

TITLE:	ACCESS CONTROL POLICY		
POLICY #:	P-CCSP-008	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



State of Colorado Cyber Security Policies

Access Control 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). “Staff” includes employees, temporary employees, and contractors, interns and volunteers within an Agency that use Agency Information Technology (IT) resources.

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 limit user access to the minimum required to perform assigned duties. Access control mechanisms for systems must be established by each Agency and incorporate the need to balance access limits with the need to execute business functions.

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:	ACCESS CONTROL POLICY		
POLICY #:	P-CCSP-008	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



Definitions

Security Enclave - is a logical boundary surrounding all resources that are controlled and protected. The protected resources are called a domain (or enclave or protected sub-network). There may be overlapping domains of varying protection, so that the most sensitive resources are in the innermost domain, which is the best protected. Protection the security perimeter may be by physical controls, identification and authentication, encryption as well as other forms of access control.

Access Control - Access controls are typically logical controls designed into the hardware and software of a computing system. Identification is accomplished both under program control and physical controls.

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

Executive Director – is responsible for designating and approving system owners, data owners, and system administrators for all major applications and critical systems.

Agency Chief Information Officer (CIO) – is responsible for:

- Ensuring the requirements of this policy are integrated into the departmental system procedures.
- Ensuring all legacy systems that cannot meet this policy are retired or upgraded.

Agency Information Security Officer (ISO) – is responsible for assuring ongoing monitoring and auditing the effectiveness of the Access Control Policy.

IT Staff – is responsible for implementing access control policies that prevent unauthorized access to systems and information.

End User – is responsible for submitting a System Access Request Form.

System Owner – is responsible for:

- Approving role-based access on a need-to-know basis.
- Approving System Access Request Forms

Requirements

All Agencies shall develop and implement policies and procedures that support the following:

Hiring Practices

- Agencies shall develop procedures that ensure that prior to granting access to sensitive systems and data, all new hires have received orientation and training that includes their responsibilities for protecting confidential information.
- All new hires shall sign the Agency-appropriate use policy before allowing access to sensitive systems and data.

TITLE:	ACCESS CONTROL POLICY		
POLICY #:	P-CCSP-008	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



Transfer / Termination Practices

Staff Resignation

- Agencies are to develop procedures that ensure staff supervisors immediately notify the Agency's IT group responsible for granting and revoking access upon receipt of a subordinate's resignation.
- Agencies are to develop procedures that govern determining whether access privileges are to be continued for the notice period, adjusted temporarily, or immediately terminated upon an employee's resignation.
- Agencies are to develop procedures that ensure lists of terminated staff are reconciled with user accounts on Agency IT systems so that all access credentials are revoked, retrieved, changed, or otherwise become inaccessible to the terminated staff member.
- Agencies are to adhere to procedures that support the termination of physical access, in accordance with the Physical Security Policy, P-CCSP-010.

Staff Termination

- Agencies are to develop procedures that ensure the IT group responsible for granting and revoking access is notified immediately upon termination of a staff member.
- The IT Department is to implement procedures to immediately terminate all facility and system access rights on notice of termination.

IT Staff Resignation, Termination and Transfer

- Agencies are to ensure the above procedures for staff resignation or termination are followed for IT staff resignation or termination.
- Account Passwords used for administration, paying special attention to any administrative passwords (such as "root"), are to be changed immediately on all systems when an IT staff member resigns, is transferred, or is terminated.

System Access Request

- Agencies are to develop procedures that, prior to initial access, each Agency's Human Resources (HR) representative has verified that an Agency Acceptable Use Policy (AUP) has been distributed to each user and a record of receipt and acknowledgement is maintained in the user's employee file or staff record.
- Agencies are to keep written records of IT System Access Requests, changes, terminations, and transfers for one year after the term of employment.
- All Agency systems are to have a "System Owner" that is responsible for approving and disapproving access requests for each given system. The System Owner grants access to requestors using a "least privilege" methodology.
- All Agencies are to employ a similar Access Request procedure for granting access to Sensitive Areas. See Physical Security, P-CCSP-010 for details.

TITLE:	ACCESS CONTROL POLICY		
POLICY #:	P-CCSP-008	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



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.

Access Credentials

- Systems that are not intended to be used anonymously must require a unique username to access.
- All systems must at a minimum require a password or other unique, private token to be validated prior to access.
- System Administrators must have individual accounts or use utilities such as “sudo” or “Run As” to perform system administration tasks.
- Service accounts must be unique per application and not allow interactive access by providing a user shell.
- Privileged accounts are not to be used for non-administrative uses if possible. System administrators are to use their individual access accounts when making changes to systems to ensure accountability.

Password Requirements

Strong passwords are required to log into critical State systems. Strong passwords must:

- Be at least eight characters in length
- Be changed at least every 60 days.
- Require the use of three out of four of the following:
 - 1) Capital letters
 - 2) Lower case letters
 - 3) Numbers
 - 4) Special characters

Log-in Requirements

- All systems must record successful and failed access attempts.
- Users are required to utilize their own individual, unique User IDs when logging into the Agency networks and applications.
- Where technically feasible, technical password controls must be implemented that enforce the guidelines in this document.

Portable Computers

- Portable systems must be considered a stand-alone “enclave” and therefore have a local firewall deployed to restrict access to it.
- Portable systems (laptops) must use full disk encryption with pre-boot authentication enabled. (See Mobile Computing Policy, P-CCSP-018).

TITLE:	ACCESS CONTROL POLICY		
POLICY #:	P-CCSP-008	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



Role Based / Least Privilege Access

- System owners must ensure that system roles are defined and provide that varying levels of access are established and are appropriate for the varying levels required for users to perform their job duties.
- Roles must only be granted based on the minimum functions required by users to perform their duties, including system or service accounts.
- Role access requests must be approved by the data owner.
- Roles must be clearly listed on a System Access Request form.

Administrative Credentials and Sessions

- Connections to the systems to perform administrative functions must be encrypted (e.g., SSH, SSL, RDP).
- Administrative credentials must use two-factor authentication or must adhere to password standards in this document if not using two-factor authentication. If using a password, it must be changed at least every 60 days.

Physical Access Controls

Specific physical access control guidance can be found in the Physical Security Policy, P-CCSP-010.

Guidelines

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

Hiring Practices

- New employees are to sign a *Statement of Understanding* acknowledging acceptance of responsibilities contained in the Colorado Cyber Security Program Policies and the Agency Acceptable Use Policy (AUP).

Termination / Transfer Practices

- Remote access, as well as the usage of any portable equipment assigned (hardware, software and other materials), are to be discontinued immediately on staff resignation or termination.

System Access Request

- System Access Request Forms are to contain signature blocks for each approver of each system. Approvers must be designated by the System Owner. Signatures must be affixed to the document prior to granting access or processing changes.
- System Access Request Forms must include acknowledgement of a previously-signed *Statement of Understanding* which should be available for review in the requestor's employee file.
- System Access Request Forms are to be periodically audited to ensure accounts that no longer require access are disabled or removed from the system or application.

TITLE:	ACCESS CONTROL POLICY		
POLICY #:	P-CCSP-008	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



Granularity of Access

Where practical, user access is to be granted to specific applications, menus, and data as identified on an approved System Access Request Form.

Verification of Need to Know

Granting or changing user access is to include written verification by the user’s supervisor of the users need-to-know.

Administrator Restrictions

Administrator privileges are to be limited to the minimum number of staff. Those granted such privileges are considered Positions of Trust.

User Authentication

When passwords are used to authenticate a user the following guidelines are to be used:

- Passwords may not be reused for at least six password change periods and changed passwords can not use the same phrase with simple changes like Password1 to Password2.
- All passwords are to be encrypted in transmission and in storage.

Two-factor authentication is preferred for all accounts on all systems, but especially for accounts on critical State systems or for Administrator accounts on any system.

User Identification

Group accounts are to be avoided where ever possible. In the event shared accounts are required for administrative use, utilities such as “sudo” or “Run As” are used in conjunction with the appropriate logging level to provide traceability.

Guest accounts are to be disabled.

References

- ISO 17799 Section 2
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12 Chapter 17
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46
- CCSP Personnel Security Policy, P-CCSP-010
- CCSP System and Applications Security Operations Policy, P-CCSP-007

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.