

<b>TITLE:</b>	SECURITY TRAINING AND AWARENESS		
<b>POLICY #:</b>	P-CCSP-015	<b>EFFECTIVE DATE:</b>	DECEMBER 20, 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	FIRST RELEASE



# State of Colorado Cyber Security Policies

## Security Training and Awareness

### Overview

This policy document is part of the State of Colorado Cyber Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). All Agencies within the scope of this Policy must support and comply with the Requirements section of this document. Additional best-practice guidance is outlined in the Guidelines Section which has been designed to help an Agency achieve the objective of this Policy.

For the purposes of this document, an “Agency” includes organizations as defined in C.R.S. 24-37.5-102(5).

### Authority

C.R.S. 24-37.5-401(1), C.R.S. 24-37.5-403(2)(b)-(c), C.R.S. 24-37.5-404(2)(b).

### Scope

This policy document applies to every State agency ("Agency") as defined in C.R.S. 24-37.5-102(5). "State agency" means every state office, whether legislative, executive, or judicial, and all of its respective officers, departments, divisions, commissions, boards, bureaus, and institutions. "State agency" does not include State-supported institutions of higher education, the department of higher education, the Colorado commission on higher education, or other instrumentality thereof.

### Policy

Agencies shall ensure employees, contractors, and users of private State and Agency systems receive initial and ongoing Cyber Security Training.

THE ENCLOSED POLICIES AND PROCEDURES ARE FOR OFFICIAL USE ONLY WITHIN THE STATE OF COLORADO. THE MATERIAL MAY NOT BE COPIED OR REDISTRIBUTED WITHOUT THE PERMISSION OF THE CISO FOR THE STATE OF COLORADO.

<b>TITLE:</b>	SECURITY TRAINING AND AWARENESS		
<b>POLICY #:</b>	P-CCSP-015	<b>EFFECTIVE DATE:</b>	DECEMBER 20, 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	FIRST RELEASE



## Requirements

The Cyber Security Training Program details shall be outlined in the Agency Cyber Security Plan and support:

- All end users of systems must complete initial Cyber Security Training.
- All users must complete refresher training annually.
- Training content must be refreshed/reviewed annually.
- Training activities are to be recorded and kept in the employee's file for the duration of his/her employment.
- Annual reporting to the CISO of the Agency training completion statistics.
- Periodic delivery of security awareness training to the staff.
- Description of consequences for failure to comply with training requirements, to include the possibility of termination.

Cyber Security Training Content must include:

- The Agency's End User Acceptable Use Policy
- Colorado Cyber Security Plan overview

The Agency Cyber Security Training Program must meet the following standards:

- Initial training is required prior to use of State or Agency systems.
- Be approved by an executive with the authority to enforce the sanctions for non-compliance.

## Roles and Responsibilities

**Agency Executive Management** – is responsible for enforcing sanctions on Agency staff members that do not comply with his/her responsibilities.

**Agency Chief Information Officer (CIO)** – is responsible for ensuring appropriate budget and intra-agency executive support is available to support the Agency Cyber Security Training initiatives

**Agency Information Security Officer (ISO)** –responsible for:

- Functioning as the Agency Cyber Security Training Coordinator.
- Documenting the Agency's training standards in the Agency's Cyber Security Program Plan.
- Coordinating a periodic audit of training program effectiveness and ensuring all users receive initial and ongoing training.
- Reporting the effectiveness of the training program to the CIO.

**Agency staff** – is responsible for the following cooperating with the Agency Cyber Security Training Coordinator to receive the proper training in a timely manner.

<b>TITLE:</b>	SECURITY TRAINING AND AWARENESS		
<b>POLICY #:</b>	P-CCSP-015	<b>EFFECTIVE DATE:</b>	DECEMBER 20, 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	FIRST RELEASE



## Guidelines

This section describes best practices for meeting the objective of this policy.

### Initial and Refresher Training

A response or “quiz” is to be administered and scored once initial or refresher training is completed. This could be as simple as a 10 question brochure that is distributed with the training material in hardcopy.

Training completion is to be tracked centrally and should contain a statement by the user that he/she has completed the training and agrees with the System Access and Acceptable Use Policy, P-CCSP-013. This statement is to be filed in the employee file with the Agency Human Resources division.

### Training Awareness

Examples of training awareness initiatives include:

- Posters and other “marketing” material
- E-mail-based or memo-based security reminders
- Lunch-and-learn sessions

### State Administered Training

When approved by the CISO, State training is to meet the requirements of this policy. Until then, training materials specified by the State are to be distributed for use at the Agency level. If the Agency desires it may use it in lieu of or as augmentation to Agency training materials.

THE ENCLOSED POLICIES AND PROCEDURES ARE FOR OFFICIAL USE ONLY WITHIN THE STATE OF COLORADO. THE MATERIAL MAY NOT BE COPIED OR REDISTRIBUTED WITHOUT THE PERMISSION OF THE CISO FOR THE STATE OF COLORADO.