CITY OF BOULDER

****

POLICIES AND PROCEDURES

CONNECTED PARTNER SECURITY POLICY

EFFECTIVE DATE:

LAST REVISED: 12/2006

_____

CHRISS PUCCIO, CITY IT DIRECTOR

Table of Contents

1. INTRODUCTION

The City of Boulder's holistic approach to information technology security extends to partners and affiliates with access to the City of Boulder network and other City resources. This document details the City's policy on security awareness and compliance as it relates to its partners and affiliates.

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 partners/affiliates are responsible for knowing and complying with all components of this policy. Questions about the policy should be directed to the City of Boulder IT Department.

2. POLICY

A. Acceptable Use / Allowed Services

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.

A.2 Policy

- **A.2.1:** Use of City systems and resources for personal use by partners/affiliates is not permitted.
- **A.2.2:** 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 for any purpose. 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, or (5) breach of system security. The contents of these systems may be disclosed by City of Boulder Management within or outside of the City of Boulder without partner/affiliate 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.
- **A.2.3:** Recognizing that technology processes are constantly changing, for any current or future technology-related issues not explicitly covered by this policy, partners/affiliates should act in the spirit of this policy. Any questions should be directed to the City of Boulder IT Director.

B. Personnel Background Screening

B.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.

B.2 Policy

All City of Boulder partners/affiliates 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.

B.3 Requirement

- **B.3.1:** Any City of Boulder partner/affiliate 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.

C. Remote Access

C.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, dial-in or cable modems, other leased-line services, VPN, and wireless.

C.2 Policy

Only individuals with specific business need may be granted remote access to the City of Boulder network. Requests for remote access 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 partners/affiliates with remote access privileges to the City network to ensure that their remote access connection is given the same consideration as an on-site connection to the City network.

C.3 Requirements

- **C.3.1:** At no time may City of Boulder partners/affiliates provide their remote login information to anyone.
- **C.3.2:** Nonstandard remote access modes, hardware, or configurations must be approved by the City of Boulder IT Department.
- **C.3.3:** All 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.
- **C.3.4:** 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.
- **C.3.5:** Any violations of these guidelines may result in the termination of the remote access channel.

D. Authentication

D.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 partners/affiliates with access to City of Boulder systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

D.2 Policy

- **D.2.1:** All partner/affiliate accounts with the City of Boulder must have a password.
- **D.2.2:** 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.
- **D.2.3:** All user-level passwords (e.g., email, web, desktop computer, etc.) on systems that allow partners/affiliates to independently change the password must be changed at least every 120 days.
- **D.2.4:** Passwords must not be inserted into unencrypted email messages.
- **D.2.5:** All passwords must conform to the requirements described below.

D.3 Requirements

D.3.1 General Password Construction Standards

Acceptable passwords have the following characteristics:

- **D.3.1.1:** Contain both upper and lower case characters (e.g., a-z, A-Z).
- **D.3.1.2:** Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./).
- **D.3.1.3:** Are at least eight alphanumeric characters long.
- **D.3.1.4:** Are not a word in any language, slang, dialect, jargon, etc.
- **D.3.1.5:** Are not based on personal information, names of family, etc.
- **D.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.

D.3.2 Password Protection Standards

D.3.2.1: Partners/affiliates 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.).

D.3.2.2: Partners/affiliates must not share City of Boulder passwords with anyone. All passwords are to be treated as sensitive, confidential information.

D.3.2.3: If an account or password is suspected to have been compromised, the incident must be reported to the City of Boulder IT Department and the password changed.

E. Virus Protection

E.1 Overview

Viruses, worms, and Trojan horses are designed to infect, control, and damage computers and networks. They are discovered daily, and each is designed to serve a unique function or purpose. 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 the City of Boulder and its partners/affiliates.

E.2 Policy

Virus protection software must be installed and maintained on all systems connected to the City of Boulder network.

E.3 Requirements

- **E.3.1:** Virus protection software must be installed and maintained on all systems.
- **E.3.2:** Virus protection software updates must be downloaded and installed as they become available.
- **E.3.3:** Virus protection software must be configured to scan for viruses in real time.

F. Ongoing Vigilance

F.1 Overview

The overall security of the City of Boulder requires daily attention from every member of the staff, including partners/affiliates. The most important thing partners/affiliates can do for the City's computer security is to remain vigilant and aware of security issues.

F.2 Policy

All users of City of Boulder computing resources are responsible for being alert to possible system security compromises.

F.3 Requirements

In the City of Boulder environment, partners/affiliates should consider the following as examples of suspicious activities:

- **F.3.1:** Anyone asking for their own password or authentication credentials
- **F.3.2:** Unexpected, significant changes in performance, response time, or usability
- **F.3.3:** Unusual or inconsistent log entries

G. Documentation

G.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.

G.2 Policy

Partners/affiliates must document with designated City IT staff all activities relating to City resources, including but not limited to installations, upgrades, patches, configuration changes, application installations/removals, and service activations/deactivations.

H. Managing Software Patches and Upgrades

H.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.

H.2 Policy

All systems connecting to the City of Boulder network must be patched to current levels.

H.3 Requirements

- **H.3.1:** Only patches from verified, known, reputable sources should be applied to systems.
- **H.3.2:** Regular auditing of patch compliance may be conducted to ensure proper policy compliance and system integrity.

I. External Connections

I.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.

I.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.

I.3 Requirements

- **I.3.1:** When approved, access through external connections should be limited to only those resources that are absolutely necessary to meet the business need.
- **I.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.
- **I.3.3:** 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.

J. Non-City-Owned Equipment

J.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.

J.2 Policy

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

J.3 Requirement

- **J.3.1:** Non-city-owned equipment must comply with the requirements in all sections of this policy.

K. Account Types

K.1 Overview

Vendors needing access to systems on the City of Boulder network will adhere to the following policy that establishes what type of account is appropriate for the vendor. If a vendor is determined to need access, it will have one of two types of access: individual accounts or shared accounts.

K.2 Policy

City of Boulder's preferred method of providing vendors with access for remote support is through individually identifiable accounts, particularly in the case where administrative rights are required. If a vendor has dedicated technicians that will provide support, they need to have their own accounts. If a vendor has a pool of 10 or more technicians that might or might not provide remote support, and that don't promote code in the City of Boulder environment, City of Boulder will consider letting the vendor use one account, based on the following procedures:

K.3 Procedure

K.3.1 Vendors with Individual Accounts

Individual accounts are those accounts that are associated with a particular person. For example, vendor X will have multiple accounts associated with it, one for each person that will need access to the City of Boulder network.

K.3.1.1: If **any** of the following conditions are met, the vendor must use individual accounts:

- **K.3.1.1.1:** Vendor provides eight or more hours of support in a month
- **K.3.1.1.2:** Vendor promotes code in the City of Boulder environment
- **K.3.1.1.3:** Vendor has a pool of less than 10 technicians that might provide support

K.3.1.2: Vendor requirements:

- **L.3.1.2.1:** Signed user security policy agreements each individual receiving access
- **L.3.1.2.2:** Agreement that in the event a vendor employee is terminated City of Boulder will be notified and the password will be changed within 24 hours

K.3.2 Vendors with Shared Accounts

Shared Accounts are those accounts that are used by multiple individuals. In this case, there is one account associated with a vendor for all people requiring access to the City of Boulder network.

If none of the Individual Account conditions apply, then a vendor may elect to have a shared account.

K.3.2.1 Vendor requirements:

- **K.3.2.1.1:** User security policy agreement signed by a supervisor within the vendor company
- **K.3.2.1.2:** Demonstrated ability and willingness to provide in a timely manner a log describing who used the shared account, when it was used, and what it was used for.
    - **K.3.2.1.2.1:** If the vendor is not willing or able to provide this log, the shared account will be removed and the vendor will be required to use individually identifiable accounts, obtained through the standard City of Boulder staff entry process for vendors.
- **K.3.2.1.3:** Agreement that in the event an employee who has access to the shared login is terminated, the vendor will notify City of Boulder and change the password within one hour of termination.

3. DISCIPLINARY ACTION

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

4. CONSTRUCTION AND INTERPRETATION

Partners/affiliates 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 City of Boulder IT Department. The IT Department may refer the matter to the Human Resources Director for advice, or to the City Manager for final resolution.

5. 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. Policy sections may be reviewed and changed any time at the discretion of the policy review committee. It is the policy review committee's responsibility to communicate any policy changes to the City of Boulder IT staff.