

CIO Campus-wide Policy

Effective:	March 2010
Responsible Office:	Office of the Associate VC for IT and CIO
Policy Title:	Account Activation, Authentication and Termination Policy (replaces Access and Authorization Policy)
Approved:	Office of the Associate VC for IT and CIO
Purpose:	Outlines expectations for the electronic identifier (IdentiKey) including access and password requirements, account lockout, and termination.

A. Background:

CU-Boulder must protect its information technology (IT) resources and support federal regulations and system policy governing the privacy and security of sensitive data by requiring the use of electronic identifiers and secure passwords to control access. This policy and related procedures set standards for the primary electronic identifier on the CU-Boulder campus – the IdentiKey. These standards include requirements for strong passwords, protecting passwords, lockout, termination, and compromised account responsibilities. CU-Boulder owns and manages information technology systems that are accessed using a university electronic identifier or IdentiKey. The IdentiKey consists of a login and password paired together that is unique to each individual, providing access and authorization to a variety of electronic resources, depending on the individual's responsibilities and privileges.

B. Policy Statement:

IdentiKeys allow users to access the wired and wireless network, as well as connect to resources such as CULink, CULearn, CUConnect, and campus computer labs. To protect these resources from unauthorized use, CU-Boulder requires the IT resource user to follow procedures which include specific rules regarding obtaining, changing, and terminating the IdentiKey. In addition, to avoid unauthorized access to IT resources, the IT resource user must follow specific rules for creating, using, and reporting suspected compromised IdentiKey passwords.

(See Account Activation, Authentication, and Termination Procedures for current procedures and rules.)

C. Definitions:

IdentiKey: a CU login name and password, that in combination is unique and allows a user access to the wired and wireless network, as well as connect to resources such as CULink, CULearn, CUConnect, and campus computer labs. IdentiKey is managed with CU-Boulder's Identity Manager.

IT Resource User: Individuals that are authorized to use University IT resources. Examples of users include: faculty, staff, students, researchers, vendors, volunteers, contractors, or sponsored affiliates of the University.

D. Responsible Organization:

The Office of the VC for IT and CIO will be responsible for the enforcement, maintenance, and review of this policy.

CIO Campus-wide Policy

E. History:

Initial Policy Effective: October 2003

Supersedes: Access and Authorization Policy

CIO Campus-wide Policy

Effective:	March 2010
Responsible Office:	Office of the VC for IT and CIO
Procedure Title:	Account Activation, Authentication and Termination Procedure
Approved:	Office of the VC for IT and CIO
Purpose:	Outlines the process for the electronic identifier (IdentiKey) including access and password requirements, account lockout, and termination.

A. Procedures associated with account activation, authentication, and termination:

1. Create Strong Passwords:

To achieve appropriate security when authenticating to IT resources, the University has established rules for creating a strong, unique IdentiKey password. These passwords must be strong enough to withstand attempts by unauthorized users attempting to compromise them. IT resource users will not be required to make frequent password changes once the strong password is established. Periodic password changes are recommended as good practice.

Rules when creating a unique password:

- Must be at least 10 characters long
- Must include at least 3 character classes (alpha, numeric, symbols)
- Cannot contain your CU Login Name
- Cannot contain your first or last name
- Cannot contain 3 or more contiguously repeated characters (a password with the string 'aaa' will not be allowed)
- Cannot contain the following characters: tab, space, double-quote (“), colon (:)

2. Protect Passwords:

To avoid unauthorized access to IT resources, IT resource users must follow the APS “IT Resource User Responsibilities Policy” which states that passwords must be protected and not shared.

3. Setting or Resetting Passwords:

Passwords cannot be obtained through the IT Service Center. The IT resource user will set his or her own password through the activation process that entails accepting the Computing & Network Resources Policy, setting security questions, and setting a password. Activation requires personal information (e.g. ID number, date of birth, etc.)

After five failed login attempts the IT resource user will be locked out of his or her account and will need to reset the password through Identity Manager or the IT resource user can wait five minutes and attempt to login again. Refer to the [IdentiKey Information page](#) for additional details. If the password needs to be reset, the IT resource user will need his or her CU Login Name and answers to his or her security questions.

CIO Campus-wide Policy

4. Termination of Account:

An IdentiKey will be terminated only when all relationships (e.g. affiliations) between an IT resource user and the university no longer warrant an IdentiKeyⁱ.

Termination of an IdentiKey triggers a process that revokes the IdentiKey itself and begins the revocation of all access privileges associated with the IT resource user's IdentiKey. The typical process for terminating an IdentiKey occurs when the IT resource user loses all affiliation with the university (i.e. from resignation, termination, matriculation, etc.), which is initiated by either the payroll liaison (in the instance of an employee) or the Registrar Office in the case of students. In these instances, changes are made in the systems of record (i.e. PeopleSoft, ISIS, etc.) and no further activity is needed to terminate an IdentiKey.

In the instance of necessitating an immediate termination of an IdentiKey for an employee or other non-student affiliate, the Organization Unit Head or Appointing Authority can contact the IT Service Center. In the instance of students, the Registrar's Office has the authority to initiate the termination of an IdentiKey for a student. The Registrar's Office would contact the IT Service Center.

5. Compromised Account:

An IT resource user who suspects that his or her password has been compromised must reset his or her password immediately through Identity Manager. Refer to [Identity Manager](#) page for additional details. If the IT Security Office discovers that a password has been compromised the account will be disabled and the IT resource user will be notified. Additionally, if a password is compromised, lost or stolen, the IT resources user will report the incident to the ITS Service Center (5-HELP or 303.735-4357)

B. Responsible Organization:

The Office of the VC for IT and CIO will be responsible for the enforcement, maintenance, and review of these procedures.

Effective March 2010

ⁱ As one relationship may be terminated, such as employment, another may remain, such as alumni status. Given this, access to services should be based upon authorization to online services or data resources, not simply on authentication using IdentiKey credentials.