patches and Upgrades section of this document.
- **G.3.10:** All remote access with designated time limits will only be available during the specified times. Any changes to the scope of remote access time requires the approval of the City of Boulder IT Department.
- **G.3.11:** Any violations of these guidelines may result in the termination of the remote access channel, and the City may pursue legal remedies if access is used inappropriately.
- **G.3.12:** Two-factor authentication is required for anyone accessing the CDE remotely from a non-trusted network. A non-trusted network is any network not part of the City of Boulder Network infrastructure.
- **G.3.13:** All remote access by vendors to the CDE will be enabled only when and while necessary and will be monitored during use.
- **G.3.14:** Citrix can not be used to host an application that facilitates access to systems within the CDE with the purpose to allow for the entry, display or reporting of any Credit Card PAN data.

H. Change Management

H.1 Overview

This section defines when the change management process should be initiated at the City of Boulder, and provides guidelines on the tools to be used and the steps necessary to complete the change process.

H.2 Policy

- **H.2.1:** Any programmatic or architecture change to the production environment should be considered a change to be tracked by the change management process.
- **H.2.2:** The IT ticketing system is to be used as the City of Boulder's IT incident, problem, and change tracking system.
- **H.2.3:** A change request can be initiated in a variety of ways; two of the most likely scenarios are user requests and IT requests.

H.2.4 Change Submission Process

The classification of the change will ultimately determine how the proposed change is entered into the IT Ticketing System. Pre-approved changes are generally maintenance items that are needed to support the ongoing operation of the system, and are of low risk. All other changes tend to be higher risk or involve the implementation of a new system or functionality. Regardless of the classification, the following steps should be followed:

- **H.2.4.1:** Definition of the scope of the proposed change.
- **H.2.4.2:** Peer review of proposed change to ensure accuracy.
- **H.2.4.3:** Assessment of risk.
- **H.2.4.4:** Thorough pre- and post- change testing.

I. Authentication

I.1 Overview

As the front line of protection for user accounts, passwords are an important aspect of IT security. A poorly chosen password may result in the unexpected compromise of elements of the City of Boulder's network. As such, all City of Boulder employees, contractors, and vendors with access to City of Boulder systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. City of Boulder administrators are responsible for promoting the creation and use of secure passwords by users.

I.2 Policy

- **I.2.1:** All accounts, including accounts within major applications such as GroupWise, PIN, HRIS, BFS, etc., must have a password.
- **I.2.2:** Mobile devices (e.g., laptops, blackberries, palm devices) must be password protected.
- **I.2.3:** All system-level passwords (e.g., root, enable, administrator, application administration accounts, etc.), including major application and database administrative passwords, must be changed on at least a quarterly basis.
- **I.2.4:** All system-level passwords (e.g., root, enable, administrator, application administration accounts, etc.), including major application and database administrative passwords, must be changed when an administrator is no longer employed by the City.
- **I.2.5:** All user-level passwords (e.g., email, web, desktop computer, etc.) on systems that allow the user to independently change the password must be changed at least every 120 days.
- **I.2.6:** User accounts that have system-level privileges must have a unique passwords from all other accounts held by that user.
- **I.2.7:** Passwords must not be included in unencrypted email messages.
- **I.2.8:** System-level passwords must be documented and stored in a secure manner.
- **I.2.9:** Users may be held responsible for system access made using their user accounts.
- **I.2.10:** All user-level and system-level passwords must conform to the requirements described below.

I.3 Requirements

I.3.1 General Password Construction Standards

Passwords are used for various purposes at the City of Boulder. Some of the more common uses include user-level accounts, web accounts, email accounts, screen saver protection, voicemail, application access, and local router logins.

Acceptable passwords have the following characteristics:

- **I.3.1.1:** Contain both upper and lower case characters (e.g., a-z, A-Z).
- **I.3.1.2:** Have digits and punctuation characters as well as letters (e.g., 0-9, !@#\$%^&*()_+|~- =\{}[]:"';<>?,./).
- **I.3.1.3:** Are at least eight alphanumeric characters long.
- **I.3.1.4:** Are not a word in any language, slang, dialect, jargon, etc.
- **I.3.1.5:** Are not based on personal information, names of family, etc.
- **I.3.1.6:** Are easily remembered by the user. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

I.3.2 Password Protection Standards

- **I.3.2.1:** Users must not have the same password for City of Boulder accounts as for non-City of Boulder accounts (e.g., personal ISP account, benefits, etc.).
- **I.3.2.2:** Users must not share City of Boulder passwords with anyone. All passwords are to be treated as sensitive, confidential information.
- **I.3.2.3:** Users must not use the “Remember Password” feature of applications (e.g., web applications).
- **I.3.2.4:** Users should not write passwords down and store them anywhere in their work areas. If passwords must be written down to aid memory, the passwords must be stored and treated as sensitive information (similar to a user’s Social Security number, credit card number, bank ATM PIN number, etc.). Users must not store unencrypted passwords in a file on any computer system (including PDAs or similar devices).
- **I.3.2.5:** If an account or password is suspected to have been compromised, the incident must be reported to the IT Department and the password changed.
- **I.3.2.6:** City of Boulder administrators or their delegates must perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked, the user will be required to change it.

J. Elevated Privileges

J.1 Overview

The principle of least privilege is the goal to give users only the access and privileges they need to perform their job duties. This section of policy defines the standards for requesting elevated privileges, how elevated privileges are granted, and what the elevated privileges can be used for.

J.2 Policy

- **J.2.1:** The City of Boulder’s Change Management process must be followed to request elevated privileges.
- **J.2.2:** The IT department reviews and grants requests for elevated privileges.
- **J.2.3:** On Microsoft systems, Administrators should have two accounts, one account configured with user-level access and one account configured with elevated privileges. Administrators should only use the account with elevated privileges when necessary, i.e., not for day-to-day use.
- **J.2.4:** On Unix/Linux systems, sudo must be used for elevated privileges so individual commands that require elevated privileges can be logged.
- **J.2.5:** On Microsoft systems the “run as” command can be used for elevated privileges.
- **J.2.6:** Elevated privileges must only be used to conduct the task represented in the request. Elevated privileges are not to be used for any other purpose

K. Asset Management / Software Policy

K.1 Overview

This section defines standards for life cycle management of hardware and software at the City of Boulder. Asset management provides a road map for the selection, acquisition, implementation, and upkeep. Sound asset management practices benefit the City by facilitating support, lowering costs, and ensuring maximum reliability and security. This section is based on two existing City policies, the Technology Acquisition policy and the City Software policy. These two policies should be reviewed along with this policy section.

K.2 Policy

K.2.1 General Use and Ownership

- **K.2.1.1:** All computing resources owned or leased by the City of Boulder, including but not limited to computer hardware, software, and peripheral devices, are the property of the City of Boulder. These systems are to be used for business purposes in serving the interests of the City, and of the City's residents in the course of normal operations.
- **K.2.1.2:** All software applications installed on City computing resources are subject to certain criteria, including, but not limited to, whether the application fulfills a business need required by the City, whether a comparable application fulfilling the same business need is already in use at the City, and the application's compatibility with current City technical standards.
- **K.2.1.3:** All purchased software installed on City computing resources must be owned by the City, and must have accompanying documentation proving City ownership before the software can be installed. Privately owned software cannot be installed on City computing resources, regardless of the license terms and conditions.
- **K.2.1.4:** All software developed by the City must conform to the City's Software Application Security Policy.
- **K.2.1.5:** All PA-DSS certified software within the CDE must be administrated to meet the software documentation provided by the software vendor.
- **K.2.1.6:** All software installed on systems that operate within the CDE must be approved and installed by IT to ensure the security and integrity of the CDE is maintained.

K.2.2 Unacceptable Use

The following activities are, in general, are prohibited with regard to City computing resources. This list is not meant to cover all prohibited activities, but it attempts to provide a framework for activities that fall into the category of unacceptable use related to this policy.

- **K.2.2.1:** Unauthorized downloading, installation or use of any software, including but not limited to demo (evaluation), beta, freeware, and shareware software.
- **K.2.2.2:** Installation or use of any software not legally owned and acquired by the City.
- **K.2.2.3:** Installation or use of any software that degrades network performance or otherwise consumes City computer resources for non-City business.

K.2.3 Software Purchasing

The IT Department will set the standard for enterprise-wide software, including, but not limited to, network operating systems, workstation operating systems, office productivity suites, database formats, Internet browsers, web development, and email.

K.2.4 Software Installation

- **K.2.4.1:** All software installations will be done either by authorized IT Department staff or other City staff authorized by IT to perform installations. This includes, but is not limited to, shrink-wrapped, downloaded, and vendor-supplied software, open source or free software, software accompanying peripheral devices (including drivers), and software upgrades for applications already installed. The presence of administrative rights on a City computer does not imply approval to install software.
- **K.2.4.2:** Software that was not obtained by the IT Department on behalf of the user must be accompanied by a valid license and proof of ownership.
- **K.2.4.3:** Software that has no City-related business need (e.g., screensavers not native to Windows, MP3 players, personal applications, and games) will not be installed on City computing resources.
- **K.2.4.4:** Privately owned software will not be installed on City computer resources regardless of license terms and conditions, time of usage, or purpose.

K.2.5 Software Licensing

The City and its employees must acquire, reproduce, distribute, transmit, and use computer software in compliance with software copyright laws and maintain only legal software on the City's computing resources.

K.2.6 Auditing

The City reserves the right to monitor use of City computing resources to enforce this policy. Any software that is deemed to pose an immediate security risk, or that is otherwise harmful to the computer or other City computing resources, will be uninstalled or disabled upon discovery.

K.2.6 Disciplinary Action

Violation of this policy may result in disciplinary action, up to and including termination of employment.

L. Hardware Disposal

L.1 Overview

When equipment is retired after reaching end-of-life, or if it is replaced because of failure, it is extremely important that it be disposed of in a secure manner to avoid disclosing City of Boulder data unknowingly to parties that come into possession of the equipment in the future.

Before any City-owned or managed hard disk or system containing a hard disk is transferred, donated, or disposed of, it must be sanitized by reformatting the hard drive in a secure manner or by using an approved wipeout utility. Diskettes and other magnetic storage media that contain any City of Boulder data or software must be sanitized when they are no longer needed. Portable media may be reused after overwriting or demagnetizing, or it may be destroyed. Simply deleting a file is not sufficient to prevent someone from undeleting the file later.

L.2 Requirements

- **L.2.1:** IT administrators must use an approved sanitization program on all systems before they are sent out for donation or disposal.
- **L.2.2:** Hard disks of server systems should be wiped of all information and software in a secure manner, or removed and physically destroyed by crushing, drilling, or incinerating.
- **L.2.3:** Portable media, such as tapes, floppy disks, and CD-ROMs, may be destroyed by crushing, incinerating, shredding, or melting. If it is to be reused, portable media must be erased using a secure program such as Norton Utilities' WIPEINFO before being reused by other parties.
- **L.2.4:** Damaged storage devices containing very sensitive data may require a risk assessment to determine whether the item must be destroyed, repaired, or discarded.

M. Information Sensitivity

M.1 Overview

This section of the policy is intended to help City of Boulder employees determine appropriate methods of handling electronic representations of sensitive information. The definition of what is not to be disclosed to the public is determined by Colorado's Open Records Law (C.R.S 24-72-201) and other applicable city, state, and federal law.

The information covered in these requirements includes, but is not limited to, information that is either stored or shared via any electronic means.

It should be noted that the sensitivity level definitions were created as requirements and to emphasize common sense steps that employees can take to protect sensitive City of Boulder information (e.g., sensitive City of Boulder information should not be left unattended in conference rooms).

The Software Application Security Policy should be reviewed for information sensitivity as it relates to software development at the City of Boulder. Questions about the proper classification of a specific piece

of information should be addressed to the City Attorney. Questions about these requirements should be addressed to the IT Director.

M.2 Policy All information handled at the City of Boulder is categorized into two main classifications:

- City of Boulder Public – information that has not been classified as exempt from the Colorado Open Records Law
- City of Boulder Protected – information that has been categorized as exempt from the Colorado Open Records Law such as records of investigations, medical data, personnel files; letters of reference, trade secrets, library records; addresses of public school children; and sexual harassment complaints under investigation. The following definitions are appropriate for further subdividing the Protected category:
- Protected Health Information (PHI): PHI is electronic information covered by the HIPAA Privacy and Security rules.
- Sensitive Personally Identifiable Information (Sensitive PII): Sensitive PII includes any data that could be used to discriminate (e.g., race, ethnic origin, religious or philosophical beliefs, political opinions, trade union memberships, sexual lifestyle, physical or mental health), **OR** facilitate identity theft (e.g., mother's maiden name), **OR** permit access to a customer's account (e.g., passwords or PINs). Sensitive PII includes all PHI and credit card information.
- Personally Identifiable Information (PII): PII includes any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains, **OR** from which identification or contact information of an individual person can be derived. PII does **NOT** include information that is collected anonymously (i.e., without identification of the individual user) or demographic information not connected to an identified individual.
- City of Boulder employees are encouraged to use common sense judgment in securing City of Boulder Protected information to the proper extent. If a user is uncertain of the sensitivity of a particular piece of information, he should contact his direct manager.

M.3 Requirements

- **M.3.1:** Credit card data, specifically the full 16-digit credit card number, the card verification code or value, the Personal Identification Number (PIN), the PIN verification value data elements, the card-validation code or value (the three-digit or four-digit number printed on the front or back of the card), must not be stored electronically at the city of Boulder, which includes, but is not limited to voice mail, voice recordings, emails, email attachments, application logs, database, data files or scanned images.

N. Email Handling / Restrictions

N.1 Overview

This section establishes the City of Boulder's terms of the use of email for electronic communications. The use of email at the City of Boulder is intended as a business tool. It serves as a fast, efficient way to communicate, and it can be used as an appropriate substitute for face-to-face meetings, telephone calls, or internal memorandums. Email should be treated like any other company record.

N1.1 Email Administration

City of Boulder network, system and application administrators are responsible for creating and maintaining an infrastructure that can support the safe and successful delivery of email within the organization and to residents, partners, and others via the Internet.

N.1.2 Email Archiving

City of Boulder administrators will retain and archive all email as part of regular nightly network backups. The archive will reside on the City's backup media with access limited to the administrator staff. This archive may be reviewed at any time to ensure that users are complying with all company policies.

Executive and security management will create a plan for conducting this review and outline appropriate remedies for violators.

O. Virus Protection

O.1 Overview

Viruses, worms, and Trojan horses are designed to infect, control, and damage computers and networks. Viruses can spread from a disk, over the network, via email, or in a file, and they can do anything to a system from changing or deleting files to attacking other systems. The purpose of this virus protection policy is to minimize the risk of these types of threats to City of Boulder workstations, laptops, and servers.

O.2 Policy

Virus protection software must be installed and maintained on all systems connected to the City of Boulder network. City email systems must be configured to scan and filter the content of messages to prevent the spread of viruses, worms, Trojan horses, or other executable items that could pose a threat to the security of systems and networks.

O.3 Requirements

- **O.3.1:** Virus protection software must be installed and maintained on all systems.
- **O.3.2:** Virus protection software updates must be downloaded and installed as they become available.
- **O.3.3:** Virus protection software must be configured to scan for viruses in real time.
- **O.3.4:** Files or macros attached to an email from an unknown, suspicious, or untrustworthy source must never be opened. These attachments must be deleted immediately, and then “double deleted” by emptying the Trash.
- **O.3.5:** Files must never be downloaded from unknown or suspicious sources.
- **O.3.6:** Direct workstation disk sharing with read/write access must never be done unless there is an absolute business requirement to do so.
- **O.3.7:** Removable storage media from unknown sources must always be scanned for viruses before being used.
- **O.3.8:** The incident response policy described in the Exception Reporting policy section of this document must be followed if a virus has been detected.

P. Wireless Communication

P.1 Overview

All wireless data communication devices (e.g. personal computers, cellular phones, PDAs, etc.) connected to any of the City of Boulder's internal networks are subject to the following restrictions on wireless communication. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to the City's networks do not fall under the purview of this policy.

P.2 Policy

Wireless networking devices are permitted to carry City of Boulder data if and only if they utilize encryption in accordance with the Encryption policy section of this document. Unauthorized installation of wireless access points or devices is prohibited. Integrating wireless networking into the CDE is prohibited unless explicitly approved by the IT Director or his designate. All wireless network installations must be performed by or in coordination with the IT Department.

P.3 Requirements

- **P.3.1:** All wireless networks must use secure protocols. For 802.11b/802.11a/802.11g wireless networks, use of an encryption key rotation protocol, such as TKIP, is required when standardized by industry.
- **P.3.2:** Wireless networks must be configured to perform some form of user and/or device authentication before providing network access to provide reasonable assurance that a connecting user/device is legitimate.
- **P.3.3:** The use of WEP is prohibited.
- **P.3.4:** All vendor default passwords must be changed immediately upon implementation of the wireless network.

Q. Networking Device Security

Q.1 Overview

This section of the policy describes a required minimum security configuration for all routers, switches, and hubs connecting to the City of Boulder network.

Q.2 Policy

Every router, switch, hub, and firewall must meet the following configuration standards:

- **Q.2.1:** The administrative/enable password on the device must be kept in a secure, encrypted form.
- **Q.2.2:** The following must be disallowed:
 - IP directed broadcasts
 - Incoming packets sourced with invalid addresses such as RFC 1918 and RFC 2827 addresses
 - Unnecessary services and daemons
 - All source routing
 - All non-secure or unencrypted web services
 - All unused management consoles
- **Q.2.3:** Unused interfaces/ports serving public or insecure areas must remain in a disabled state.
- **Q.2.4:** Access rules must be added as business needs arise.
- **Q.2.5:** Access to City resources must be isolated from access provided to non-City entities (e.g., library patrons, public access kiosks).
- **Q.2.6:** Reverse path verification should be enabled at network edge.
- **Q.2.7:** Network time synchronization among devices must be enabled to coordinate events.
- **Q.2.8:** Event logging to a central server must be configured.
- **Q.2.9:** Restrictions must be placed on active management consoles.
- **Q.2.10:** The device must be included in the City's enterprise management system with a designated point of contact.
- **Q.2.11:** Core network devices must be monitored and the administrator must be notified of problems via phone, pager, or email.
- **Q.2.12:** Device configuration backups must be secured on a central server.
- **Q.2.13:** Every router, switch, hub, and firewall must have the following statement posted in clear view:
 - "ATTENTION This system is for the use of authorized personnel for official purposes. Unauthorized access is prohibited. Users of this system should have no expectation of privacy in its use. All access to this system is subject to monitoring and recording by security personnel. Evidence of possible abuse or criminal activity using this system may

be provided to appropriate officials. Use of this system implies consent to all of the conditions stated above.”

- **Q.2.14:** Firewalls in the CDE must limit inbound and outbound traffic to that which is necessary for the CDE and prohibit direct public connections for inbound and outbound traffic between the Internet and the CDE and only allow approved internet access for critical credit card processing. Server Security.

R.1 Overview

No amount of policy or security technology will be effective if the City of Boulder’s servers are insecure. This section of the policy establishes standards for the base configuration of internal server equipment that is owned and/or operated by the City. Effective implementation of this policy will minimize unauthorized access to City of Boulder proprietary information and technology.

R.2 Policy

All internal servers deployed at the City of Boulder must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by the operational group, based on business needs and approved by the City Information Technology Department.

- **R.2.1:** Servers must be registered in a City of Boulder server inventory. At a minimum, the following information must be recorded:
 - **R.2.1.1:** Primary and backup server contact(s) and location(s)
 - **R.2.1.2:** Hardware description and operating system/version
 - **R.2.1.3:** Main functions and applications, if applicable
- **R.2.2:** Information in the City of Boulder server inventory must be kept up to date; documentation auditing must be conducted periodically to ensure that documentation is current.
- **R.2.3:** Configuration changes for production servers must follow the appropriate change management procedures.
- **R.2.4:** Operating system configuration should be in accordance with approved City of Boulder requirements.
- **R.2.5:** Only designated administrators may add servers to the network.
- **R.2.6:** Only designated administrators may add services to the servers.
- **R.2.7:** Services and applications that will not be used must be disabled where practical.
- **R.2.8:** Access to services must be logged and/or protected through access-control methods, if possible.
- **R.2.9:** The standard security principle of providing the least required access to perform a function must be used.
- **R.2.10:** Administrator/root access must not be used when a nonprivileged account will do.
- **R.2.11:** If a method for secure channel connection is technically feasible, privileged access must be performed over such a secure channel (e.g., encrypted network connections using SSH or IPSec).
- **R.2.12:** Servers must be physically located in an access-controlled environment. Servers are specifically prohibited from being operated in uncontrolled areas (e.g., cubicles, conference rooms, or public access areas).
- **R.2.13:** Critical server services must be monitored and the administrator must be notified of problems via phone, pager, or email.
- **R.2.14:** All security-related events on critical or sensitive systems must be logged and audit trails saved in accordance with the Backups section of this document.
- **R.2.15:** Security-related events must be reported to the Assistant Director of Network Services, who will review logs and report incidents to others as necessary. Corrective measures will be prescribed as needed.

- **R.2.16:** Audits of server security must be performed on at least a yearly basis using industry-recognized security assessment tools and practices.

R. Encryption

S.1 Overview

Data encryption is essential to allowing data to be conveniently exchanged across a network without unknowingly exposing it to others. The purpose of this section of the policy is to provide guidance that limits the use of encryption to those algorithms and implementations that have received substantial public review and have been proved to work effectively. Additionally, this section provides direction to ensure that federal regulations are followed and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

S.2 Policy

All sensitive (City of Boulder Protected) electronically-stored or electronically-transmitted data (including data sent in email) must be encrypted.

S.3 Requirements

Proven, publicly-disclosed algorithms such as DES, 3DES, Blowfish, Twofish, RSA, DSA, AES, RC5, and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Secure Socket Layer version 2 (SSL2) typically uses DSA encryption. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric cryptosystem keys must be of a length that yields equivalent strength. The City of Boulder's key length requirements must be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the City.

Staff must be aware that the export of encryption technologies is restricted by the U.S. government.

S. Database Administration

T.1 Overview

This section of the policy specifies requirements for securely storing and retrieving database user names and passwords (i.e., database credentials) for use by a program that will access a database running on the City of Boulder network.

Computer programs running on the City's network often require the use of one of the many internal database servers. In order to access one of these databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

T.2 Policy

In order to maintain the security of the City's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

T.3 Requirements

T.3.1 Storage of Database User Names and Passwords

- **T.3.1.1:** Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable.

- **T.3.1.2:** Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
- **T.3.1.3:** Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication, as long as the LDAP server is accessed only through encrypted (usually SSL) means. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- **T.3.1.4:** Database credentials may not reside in the documents tree of a web server.
- **T.3.1.5:** For databases containing City of Boulder Protected data, pass-through authentication (i.e., Oracle OPSS authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.
- **T.3.1.6:** Passwords or passphrases used to access a database must adhere to the authentication standards outlined in this document.

T.3.2 Retrieval of Database User Names and Passwords

- **T.3.2.1:** If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.
- **T.3.2.2:** The scope into which database credentials may be stored must be physically separated from the other areas of application code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.
- **T.3.2.3:** For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

T.3.3 Access to Database User Names and Passwords

- **T.3.3.1:** Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- **T.3.3.2:** Database passwords used by programs are system-level passwords as defined in the Authentication section of this document.
- **T.3.3.3:** Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Authentication section of this document. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

T. Ongoing Vigilance

U.1 Overview

The overall security of the City of Boulder, its assets, and ultimately each employee's position requires daily attention from every member of the staff. The most important thing network and systems administrators can do for the City's computer security is to encourage all users to remain vigilant and aware of security issues.

U.2 Policy

All users of City of Boulder computing resources are responsible for being alert to possible system security compromises. Administrators are responsible for assisting and instructing users to follow established security policies and to be vigilant with regard to suspicious events. Administrators are also responsible for monitoring security aspects of the City's systems on a regular basis.

U.3 Requirements

U.3.1 User Responsibilities

In the City of Boulder environment, users should consider the following as examples of suspicious activities:

- **U.3.1.1:** Anyone asking for their own password or authentication credentials
- **U.3.1.2:** Unexpected email attachments from outside the City of Boulder, especially generic messages or attachments with unfamiliar file types
- **U.3.1.3:** Solicitations by people or programs to install or activate new functionality on their computers (e.g., “Download and install now?” pop-up boxes and the like should not be used without authorization from the IT Department)
- **U.3.1.4:** Strange files or programs on their computer or a server
- **U.3.1.5:** Unusual or inconsistent log entries
- **U.3.1.6:** Unexpected application or server failure
- **U.3.1.7:** Unexpected, significant changes in performance, response time, or usability

U.3.2 Administrator Responsibilities

Likewise, administrators must take responsibility for monitoring various aspects of the system on a regular basis, including:

- **U.3.2.1:** Reviewing firewall, intrusion detection system, operating system, and application security logs at least weekly.
- **U.3.2.2:** Reviewing performance monitoring trends with regard to security at least twice a month, looking for abnormal bandwidth, disk, or processor use.
- **U.3.2.3:** “Prowling around” for suspicious system behavior or unexpected files/accounts at least once a month.
- **U.3.2.4:** Comparing actual software and operating system patch levels to documented patch levels at least once a quarter.
- **U.3.2.5:** Validating that user accounts and permissions match documented (and actual) requirements at least semiannually.

U. Documentation

V.1 Overview

Documentation is one of the most critical ingredients in security. It provides a baseline for identifying changes and a tool for debugging problems. As a necessary tool for building a secure network environment, it should be a high priority.

V.2 Policy

At a minimum, the following information must be available for each system and network device:

- Make, model, and serial number
- Technical specifications (processor, memory, disk, network interfaces, etc.)
- Applications in use (OS, network servers, security applications)
- Application versions and patch levels
- Vendor support agreement contact information

Network administrators must maintain a logical network diagram that is clear, easy to read, and up to date. Every network device must be identified on the diagram, including LAN and WAN components. The diagram must include as much relevant detail (IP addresses, host names, etc.) as possible without overcrowding the diagram. Additional information may be stored in spreadsheets or similar form.

All network equipment, servers, network cables, and similar components must be physically labeled with relevant details (e.g., host name, IP address, network interface port, etc.) so as to uniquely identify them.

V. Managing Software Patches and Upgrades

W.1 Overview

Because software vendors release so many security-related patches and upgrades, it is essential that they be addressed in a timely, professional manner to ensure the overall security of the computing environment. It is the City administrators' responsibility to apply available patches to all systems.

W.2 Policy

All systems must be patched to current levels. The City's network, system and application administrators are responsible for daily monitoring of patch and upgrade announcements from all vendors whose software products are in use in the organization. Administrators must meet as needed to prioritize patches and upgrades, placing those with significant security impact at the top of the list. All security-related patches and upgrades must be reviewed within 72 hours, and critical patches must be applied within 10 days of release from the vendor. All other patches and upgrades must be applied as soon as practical, not to exceed 30 days from the date of release from the vendor. The City's policy exception process must be followed for systems or applications that cannot meet these requirements.

W.3 Requirements

- **W.3.1:** Patches must be reviewed within 72 hours.
- **W.3.2:** Critical patches must be applied within 10 days.
- **W.3.3:** Non-critical patches must be applied within 30 days.
- **W.3.4:** Only patches from verified, known, reputable sources may be applied to systems.
- **W.3.5:** All new systems must be at current patch levels prior to being added to the City network.
- **W.3.6:** Network, system and application administrators must keep a log of patch applications.
- **W.3.7:** Regular auditing and validation of patch compliance must be conducted to ensure proper policy compliance and system integrity.

W. External Connections

X.1 Overview

External connections between the City of Boulder network and those of third parties are sometimes necessary to facilitate effective business communications between organizations. It is possible to deploy them in such a way that they present only a minimum amount of security risk to the organization, but care must be taken to ensure this is the case.

X.2 Policy

All external connections to the City of Boulder network shall be implemented on a case-by-case basis and must be approved by the Assistant Director of Network Services. No external connections are allowed on even an ad hoc or temporary basis without approval from the Assistant Director of Network Services after careful consideration of the security impact.

X.3 Requirements

- **X.3.1:** When approved, access through external connections should be limited to only those resources that are absolutely necessary to meet the business need.
- **X.3.2:** Third parties must notify the City of Boulder of employment status changes of personnel who utilize the external connection. Adequate steps should be taken by both the City of Boulder and the third party to revoke any access to unauthorized personnel.

- **X.3.3:** The City of Boulder should always place external connections on the outside of a City-owned and operated firewall, never relying on the firewall of the connecting party to protect the City.
- **X.3.4:** All external connections made over public networks must adhere to the Encryption policy section of this document.
- **X.3.5:** External connections should be approved for a limited (possibly renewable) time period, such as six months or a year, so their purpose and necessity can be re-evaluated on a regular basis.
- **X.3.6:** Third parties requiring connection to the City of Boulder network must read and conform to the Connected Partner Security Contract Addendum.

X. Auditing

Y.1 Overview

This provides the authority for members of the City of Boulder IT staff to conduct a security audit on any system at the City.

Audits may be conducted to:

- Ensure integrity, confidentiality, and availability of information and resources.
- Investigate possible security incidents to ensure conformity to City of Boulder security policies.
- Monitor user or system activity where appropriate.
- Meet regulatory or contractual obligations.

This section of the policy covers all computer and communication devices owned, leased, or operated by the City. This section also covers any computer and communications devices that are present on City of Boulder premises, or connected via a VPN, but which may not be owned or operated by the City.

Y.2 Policy

Audit activity must be approved by the City's IT Director. When approved, and for the purpose of performing an audit, any access and information needed will be provided to members of the City of Boulder's IT staff. All information resulting from an audit must be handled securely, confidentially and on a need-to-know basis.

Access for auditing purposes may include the following unless otherwise prohibited by law or other City policy:

- **Y.2.1:** User-level and/or system-level access to any computing or communications device.
- **Y.2.2:** Access to information (electronic, hardcopy, etc.) that may be produced, transmitted, or stored on City of Boulder equipment or premises.
- **Y.2.3:** Access to work areas (labs, offices, cubicles, storage areas, etc.).
- **Y.2.4:** Access to interactively monitor and log traffic on City of Boulder networks.
- **Y.2.5:** Access to all security-related events on critical or sensitive systems and devices.

Additional information:

- **Y.2.6:** Auditors will work to minimize the impact on production systems and networks.
- **Y.2.7:** Administrators and users must require proper documentation and identification prior to providing any access requested by auditors. Additionally, audit team members should offer proper documentation and identification when approaching an administrator or user.
- **Y.2.8:** Internal and external audits will be conducting as needed and on a regular schedule as per the city's annual work plan.
- **Y.2.9:** The presence of wireless access points will be tested for by using a wireless analyzer or by deploying a wireless IDS/IPS to identify all wireless devices in use on a quarterly basis for the CDE and annually for the non-CDE.

- **Y.2.10:** Internal and external network vulnerability scans will be run at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

Y. Non-City-Owned Equipment

Z.1 Overview

When equipment that the City does not own is attached to the City network, it must be secure to the same degree that City-owned equipment is secure and adhere to this policy. This protects both the equipment owner and the City from a security breach resulting from previous misconfiguration or violation.

Z.2 Policy

All non-City-owned equipment must conform to the same requirements as City-owned equipment, as outlined in this policy, while connected to the network by any means.

Z.3 Requirements

- **Z.3.1:** Non-City-owned equipment must comply with the requirements in all relevant sections of this policy including, but not limited to, the following: Acceptable Use/Allowed Services, Remote Access, Virus Protection, Server Security, and Managing Patches and Upgrades.

Z. Mobile Devices

AA.1 Overview

Data that leaves City facilities on mobile devices (laptops, tablets, PDAs, phones) or removable media (CDs, DVDs, USB “thumb drives,” etc.) is at elevated risk of compromise. It is critical that City employees take extra security measures to ensure that data on mobile devices and removable media is secure. This protects the privacy and security of the City, its employees, and its residents.

AA.2 Policy

No City of Boulder Protected information may be removed from City facilities on mobile devices or removable media without adequate security controls.

AA.3 Requirements

- **AA.3.1:** Protected or otherwise sensitive information must be encrypted using an encryption program approved by the IT department before it can be removed from City facilities on a mobile device or removable media.
- **AA.3.2:** All City mobile devices containing Protected information or operating within the CDE must have their full hard disks or storage media encrypted using a disk or partition-level application approved by the IT department.
- **AA.3.2:** All portable devices containing any City information should be configured to use a password-protected screensaver that activates after a period of inactivity.

AA. System / Application Certification Checklists

BB.1 Overview

Security certification checklists help ensure security policies and practices are applied in a consistent manner, and that new systems and application implementations meet existing security policies. The City has developed system and application checklists that help ensure the City’s systems and applications meet a

baseline level of security. Certification checklists must be updated as security policy changes, and new checklists will need to be created as the City adopts new technologies.

BB.2 Policy

All new system and application implementations must follow a certification checklist if the system or application is listed in the requirements section of this policy.

BB.3 Requirements

- The following system and application checklists must be followed:
- **BB.3.1:** Linux Hardening Checklist
- **BB.3.2:** Windows Server Hardening Checklist
- **BB.3.3:** Netware Hardening Checklist
- **BB.3.4:** MySQL Hardening Checklist
- **BB.3.5:** MSSQL Hardening Checklist
- **BB.3.6:** Oracle Hardening Checklist
- **BB.3.7:** Printer Hardening Checklist

BB. Exception Reporting

CC.1 Overview

The key to effective security is to set policy that can be achieved, and to ensure compliance with that policy. The City of Boulder exception handling committee will review and maintain all policy exception requests submitted using the Policy Exception Request Form.

CC.2 Policy

Users must fill out the Policy Exception Request Form in order to request a change to existing City of Boulder Policy. The City of Boulder exception handling committee will review the request.

CC.3 Requirements

- **CC.3.1:** Exceptions must be submitted on a City of Boulder Policy Exception Request Form.
- **CC.3.2:** All policy exceptions must be reviewed by the City's exception handling committee.
- **CC.3.3:** The exception handling committee must approve or deny the policy exception request, and then document the committee's decision.
- **CC.3.4:** The exception handling committee must annually review all previously granted exceptions and determine whether they still need to stand.
- **CC.3.5:** Policy exceptions that have been granted must be available to the appropriate IT staff for viewing and consideration.
- **CC.3.6:** Exception handling committee members must carefully balance security regulations, risk management, and precedent setting when granting policy exceptions.
- **CC.3.7:** Policy exceptions must be only granted based on business need.
- **CC.3.8:** Policy exceptions not approved by the exception handling committee will be considered noncompliance and may be subject to disciplinary action.

III. DISCIPLINARY ACTION

Violation of this policy may result in disciplinary action, up to and including termination of employment.

IV. CONSTRUCTION AND INTERPRETATION

Employees who have questions concerning possible conflict between their interests and those of the City, or the interpretation and application of any of these rules, should direct their inquiries to the IT Department Director. The IT Department Director may refer the matter to the Human Resources Director for advice, or to the City Manager for final resolution.

V. EXCEPTIONS/CHANGE

This policy supersedes all previous policies covering the same or similar topics. Any exception to this policy may be granted only by the IT Director. This policy may be reviewed and changed at any time.

VI. REVIEW AND REVISION

This policy supersedes all previous policies covering the same or similar topics. At a minimum, this policy will be reviewed in its entirety on an annual basis by the City of Boulder IT policy review committee and updated as necessary. The policy review committee should include management stakeholders, cross-functional IT department members, and end-user representatives. Any revisions to this policy must be approved by the City Manager. It is the policy review committee's responsibility to communicate any policy changes to the City of Boulder IT staff.