University of Colorado

Information Technology Services

2007 CU-Boulder Restricted Data System Security Requirements

Table of Contents

1 General compliance

Maintain the system in compliance with the CU-Boulder Minimum Security Standards.

2 Network Security

a. Acquire approval from the IT Security Office for any new external network connections. Firewall configurations must not be made in an "ad-hoc" manner and require change control procedures.

b. Install and configure host firewall software as follows:

   i. Deny all traffic from "untrusted" networks/hosts except for publicly accessible services.

   ii. Restrict access to services (i.e., authenticated services) to trusted campus networks and campus VPN addresses.

3 Protect Stored Data

a. Verify that restricted data is disposed of in accordance with University policies.

b. Encrypt all passwords as required by Private Data standards

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

d. Shred or incinerate hardcopy materials

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

4 Encryption

Encrypt transmission of restricted data across public networks. Where feasible restricted data should be encrypted during transmission over the Internet, because it is easy and common for a hacker to intercept and/or divert data while in transit.

a. When encryption is used ensure that strong cryptography and encryption techniques such as Secure Sockets Layer (SSL), Internet Protocol Security (IPSEC), S/MIME, or PGP are implemented to safeguard restricted 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 restricted data

b. Encrypt non-console administrative access. Use technologies such as SSH or RDP.

5 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 restricted 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.

6 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 restricted data.

b. Ensure proper user authentication and password management consistent with the ITS Access and Authorization policy

c. Implement system logging as described in the Minimum Security Standards implementation guide

7 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.

8 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. At minimum quarterly test security controls, limitations, network connections, and restrictions routinely to make sure they can adequately identify or stop any unauthorized access attempts.

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

   i. Understand steps required to report and handle a security incident published at http://www.colorado.edu/ITS/security/report.html

   ii. Test the plan at least annually.

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

h. 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. Test restores of backups on a regular basis.

9 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 procedures clearly define information security responsibilities for all employees and contractors.

c. Make all employees aware of the importance of restricted 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.

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

10 Restrict physical access to restricted data

Any physical accesses to data or systems that house restricted data allow the opportunity to access or access data, or remove systems or hardcopies, and should be appropriately restricted.

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

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

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

d. Maintain strict control over the storage and accessibility of media that contains restricted 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 restricted data.

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

f. Shred or incinerate hardcopy materials

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