

**Effective:** October 2, 2003  
**Responsible Office:** CIO  
**Policy Title:** Access and Authorization Policy  
**Approved:** *IT Council*  
**Purpose:** Outlines standards for access and password requirements.

---

## **A. Rationale of Policy:**

Information Technology Services (ITS) is the largest single provider of computing resources on the Boulder campus, maintains the bulk of the campus networks, and controls the telecommunication switch. A lack of standards or consistency in access and authorization controls for ITS systems can have a serious impact for IT on the Boulder campus. The impact is furthered since the campus will generally mirror actions or standards taken by ITS.

The Access and Authorization Policy sets standards for access requirements and methodologies, password and password management, and authorization requirements and mechanisms. The policy also includes procedures for handling policy exceptions and auditing policy compliance.

## **B. Policy:**

### **1. Scope of Policy**

This policy will include all systems owned or maintained by ITS that provide services to the campus or directly support campus IT resources. This includes for example remote access servers, network routers and switches, Internet servers, and campus information systems.

### **2. Access requirements and methodologies used for ITS systems**

Faculty, staff and students who are currently affiliated with the University of Colorado at Boulder (CU-Boulder) are eligible to use computer accounts (e-mail, web, and Identikey). The UCB Enterprise Directory defines affiliation with the University.

All ITS system users have the responsibility to use University services in an effective, efficient, ethical, and legal manner. Users must agree to the "Use of CU-Boulder's Computing and Network Resources" policy when they receive an account.

As an affiliate with the University and verified through the Directory, an individual is eligible for a computing account and network access. A student can also create his or her account through Self Account Creation (SAC).

### **3. Unit discretion for ITS managed systems but that ITS does not own**

Service agreements for systems that ITS manages but does not own must specify access requirements. The owner of the system is responsible for specifying application level access and ITS will control system level access. The requirements must ensure that systems managed by ITS do not allow unauthorized access to other University systems. Refer to any University-wide policies that will govern the system(s) in question.

#### **4. Password requirements for ITS systems**

All ITS systems must support strong passwords by including a mix of character classes (lower-case letter, upper-case letter, number, punctuation, and meta-character) and contain 6 or more characters. Passwords must **not** contain:

- A single word that can be found in the common English dictionary in any form, even with an uppercase letter in the middle (window, tree, treetop would all fail)
- Your personal name, common names, or log-name (i.e., john, jonathan)
- Proper nouns, including geographic locations (i.e., Colorado, Mongolia)
- Three or more consecutive repeated characters (e.g., “aaa” would fail)

#### **5. Password controls for ITS systems**

Individual account passwords will not be given out or shared under any circumstances. [Users should refer to the “Use of CU-Boulder's Computing and Network Resources” policy.](#)

Group accounts are not recommended. Where group accounts are necessary then strong account protection is required. The following ITS mandated protections apply.

- Account owner will agree to a separate rights and responsibilities agreement with the understanding that any violation of the agreement will result in termination of the account. The agreement must indicate the account purpose and individuals who will have access to the account.
- Group accounts must be pre-authorized by ITS.
- Group accounts will be audited regularly to ensure ownership is current, the account is still necessary, and account agreements are renewed.
- Passwords must be changed at regular and frequent intervals.
- Where the level of risk associated with a group account is significant, additional restrictions will be in place.

Where technically feasible, only the individual account owner can change passwords for ITS systems. Password changes can be made either via the web using the data verified from the Directory or using built-in system functions after authenticating to the system. When it is not technically feasible, and an ITS employee must reset a user’s password, the user will be forced to change his or her password at the next logon.

If ITS staff observes compromised passwords (for example, default passwords, a cracker's sniffer log, routine network monitoring, or the user has shared the password) the user’s account password will be rendered invalid and the user will be required to change their password.

#### **6. Standards for account longevity, lockout, or removal of access**

Account longevity will be tied to University affiliation and verified through the Directory. When affiliation cannot be verified access will be denied. A 30-day grace period may be allowed for University graduates or former staff for systems that do not contain sensitive or secure data.

Users should refer to the “Use of CU-Boulder’s Computing and Network Resources” policy for information regarding removal of access to ITS systems. Permanent revocation of an account or removal of home page material will only occur after due process. Inappropriate use of University technology resources may result in termination of access, disciplinary review, suspension, expulsion, termination of employment, legal action, or other disciplinary action. ITS will, when necessary, work with other University offices such as the Office of Judicial Affairs (in cases involving students), the CU Police Department, deans of schools and colleges, the Office of Legal Counsel, and others in the resolution of problems.

## **7. Requirements for critical data and levels of authentication based on risk**

All authentications to ITS systems will be encrypted. Systems that contain critical or secure data will require an encrypted session for transmission of the data over the campus network or Internet.

ITS systems that contain critical data will run a systematic audit to verify the strength of user passwords.

Systems that contain critical data will implement stronger account protection including account lockout and password change policies.

All IT systems contain some level of secure data. System managers must take additional steps to protect secure data as appropriate to the risk associated or mission criticality of the system.

## **8. Authorization requirements for ITS systems**

An authorization mechanism that controls the privileges granted to each user is required for all ITS systems. Each system manager is responsible to ensure that each individual's system governed role matches the privileges that user is entitled to receive.

The UCB Enterprise Directory will be used as the authoritative source for affiliation data for those systems that require affiliation checking as part of the authorization mechanism.

## **C. Definitions**

- Access: Process by which use of ITS systems is allowed
- Authentication: Mechanism used to prove identity
- Authorization: Mechanism to permit or deny actions desired by the user
- Critical data: Data that is protected by the Privacy Act, Trade Secrets Act, FERPA, HIPAA, or contractual obligations
- Directory: UCB Campus Enterprise Directory
- Encrypted: Data that is scrambled by means of a key or cipher
- Group Accounts: Any account where a common logname is shared by two or more individuals
- Secure data: Data that if made public could enable damage to be done to the system or the University or data that protects or enables security

## **D. Procedures**

## **1. Process for granting exceptions to the policy**

Any systems to be grandfathered will be reviewed and approved by the Access and Authorization policy group. After implementation of the policy, requests for exceptions should be presented for approval to the Executive Director of ITS or his designee.

## **2. Procedures for auditing access and authorization policy compliance**

Policy compliance will be reviewed annually by the ITS Architecture and Security group as part of the risk assessment process. Lack of compliance with the policy could result in a system being disconnected from the campus network, a staff member or group losing management of the problem system, or other disciplinary actions.

## **E. References**

Use of CU-Boulder's Computing and Network Resources <http://www.colorado.edu/policies/cnr/>

## **F. Responsible Organization**

The CIO Office will be responsible for the maintenance and review of this policy.