

TITLE:	PERSONNEL SECURITY		
POLICY #:	P-CCSP-012	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



State of Colorado

Cyber Security Policies

Personnel Security

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

All Agencies shall adhere to a framework for personnel security assurance that includes mechanisms to ensure the integrity of key personnel and that maintains the ongoing security of IT and Information Resources.

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.

TITLE:	PERSONNEL SECURITY		
POLICY #:	P-CCSP-012	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



Definitions

For the purposes of this document, refer to C.R.S. 24-37.5-102, C.R.S 24-37.5-402 and the Colorado Cyber Security Program Policy Glossary for any terms not specifically defined herein.

Roles and Responsibilities

Agency HR Manager – is responsible for:

- Coordinating background checks for staff in positions of trust.
- Responding to requests from other State agencies regarding the status of staff background check pass/fail and initial training status.
- Ensuring that new hire orientation includes Cyber Security training.

Agency IT System Administrators – are responsible for implementing procedures as directed by user supervisors to immediately terminate all facility- and system-access rights when requested;

Requirements

All departments must ensure this policy is upheld within their department.

Background Checks

Agencies must:

- Define “positions of trust” within their agency that are suitable for background checks. Include the definitions of “positions of trust” in the Agency Cyber Security Plan.
- Define “failure criteria” for their agency and document in the Agency’s Cyber Security Plan.
- Perform initial background checks on all new employees or contractors appointed to “positions of trust.”
- Perform ongoing background check updates on existing employees and contractors in positions of trust at least every three years.
- Ensure the background check includes local criminal, national criminal, credit, education, and reference checks. Include drug testing where applicable.
- Record a pass or fail in the individual’s employee file or contractor record.
- Require passing criteria as a condition of employment.
- Document the background check procedures and integrate them into the agency’s new-hire or human resources management procedures.

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.

TITLE:	PERSONNEL SECURITY		
POLICY #:	P-CCSP-012	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



Training

(See Security Training and Awareness Policy, P-CCSP-015 for additional details)

Agencies must:

- Provide all new users with Cyber Security Training including the System Access and Acceptable Use Policy, P-CCSP-013 as part of new-hire orientation

References

- Security Training and Awareness Policy, P-CCSP-015
- System Access and Acceptable Use Policy, P-CCSP-013

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.