University of Colorado

Information Technology Services

2007 CU-Boulder Private Data System Security Requirements

Table of Contents

1 General compliance requirements

Maintain the system in compliance with the CU-Boulder Minimum Security Standards and relevant governmental regulations or contractual requirements.

2 Install and maintain a firewall to protect data

Firewalls are hardware or software devices that control computer traffic allowed into CU-Boulder's network from outside, as well as traffic into more sensitive areas within CU-Boulder's network. All systems need to be protected from unauthorized access from the Internet, whether for e-commerce, employees' Internet-based access via desktop browsers, or employees' email access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems.

NOTE: Credit card associations require hardware not software firewalls.

a. Private data systems must be behind a network firewall. Firewall management must have formal process for approving all external network connections so as to ensure that changes are not be made in an "ad-hoc" manner and require change control procedures. Firewalls will be configured so as to:

    i. Deny all traffic from "untrusted" networks/hosts, except for ports required for client communication. For example:

        - Web protocols -HTTPS typically TCP port 443.
        - System administration protocols (e.g., Secure Shell (SSH) or Terminal Services)
        - IPSec or VPN protocols

    ii. Restrict connections between publicly accessible servers and any component storing private data, including any connections from wireless networks. The firewall configuration must deny all traffic except for protocols required by the business.

b. Any system component that is storing financial data (e.g., bank routing and account numbers or credit card account numbers) or Social Security Numbers must be located on an ITS provided CU-Boulder private address network segment

c. Systems containing credit card holder information must implement Internet Protocol (IP) masquerading to prevent internal addresses from being revealed to the Internet. Use technologies that implement RFC 1918 address space, such as Port Address Translation (PAT) or Network Address Translation (NAT).

d. Monitor network equipment load and status with reasonable regularity.

3 Patch management

Keep security patches up-to-date and maintain change control

Attackers use security vulnerabilities to gain privileged access to systems. These vulnerabilities are fixed via security patches from vendors, and all systems need to have current software patches to protect systems against exploitation by employees, external hackers, and viruses.)

a. Make sure all systems and software have the latest vendor-supplied security patches.

   i. Keep up with vendor changes and enhancements to security patches.

   ii. Install new/modified security patches within one week of release.

b. Test all security patches before they are deployed.

c. After installation, verify that patches installed correctly

d. Follow change control procedures for system and software configuration.

4 Protect Stored Data

Encryption is the ultimate protection mechanism because even if someone breaks through all other protection mechanisms and gains access to encrypted data, they will not be able to read the data without further breaking the encryption. Care however must be made to protect encryption keys. If keys are lost you will no longer be able to access the data and if keys are stolen your data may be exposed to an attacker.

a. Keep private data storage to a minimum. Limit your storage amount and retention time to that which is required for business, legal, and/or regulatory purposes.

b. Verify that private data is disposed of in accordance with University policies.

c. Applications must not store sensitive authentication data (including Magnetic Stripe (CVV) data, CVV2 data, PINs, and passwords) subsequent to a transaction authorization.

d. Encrypt all passwords

e. Mask account numbers when displayed to customers or other external parties.

f. Render financial information unreadable anywhere it is stored (including data on portable media and in logs) by using any of the following approaches:

   - One-way hashes (hashed indexes), such as SHA-2 (SHA-1 while permitted should be avoided)
   - Truncation
   - Index tokens and PADs, with the PADs being securely stored
   - Strong cryptography, such as Triple-DES or AES with associated key management processes and procedures.

g. When implementing cryptographic solutions ensure systems are isolated so that secret data cannot be disclosed.

h. Protect encryption keys against both disclosure and misuse:

   i. Restrict access to keys to the fewest number of custodians necessary.

   ii. Store keys securely in the fewest possible locations and forms.

i. Fully document all key management processes and procedures.

5 Encryption

Private Data should be encrypted during transmission, because it is easy and common for a hacker to intercept and/or divert data while in transit. Encryption of data at rest is important in the event of either physical access or loss of a system.

a. Use strong cryptography and encryption techniques such as Secure Sockets Layer (SSL) or Internet Protocol Security (IPSEC) to safeguard private data during transmission over public networks.

NOTE: ITS does not consider Point to Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP) secure for private data

b. Never send private data via unencrypted e-mail.

c. Encrypt non-console administrative access. Use technologies such as SSH or RDP that are properly configured to use strong encryption and limit access to trusted hosts.

6 Restrict access to data by business need-to-know.

This ensures critical data can only be accessed in an authorized manner.

a. Develop a data control policy. Limit access to computing resources and private data to only those individuals whose job requires such access.

b. Establish a mechanism for systems with multiple users that restricts access based on a user's need to know.

7 Assign a unique ID to each person with computer access.

This ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

a. Uniquely identify all users before allowing them to access system resources or private data.

b. Employ at least one of the methods below to authenticate all users:

- CU-Access for CU-Boulder affiliated users
- Token devices (i.e., Secured, certificates, or public key)
- Biometrics

c. Implement two-factor authentication (i.e., using two of the authentication mechanisms listed in 6.b above) for system administrator or "root" remote access to systems containing private data. Use technologies such as RADIUS or TACACS with tokens.

d. Ensure proper user authentication and password management for privileged users (e.g., administrators, developers):

   i. Control the addition, deletion, and modification of user IDs, credentials, or other identifier objects.

   ii. Immediately revoke accesses of terminated users.

   iii. Remove inactive user accounts at least every 90 days.

   iv. Distribute password procedures and policies to all users who have access to private data.

   v. Do not permit group passwords.

   vi. Change privileged user passwords at least every 180 days.

   vii. Ensure password strength is compliant with the ITS Access and Authorization Policy http://www.colorado.edu/its/docs/policies/accesspolicy.html.

   viii. Use passwords containing both numeric and alphabetic characters.

   ix. Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.

   x. Monitor system access attempts. Limit repeated attempts by locking out the user ID after not more than six attempts.

   xi. Set the lockout duration to thirty minutes or until administrator enables the user ID.

   xii. If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.

   xiii. Authenticate all access to any database containing private data. This includes access by applications, administrators, and all other users.

8 Secure configurations

Do not use vendor-supplied defaults for system passwords and other security parameters. Attackers (external and internal to CU-Boulder) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.)

a. Always change the vendor-supplied defaults before you install a system on the network (i.e., passwords, SNMP community strings, unnecessary accounts, etc.).

b. Develop system configuration standards for all networks components. Make sure these standards address all known security vulnerabilities and industry best practices.

   i. Implement only one application or primary function per network component (i.e., one application per server).

   ii. Disable all unnecessary services

   iii. Configure system security parameters to prevent misuse.

   iv. Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems (e.g., unnecessary web servers). Network components include, but are not limited to servers, routers, switches, and firewalls.

c. Establish a process to identify newly discovered security vulnerabilities. Update your standards to address new vulnerability issues.

9 Access management

Track all user access to financial information (e.g., bank routing and account numbers or credit card account numbers) or Social Security Numbers by a unique IDLogging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

a. Establish a process for linking all data access activities (especially those with root or administrative privileges) to an individual user or system.

b. Implement automated audit trails to reconstruct the following events:

   i. All accesses to private data

   ii. All actions taken by any individual with root or administrative privileges

   iii. Access to all audit trails

   iv. Invalid logical access attempts

   v. Use of identification and authentication mechanisms

   vi. Initialization of the audit logs

   vii. Creation and deletion of system level objects

c. Record the following audit trail entries for each event:

   i. User identification

   ii. Type of event

   iii. Date and time

   iv. Success or failure indication

v. Origination of event

vi. Identity or name of affected data, system component, or resource

d. Secure audit trails so they cannot be altered in any way.

e. Review security, firewall, and server logs at least daily.

f. Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations. An audit history usually covers a period of 2 years or more.

10 Regularly test security systems and processes

Vulnerabilities are continually being discovered by hackers/researchers and introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and through changes. Additionally, elements CU-Boulder relies on during an emergency, such as disaster recovery plans and incident response plans, should be tested to ensure they work as expected.

a. Test security controls, limitations, network connections, and restrictions routinely to make sure they can adequately identify or stop any unauthorized access attempts.

b. Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades).

c. Software and application development is based on industry best practices and information security is included throughout the software development life cycle.

i. Before promoting custom application code to the production site, review it carefully to identify any potential coding vulnerability.

ii. Development of web software and applications is based on the Open Web Application Security Project guidelines (www.owasp.org).

d. Perform penetration testing on network infrastructure and applications at least once a year and after any significant infrastructure or application upgrade or modification (e.g., operating system upgrade, sub-network added to environment, web server added to environment, etc.).

e. Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files.

i. Designate specific personnel to be available on a 24/7 basis to respond to reports of unauthorized critical system or content file changes.

ii. Perform critical files comparisons at least daily (or more frequently if the process can be automated).

Critical files are not necessarily those containing private data. For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of

which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the merchant or service provider.

a. Be prepared to respond immediately to a system breach.

   i. Understand the CU-Boulder Incident Response Plan

   ii. Test the plan at least annually.

   iii. Provide appropriate training to staff with security breach response responsibilities.

b. Make sure media is backed up nightly to adequately facilitate recovery. Store media back-ups in a secure off-site facility, which may be either an alternate third-party or a commercial storage facility.

11 Security Awareness

Ensure that all employees and contractors understand and have agreed to comply with CU-Boulder policies. A strong security policy sets the security tone for the whole business unit, and lets employees know what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

a. Develop daily operational security procedures that are consistent with requirements in this specification.

b. Make sure your security policy and procedures clearly define information security responsibilities for all employees and contractors.

c. Assign to an individual or team the following information security management responsibilities:

   i. Establish, document, and distribute security policies and procedures.

   ii. Monitor and analyze security alerts and information and distribute to appropriate personnel.

   iii. Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

   iv. Administer user account and authentication management, including additions, deletions, and modifications resulting from user changes and terminations.

   v. Monitor and control all access to data.

d. Make all employees aware of the importance of private data security:

   i. Educate employees through posters, letters, memos, meetings, promotions, etc.

ii. Require employees to acknowledge in writing they have read and understood University and CU-Boulder policies and procedures and will not inappropriately disclose University data.

e. Screen all potential employees to minimize the risk of attacks from internal sources.

f. Contractually require all associated 3rd parties with access to private data to adhere to requirements in this specification. At a minimum, the agreement should ensure that 3rd parties are responsible for security of private data, will not disclose University data, and that 3rd parties are aware of their responsibility for being compliant with requirements in this specification.

12 Physical Security

Restrict physical access to data containing financial information (e.g., bank routing and account numbers) or credit card account numbers) or Social Security Numbers. Any physical accesses to data or systems that house private data allow the opportunity to access or access data, or remove systems or hardcopies, and should be appropriately private.

a. Use appropriate facility entry controls to limit and monitor physical access to systems that store or process private data

b. Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where private data is accessible. "Employee" refers to full-time and part-time employees, temporary employees/personnel, and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually more than one day.

c. Make sure all visitors are:

i. Authorized before entering areas where private data is processed or maintained.

ii. Given a physical token (e.g., badge or access device) that identifies them as non-employees containing a fixed expiration date.

iii. Asked to surrender the physical token before leaving the facility or at the date of expiration.

d. Use a visitor log to retain a physical audit trail of visitor activity. Retain this log for a minimum of three months.

e. Physically secure all paper and electronic media (e.g., computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, faxes, etc.) that contain private data.

f. Maintain strict control over the internal or external distribution of any kind of media that contains private data

i. Label the media as "CU-Boulder Private".

ii. Send the media via secured courier or a delivery mechanism that can be accurately tracked.

g. Ensure management approves all media that is moved from a secured area (especially when media is distributed to individuals).

h. Maintain strict control over the storage and accessibility of media that contains private data:

i. Properly inventory all media and make sure it is securely stored.

ii. Implement data retention and disposal policies and procedures for all media containing private data.

i. Destroy media containing private data when it is no longer needed for business or legal reasons:

j. Shred or incinerate hardcopy materials

k. Purge, degauss, shred, or otherwise destroy electronic media so that private data cannot be reconstructed.