

TITLE:	SYSTEM ACCESS AND ACCEPTABLE USE POLICY		
POLICY #:	P-CCSP-013	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



State of Colorado Cyber Security Policies

System Access and Acceptable Use Policy

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).

Users of State systems can introduce errors or compromise critical data through intentional or unintentional acts. This policy requires all Agencies to develop an Acceptable Use Policy that governs user behavior when accessing State systems. An effective Acceptable Use Policy mitigates risks to State data and systems introduced by system users.

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).

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:	SYSTEM ACCESS AND ACCEPTABLE USE POLICY		
POLICY #:	P-CCSP-013	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



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 ensure users of private State systems abide by a common set of minimum criteria and acknowledge that they understand these criteria and agree to comply with them prior to obtaining access to such systems.

Definitions

For the purposes of this document, please 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

Executive Director – is responsible for:

- Designating the responsibility of collecting and storing acknowledgement of Acceptable Use Policies.
- Delegating the responsibility of enforcing sanctions for Acceptable Use Policy violations.
- Ensuring an Acceptable Use Policy is developed and disseminated in accordance with this Policy.

Agency Chief Information Officer (CIO) – is responsible for ensuring an End User System Access and Acceptable Use policy statement is provided to staff, contractors and visitors that use private State systems prior to granting them access.

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

- Conducting periodic audits of Acceptable Use Policy (AUP) acknowledgements submitted by IT system users in accordance with the Access Control Policy.
- Performing periodic audits for rogue or unapproved software.

Agency Staff – is responsible for reading, understanding and adhering to the policy and cooperating with the Agency ISO or CISO in investigations.

Agency Staff Supervisor – is responsible for ensuring that his/her subordinates have read, understood, and have agreed to the AUP and all other security policies as a condition of employment or a condition for granting access.

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:	SYSTEM ACCESS AND ACCEPTABLE USE POLICY		
POLICY #:	P-CCSP-013	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



Requirements

Each Agency shall develop an End User Acceptable Use Policy (AUP) specific to its organization's needs. The following requirements apply:

- AUPs must identify roles and responsibilities for managers, employees, and system administrators.
- AUPs must contain sanctions for non-compliance.
- AUPs must not supercede State or Federal regulations
- AUPs must require compliance with the Colorado Cyber Security Program and Agency Policies.
- Agency employees must provide acknowledgement of the terms and conditions outlined in the AUP prior to using private Agency systems.
- Vendors, contractors, and visitors must provide acknowledgement of the terms and conditions of an AUP prior to using Agency systems.
- Agencies must record the user's acknowledgement of the AUP and maintain such acknowledgement as long as the agency systems are in use by that user.
- AUPs must define a security incident and instruct the user how to report suspected and actual incidents.
- AUPs must address usage of e-mail, Internet, telephone, remote access, and State applications.
- AUPs must state that the user has no right to privacy when using agency or State systems and that all electronic communications on State systems are monitored.
- AUPs must require the end user to use agency and State systems in a responsible, lawful, and ethical manner.
- AUPs must address responsibilities for managers with regard to hiring, transfer, and termination procedures for employees or contractors for whom they are responsible.
- AUPs must state that the use of State e-mail addresses in non-business related forums such as newsgroup postings, discussion boards, or instant messaging is expressly prohibited.
- AUPs must state that only approved software may be deployed on Agency IT systems, including P2P software, Internet Browser plug-in software, screen savers, PDA synchronization software, and encryption software, and must address procedures to request such software.
- AUPs must address the proper handling of State Data based on sensitivity (see CCSP Data Handling, and Disposal Policy P-CCSP-011).

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:	SYSTEM ACCESS AND ACCEPTABLE USE POLICY		
POLICY #:	P-CCSP-013	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



- AUPs must specify the appropriate use of agency-owned and personally-owned removable media or external devices.
- AUPs must state that the disabling of security controls is a violation of policy.
- AUPs must specifically restrict intentional attempts to compromise State systems or data, to include network scanning, vulnerability scanning, security testing, or password cracking unless specifically authorized.

Each Agency shall identify in their Cyber Security Program Plan the methods of monitoring for AUP violations, for enforcing sanctions, and for updating the Cyber Security Program Plan to include enhancements to user training and awareness.

Guidelines

See Sample Agency Acceptable Use Policy, G-CCSP-012-1.

References

Sample Agency Acceptable Use Policy, G-CCSP-012-1.

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.