University of Colorado

Procedure

Category – Information Management and Technology **P**

IT Security Training Standards and Core Topics

Effective:	January 1, 2007
Responsible Office:	Office of Information Security
Related APS:	IT Security in Personnel Job Descriptions, Responsibilities, and Training
Brief Description: Identifies minimum requirements and core training topics for *IT security* awareness and education programs.	

I. DEFINITIONS

Italicized terms used in this procedure are defined in the Administrative Policy Statement *Dictionary*. Underlined terms are defined in the associated Administrative Policy Statement: IT Security in Personnel Job Descriptions, Responsibilities, and Training.

II. PROCEDURE DESCRIPTION

Information technology *(IT) security* awareness and education programs are vital components of the University's *IT Security Program*. *IT resource users* must be aware of their responsibilities to protect University information and be adequately trained to fulfill those responsibilities. This procedure establishes the minimum requirements and core training topics for campus *IT security* awareness and education programs.

A. Training Requirements: The minimum requirements for *IT security* training programs are as follows:

1. University employees, associates and other individuals should receive *IT security* training before or at the time they are given access to University information and *IT resources*. Otherwise, training must be provided as soon afterward as reasonably possible.
2. University employees, associates and other individuals must receive regular refresher training that reinforces *IT security* concepts, practices, and responsibilities; and addresses any new *IT security* issues that may arise.
3. University employees, associates and other individuals must receive periodic reminders about available IT security awareness and education materials. *IT security* reminders must be delivered using normal campus communications or other means with equivalent or greater effectiveness.
4. Training objectives and content must be aligned with the roles and responsibilities of the trainees to ensure a targeted and focused training effort.
5. Where practical, training must use real world examples to clearly illustrate learning principles and illuminate situations that may be encountered by trainees.
6. Training content and attendance shall be documented and made available to the campus *IT security principal* upon request.
7. Where feasible trainees must complete an assessment to determine the degree to which training objectives are met.
8. Training objectives and content must be reviewed periodically to ensure they reflect changes in campus needs, policies, and technologies, as well as external requirements, such as federal and state laws and contractual obligations.

B. **Training Topics**: The core topics to be included in *IT security* training programs are as follows:

1. Importance of *IT security* and privacy.
2. *IT security* and privacy responsibilities of the campus and University system.
3. *IT security* and privacy responsibilities of the trainee.
4. Relevant University and campus policies and supporting documents.
5. Common terms and concepts (e.g., *sensitive information*, defense in depth, strong password protection, virus protection, encryption).
6. Best practices for information security and privacy.
7. Where to find additional *IT security* and privacy information and resources.

V. HISTORY

Amended: New procedure, no amendments.
Initial Policy Effective: January 1, 2007
Supersedes: New procedure, no previous procedures.